



**LEGAL PROBLEMS OF E-COMMERCE TRUSTMARK
IN THAILAND**

BY

MS. CHATANUT KHIEWCHAM

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE MASTER OF
LAWS PROGRAM IN BUSSINESS LAWS
(ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2015
COPYRIGHT OF THAMMASAT UNIVERSITY**



**LEGAL PROBLEMS OF E-COMMERCE TRUSTMARK
IN THAILAND**

BY

MS. CHATANUT KHIEWCHAM

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE MASTER OF
LAWS PROGRAM IN BUSSINESS LAWS
(ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2015**

COPYRIGHT OF THAMMASAT UNIVERSITY



THAMMASAT UNIVERSITY
FACULTY OF LAW

THESIS

BY

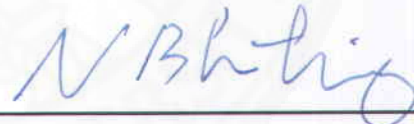
MS. CHATANUT KHIEWCHAM

ENTITLED

LEGAL PROBLEMS OF E-COMMERCE TRUSTMARK IN THAILAND

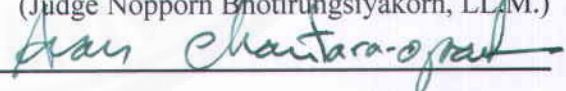
was approved as partial fulfillment of the requirements for
the degree of the Master of Laws Program in Business Laws
on August 10th, 2016

Chairman



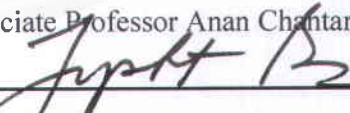
(Judge Nopporn Bhotirungsiyakorn, LL.M.)

Member and Advisor



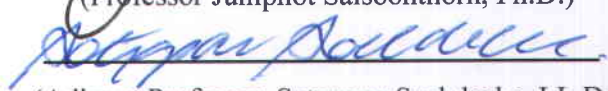
(Associate Professor Anan Chantara-opakorn, J.S.D.)

Member and Co-advisor



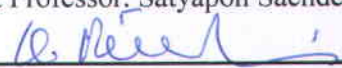
(Professor Jumphot Saisoonthorn, Ph.D.)

Member



(Adjunct Professor, Satyapon Sachdecha, LL.D.)

Dean



(Professor Dr. Udom Rathamarit)

Thesis Title	LEGAL PROBLEMS OF E-COMMERCE TRUSTMARK IN THAILAND
Author	Ms. Chatanut Khiewcham
Degree	The Master of Laws
Major Field/Faculty/University	Business Laws Program (English Program) Faculty of Law, Thammasat University
Thesis Advisor	Associate Professor Anan Chantara-opakorn, J.S.D.
Thesis Co-Advisor	Professor Jumphot Saisoonthorn, Ph.D.
Academic Years	2015

ABSTRACT

Thailand is one of many nations that offer E-commerce trustmark schemes to overcome the lack of trustworthiness in e-commerce transactions. However, the characteristics of Thai e-commerce trustmarks i.e. DBD (Department of Business Development) Registered and DBD (Department of Business Development) Verified, which are both administered by Department of Business Development (“DBD”) , Ministry of Commerce, do not follow the principles that those in developed countries follow. As there is no specific Thai law for this case, both trustmarks are registered as certification marks under the Trademark Act B.E. 2534 even though their characteristics and purposes are different from certification mark principles. Moreover, the trustmark issuance and monitoring will be considered, if e-consumers who rely on such trustmarks have suffered loss due to the negligent actions of DBD. It is unclear whether e-consumers can make any claim against DBD for damage when they rely on a trustmark issued by DBD.

The purpose of this thesis, is to study the principles of e-commerce trustmarks in Thailand, the United States and European Union with a view to setting out appropriate legal measures to revise issues associated with trustmark principles in Thailand. The method used in this thesis to achieve this will be documentary research in textbooks, journals, statutes, government publications, newspapers, experts’

opinions, public information public on the internet and other relevant documents that have originated from Thailand, the United States and the European Union.

The results will touch on five issues:

1. the characteristic of trustmarks - the DBD should change its position to be as a supervisory one of trustmark principles as is the case in the U.S. and E.U., the DBD should support and oversee non-profit organizations or companies in the private sectors that promote e-commerce trustmarks in Thailand.
2. trustmark certification process - if the DBD proposes its trustmark (DBD Registered) to be protected under the Trademark Act, the authorized use of DBD Registered should be in writing and signed by the authorized persons of the DBD, as for the pre-certification phase of DBD Verified, the standards of certification should be set up by a specialist association and follow the international practices i.e. those set out under Regulation (EU) No. 910/2014; in the part of post-certification phase, the certified applicant who has had his trustmark revoked, should not have the right to re-apply for certification again, although it was pass 5 years. A blacklist of untrusted e-merchants should be published.
3. The legal relationship and liability of trustmark service provider - the DBD, as a trust service provider should be liable to the e-consumers for damage caused intentionally or negligently, if they have failed to comply with their obligations.
4. The monitoring of trustmark receivers - a periodic evaluation should be established as a necessary step of monitoring, as specified by McAfree, and Norton. The DBD should request a reasonable fee or some funding to support improved monitoring.
5. Enforcement of laws specific to trustmarks - enforcement laws should be legislated according to the principle of the Regulation (EU) No 910/2014, especially regarding a qualified trust service provider's liability and burden of proof, trustmark issuance procedure, and monitoring process including setting up a supervisory body to control all trustmark aspects.

Keywords: E-commerce, Trustmark, Web seal

ACKNOWLEDGEMENTS

This thesis would not have been possible without the support of my family, advisors, thesis committee members, university officers and friends. To my family, thank you for being by my side in the hard times, and for believing and respecting my dreams. I am especially grateful to my parents, who supported me emotionally and financially. I always knew that you believed in me and wanted the best for me.

I would like to express my special appreciation and thanks to my advisors, Assoc. Prof. Dr. Anan Chantara-opakorn and Prof. Dr. Jumphot Saisoonthorn for their time and careful attention to detail and guidance throughout my thesis. I would also like to thank my thesis committee members, Judge Nopporn Bhotirungsiyakorn and Adjunct Professor Satyapon Sachdecha for their brilliant comments and suggestions. To university officers, thank you for your hospitality and suggestion. If I had not received your advice, I would not have completed my thesis.

Lastly, I would like to thank my friends for always cheering me up when I was feeling down and nervous. I hope we will graduate all together. Thank you, you all.

Ms. Chatanut Khiewcham

TABLE OF CONTENTS

	Page
ABSTRACT	(1)
ACKNOWLEDGEMENTS	(3)
LIST OF TABLES	(8)
LIST OF FIGURES	(9)
CHAPTER 1 INTRODUCTION	1
1.1 General Background	1
1.2 Hypothesis	2
1.3 Objectives of Study	3
1.4 Scope of Study	3
1.5 Methodology	4
1.6 Expected Result	4
CHAPTER 2 NATURE AND PROBLEMS OF E-COMMERCE TRUSTMARKS	5
2.1 Nature of E-commerce	5
2.1.1 Background	5
2.1.2 Definitions and Types	6
2.1.3 Benefits of E-commerce	7

2.2 Nature of Trustmark	8
2.2.1 Background	8
2.2.2 Definitions and Types of Trustmarks	11
2.2.3 Legal relationship	12
2.2.4 The Certification Process	13
2.2.4.1 Setting the Standard	13
(1) The role of standards	13
(2) Official and de facto standards	14
2.2.4.2 Evaluation	14
(1) Internal audit based on internal standards	15
(2) Internal audit based on third-party standards	15
(3) External audit	15
2.2.4.3 Issuance or denial of the trustmark	15
2.2.4.4 Monitoring	15
2.2.4.5 Confirmation, suspension, or revocation	16
2.2.5 Fee	16
2.2.6 The key elements of a trustworthy certification practice	16
2.2.6.1 Certifier independency	16
2.2.6.2 Impartiality in the auditing procedure	17
2.2.6.3 Active monitoring of the certified company	17
2.2.6.4 Certifier enforcement power	17
2.2.6.5 Certifier accountability	17
2.2.7 Benefits of Trustmark	18
2.2.8 Difference between certificate marks and trustmarks	18
2.3 Problems	21
2.3.1 The characteristics of trustmarks in Thailand	21
2.3.2 The legal relationship with and liability of trustmark service providers	21
2.3.3 The monitoring of trustmark receivers	21
2.3.4 Enforcement of laws specific to trustmarks	22

CHAPTER 3 E-COMMERCE TRUSTMARK UNDER INTERNATIONAL TRUSTMARK ALLIANCE AND FOREIGN LAWS	23
3.1 International Trustmark Alliance	23
3.1.1 Global Trustmark Alliance (GTA)	23
3.1.2 World Trustmark Alliance (WTA)	23
3.2 Foreign Laws	24
3.2.1 The United States	24
3.2.1.1 The characteristics of trustmarks in the United States	24
3.2.1.2 Trustmark certification process	29
3.2.1.3 Fee	31
3.2.1.4 The legal relationship with and liability of trustmark service Providers	34
(1) The legal relationship	34
(2) Liability of trustmark service provider	35
(3) Damage and fault in case of breach of trust	38
3.2.1.5 The monitoring of trustmark receivers	42
(1) Passive monitoring	42
(2) Active monitoring	42
3.2.1.6 Enforcement of laws specific to trustmarks	43
3.2.2 European Union	44
3.2.2.1 The characteristics of trustmarks in European Union	44
3.2.2.2 Trustmark certification process	48
3.2.2.3 Fee	48
3.2.2.4 The legal relationships and liability of trustmark service Providers	53
(1) The legal relationship	53
(2) Liability of trustmark service provider	53
(3) Damage and fault in case of breach of trust	56
3.2.2.5 The monitoring of trustmark receivers	57
(1) Passive monitoring	57
(2) Active monitoring	57

3.2.2.6 Enforcement of laws specific to trustmark	58
CHAPTER 4 E-COMMERCE TRUSTMARK UNDER THAI LAWS	61
4.1 The characteristics of trustmarks in Thailand	61
4.1.1 Certification mark principle under Trademark Act B.E. 2534	61
4.1.2 DBD's authorization under Trademark Act B.E. 2534	62
4.1.2.1 DBD Registered	65
4.1.2.2 DBD Verified	67
4.2 Trustmark certification process	67
4.3 Fee	69
4.4 The legal relationship with and liability of trustmark service Providers	71
4.4.1 The legal relationship	71
4.4.2 Liability of trustmark service provider	73
4.4.3 Damage and fault in case of breach of trust	74
4.5 The monitoring of trustmark receivers	74
4.5.1 Passive monitoring	74
4.5.2 Active monitoring	75
4.6 Enforcement of laws specific to trustmarks	76
4.7 Analysis of problems	76
4.7.1 The characteristics of trustmarks	76
4.7.2 The legal relationship with and liability of trustmark service Providers	77
4.7.3 The monitoring of trustmark receivers	77
4.7.4 Enforcement of laws specific to trustmark	78

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	79
5.1 Conclusions	79
5.2 Recommendations	80
5.2.1 The characteristics of trustmarks	81
5.2.2 Trustmark certification process	81
5.2.3 The legal relationship with and liability of trustmark service Providers	82
5.2.4 The monitoring of trustmark receivers	82
5.2.5 Enforcement of laws specific to trustmarks	83
REFERENCE	84
APPENDICES	91
APPENDIX A	92
APPENDIX B	101
APPENDIX C	147
APPENDIX D	148
APPENDIX E	155
APPENDIX F	161
APPENDIX G	167
BIOGRAPHY	168

LIST OF TABLES

Tables	Page
3.1 Annual fee of TRUSTe	32
3.2 Annual fee of BBBOnline	33
3.3 An overview of different procedural issues concerning the application for the Trustmark, fees and reviews.	51



LIST OF FIGURES

Figures	Page
2.1 Amazon net sales 2001-2012 (USD billions)	5
2.2 The expected B2C E-commerce Sales, by region 2001 and 2016	6
2.3 Information asymmetry	8
2.4 A Proposed Model for Consumers' Trust in Internet Shopping	9
2.5 Legal relationships	12
2.6 Certification process	13
3.1 DPB Platform	25
3.2 The best site seal in year 2013	29
3.3 Norton price packages	34
3.4 US Legal Relationship	35
3.5 Hierarchical Structure of the TrustUK Scheme	46
3.6 The Ranges of Member Fee	52
3.7 EU Legal Relationship	53
4.1 Steps for Issuance of the e-Commerce Trustmark (DBD Registered)	68
4.2 Steps for Issuance of the e-Commerce Trustmark (DBD Verified)	70
4.3 Thai Legal Relationship	72

CHAPTER 1

INTRODUCTION

1.1 General Background

The 2013 Thailand Internet User Profile survey conducted by the National Statistical Office, Ministry of Information and Communication Technology indicated an increase in internet use by Thai family members.¹ The survey found that Thai people, aged 6 years old and above, used the computer, internet and mobile phone over the last 5 years, from 2009-2013.² The internet users had increased from 29.3% (17.9 million people) to 35.0% (22.2 million people), the internet users had increased from 20.1% (12.3 million person) to 28.9% (18.3 million people), and mobile phone users had increased from 56.8% (34.8 million people) to 73.3% (46.4 million people).³ When looked at by age group, 58.4% of internet users in 2013 were between 15 and 24 years old. The survey showed that the information and communication technology had become as a tool for people to access information, communication and buy goods online instead of visiting shops.⁴

While increasing e-commerce businesses are increasing in worldwide, lack of trust is still the main obstacle of e-commerce. Security, privacy, unfamiliarity with services, lack of direct interaction, and credibility of information seem to be at the top of the list of consumers' concerns in making online transactions.

This is also true in Thailand. The value of B2B (Business-to-Business) E-commerce in Thailand is a double of B2C (Business-to-Consumer). The 2014 Household Survey on the Use of Information and Communication Technology showed that many people have never booked or purchased goods and services via the internet because they were afraid of being deceived (36.7%), they were unable to see the actual goods (36.2%), they were

¹ The National Statistical Office, "The 2013 Survey on the Internet Users' Profile in Thailand" (2013).

² *Id.*

³ *Id.*

⁴ *Id.*

concerned about security (3.7%).⁵ This indicates that lack of trust in e-commerce is the most important obstacle to e-commerce in Thailand. Trustmark schemes have been created to counter trustworthiness in e-commerce.

Thailand adopted a trustmark scheme since around 2011, when “DBD Registered” was created to register e-merchants. A survey for the years 2003 to 2015 showed that new applicants are increasing as a total of 12,573 e-merchants, are now able to use DBD Registered.⁶ “DBD Verified” was then created as a more reliable alternative to DBD Registered. DBD Verified is used by 130 e-merchants, according to the statistics from the period July, 2014 - July, 2015.⁷ Although no cases have come before the Supreme Court, it is clear that e-consumers’ complaints are in an increasing trend. The statistics for July 2015⁸ showed that, eight persons submitted complaints about the trustmark receivers (the e-merchants) to the Department of Business Development, the trustmark service provider. Four persons claimed that they had paid for goods but did not receive the ordered goods, three persons did get goods as their requested, one person received poor quality goods. This is reason enough to consider why the e-merchants who are granted trustmarks from the Department of Business Development, breach trust. It is important to recognize all the factors that could be the cause of this such as ineffective issuance procedure, criteria or monitoring.

1.2 Hypothesis

Thailand is one of many nations that has implemented as e-commerce trustmark scheme to solve a lack of trustworthiness in e-commerce transactions. However, the characteristics of Thai e-commerce trustmarks i.e. DBD (Department of Business Development) Registered and DBD (Department of Business Development) Verified,

⁵ The National Statistical Office, "*The 2014 Household Survey on the Use of Information and Communication Technology*" p.53, <http://service.nso.go.th/nso/nsopublish/service/survey/ICTFull57-1.pdf>.

⁶ Department of Business Development, "*Statistics DBD Registered and DBD Verified 2558*" p.1, <http://www.trustmarkthai.com/ecm/public/newsletter/view.html?id=981>.

⁷ *Id.*

⁸ *Id.*

which conducted by Department of Business Development (“DBD”), Ministry of Commerce, do not follow the principles adopted by the developed countries. Because there is no specific Thai law applied for trustmarks, both trustmarks are registered as certification marks under the Trademark Act B.E. 2534 even though they differ so much in nature and purpose. Moreover the trustmark issuance and monitoring will be considered; this is important if e-consumers who rely on such trustmarks have suffered loss due to the negligence actions by the DBD. It is unclear whether e-consumers can make any claim against DBD for damage when they rely on trustmark issued by DBD.

1.3 Objectives of Study

1. To study the principles of e-commerce trustmarks in Thailand;
2. To study the principles of e-commerce trustmarks in the United States and European Union;
3. To outline appropriate legal measures as a solution and guidance to revise Trustmark principles in Thailand.

1.4 Scope of Study

This thesis will study the legal problems of e-commerce trustmarks in Thailand starting by giving the background of the e-commerce trustmarks, the purpose of trustmark issuance, and the enforcement of existing laws by comparing with the United States and European Union laws on trustmarks. The thesis will analyze the problems thereof, and then propose the legislative solutions.

1.5 Methodology

The method used in this thesis is documentary research. Thai, the United States and European Union textbooks, journals, statutory laws, government publications, newspapers, expert opinions, public information public on the internet and other relevant documents will be considered.

1.6 Expected Result

1. To thoroughly understand the principles of e-commerce trustmarks in Thailand;
2. To thoroughly understand the principles of e-commerce trustmarks in the United States and European Union;
3. To provide appropriate legal measures as a solution and guidance to revise trustmark principles in Thailand.



CHAPTER 2

NATURE AND PROBLEMS OF E-COMMERCE TRUSTMARKS

2.1 Nature of E-commerce

2.1.1 Background

The growth of internet users and business websites has become the source of worldwide e-business via the internet and is the biggest tool for cross-border business. Consumers can carry out e-commerce transactions quickly and easily without limits to time and place. E-commerce is a good channel for doing business now and this will increase further as shown by Amazon net sales 2001-2012, and the expected B2C E-commerce sales worldwide by region 2001-2017 conducted by eMarketer given below.

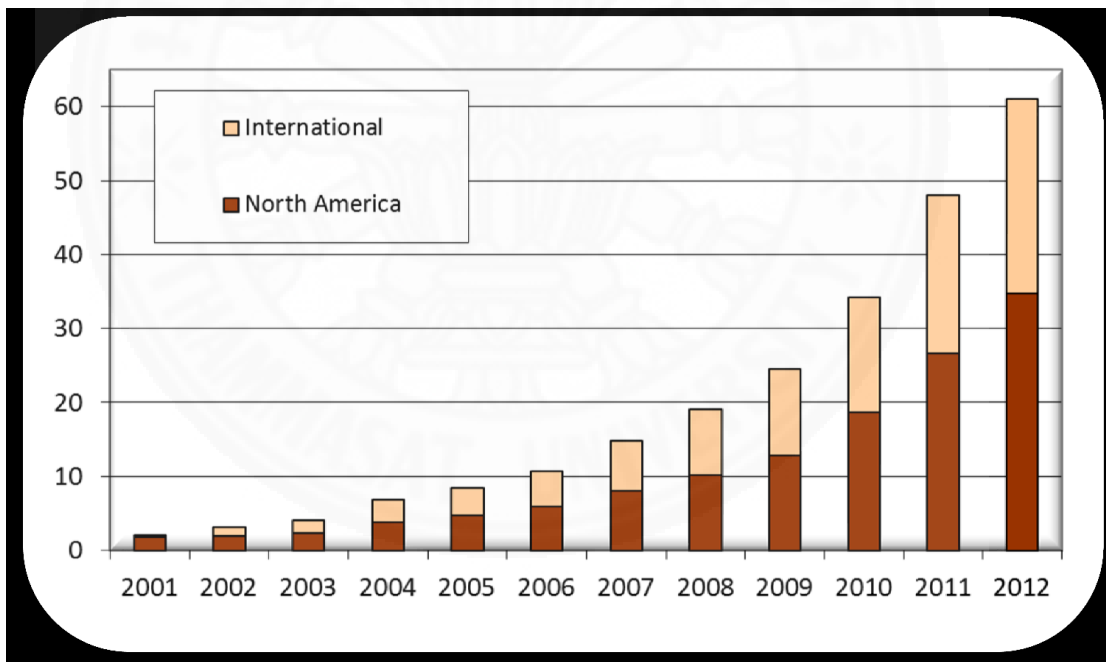


Figure 2.1 Amazon net sales 2001-2012 (USD billions)

From \$2.5 billion to \$ 61 billion - ~ 43% outside North America⁹

⁹ Torbjorn Fredriksson, "E-commerce and Development Key Trend and Issues" p.6, http://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/fredriksson_ecommerce_e.pdf.

B2C Ecommerce Sales Worldwide, by Region, 2012-2017
billions

	2012	2013	2014	2015	2016	2017
Asia-Pacific	\$301.2	\$383.9	\$525.2	\$681.2	\$855.7	\$1,052.9
North America	\$379.8	\$431.0	\$482.6	\$538.3	\$597.9	\$660.4
Western Europe	\$277.5	\$312.0	\$347.4	\$382.7	\$414.2	\$445.0
Central & Eastern Europe	\$41.5	\$49.5	\$58.0	\$64.4	\$68.9	\$73.1
Latin America	\$37.6	\$48.1	\$57.7	\$64.9	\$70.6	\$74.6
Middle East & Africa	\$20.6	\$27.0	\$33.8	\$39.6	\$45.5	\$51.4
Worldwide	\$1,058.2	\$1,251.4	\$1,504.6	\$1,771.0	\$2,052.7	\$2,357.4

Note: includes products and services ordered and leisure and unmanaged business travel sales booked using the internet via any device, regardless of the method of payment or fulfillment; numbers may not add up to total due to rounding
Source: eMarketer, Jan 2014

167707 www.eMarketer.com

Figure 2.2 The expected B2C E-commerce Sales, by region 2001 and 2016¹⁰

2.1.2 Definitions and Types

In April 2000, OECD member countries have agreed on two definitions of electronic commerce transactions as follows:

1. Broad definition

“An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over computer mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off-line.”¹¹

¹⁰ E-marketer, “Global B2C Ecommerce Sales to hit \$1.5 Trillion this year driven by growth in emerging markets”, <http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575>.

¹¹ The Organisation for Economic Co-operation and Development (OECD), “Measuring the Information Economy 2002”, <http://www.oecd.org/internet/ieconomy/2771174.pdf>.

2. Narrow definition

“An Internet transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over the Internet. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off-line.”¹²

Electronic commerce can therefore be said to mean a buying and selling of products and services via computer medium networks (broad definition), and the Internet (narrow definition) whether the payment and delivery is offline or online. Orders received or placed by fax, telephone or normal mail are excluded, i.e. online shopping websites and social networks¹³.

E-commerce can be divided into three categories as follows:

1. Business to Business (B2B), e.g. Cisco
2. Business to Consumer (B2C), e.g. Amazon
3. Consumer to Consumer (C2C), e.g. eBay.¹⁴

2.1.3 Benefits of E-commerce

For some e-merchants, e-commerce will bring benefits by increasing value and quantity of goods or services sold; more business; and a reduction in business capital due to e-marketing and a cross-broader selling, 24 hours and 7 days a week online selling; as well as allowing SMEs to do business in worldwide.

For e-consumers, they will have many opportunities to get product information and comparing goods or services before deciding to purchase in a fast and easy way from their home via the internet.

¹² *Id.*

¹³ Torbjorn Fredriksson, *supra* note 6, at 2.

¹⁴ Investorwords, “*E-commerce definition*”, http://www.investorwords.com/1637/e_commerce.html.

2.2 Nature of Trustmark

2.2.1 Background

Although online shopping is a global phenomenon, e-customers can feel a lack of confidence in online merchants because they do not know their identity, cannot ascertain whether they are fraudulent and cannot physically check the quality of products or services before they decide to make a purchase. Moreover, the safety and security of sending personal and financial information through the internet is unmonitored. We may say that the main reason for this issue is information asymmetry.

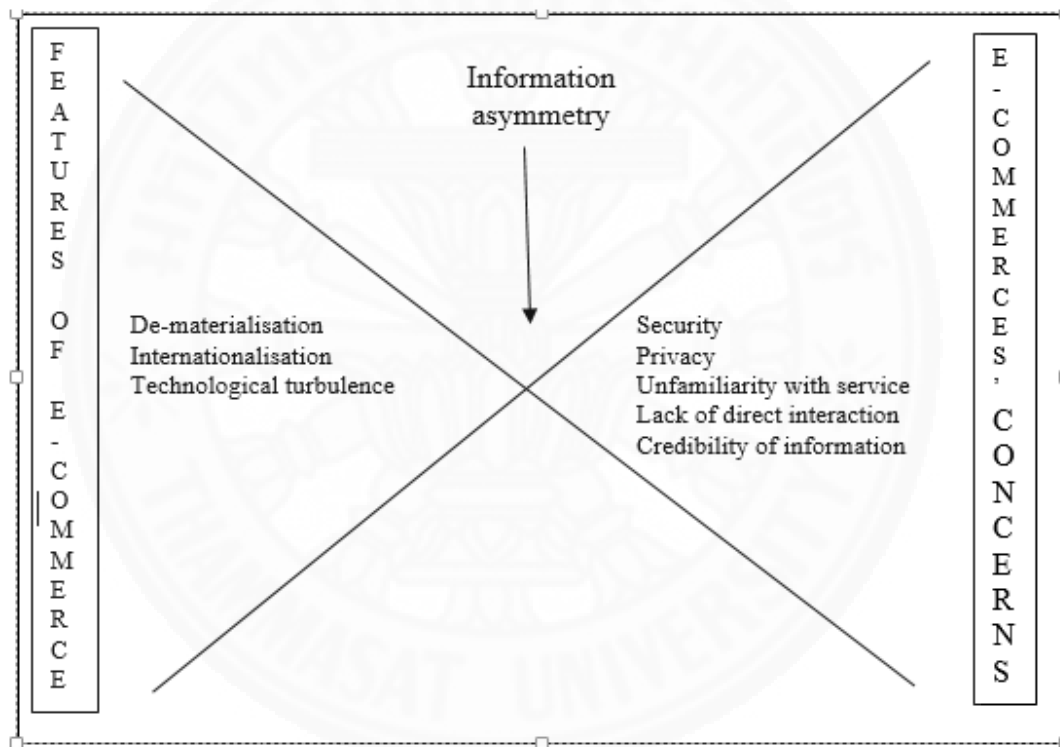


Figure 2.3. Information asymmetry¹⁵

Many researchers have studied the influence of perceived trustworthiness on building trust as show in the following figure.

¹⁵ Paolo Balboni, *Trustmarks in E-commerce: the Value of Web Seals and the Liability of their Providers*, 24 (2009).

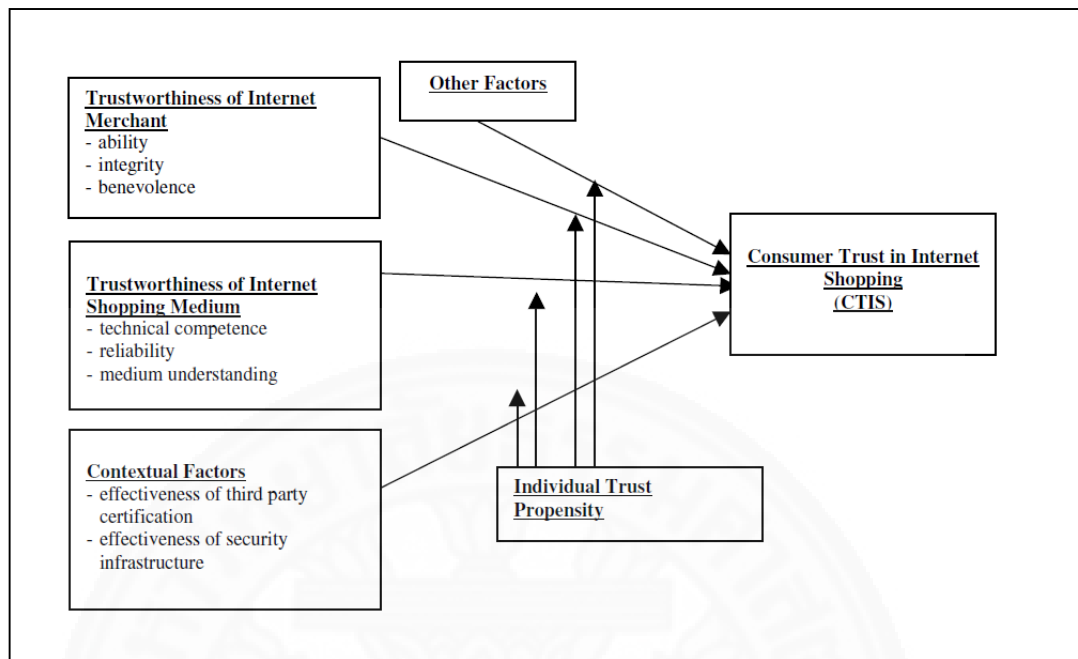


Figure 2.4. A Proposed Model for Consumers' Trust in Internet Shopping¹⁶

To counter this, different methods are used by web shop designers to increase trustworthiness of shops such as using a professional layout, showing user feedback, and using advertisements and third party certification-trustmarks. This research will outline e-consumers' concerns and the reasons why trust needs to be built.

Developing trust is an important factor under conditions of uncertainty and risk and this is certainly the case in e-commerce. Trustmarks are mostly designed by trustmark organizations to increase consumer trust in e-commerce and protect consumers from unfair behaviour during online shopping.¹⁷

¹⁶ Matthew K. O. Lee and Efraim Turban, "International Journal of Electronic Commerce" p.80, <http://www.jstor.org/discover/10.2307/27751003?uid=3739136&uid=2129&uid=2&uid=70&uid=4&sid=21104612913751>.

¹⁷ Elena Chernovich, "Trust in E-commerce : the moral agency of trustmarks," (Master Degree, Philosophy of science, technology and society, University of Twente, 2012), 6, in essay, http://essay.utwente.nl/63443/1/Chernovich,_Elena_-_S1042726_-_Master_Thesis.pdf.

Further, trustmarks are self-regulated. This is effective for the following reasons:

“(1) self-regulation is more easily accepted by the regulatory entities, which translates into better compliance with rules;

(2) as a result of the trustmark providers' superior knowledge of data transactions in the outsourcing business, self-regulation permits more diversity (and flexibility) with respect to the methods of compliance with legal rules; and

(3) self-regulation may be characterized as a "retreat from bureaucratic 'command and control' methods of regulation" which are more likely to constitute regulatory imperialism in the international context.”¹⁸

Self-regulation was implemented to express the feelings of perhaps the majority of Internet users, who were afraid that governments might take their internet freedom away.¹⁹ This was expressed powerfully by J.P. Barlow, the founder of the Electronic Frontier Foundation expressed the self-regulatory character of the Internet as below:

“You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. ... We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.”²⁰

A majority of authors accept the idea of self-regulation as it relates to the forming of mutual relationships in the form of agreements. It can be said that “self-regulation of the Internet by means of leaving everything for parties to set out in a contract is contrasted with a top-down approach of regulating Internet behavior by means of harmonized statutes”.²¹

¹⁸ Sunni Yuen, “*Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross –Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry.*”, **9 Colum. Sci. & Tech. L. Rev.** **41** (2007-2008).

¹⁹ Przemyslaw Paul Polanski, **Customary Law of the Internet: in the Search for a Supranational Cyberspace Law**, 85 (2007).

²⁰ Barlow, J.P. (8 February 1996), *A Declaration of the Independence of Cyberspace*.

²¹ Przemyslaw Paul Polanski, *supra note* 19 at 86.

2.2.2 Definitions and Types of Trustmarks

Trustmarks are seals or labels that represent a certification of the web shop when displayed. Online trustmarks thus aim to assure consumers that a particular online seller has been validated by a trustmark service provider and was found to be safe. Therefore a trustmark is a part of certification. The word “certification” derives from the Latin adjective *certus*, which means “determined, resolved, fixed, settled, purposed”.²² The most common perception of certification is that it gives some form of guarantee, generally of quality and dependability in their widest sense. The key element in the certification process is the third party, an independent party who is expected to give an assurance (a guarantee) of the qualities of some products or services through the issuance of a certificate.²³

Ton Wagemons defined trustmark as a symbol or a mark which is displayed for the purpose of informing website users that the e-merchant’s website has been examined and passed the quality test under the standard or regulation conducted by that organization.²⁴

The OECD defines trustmarks as: “Electronic labels or visual representations indicating that an e-merchant has demonstrated its conformity to standards regarding, e.g., security, privacy, and business practice”.²⁵

In summary, a trustmark is a symbol or mark used in the e-merchant’s website for the purpose of showing that such a website has met the standards of the trustmark service provider.

²² Lewis, C.T. (1996) *A Latin Dictionary* (New York: Oxford University Press), p. 320.

²³ Paolo Balboni, *supra* note 15, at 39.

²⁴ Ton Wagemons, *An Introduction to the labeling of websites*, (United States: 2003), p.3.

²⁵ Organization for Economic Co-operation and Development – Working Party on Indicators for the Information Society (2008), p. 26.

Trustmarks may be divided into a number of categories. Three different archetypical types of trustmarks can be distinguished as follows:

1. Commercially owned cross-border trustmarks,
2. Domestic trustmarks, and
3. Single – aspect such as reliability or security or privacy trustmarks.

2.2.3 Legal relationship

The legal relationship between Trustmark Organizations (TMOs) and their clients (e-merchants) is a contractual relationship whereby e-merchants shall be agreed to perform according to TMOs' standard similar to part of legal relationship between e-merchants and e-consumers. E-merchants have a responsibility to perform their obligations under purchase and sale contracts, and service contracts. However, there seems to be a tortious relationship between TMOs and e-consumers who rely on the certificates, although a contractual relationship cannot be excluded a priori.²⁶ This is illustrated in the figure below.

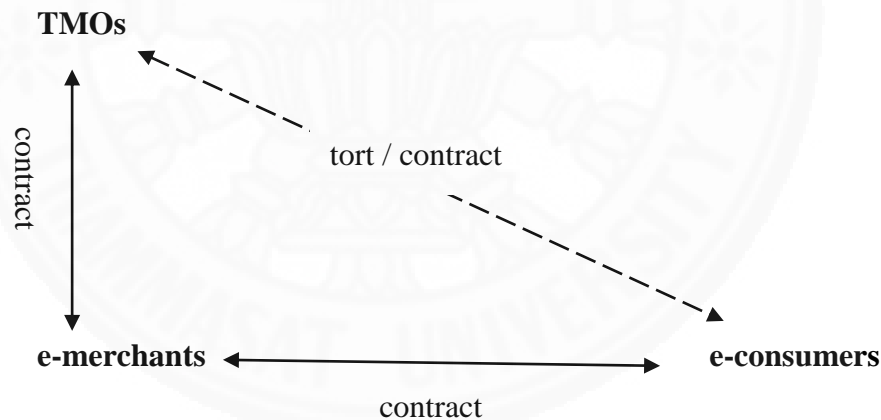


Figure 2.5. Legal relationships²⁷

The reason why e-consumers bring claims against TMOs is that it is easier to seek redress directly from the TMOs who issued the trustmark to the e-merchant than from the e-merchant itself.

²⁶ Paolo Balboni, *supra* note 15, at 4.

²⁷ *Id.*

“1. The TMOs should be easier to localize, its contact details should be clearly stated in the website;

2. It should have more money to satisfy the e-consumers/ request for compensation as TMOs should generally be better capitalized than the small e-merchants that they certify.”²⁸

2.2.4 The Certification Process

Certification is a process which is divided into five stages. The first and second stages are in the pre-certification phase and the third stage is the issuance of the certificate. The fourth and fifth stages are in the post-certification phase. See the summary in the figure below:

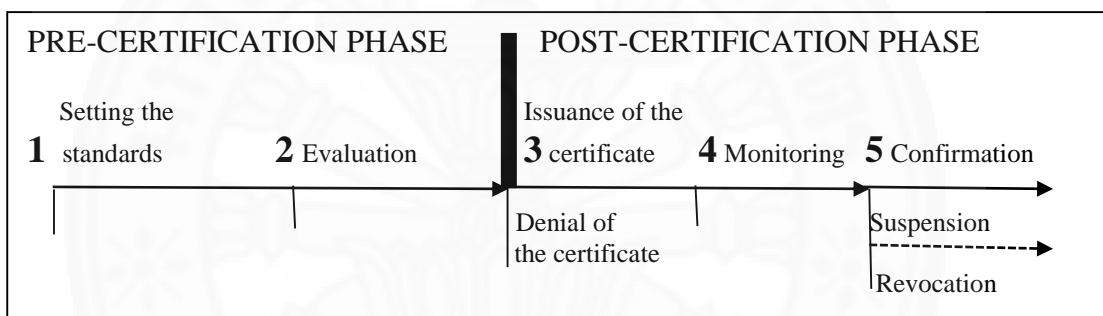


Figure 2.6 Certification process²⁹

2.2.4.1 Setting the Standard

(1) The role of standards

There are many different products and services. Standards are a good way to compare them. Drafting standards is the first important step to start the certification process in TMOs practice as this enables products and services to be evaluated and compared worldwide under the same rules. Many national and international organisations set uniform standards in different sectors and some business organizations mutually agreed to develop their own standards that will be used in worldwide.³⁰

²⁸ *Id.*

²⁹ *Id.* See p. 40.

³⁰ *Id.* See p. 41.

(2) Official and de facto standards

Standards will be divided in a different criteria. This research will specify a distinction between official and de facto standards. It may say that official standard is as formal standards which are open and public. The International Organisation for Standardisation (ISO) defines an official standard as follows:

“[A] document established by consensus and approved by a recognized body, which provides, for common and repeated use, rule, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.”³¹

A de facto standard is a standard that has become a standard due to it being used widely more than is stated by some official organisations or governments and it can differ substantially in origin, nature, and status.³²

An official standard is more reliable than a de facto standard because they are mostly created by standardisation institutes and organization. However, a de facto standard is more flexible and can be easily updated in order to comply with the market needs. Regardless of the type of standards, they are a substantial part of the trademark certification process, and TMOs should set the reasonable and appropriate standards to verify such things.

2.2.4.2 Evaluation

The second stage is the evaluation of products, services, practices or policies to be verified. There are many methods for evaluation; the most common method is the audit. Although the word of audit normally refers to “an official examination of the business and financial records of a company in order to see that they are true and correct”,³³ an audit will be understood more generally here to mean a “systematic quality verification procedure”.³⁴

³¹ See (<http://www.iso.org/iso/home/standards.htm>).

³² The Linux Information Project, “*De Facto Standard Definition*”,p.1, http://www.lininfo.org/de_facto_standard.html.

³³ Paolo Balboni, *supra note* 15, at 43.

³⁴ *Id.*

(1) Internal audit based on internal standards

This is self-evaluation according to the standards of the company; the company will set its own standards or use standards set by third parties. The result of the internal audit under internal standards is the same as a guarantee issued by its company that complies with the internal standards. Otherwise, this method is very limited and may not be reliable due to there being no double-check process by a third party.

(2) Internal audit based on third-party standards

This type of evaluation is conducted within the company in the same way as the first type of evaluation, the main difference is the internal standards are set and conducted by a third party which could be an international organisation or a specialist. The process normally involves a questionnaire; an authorized representative of the company has to fill out a questionnaire prepared by a third party, sign it, and affirm that all answers are true and correct. Then, the certifier will evaluate and make conclusions based on all the results; the certifier will decide whether or not to issue a trustmark.

(3) External audit

An external audit can give strong and reliable warranties because it is conducted by a third party under external standards.

2.2.4.3 Issuance or denial of the trustmark

The pre-certification phase will be completed when the result of the evaluation is concluded and the certifier issues or denies the trustmark. The post-certification procedure then begins.

2.2.4.4 Monitoring

After the certificate has been issued, the monitoring stage begins. There are two types of monitoring. First, there is passive monitoring which begins when the certifier receives a complaint; the certified company will be examined under the certifier's program. In the case of active monitoring, the certifier and the certified company will

agree to a periodical check, such as every 30 to 90 days. The frequency and the level of investigations depend upon the sector of the trustmark.

2.2.4.5 Confirmation, suspension, or revocation

After the monitoring stage, if the certified company still meets the standards of the certifier, the certificate will be confirmed. If the certified company no longer complies with the standards of the certifier, the trustmark will be revoked. In some cases, if the certifier encounters non-compliance they will set a timeframe for the certified company to bring its products, services, practices or policies in line with the standards. If the certified company can meet the standards by the suspension time, the trustmark will not be revoked.

2.2.5 Fee

Every trustmark service providers always requires a fee from e-merchants for administering the trustmark scheme. It is also important in terms of independence. TMOs will be considered independent if their funding structure and the composition of their board of directors are neutral.³⁵ If the fee is required as low as possible, TMOs will necessarily get sponsorship, which have negative effects on their independence.³⁶ Thus, a reasonable fee is most appropriate.

2.2.6 The key elements of a trustworthy certification practice

We may analysis the five necessary conditions in the trustmark process for a trustworthy trustmark practice as follows:

2.2.6.1 Certifier independency

The certifier should be an unbiased, independent entity that has no conflicts of interest with the trustmark candidate.³⁷ The following questions should be answered: “What are

³⁵ Paolo Balboni, *supra* note 15, at 53.

³⁶ Paolo Balboni, *supra* note 15, at 54.

³⁷ See Havighurst, C.C. (1994), p. 2; Astrue, M.J. (1994), p. 75.

the trustmark fees paid for?” and “Does the certifier receive financial funding from potential clients?”³⁸

2.2.6.2 Impartiality in the auditing procedure

In the pre-trustmark phase, the company must be internally audited according to the official standards by an independent party.³⁹

2.2.6.3 Active monitoring of the certified company

The trustmark will become out of date after the trustmark is issued or after the certified company has been audited. Therefore, active monitoring is necessary. For the purpose of issuing a trustmark, it is necessary to verify the quality of the certified object. Thus, there should be active evaluation within specified periods.

2.2.6.4 Certifier enforcement power

Certifier enforcement power is also a very essential aspect of the system. The certifier shall have the power to take appropriate measures in case the certified company does not comply with the certifier’s standards by revocation or suspension. If the certifier does not have such power, then this will affect the consumers as they will lose confidence in the whole certification system.⁴⁰

2.2.6.5 Certifier accountability

It is generally understood that the trustmark is a “sort of guarantee”⁴¹ of the information provided through the trustmark. The certifier will be responsible to the third party who believes that certified objects meet the certifier’s standard. Therefore, the certifier shall have a responsibility when they certify to avoid giving e-consumers misleading information.⁴²

³⁸ Paolo Balboni, *supra* note 15, at 46.

³⁹ See *supra* Subsection 2.2.3 External audit.

⁴⁰ Paolo Balboni, *supra* note 15, at 48.

⁴¹ See Rae, A. et al. (1995), p. 6; Dean, H. & Biswas, A. (2001), pp. 41-57.

⁴² Paolo Balboni, *supra* note 15, at 48.

2.2.7 Benefits of Trustmark

There are five major concerns in e-commerce. These are: “security, privacy, unfamiliarity with services, lack of direct interaction, and credibility of information”.⁴³ A trustmark is built to solve all these concerns. In fact, it is not only e-consumers who benefit from trustmarks but also e-merchants and governments. For e-consumers, they will receive a sort of guarantee of quality of the e-merchants’ business practice, their privacy statement, or the security level of their website from an independent third party. They will have reliable information to decide and compare what they are buying online. Overall, they will have a better buying experience.⁴⁴

For e-merchants, a trustmark can help them become successful more rapidly, especially SMEs. By providing e-consumers with easy access to information, e-merchants can increase their chances of success. The self-regulation of the sector and setting their own standards prevents governments from interfering.⁴⁵

Moreover, trustmarks are helpful for governments as it relieves them of the burden of regulating industries themselves. Furthermore, e-commerce is boosted by trustmarks and governments will receive the taxes related to revenues generated by it.⁴⁶

2.2.8 Difference between certificate marks and trustmarks

A certificate mark is a term which indicates that a product or service has been certified by a third party to comply with a set of requirements.⁴⁷ The US Patent and Trademark Office defines certificate marks as:

“[A]ny word, name, symbol, or device, or any combination thereof (1) used by a person other than its owner, or (2) which its owner has a bona fide intention

⁴³ The European Consumer Centres’ Network, “*Trust marks report 2013 “Can I trust the trust mark?”*”, p.7, http://ec.europa.eu/dgs/health_consumer/information_sources/docs/trust_mark_report_2013_en.pdf.

⁴⁴ Paolo Balboni, *supra* note 15, at 28.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ Gilad L. Rosner, “*Trustmarks in the Identity Ecosystem*”, p. 3, <http://oixuk.org/wp-content/uploads/2014/09/Trustmarks-paper-FINAL-v2.pdf>.

to permit a person other than the owner to use in commerce and files an application to register on the principal register established by this chapter, to certify regional or other origin, material, mode of manufacture, quality, accuracy, or other characteristics of such person's goods or services or that the work or labor on the goods or services was performed by members of a union or other organization.”⁴⁸

The UK Intellectual Property Office (IPO) states that:

“The main feature of a certification mark is that it is used not by the proprietor of the mark but instead by his authorized users for the purpose of guaranteeing to the relevant public that goods or services possess a particular characteristic.”⁴⁹

The UK Trade Marks Act 1994 defined a certificate mark as “similar to the US definition, except that it does not provide for certification of labour on goods or services performed by a member of a union or other organization”⁵⁰

In summary, a certificate mark is, by its very nature, unlike any types of other marks. It does not indicate the origin or source of the goods or services and it is not used by the registered owner.⁵¹ However, it is declared on the goods or services to certify something to other that has been reviewed, tested, and found to meet the standard in accordance with the required quality, safety, price, or some other characteristic such as the GOOD HOUSEKEEPING Seal which certified other service that meet the qualified standard.⁵²

In relation to trustmarks, much of the literature has focused on their use in e-commerce, sometimes there are called “web seals”. As defined in the EU online trustmarks:

⁴⁸ See 15 U.S.C. § 1127.

⁴⁹ Gilad L. Rosner, *supra* note 47, at 3.

⁵⁰ Jeremy Phillips and Llanah Simon, *Trade Mark Use*, p. 150 (2005).

⁵¹ Daborah E. Bouchoux, *Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets*, p. 19 (2000).

⁵² *Id.*

“Trustmarks aim to assure consumers that a particular site or online seller has been validated by a trustmark provider and is found to run a safe sales process. They are designed to increase consumers’ trust in the webshop that carries the trustmark”⁵³

On the other hand, a trustmark is a label or visual representations indicating that a product, process, or service conforms to specific quality characteristics to e-merchants.

The US NSTIC (National Strategy for Trusted Identities in Cyberspace) captures this breadth succinctly:

“A trustmark is used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority.”⁵⁴

Accordingly, a trustmark has some different characteristics from a certification mark because it has different purposes. A certificate mark is used by one person to certify the goods or services of others but a trustmark is used by one organization to certify the websites of others. Moreover, the principles of a certificate mark is created as regulated rules by government sector for protection the mark owner’s right over a certificate mark but a trust mark is created under the purpose of self-regulation which applied between private sector (act as a trustmark service provider) - private sector (act as a merchant), they are allowed to revise or change a mark which is more proper to their business than a certificate mark principle. Due to a certificate mark can be enforced against other only in the territory that the owner has registered such mark but a trust mark can be used in worldwide, the trustworthiness depend on a reliable of a trustmark service provider.

Trustmarks are also distinct from brands because brands relate to origins and trustmarks relate to processes.⁵⁵ For example, the IBM logo indicates the source of a product whereas a mark from the British tScheme Organization indicates that a service has

⁵³ Gilad L. Rosner, *supra* note 47, at 3.

⁵⁴ Gilad L. Rosner, *supra* note 47, at 4.

⁵⁵ Gilad L. Rosner, *supra* note 47, at 6.

undergone a certification process.⁵⁶ Moreover, brand are used to communicate characteristics but for something to be called a trustmark it must be a process or mechanism that allows someone to trust it.⁵⁷ Whereas the Rolex watch brand is used to communicate quality, trustworthiness and an aspirational sense of value and class, the Better Business Bureau OnLine seal is meant to communicate reliability and trustworthiness.⁵⁸

2.3 Problems

2.3.1 The characteristics of trustmarks in Thailand

Department of Business Development, Ministry of Commerce has set up two types of e-commerce trustmarks in Thailand: 1. DBD Registered, and 2. DBD Verified. Both are issued by the government sector. However, as mentioned earlier most international principles are self-regulated and conducted by non-profit organizations.

2.3.2 The legal relationship with and liability of trustmark service providers

It is not clear whether the DBD as part of the government should be liable to e-consumers who rely on such trustmarks or not. This section will also consider the legal relationship between the DBD and e-merchants.

2.3.3 The monitoring of trustmark receivers

Only passive monitoring applies in both the provisions of regulation to use DBD Registered and DBD Verified, no active monitoring is stated. Moreover, the evaluation processes are set only in the issuance of DBD Verified.

⁵⁶ *Id.*

⁵⁷ Gilad L. Rosner, *supra* note 47, at 6-7.

⁵⁸ *Id.*

2.3.4 Enforcement of laws specific to trustmarks

There is no specific enforcement law applied to DBD Registered and DBD Verified. Instead, the DBD uses powers under the Trademark Act B.E. 2534 to register both DBD marks as certificate marks. Therefore, they are not trustmarks and cannot function as trustmarks. Although the DBD has tried to adopt them as trustmarks, they bear no relation to them and indicate a misunderstanding of the nature of certificate marks.



CHAPTER 3

E-COMMERCE TRUSTMARK UNDER INTERNATIONAL TRUSTMARK ALLIANCE AND FOREIGN LAWS

3.1 International Trustmark Alliance

3.1.1 Global Trustmark Alliance (GTA)

The Global Trustmark Alliance (GTA) is a membership organization created to encourage cross-border e-commerce by increasing consumer trustworthiness, encouraging good online business practices, and discouraging the development of burdensome, disparate governmental regulation.

GTA members are local trustmark organizations worldwide and other organizations supporting the development of online trustmarks. Participating businesses agree to abide by an international code of conduct for cross-border transactions, to participate in out-of-court dispute resolution procedures based on code standards, and to display an international seal on their website signaling their participation in the GTA.⁵⁹

3.1.2 World Trustmark Alliance (WTA)

The World Trustmark Alliance (WTA) developed from the Asia-Pacific Trustmark Alliance (ATA) in 2010. WTA members are worldwide organizations with 37 business operators from 30 countries, i.e. APEC (Asia-Pacific Economic Cooperation), Europe, US, etc. The main objective of the organization is to promote trust in the e-commerce environment. Therefore, in the mutual interest of both trust organizations they agree to work together to achieve similar objectives and can deal with the border issue.⁶⁰

Since countries have different standards, these operations help to make cross-border transactions successful. Discussions and arrangements in organizations such as the WTA with many company participants will be increasingly important. Therefore, the WTA has developed guidelines for trustmark operators – good online business behavior

⁵⁹ IT Law Wiki, “*Global Trustmark Alliance*”, p.1, http://itlaw.wikia.com/wiki/Global_Trustmark_Alliance.

⁶⁰ World Trustmark Alliance, “*About us*”, p.1, <http://www.wtaportal.org/aboutus.html>.

for merchants called “Code of Conduct” – to increase recognition, privacy information protection, dispute resolution, etc. These are divided into six main chapters: disclosure of information, practices, security, privacy, ADR (alternative dispute resolution) and monitoring.⁶¹

3.2 Foreign Laws

3.2.1 The United States

3.2.1.1 The characteristics of trustmarks in the United States

Trustmark schemes in the US are administered by non-profit organisations such as trustmark service providers. Furthermore, trustmarks are distributed by private companies, especially security scanning service operators. The aim of this is to increase trust in e-commerce by issuing trustmarks to verify e-commerce websites according to their specific criteria and standards.

The important trustmarks in the U.S. are:

1. TRUSTe

TRUSTe is a non-profit organisation that represents cooperation between Electronic Frontier Foundation (EFF) and Commerce Net Consortium since 1996.⁶² The aim of this organization is the protection of data privacy by enabling businesses to safely collect and use data across their customer, employee and vendor channels.⁶³

Sample of TRUSTe⁶⁴:



⁶¹ World Trustmark Alliance, “Code of Conduct”, p.1, <http://www.wtaportal.org/code.html>.

⁶² TRUSTe, “TRUSTe history – 18 years of privacy innovation”, <https://www.truste.com/about-truste/company-history/>.

⁶³ *Id.*

⁶⁴ *Id.*

TRUSTe has created the Data Privacy Management Platform (DPB Platform) to control all phases of data privacy management, including conducting assessments, implementing compliance controls and managing ongoing monitoring.⁶⁵ Platform Certifications are included for apps, cloud, data collection and websites. TRUSTe's Program Requirements incorporate principles from privacy frameworks established by APEC, the OECD and the FTC, and also indicate from consumers, clients, advocates and regulators.⁶⁶



Figure 3.1 DPB Platform⁶⁷

2. BBBOnline

The Council of Better Business Bureaus (CBBB) is a non-profit organization and represents network cooperation in the US and Canada. CBBB has a mutually-supportive relationship with approximately 200 national partners that are leaders in their industries and 112 independent organizations across North America. CBBB is one of the national organizations that develops and administers self-regulation programs for the business community.

BBBOnline has serviced three seal programs as, 1. Reliability Seal Program, 2. Privacy Seal Program and 3. Kid's Privacy Seal.⁶⁸

⁶⁵ TRUSTe, "*TRUSTe Data Privacy Management Solution*", p.2, <http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=9GEA1GX6-488>.

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Council of Better Business Bureaus, "*Programs and Services*", p.1 <http://www.bbb.org/council/the-national-partner-program/programs-and-services/?id=234761>.

Sample of BBBOnline:



3. WebTrust

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) agreed to develop trust service principles and criteria on 5 issues as follows:

“a. Security. The system is protected against unauthorized access (both physical and logical).

b. Availability. The system is available for operation and use as committed or agreed.

c. Processing integrity. System processing is complete, accurate, timely, and authorized.

d. Confidentiality. Information designated as confidential is protected as committed or agreed.

e. Privacy. Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA”⁶⁹

Sample of WebTrust⁷⁰:



⁶⁹ Webtrust, “Trust Services Principles, Criteria, and Illustrations”, p.5, <http://www.webtrust.org/principles-and-criteria/item27818.pdf>.

⁷⁰ *Id.*

4. McAfee Secure

McAfee Secure for Websites is a security scanning service that is backed up by a McAfee trustmark which is operated by a private organization.⁷¹ The program provides daily vulnerability assessments for protection from hackers and third-party certification of their security.⁷² Initially, it is a free service; e-merchants can display the McAfee Secure trustmark once they have signed up on the McAfee website.⁷³ If e-merchants need more options, i.e. search highlighting and directory listing, then they may upgrade to a Certification Pro version and a fee is applied.⁷⁴

Sample of McAfee Secure⁷⁵:



5. Norton Secure

Norton Secure is provided by Symantec SSL, formerly VeriSign.⁷⁶ Symantec Corporation is a private company which develops and distributes various products and services that guarantee protection and foster trust between e-merchants and e-consumers.⁷⁷ The core features of SSL Certificates are:

⁷¹ Vangie Beal, “An E-Comm Buyers’ Guide to Choosing Trustmarks”, <http://www.ecommerce-guide.com/article.php/3860526/An-EComm-Buyers-Guide-to-Choosing-Trustmarks.htm>.

⁷² *Id.*

⁷³ McAfee Secure, “We help websites sell more”, <https://www.mcafeesecure.com/>.

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ Symantec, “Compare SSL Certificates”, <https://www.symantec.com/ssl-certificates/>.

⁷⁷ *Id.*

- “1. Daily Malware Scan Discover any active threats so you can take remediation actions and secure your website
2. Management Tools Tools to help you manage, find and install your SSL certificates easily
3. DSA Certificates DSA Certificates meet compliance requirements with certain government agencies
4. Unified Communications (SAN) Support Allows for multiple domain names to be protected with a single certificate. Unified Communications/ SAN certificates are required in applications like Microsoft Exchange.
5. Nearly 100% End-User Compatibility Symantec SSL Certificates are nearly 100% compatible with browsers and systems
Server specific instructions include a set of articles with operating system-specific installation instructions.
6. Installation Help Downloadable tools are run on your server and guide you through a short wizard to install your certificate on Windows and Linux.
7. Support Free support via Web and email 24x7. Extended Support plans available for additional assistance.
8. Expiration Protection Reminder emails and calls from account manager protect against certificate expirations. You also have a 30 day grace period to renew your certificate.”⁷⁸

Sample of Norton Secure⁷⁹:



⁷⁸ *Id.*

⁷⁹ *Id.*

With all these trustmark seals in existence, a question raised by the public was: which of these site seals are actually the most trusted by users?

A survey on site seals was conducted with a large sample size (2,510 responses) in 2013.. This compared up-to-date versions of 8 of the most popular site seals.⁸⁰ The results showed that Norton was the most trusted seal by customers.⁸¹

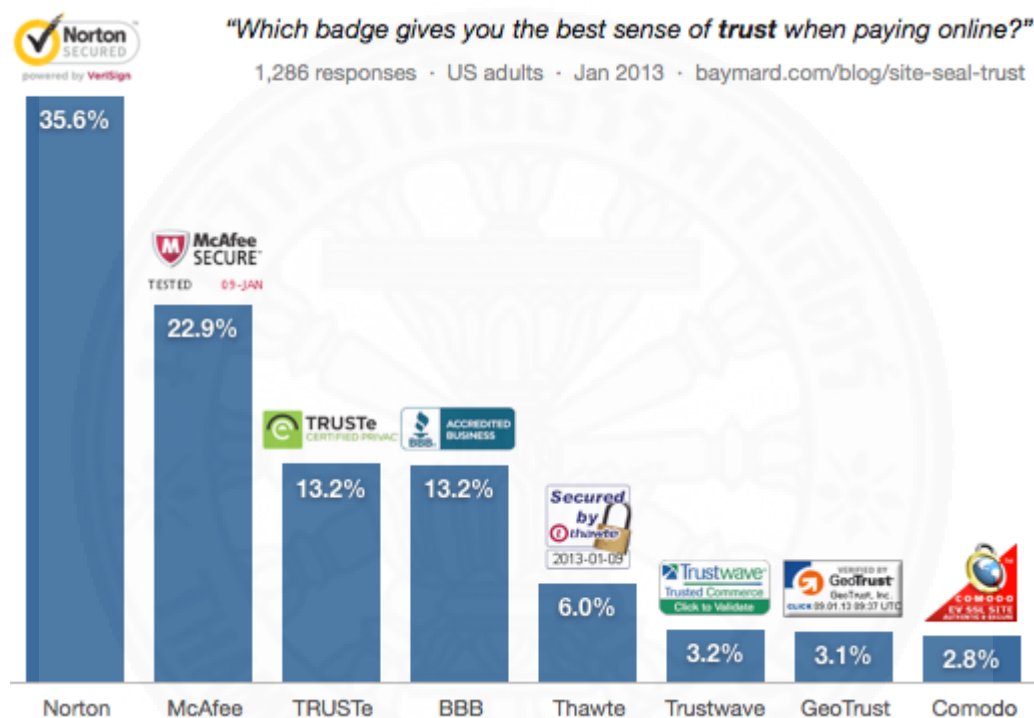


Figure 3.2 The best site seal in year 2013⁸²

3.2.1.2 Trustmark certification process

A discussion has already been provided on the trustmark certification process. This section therefore gives examples of the process.⁸³

⁸⁰ Christian Holst, “Which site seal do People Trust the most?(2013 Surveys Results)”,

<http://baymard.com/blog/site-seal-trust>.

⁸¹ *Id.*

⁸² *Id.*

⁸³ See Chapter 2.2.4.

In the case of TRUSTe, the e-merchants who intend to join TRUSTe's privacy seal program are required to do the following:

- “1) Create a privacy statement – If a website already has a privacy statement consistent with the information contained in TRUSTe's self-assessment document, it may be submitted with the application packet. If no privacy statement exists, TRUSTe provides an online Privacy Resource Guide for assistance. The Privacy Resource Guide provides the framework for creating a privacy statement, which should be tailored to reflect the specific privacy practices of the requesting company's website.
- 2) Complete the required paperwork – The requesting company should first read the license agreement. In signing the license agreement, the requesting company agrees to follow the established privacy principles outlined by TRUSTe and comply with their oversight and resolution process. An important element of the license agreement is the self-assessment form. The self-assessment form asks for a detailed account of the requesting company's internal privacy and security practices;
- 3) The application is processed - The application processing department contacts a requesting company within 10 –15 business days after receipt of the application. Once TRUSTe has verified that all of the required information has been provided, an account executive manager contacts the requesting company within 45-60 days. The account executive manager will conduct the certification and review process via a phone conference.”⁸⁴

In the case of BBBOnline, the following steps are required to join BBBOnline's privacy seal program:

- “1) the requesting company must first complete the Business Application and pay the Application and Annual Assessment Evaluation fees. The fees must be submitted with the company directing it to complete the Compliance Assessment Questionnaire;

⁸⁴ SANS Institute Reading Room site, “*Comparison of Three Online Privacy Seal Programs*”, <https://www.sans.org/reading-room/whitepapers/privacy/comparison-online-privacy-seal-programs-685>.

- 2) Complete the Compliance Assessment Questionnaire– The questionnaire is the basis for determining a company’s eligibility for the privacy seal program. The questionnaire will be assigned to a Compliance Analyst for review. Once BBBOnLine has reviewed a company’s website and has notified the company of any outstanding issues, the company is required to respond within 60 days. After 60 days without a response, all applications are considered inactive and companies will need to submit a new application and questionnaire, including additional application and evaluation fees;
- 3) Sign and submit the Participant (License) Agreement and return it to BBBOnLine.”⁸⁵

As for WebTrust, the following steps are required to join WebTrust’s privacy seal program:

- “1) Contact a specially trained, licensed WebTrust provider. A company can find a WebTrust provider by asking its CPA, Chartered Accountant, or equivalent whether he or she offers WebTrust or by contacting the American Institute of Certified Public Accountants or similar institute in the appropriate country and requesting a list of WebTrust providers.
- 2) Meet the WebTrust’s Principles for Privacy as measured by the WebTrust Criteria.
- 3) Obtain an unqualified report from the WebTrust provider.”⁸⁶

3.2.1.3 Fee

Examples of fees charged by providers are given in this part with a view to clarifying this issue.

TRUSTe: The DIY service for small business packages starts at \$500 per year and increases according to traffic to the website.⁸⁷ The cost of a certificate in order to display the TRUSTe privacy seal is dependent on a company's annual revenue.⁸⁸ In the

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ Vangie Beal, *Supra* note 69.

⁸⁸ SANS Institute Reading Room site, *supra* note 82.

case of subsidiaries, the measure to use is the overall annual revenue of the parent company. The following table displays the annual fee by amount of company revenue.⁸⁹

Company's Annual Revenue	Annual Fee
\$0 - \$1 million	\$299
\$1 - \$5 million	\$399
\$5 - \$10 million	\$599
\$10 - \$25 million	\$1,999
\$25 - \$50 million	\$2,999
\$50 - \$75 million	\$3,999
\$75 million and over	\$6,999

Table 3.1 Annual fee of TRUSTe⁹⁰

BBBOnline: The pricing starts at around \$400+ per year for their “Accredited Business” seal.⁹¹ Otherwise, the cost to activate and maintain membership varies, depending on e-merchants’ location and size of business.⁹² All BBBOnline privacy seal program applicants pay a one-time \$75.00 application fee in addition to the annual assessment evaluation fee.⁹³ The application fee is non-refundable. If a preliminary review of the company’s application does not meet the threshold standards, an assessment evaluation will not be conducted and the assessment evaluation fee will be refunded. However, if the company’s application meets the threshold standards, an assessment evaluation will be conducted and the assessment evaluation fee is non-refundable.⁹⁴ The annual fee by amount of company revenue is shown in the following table.

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ Top Alternatives, “Top 3 trust seals/certificates to display on your website”, <https://topalternatives.com/display-trust-seals-certificates-on-your-website/>.

⁹² Vangie Beal, *Supra* note 69.

⁹³ SANS Institute Reading Room site, *supra* note 82.

⁹⁴ *Id.*

Company's Annual Revenue	Annual Assessment Evaluation Fee
\$1 million or less	\$200.00
\$1,000,001-\$5,000,000	\$325.00
\$5,000,001-\$10,000,000	\$525.00
\$10,000,001-\$50,000,000	\$1,000.00
\$50,000,001-\$100,000,000	\$2,000.00
\$100,000,001-\$500,000,000	\$3,000.00
\$500,000,001-\$2,000,000,000	\$4,000.00
Over \$2 billion	\$6,000.00

Table 3.2 Annual fee of BBBOnline⁹⁵

WebTrust: Estimated costs must be obtained from a specially trained and licensed WebTrust provider. WebTrust providers are typically CPAs, Chartered Accountants or an equivalent. There are two main costs. One cost is the fee of the WebTrust provider who examines a company's electronic commerce. This fee relates to the work required to assure a company and its customers that all applicable WebTrust standards are met. The other cost is an annual fee for the digital certificate that authenticates the WebTrust seal and proves that the e-merchant has received the WebTrust mark. These costs are not published and are specific to the company for which the services are provided.⁹⁶

McAfee offers 2 versions of services to e-merchants as follows:

1. free registration version, e-merchants can use McAfee's service for free by signing up their websites according to the process;⁹⁷ and
2. Certification Pro version, a yearly subscription price is based on Web site's page views. Smaller sites may pay \$1,500 in the low range. Larger businesses with more daily page views pay more.⁹⁸

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ Vangie Beal, *Supra note 69*.

⁹⁸ *Id.*

Norton Secure offers 5 types of Symantec SSL Certificates; each package provides difference options.⁹⁹ The pricing starts from \$399 for 1 year as illustrated below:






				Most Secure	
Symantec SSL Certificates	Secure Site	Secure Site with EV	Secure Site Pro	Secure Site Pro with EV	Secure Site Wildcard
Buy SSL	BUY SSL	BUY SSL	BUY SSL	BUY SSL	BUY SSL
Renew Now	RENEW	RENEW	RENEW	RENEW	RENEW
Price: 1 year	\$399	\$995	\$995	\$1,499	\$1999
Trust Mark					
ECC: Strongest Security			✓	✓	
Warranty	\$1,500,000	\$1,750,000	\$1,750,000	\$1,750,000	\$1,500,000
Green Address Bar		✓		✓	
Critical Vulnerability Scan		✓	✓	✓	

Figure 3.3 Norton price packages¹⁰⁰

3.2.1.4 The legal relationship with and liability of trustmark service Providers

(1) The legal relationship

Most trustmark service providers are private organizations and non-profit organizations. When e-merchants agree to display a trustmark seal, e-merchants shall agree terms of service provided by TMOs. After that, the rights and obligations of both parties will be applied according to a contract, much the same way as this occurs between e-merchants and e-consumers. However, the relationship between TMOs and e-consumers is not clear. It may be said that the legal relationship of all parties is according to standard liability as described in Chapter 2, 2.2.3 Legal Relationship.

⁹⁹ Symantec, *Supra note 74*.

¹⁰⁰ *Id.*

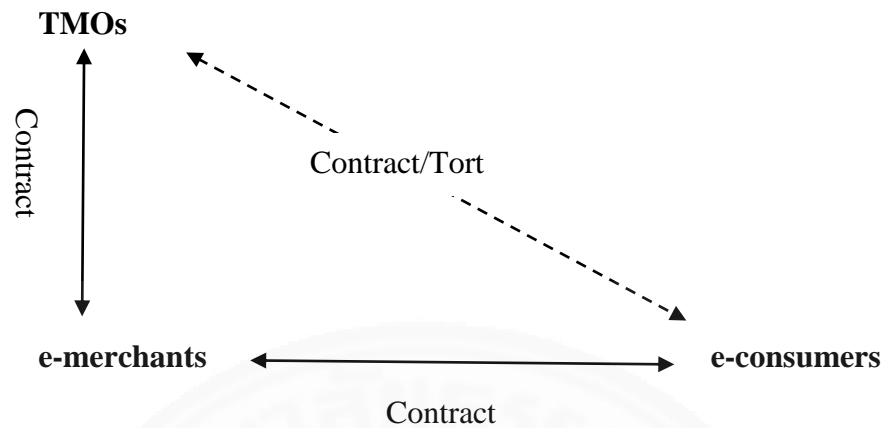


Figure 3.4 US Legal Relationship¹⁰¹

(2) Liability of trustmark service provider

There are no specific requirements set out in the event of a negligent act by a trustmark service provider. Hence, it is necessary to apply offline principles in case of torts and contract laws to determine the liability of trustmark service providers. In theory, “a misrepresentation action requires third-party reliance on the defendant’s misrepresentation”¹⁰² according to section 552(1) of the Restatement Second of Torts. In practice, there are insignificant differences between a misrepresentation action and a negligent action; the courts usually require the plaintiff to meet the specific requirements of the misrepresentation action.¹⁰³ However, only general requirements are demanded in case of a negligent action.

To determine liability of a third-party for negligence, we may use the following three legal standards:

¹⁰¹ Paolo Balboni, *supra* note 15.

¹⁰² Paolo Balboni, *supra* note 15, at 68.

¹⁰³ *Id.*

1. The near privity rule

The New York Court of Appeals decided in *Credit Alliance v. Arthur Andersen and Co.* by using the relevant test to check whether the requirement of near privity has been fulfilled for accountant third-party liability.¹⁰⁴ It determined that the following conditions had to be met:

- (1) “The accountant must have known that the financial reports were to be used for a particular purpose,
- (2) A know party or parties was intended to rely; and
- (3) Some accountants conduct linking them to that party.”¹⁰⁵

The interesting point is about the linking concept, i.e. there is a need for an action carried out by the accountant which links him to the relying party.¹⁰⁶

2. The foreseeability test

In the mid-1980s, a number of courts changed the decided approach from near privity to auditor third-party liability cases.¹⁰⁷ The decision of the New Jersey Supreme Court maintained that auditor duty extends to all:

- (1) “ Whose reliance on the audited statements is reasonably foreseeable by the auditor,
- (2) That have been influenced in their decision by the information provided in auditor statements.”¹⁰⁸

This can be summarized as “the auditor owes a duty of care to all who obtain a firm’s financial statement directly from the audited entity, but owes no such duty of care to those who obtain it from an annual report in a library or from a government file.”¹⁰⁹

¹⁰⁴ Paolo Balboni, *supra* note 15, at 70.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ Paolo Balboni, *supra* note 15, at 71.

¹⁰⁸ Paolo Balboni, *supra* note 15, at 71.

¹⁰⁹ *Id.*

3. The group and transaction test set forth in Section 552 of the Restatement (Second) of Torts

Moreover, near privity and foreseeability, Section 552 of the Restatement (Second) of Torts is almost used by the courts in accountants' third-party liability cases.¹¹⁰ This approach was applied in the case of *Rush Factors, Inc. v. Levin* for the first time in the 1968 by the Federal District Court in Rhode Island and it has been followed by almost all the courts in the US.¹¹¹

Feinman explained the important conditions according to Section 552 in his paper. He said there were roughly seven conditions which need to be fulfilled in order to prove an action of accountant negligent misrepresentation:

- “(1) the information is false;
- (2) the accountant supplies the information in the course of his business or in a transaction in which he has a pecuniary interest;
- (3) the accountant fails to exercise reasonable care in obtaining or communicating the information;
- (4) the third party justifiably relies on the information, and the reliance causes harm;
- (5) the third party is the person or is within the group for whom the defendant intends to supply the information or knows that the recipient of the information intends to supply it;
- (6) the third party relies on the information in a transaction that the defendant intends to influence, or in a substantially similar transaction; and
- (7) the third party suffers pecuniary loss.”

¹¹⁰ 284 F. Supp. 85 (D. R.I. 1968). The court expanded accountant liability for negligence from the near privity standard to specifically foreseen or known users. Applying Section 552 of the Restatement (Second) of Torts the Court maintained that an accountant should be liable in negligent misrepresentation for financial misinformation relied upon by actual foreseen and limited classes of persons.

¹¹¹ Paolo Balboni, *supra* note 15, at 72.

The accountant scheme is a similar method to the trustmark scheme; we may compare them in the case of third-party liability as both are about examiners who have a duty to examine a client's object according to their standard.¹¹² If the information is inaccurate, such information is provided by the accountant in the negligent performance of their profession, and the third-party relying on the information suffers pecuniary loss,¹¹³ then the accountant shall be liable to the third-party.¹¹⁴

After a number of years, the contractarian approach began to be used according to the public policy. This tends to exclude tort law from the scope of accountant third-party liability on the basis of three arguments.¹¹⁵ First, contractarians decide that the accountants' report is not to be considered as a guarantee. Second, third parties are actually free to choose whether or not to rely on the information provided by accountants; third parties shall assume the risk accordingly. Third, courts limit the parties' autonomies under tortious liability to contractually regulate their relationships, eventually exposing accountants to the risk of indeterminate liability.¹¹⁶

(3) Damage and fault in case of breach of trust

No reported cases have specifically addressed trustmark service provider third-party liability. However, we may analyze some case law on the third-party liability of professionals for the online provision of inaccurate business or financial information that may be applied to TMOs' third-party liability.¹¹⁷

The main doctrine on TMOs¹¹⁸ was adopted from *Jaillet v. Cashman*.¹¹⁹ TMOs grant protection from negligent third party actions; this may be called "safe harbour" for

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ *Id.*

¹¹⁵ Paolo Balboni, *supra* note 15, at 75.

¹¹⁶ Paolo Balboni, *supra* note 15, at 76.

¹¹⁷ Paolo Balboni, *supra* note 15, at 78.

¹¹⁸ See Pacini, C. & Sinason, D. (1999), p. 484.

¹¹⁹ 189 N.Y.S. 743 (Sup. Ct. 1921), *aff'd*, 194 N.Y.S. 947 (App. Div. 1922), *aff'd*, 130 N.E. 714 (N.Y. 1923)

TMOs.¹²⁰ The court held that a ticker service company was not liable for inaccurate information reported on a ticker tape which caused the plaintiff, who saw the ticker report in his broker's office, to suffer an economic loss when he sold certain stocks. Due to this, the court held that a provider of financial information was in the same relationship with the public as a newspaper, and there could be no liability for negligence absent a contractual or other special relationship unless it resulted from the provider's warranty or a specific "seal of approval".¹²¹

A New York court followed this concept in *Daniel v. Dow Jones & Co.*. The facts were that Mr. Eldridge brought an action against Dow Jones alleging that he made investment decisions based on false news reports that he received from the Dow Jones News/Retrieval service which caused him to lose a substantial sum of money.¹²² The plaintiff argued that Dow Jones was liable because the parties had a contract that created a "special relationship", thus justifying the imposition of liability for negligent misstatements.¹²³ However, the court found that there was no special relationship between the plaintiff and the defendant, and the defendant could not face unlimited third-party liability because the information that was published electronically was available through computer-to-computer.¹²⁴

The prevalent doctrine maintains that the Jalliet rule can be applied to TMOs which will thus be shielded from third-party actions in negligence.¹²⁵ TMOs usually specify the disclaimer clauses in their terms of service as the information they provide is not to be relied upon and their trustmark can be used only at the e-merchants' own risk.¹²⁶

Thus, TMOs may not be liable for a breach of contract when performing their services because no express warranty or express language exists that will make negligent misstatement a breach of contract. It may be said that TMOs have a good chance of

¹²⁰ Paolo Balboni, *supra* note 15, at 78.

¹²¹ Paolo Balboni, *supra* note 15, at 79.

¹²² Paolo Balboni, *supra* note 15, at 80.

¹²³ *Id.*

¹²⁴ See Pacini, C. & Sinason, D. (1999), p. 493-494.

¹²⁵ Paolo Balboni, *supra* note 15, at 84.

¹²⁶ *Id.*

enjoying “the Jaillet safe harbour” that protects them from e-consumers’ claims in negligence.¹²⁷

On the other hand, there are potential ways to impose negligent liability on TMOs. The following court decisions could be applied to an assurance provider, i.e. a TMO. The court decided in *Hanberry v. Hearst Corp.* that the issuance of the “Good Housekeeping” seal meant that the defendant “has taken reasonable steps to make an independent examination of the product endorsed”¹²⁸ and so the defendant shall be liable to a third party. This was similar to the decision in *LaSalle National Bank v. Duff & Phelps Credit Rating Co.*, where the court applied the near privity test and where it decided that the defendant shall be liable when the plaintiff can prove that the following 3 elements are met:

- “(a) the credit rating was provided to a selected and identified group of investors;
- (b) the purposes of the investors were known;
- (c) the linking requirement was fulfilled by the communications between the defendant and the plaintiffs.”¹²⁹

Moreover, we may consider the liability of the trustmark service provider as the elements of the Section 552 of the Restatement (Second) of Torts:

- “(1) the recipient of information has to prove that he suffered relevant pecuniary loss;
- (2) information is false and trustmark service provider fail to exercise reasonable care;
- (3) e-consumer belongs to the group for whom the trustmark service provider intend to supply.”¹³⁰

¹²⁷ Paolo Balboni, *supra* note 15, at 85.

¹²⁸ *Id.*

¹²⁹ Paolo Balboni, *supra* note 15, at 86.

¹³⁰ Paolo Balboni, *supra* note 15, at 193.

After analysis, it is clear that the chances that trustmark service providers will not be liable are bigger than the chances that trustmark service providers will be liable.

For a greater understanding of the current situation, it is useful to consider examples of the complaints process of web seals.

TRUSTe's privacy seal program provides online third-party dispute resolution for complaints reported by consumers regarding a licensed TRUSTe website. This service is called the WatchDog Dispute Resolution process.¹³¹ It is free of charge to any consumer who files a privacy-related complaint online. The TRUSTe's Feedback and Resolution process allows TRUSTe to initiate a negotiation between the e-consumer and the participating company. Whether this process do not cause a legal relationship between them. The outcome is not binding on the e-consumer but the company must comply with TRUSTe's final determination or face removal from the TRUSTe program, breach of contract legal proceedings, and/or referral to the appropriate governing body under the terms and conditions of use of TRUSTe.¹³²

Another example is BBBOnLine which uses its Privacy Policy Review Service (PPRS) to process e-consumer complaints. The PPRS is responsible in the dispute resolution process for determining the eligibility of a complaint and evaluating, investigating, analyzing and making a decision on the merits of an eligible complaint. The PPRS will make a final determination as to whether a complaint is eligible and, if so, continue with its dispute resolution process. Under the PPRS process, before filing a privacy complaint form, the complainant is required to review the eligibility criteria to verify that the complaint is a privacy matter relating specifically to the website. Next, the complainant should contact the website owner directly to make an effort in good faith to resolve the complaint through direct contact. Then, if the website owner does not satisfactorily resolve the complaint, the PPRS can be notified for help.¹³³

¹³¹ See <https://feedback-form.truste.com/watchdog/request>.

¹³² SANS Institute Reading Room site, *supra* note 82, at. 6.

¹³³ *Id.*

The final example is WebTrust. The WebTrust privacy program encourages the use of the twelve principles that form the basis of the arbitration process developed by the National Arbitration Forum (NAF).¹³⁴ NAF is an organization that is based in the US and has developed an arbitration process that is widely used. It is the model adopted by WebTrust regardless of whether NAF or another organization is selected for the arbitration process. Complainants can file a claim with the NAF by internet, telephone or regular mail. It costs \$49 for claims less than \$1,000 and between \$49 - \$150 for claims greater than \$1,000; the losing party pays the costs. Most disputes are typically resolved within 45 to 60 days.¹³⁵

3.2.1.5 The monitoring of trustmark receivers

(1) Passive monitoring

Trustmark service providers may start the passive monitoring when they receive a complaint from an e-consumer. Otherwise, active monitoring gives more of a reason to believe in websites so trustmark service providers have set their rule in both an active and a passive evaluation to monitor trustmark receivers. Taking WebTrust as an example, the entire system security is periodically reviewed and compared with the defined system security policies. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system security reviews as part of its annual audit plan.

(2) Active monitoring

Active monitoring refers to periodic checks. An example is a security seal from McAfee which scans its e-merchants' site for malware daily.¹³⁶ In the key locations, such as a shopping cart screen, The McAfee seal indicates that the website's screen has been scanned for malware that day.¹³⁷

¹³⁴ See http://www.cpawebtrust.org/privacy_fin.htm.

¹³⁵ SANS Institute Reading Room site, *supra* note 82.

¹³⁶ Gilad L. Rosner, *supra* note 47, at 11.

¹³⁷ *Id.*



E-consumers will feel more secure whilst shopping because of this. The e-merchants' online sales will also increase.

In the event of controlling of Certification mark under Lanham Act 14(5), if any certification mark is claimed that the owner of the mark has not controlled the use of mark.¹³⁸ It means that consumers cannot rely on the mark as an indicator of the “regional or other origin, material, mode of manufacture, quality, accuracy, or other characteristic of the goods or services” displaying the mark.¹³⁹ Such certification mark shall be cancelled because of a lack of control under Lanham Act 14(5). The purpose of the certification mark controlling is required for preventing consumers from being misled.¹⁴⁰ Due to a certification mark directly sets forth specific representations about the manufacturer and the qualities of the goods to which the mark is applied, the risk to the public is particularly great.¹⁴¹ Thus it imposes an affirmative obligation on the mark holder to monitor the activities of those using the mark as specified in *Midwest Plastic Fabricators Inc. v. Underwriters Laboratories Inc.*¹⁴².

3.2.1.6 Enforcement of laws specific to trustmarks

There are no specific laws that apply to trustmark schemes in the US, different laws will apply to each case depending on the issues. Other than this, trustmark service providers are under the control of the Federal Trade Commission (FTC). For example, in the case of TRUSTe, it was charged by the FTC as it deceived consumers through its privacy seal program. The details of the case were that TRUSTe failed to conduct annual recertifications of over 1,000 incidences for companies which held TRUSTe privacy seals which were to be renewed every year. Moreover, TRUSTe become a for

¹³⁸ Craig Allen Nard, David W. Barnes and Michael J. Madison, *The Law of Intellectual Property*, 86-87, 2006.

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² See 906 F.2d 1568 (Fed. Cir. 1990)

profit organisation in 2008 but it still claimed its non-profit status after that time. Therefore, the FTC made an order that “TRUSTe will be prohibited from making misrepresentations about its certification process or timeline, as well as being barred from misrepresenting its corporate status or whether an entity participates in its program”. It was also ordered to pay \$200,000 as part of the settlement under the COPPA rule for safe harbor programs.¹⁴³

3.2.2 European Union

3.2.2.1 The characteristics of trustmarks in European Union

Trustmarks for e-commerce can broadly be defined as “any third-party mark, logo, picture or symbol that is presented in an effort to dispel consumers’ concerns about internet security and privacy and, therefore, to increase firm-specific trust levels.”¹⁴⁴ In the same way, representatives of European businesses and consumers have jointly defined a trustmark as “[a] label or visual representation showing participation in a trust mark scheme. A subscriber to a trust mark scheme can display a trustmark if he meets the trust mark requirements”.¹⁴⁵

EU member countries have a difference trustmark structure from the US. These are characterized by a hierarchical structure on 3 levels.

Level 1: Certifier is responsible for creating its generic code and using it as a guideline for “Code owner” and code of conduct which is created by a Code owner shall be approved by the Certifier.

Level 2: When trustmark service providers apply for membership of a Certifier organisation, they will be a Code owner who shall specify their own code of conduct.

¹⁴³ Federal Trade Commission, “**TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program**”, p.1, <http://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.

¹⁴⁴ Study A Pan-European Trust mark for E-Commerce Possibilities and Opportunities IP/A/IMCO/ST/2012-04. p.18.

¹⁴⁵ Ibid.

The code of conduct shall be approved by the Certifier before any trustmark is issued to any trustmark receiver or webshop.

Level 3: There are the e-commerce entrepreneurs or webshop owners who received the trustmark from the Code owner and have the right to display the trustmark logo on their website.¹⁴⁶

The EU has now specified a qualified trust service provider in Article 21 of Regulation (EU) No 910/2014 as follows:

Step 1: Trust service providers shall submit a notification of their intention and a conformity assessment report issued by a conformity assessment body to the supervisory body.

Step 2: The supervisory body will verify them according to the requirements for qualified trust service provider under Article 24, and for the qualified trust services they provide.

Step 3: If the supervisory body concludes that trust service providers comply with all specified requirements, the supervisory body will grant qualified status to them and inform the body which is responsible for establishing, maintaining and publishing national trust lists. This process shall be concluded within three months of notification. If it is delayed, the supervisory body shall inform the reason and the expect period of conclusion to the trust service provider.

Qualified trust service providers may start to issue the qualified trust service after its status has been indicated in the trust lists.

There are a number of organizations in the first level of the hierarchy in the EU.

¹⁴⁶ Natapong Kongkaew, “*Legal Problems of Liability for Trustmark Usage for Trustmark provider DBD Verified of Department of Business Development Ministry of Commerce*” (Master Degree, Law of International Business and Electronic Transaction, Bangkok University, 2009), 63, http://dspace.bu.ac.th/bitstream/123456789/903/1/natapong_kong.pdf.

1. TrustUK

TrustUK is a non-profit organisation which has been supported by the UK government since 1999. The aim of this organisation is to increase consumer protection cooperation between business entities and consumer protection associations. TrustUK is at level 1 of the hierarchical structure. Although TrustUK has its own code, the code of conduct in the bottom and top levels may be of a different characteristic as the structure of the network is dynamic.

The following figure shows TrustUK as the first level of the hierarchy. At the second level there are specific codes of the Association of British Travel Agents Ltd (ABTA), the Direct Marketing Association (DMA), the British Consumers Association and the Trusted Shops.

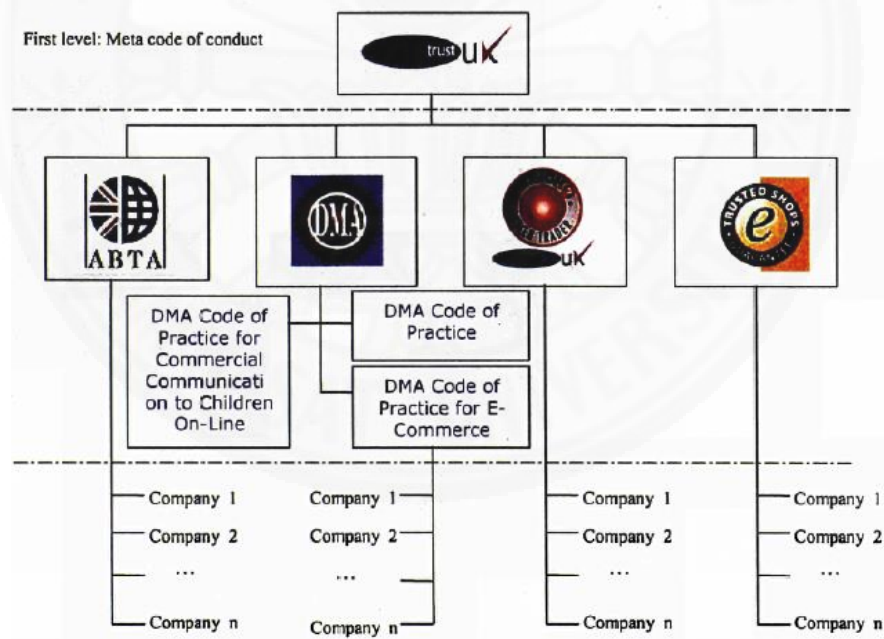


Figure 3.5 Hierarchical Structure of the TrustUK Scheme¹⁴⁷

¹⁴⁷ Guido Nannariello, "E-commerce and consumer protection a survey of codes of practice and certification processes", <http://bookshop.europa.eu/en/e-commerce-and-consumer-protection-pbLBNA19932/>.

2. Webtrader

This Webtrader scheme is a non-profit organisation under the sponsorship of the European Commission and is promoted by several European consumer associations. It has been developed in order to encourage “... the development of a safe and secure online shopping environment for consumers”.¹⁴⁸ The Webtrader code has been adopted by the consumer associations in ten countries.¹⁴⁹

Sample of Webtrader:¹⁵⁰



3. eQM-2001

This certification scheme was developed by the Institute for the Development of the Electronic Commerce (ISEC) which is one of the Italian associations that promotes the development of e-commerce. This code of practice “... defines requirement of the service supplied by the e-commerce website to guarantee an adequate qualitative level of their performances”.¹⁵¹ The ISEC’s code eQM-2001 stands for the trustmark “E-Commerce Quality Mark 2001”. It had already certified approximately 15 webshops by March 2001.¹⁵²

Sample of eQM-2001¹⁵³



¹⁴⁸ See <http://whichwebtrader.which.net/webtrader/wwt.html>.

¹⁴⁹ Ibid.

¹⁵⁰ Ibid.

¹⁵¹ See <http://www.isec.it/specifica.htm>.

¹⁵² Guido Nannariello, *supra* note 140, at 12.

¹⁵³ Ibid.

Currently, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market is applied in case of trust service as following details.

3.2.2.2 Trustmark certification process

The Regulation¹⁵⁴ does not state the trustmark certification process, mostly trustmark service provider use the certification process in 2 phases as pre-certification phase and post-certification phase as detailed in Chapter 2, clause 2.2.4. The result of the trustmarks report 2013 indicated that: “Mostly, 87% of the e-shops’ application will be submitted to an auditing process that checks whether the applicant complies with the certification requirement (also called code of conduct, code of ethics, criteria). If the applicant fails in one or more aspects, he’s offered the opportunity to rectify these within a certain deadline. Once he fully complies, the trust mark is rewarded.”¹⁵⁵

The most common criteria for trust mark certification are:

- “1. Payment of a membership fee
2. Fulfilment of the legal requirements with regards to the applicable laws
3. Compliance of the website with the technical requirements
4. Development of a complaint ordering process
5. Adoption of the terms and conditions set by the organization
6. Complaint management.”¹⁵⁶

3.2.2.3 Fee

Almost all trustmark service providers charge their members fees. This is most commonly based on a one-time administrative fee and/or certification fee as well as an annual fee.¹⁵⁷ The annual fees range from 30 Euros to 4500 Euros, with the possibility

¹⁵⁴ See Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

¹⁵⁵ The European Consumer Centres’ Network, *Supra* 43, at. 29.

¹⁵⁶ *Ibid.*

¹⁵⁷ The European Consumer Centres’ Network, *Supra* 43, at. 11.

of rising based on the number of employees and/or annual turnover.¹⁵⁸ The following is an example of the calculation from a Danish trust mark.

- “1. 0-4 employees: start fee 2.250 DKK, annual subscription 5.100 DKK.
2. 5-24 employees: start fee 3.550 DKK, annual subscription 6.700 DKK.
3. 25-99 employees: start fee 5.050 DKK, annual subscription 9.300 DKK.
4. 100-249 employees: start fee 6.650 DKK, annual subscription 12.500 DKK.
5. More than 250 employees: start fee 8.250 DKK, annual subscription 16.200 DKK.”¹⁵⁹

Below is a table that provides an overview of different procedural issues concerning the application for the trustmark, its fees and reviews.

	Application procedure	Application or audit fee	Annual fees	Recurrent review	Sanctions for noncompliance
SOAP, Czech Republic	e-mail, mail or phone	€70–285	€35	annual	certificate withdrawn
The E-Mark, Denmark	website	€280-1,000	€450-1,750	annual and random checks	certificate withdrawn
Trusted Shops, Germany	website	€89 (set up fee)	€59-99 (monthly)	annual and random checks	contractual penalty and withdrawal of certificate
Safer Shopping, Germany	website	annual fee only	€3,000-30,000	annual checks	-
EHI Euro-Label, Germany	website	€750-1,500	€500-1,000 (after first certification)	annual checks	certificate withdrawn
eQ recommendation, Hungary	sending signed declaration	none	none	sporadic checks	certificate withdrawn
W-mark, Ireland	website	€3,000-5,000	€800	every 6 month	certificate withdrawn
Segala, Ireland	website or through	varies	varies	annual renewal	certificate withdrawn

¹⁵⁸ *Id.*

¹⁵⁹ *Id.* at 49.

	Application procedure	Application or audit fee	Annual fees	Recurrent review	Sanctions for noncompliance
	certified agent				
Luxembourg e-Commerce Certified	website	annual fee only	approximately €1,000 (audit)	annually	certificate withdrawn
Euro-Label Malta	website	€47.50	€24	annually	certificate withdrawn
Thuiswinkel Waarborg, The Netherlands	mail	-	€150-29,000 (audit) plus €450 (trustmark fee)	annually (external accountants)	certificate withdrawn
EBtrust, Norway	website etc.	€3,000-12,000	-	annually, recertification process after 3 years	certificate withdrawn
E-Commerce IIiM Certyfikat, Poland	website	€100-560	€80-450	annually	special check (additional payment) and certificate withdrawn
PACE, Portugal	website	€1,000-3,000	30% of initial fee every 2nd year. Membership of PACE required (€ 500 annually, €150 application fee)	every 2 year	certificate withdrawn
Confianza Online, Spain	application form	Initial fee. Free to members of certain organisations	€550-5,500. Discounts to members of certain organisations	-	-

	Application procedure	Application or audit fee	Annual fees	Recurrent review	Sanctions for noncompliance
<u>WebTraderUK</u>	application form per mail	only annual fee	€375 + VAT	annual and random checks	certificate withdrawn
Web Trader, several countries	website	none (funded by European Commission)	none (funded by European Commission)	none	certificate withdrawn

Table 3.3 An overview of different procedural issues concerning the application for the Trustmark, its fees and reviews.¹⁶⁰

The European Consumer Centres' Network gathered information about membership fee collection from EU member countries. The results showed that 87% of trustmarks in the EU charge a membership fee except for two: Trust You (Malta) and Obchod (Slovakia).¹⁶¹

The trustmark member fee calculations vary; they are it is difficult to compare. However, a couple of similar fees can be identified which can be applied alternatively or cumulatively (some or all of them):

- “1. A one-time administrative registration fee (rarely applied by the trust marks),
2. A fee for first certification (very frequent),
3. An annual fee (required by almost all trustmarks).”

¹⁶⁰ European Consumer Centre Denmark, “E-Commerce Trustmarks in Europe”, <http://dokumenter.forbrug.dk/forbrugereuropa/e-commerce-trustmarks-in-europe/kap04.htm>.

¹⁶¹ The European Consumer Centres' Network, *Supra note* 43, at 47.

For comparison, it can be seen that the majority (13 trustmarks) of fees ranged between 100 and 200 Euros. See details below:

<100 Euro	5 trust marks (Chamber Trust France, eKomi France, Segala Ireland, eshop Malta, Wellmark Poland)
<200 Euro	13 trust mark (BeCommerce Belgium, APEK Czech Republic, dOP Czech Republic, Veddaneten! Hungary, ivsz Hungary, Aruküldök Hungary, Saugupirkti Lithuania, Thuiswinkel Netherlands, Webshop Keurmerk Netherlands, mkbOK Keurmerk Netherlands, Keur Online Netherlands, Confianza Online Portugal, Trusted.ro Romania)
<300 Euro	5 trust mark (SafeShops Belgium, Turvalineostukoht Estonia, Confianza Online Spain, ARMO Romania, Qshops Keurmerk Netherlands)
<400 Euro	1 trust mark (Certifierad E-handel Sweden)
<500 Euro	3 trust mark (E-Commerce Quality Austria, M-Commerce quality Austria, BoniCert Germany)
<600 Euro	2 trust mark (e-maerket Denmark, Trusted Shops Germany)
<700 Euro	1 trust mark (Trygg e-handel Sweden)
<800 Euro	1 trust mark (EHI Euro label Germany)
<900 Euro	
<1000 Euro	
1.000-2.000 Euro	1 trust mark (Fairbusiness Hungary)
2.000-3.000 Euro	1 trust mark (Trustmark.org UK)
3.000-4.000 Euro	
4.000-5.000 Euro	1 trust mark (TÜV SÜD Germany)

Figure 3.6 The Ranges of Member Fee¹⁶²

¹⁶² *Id.* at 48.

3.2.2.4 The legal relationship with and liability of trustmark service provider

(1) The legal relationship

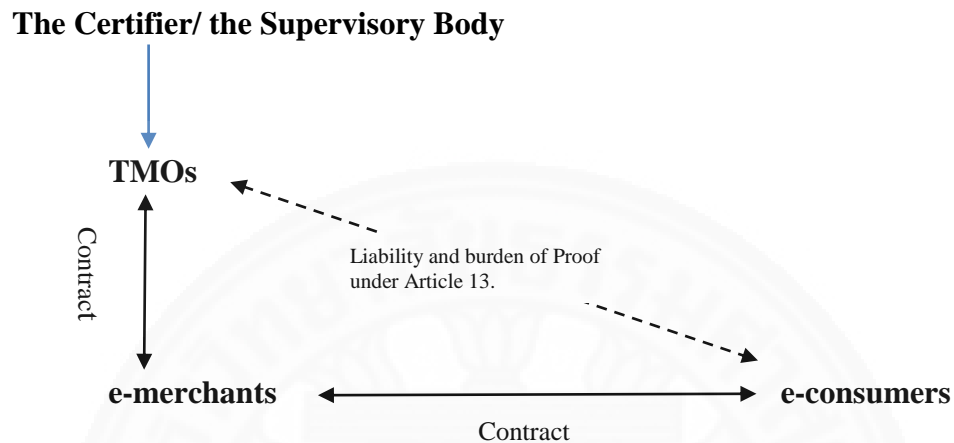


Figure 3.7 EU Legal Relationship

(2) Liability of trustmark service provider

The Regulation provides the liability of all trust service providers. Namely, they shall be liable for damages caused to any natural or legal person due to failure to comply with the obligations under the Regulation, as stated in Article 13 paragraph 1. Except when their limitations are informed to the consumers in advance, the service provider will not be liable for damages arising from the use of service exceeding the indicated limitation according to Article 13 paragraph 2.¹⁶³ In terms of the burden of proof, a qualified trust service provider has a burden to prove its intention or negligence. On the other hand, a person who claims damages from a non-qualified trust service provider shall be liable to prove under the principle of “he who asserts a matter must prove it”.¹⁶⁴

To control and enforce trust service providers, EU Member States should enact rules on penalties applicable to infringements of the Regulation. According to Article 16, such penalties shall be effective, proportionate and dissuasive.

¹⁶³ Ibid, see p.92.

¹⁶⁴ See Article 13.

Before the Regulation (EU) No 910/2014 was created, there were no reported legal cases that addressed directly the liability of trustmark service providers in England. The courts should determine and apply “the general principle of professional negligence” to the liability of trustmark service providers, mostly based on the tort of negligence. The following three conditions are determined to bring an action in negligence:

- “a) The defendant owes a duty of care to the plaintiff;
- b) The defendant has acted or spoken in such a way as to break that duty of care; and
- c) The plaintiff has suffered relevant damage as a consequence of the breach.”¹⁶⁵

This preliminary analysis focus determines whether TMOs owe a duty of care towards e-consumers. In theory, a duty of care can arise by comparing TMOs with accountants, surveyors and valuers. This rule applies especially in cases of professional negligent misstatements which cause pure economic loss. Foreseeability, proximity and policy arguments are generally the necessary requirements for the existence of a duty of care.

Hedley Byrne & Co Ltd v. Heller & Partners Ltd was the case which opened the way to third-party claims for negligent misstatements which caused economic loss and set the standards to verify whether a duty of care exists in such cases. This was termed the “reliance principle”. The court held that a professional who issues a statement to a person who is entitled to and does rely on it should be liable accordingly.¹⁶⁶ The following three elements are important for determining the duty of care.

1. Foreseeability of persons¹⁶⁷

The court takes this first step in order to check whether a reasonable person in the defendant’s position would have been able to foresee that his carelessness could cause a loss to the plaintiff or to the class of persons the plaintiff belongs to. The key point is

¹⁶⁵ Paolo Balboni, *supra* note 15, at 105.

¹⁶⁶ Paolo Balboni, *supra* note 15, at 111.

¹⁶⁷ *Id.*, at 103.

about “foreseeability”. However, in the case of professionals’ negligent misstatements which cause economic loss to third parties who relied on them, foreseeability is indeed necessary to establish professional liability but absolutely not sufficient.

2. Proximity¹⁶⁸

The second step that courts usually take is to assess whether there is enough proximity between the defendant and the plaintiff. ‘Proximity’ is about the relationship between the parties: being sufficiently proximate, the defendant would know that his failures might directly affect the plaintiff. Sometimes, courts have asked for proof of the existence of a ‘special relationship’ between the parties or of a “relationship equivalent to contract”. Another proximity factor is the so-called “defendant’s knowledge of the recipient or class”. In summary, we may say that the ‘plaintiff’s reliance’ is an important factor to establish a causal link between the defendant’s misstatement and the plaintiff’s loss. In fact, a statement only causes damage when somebody acts in reliance on it. However, the plaintiff’s reliance needs to be reasonable. It will be considered reasonable if in the case at hand other proximity factors, among the ones already mentioned, coexist (i.e., defendant’s specific professional skill and knowledge that the plaintiff or people of the class he belongs to is likely to rely on the statement; and the purposes for which the plaintiff uses the statement are congruent with the one contemplated by the defendant).

3. Policy¹⁶⁹

When foreseeability and proximity are found, this does not mean that a third party can claim for economic loss suffered due to reliance on negligently provided information. In other words, foreseeability and proximity are necessary but they are not sufficient conditions for the recognition of a third-party duty of care upon a professional who negligently provides an inaccurate statement. In addition, the imposition of a duty of care must be fair, just, and reasonable. Fairness, justice, and reasonableness are concepts which enjoy a certain degree of abstraction created to leave some discretion

¹⁶⁸ *Id.*, at 105.

¹⁶⁹ *Id.*, at 107.

to courts in their decision, especially in third-party liability claims for negligent misrepresentation.

It is important to balance these three factors to determine the liability of a professional; these can then be tailored to the liability of TMOs.

It is important to balance these three factors for determine the liability of professional, which we may tailor to the liability of TMOs.

(3) Damage and fault in case of breach of trust

According to Article 13 paragraph, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the Regulation (EU) No 910/2014, unless the trust service providers inform their e-merchants in advance of the limitations on the use of the services they provide and where those limitations are recognizable to third parties, i.e. e-consumers. Otherwise, these liability provisions shall be applied in accordance with national rules on liability.

It is a clearly-stated provision that trust service providers shall be liable for damage. To calculate the damages, initially we have to determine whether it is a contractual or tort relationship between a trust service provider and e-consumer. If it is a contract, the damages are assessed by what the parties would have seen as the damage caused by a breach at the time the contract was formed; the date of the contract. In tort, damage is assessed by reference to the date the tort was committed. In this situation, this is a contractual relationship between a trust service provider and an e-merchant and it is also a contractual relationship between an e-merchant and an e-consumer. Hence, it may be foreseen that it is a contractual relationship between a trust service provider and an e-consumer. Damages may therefore be calculated at the time the contract was formed.

3.2.2.5 The monitoring of trustmark receiver

(1) Passive monitoring

Security requirements apply to the trust service providers, equivalent to the level of risk inherent to their activity. EU Member States are also required to designate a supervisory body for setting the trust service providers' standard guidance and controlling them according to Article 17-19.¹⁷⁰

(2) Active monitoring

Qualified and non-qualified trust service providers are required to notify the supervisory body and other relevant bodies, of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained herein, without undue delay but in the event within 24 hours after having become aware of it according to Article 19 paragraph 2.

Moreover, if the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

¹⁷⁰ European Payments Council, “*Next Step to Create the Digital Single Market: EU Lawmakers Adopt the New Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*”, p.1, http://www.europeanpaymentscouncil.eu/pdf/EPC_Article_338.pdf.

3.2.2.6 Enforcement of laws specific to trustmarks

Subject to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, which deals with electronic signatures without states about a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. Therefore, the regulation, namely “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market” enhances and repeals Directive 1999/93/EC.¹⁷¹ As such, the specific regulation applies to trust service entered into force since 17 September 2014.

E-commerce transactions across borders are also a big concern so many countries have mutually agreed to launch a project to ensure consumers recognize a certain trustmark across borders, i.e. the EMOTA European Trustmark.¹⁷² The EMOTA was established by the EMOTA members (Austria, Belgium, Greece, Germany, Italy, Portugal, The Netherlands, Spain, Sweden, and Switzerland) with the aim of offering consumers convenient, reliable, safe and legally compliant services.¹⁷³ They also created the EMOTA European Trustmark Accreditation Criteria for national providers (“the Accreditation Criteria”) as the following:

“A. Code of conduct with high level of consumer protection:

- Transparent information about the trader
- Clear, complete and accurate product description
- Transparent pricing, inclusive of all charges and taxes
- Accurate information to the customer on product availability and delivery times
- Delivery according to the specifications and timing indicated to the

¹⁷¹ The European Union, “*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July on electronic identification and trust services for electronic transactions in the internal market*”, p.73.

¹⁷² The European Multi-channel and Online Trade Association., “*EMOTA European Trustmark*”, <http://www.emota.eu/#!european-trustmark-/c1f52>.

¹⁷³ *Id.*

customer

- Clear returns process and prompt reimbursement
- Accessible customer service and timely complaint management
- Protection of personal data according to EU and national legislation
- Appropriate protection of minors
- Secure payment methods

B. Comprehensive accreditation process:

- Online, fully documented, interactive and accessible procedure which enables and ensures merchants' compliance with the Trustmark requirements
- Online and interactive support and advice to facilitate any necessary Improvements to be made by the merchant before the Trustmark can be awarded
- Auditable record of accreditation and Trust Mark performance including the retention of approved Terms & Conditions

C. Continuous monitoring of traders' compliance:

- Minimum annual review of compliance
- Additional checks may be performed at any time on an exception basis

D. ADR schemes:

- Traders should provide information about ADR/ODR services to resolve consumer complaints

E. Enforcement and sanctions:

- The Trust Mark organization will address any relevant issues with the trader, who will need to correct them promptly
- The Trust Mark can be withdrawn if the trader does not comply with the code of conduct or in the case of insolvency.”¹⁷⁴

¹⁷⁴ The European Multi-channel and Online Trade Association, “*EMOTA European Trustmark Accreditation Criteria for national trustmark providers*”. http://media.wix.com/ugd/b18286_9e22f83c2d8d491cb6c5261a61db509d.pdf.

The **EMOTA European Trustmark Merchant Charter** ("the Merchants Charter") adopted by the EMOTA members and approved by the Board of Directors of EMOTA establishes the following:

"As an online shopper with an EMOTA-accredited merchant, you have the right to:

1. Clear, comprehensive and accurate product description and merchant information before you place your order;
2. Convenient, reliable, safe and legally compliant service;
3. Notification of all costs and any limitations / conditions prior to checkout;
4. Charges that are complete and simple to understand – including any tax and delivery and surcharges;
5. Access information on your order progress / history;
6. Delivery as specified at the time of order;
7. Your purchases arriving in good condition;
8. Helpful support with damaged / failed / late / attempted deliveries;
9. A clear returns process, with any limitations / conditions notified prior to purchase;
10. Your personal data and rights being properly protected and managed."¹⁷⁵

¹⁷⁵ Ibid.

CHAPTER 4

E-COMMERCE TRUSTMARK UNDER THAI LAWS

4.1 The characteristics of trustmarks in Thailand

4.1.1 Certification mark principle under Trademark Act B.E. 2534

A certification mark is defined in section 4 of the Trademark Act B.E. 2534 as a mark used or proposed to be used by the owner thereof on or in connection with goods or services of another person to verify the origin, make-up, method of production, quality or other characteristics of such goods or to certify as to the nature, quality, type or other characteristics of such services.¹⁷⁶ This means that the owner of a certification mark allows someone to use his mark on goods or services for the purpose of certifying some qualification of the goods or services.¹⁷⁷

In order to register a certification mark, the applicant must comply with the provisions on registration of trademarks, submit to the regulations on use of the certification mark together with the application for registration according to section 82 (1), and demonstrate an ability to certify the characteristics of the goods or services as provided in the regulations under section 82 (1) according to section 82 (2).¹⁷⁸ Moreover, the Regulations under section 82 (1) indicate the origin, composition, method of production, quality or other characteristics which are to be certified including the rule, procedures and conditions for authorizing use of the certification mark.¹⁷⁹

In the part of the right of the owner of the certification mark, in addition to the same right as the owner of trademark. The owner of a registered certification mark is prohibited according to section 90 from using the mark on his own goods or services

¹⁷⁶ See section 4 of Trademark Act B.E. 2534 as amended by the Trademark Act (No.2) B.E. 2543.

¹⁷⁷ ชัยยศ เหมะรัชตะ, *ลักษณะของกฎหมายทรัพย์สินทางปัญญา*. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2550. (Chaiyot Hemaratchata, *the principle of intellectual property*. Bangkok: Nititham, 2007)

¹⁷⁸ See section 82 of Trademark Act B.E. 2534 as amended by the Trademark Act (No.2) B.E. 2543.

¹⁷⁹ See section 82 paragraph 2 of Trademark Act B.E. 2534 as amended by the Trademark Act (No.2) B.E. 2543.

and from licensing it to other persons to act as certifier by authorizing the use of the certification mark.¹⁸⁰ Being given authorisation for others to use a certification mark for goods or services must be in writing and be signed by the owner of the certification mark under section 91.¹⁸¹

4.1.2 DBD's authorization under Trademark Act B.E. 2534

The DBD has created the two types of e-commerce trustmarks in Thailand: 1. DBD Registered, and 2. DBD Verified.¹⁸² DBD Registered is a trustmark given to certify that the merchant, either an ordinary or a juristic person, has successfully registered his/her online business operations with the DBD, and that the buying and selling of products or services can be conducted as e-commerce transactions.¹⁸³ DBD Verified is only given to a juristic person that has registered its online business operations and met all qualifications and criteria specified by the DBD for certifying reliability of electronic business operations.¹⁸⁴ The reliability level of DBD Verified is higher than DBD Registered.¹⁸⁵

DBD Registered has no expiry date. The registered e-merchants can use and display DBD Registered seals on their websites for the duration of their electronic commerce operations under section 4 of the Regulation on the use of DBD Registered except in case of revocation and cancellation under section 7-8. On the other hand, DBD Verified is valid for one year whereupon it must be approved for renewal.

Subject to section 91 of Trademark Act B.E. 2534, "the authorization of others to use a certification mark for goods or services shall be in writing and signed by the owner of the certificate mark." This provision states about a form of a certificate evidence. All juristic act and contract which are not in the form prescribed by law is void under

¹⁸⁰ See section 90 of Trademark Act B.E. 2534 as amended by the Trademark Act (No.2) B.E. 2543.

¹⁸¹ See section 91 of Trademark Act B.E. 2534 as amended by the Trademark Act (No.2) B.E. 2543.

¹⁸² Department of Business Development, Ministry of Commerce, "*Frequently Asked Questions*", p.10, <http://www.trustmarkthai.com/ecm/content/faq001.pdf>.

¹⁸³ *Id.*

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

section 152 of Civil and Commercial Code¹⁸⁶. DBD Registered and DBD Verified are registered as the certificate marks under Trademark Act B.E. 2534, thus to authorize other to use the marks, the DBD shall provide a certificate in writing and signed by its authorized person for each registered trademark owner.

In fact, the DBD approves an e-merchant on DBD Registered, the DBD send a trademark source code via email to the e-merchant's e-mail address. A successful e-merchant is required to show the DBD Registered seal on the first page of its e-commerce website. There is no written evidence or procedure which shows us that the authorized use of DBD Registered is made in writing and signed by the DBD as its obligation specified in section 91 of the Trademark Act B.E. 2534.¹⁸⁷ It may be said that is not a lawful authorization of a certificate mark under the Trademark Act and such authorization of DBD Registered is void under section 152 of Civil and Commercial Code. The e-merchants may be at risk of an unauthorized use of DBD Registered, which would be damaging for them and lost trust. The Supreme Court decision no. 5219/2550 can be used to illustrate this.¹⁸⁸ The defendant was granted use of a service mark called "THE HIDE -AWAY" and LEMON BABY picture by Hide a way Co., Ltd. The Trademark licensing agreement was made in writing for 5 years but the agreement was not registered to the trademark registrar according to section 68 paragraph 2 and section 80 of Trademark Act. The defendant was claimed against for unauthorized use of such a service mark; the court held that the trademark licensing agreement was invalid. However, in this case some content granted the defendant use of technical information under a service mark and trademark "The Hide Away Thai Herbal Steam Sauna". Further, the action of the defendant was not intentional or negligent. Neither did it cause damage to the plaintiff as the defendant did not infringe the plaintiff's service mark by advertising another service mark. Like the court decision in the Supreme Court decision no.386/2549,¹⁸⁹ the court held that the trademark

¹⁸⁶ See section 152 of Thai Civil and Commercial Code.

¹⁸⁷ วัช ดิงสมิตร, "คำอธิบายกฎหมายเครื่องหมายการค้า". กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2545, น. 173 (Wat Tingsaming, "*the explanation of trademark law*". Bangkok: Nititham, 2002, p. 173)

¹⁸⁸ Justice court electronic library, "*Specific Supreme Court Decision – Section 80*", p.1, http://www.library.coj.go.th/pongkun_68.php?idmain=102&&kotmaiyo=-&&mattra=80.

¹⁸⁹ *Id.*

licensing agreement was invalid as it was not made as a specific form under the Trademark Act but it did not cause all content in such an agreement to be invalid. However, in the case of DBD Registered, no provision stated about separate provisions or stated that some provision would survive if some provisions were invalid. Hence, it may be foreseen that regulation of use of DBD Registered will be interpreted as totally invalid if someone sues the e-merchant.

In fact, when the Department of Business Development allow the e-merchant to use DBD Registered, the Department will send a trustmark source code via email to the e-merchant's e-mail address. A granted e-merchant is required to show the DBD Registered seal in the first page of its E-commerce website. (See details in 4.2.1) No writing evidences and procedure show us that the authorized use of DBD Registered is made in writing and signed by the Department as its obligation specified in section 91 of Trademark Act B.E. 2534. It may say that is not a lawful authorization of a certification mark under Trademark Act and such authorization of DBD Registered is invalid under section 91 of Trademark Act B.E. 2534. The e-merchants may in risk to be claimed for unauthorized use of DBD Registered, get damage and loss trustworthiness in their business. To determine this case, we may compare with the Supreme Court decision no. 5219/2550.¹⁹⁰ The defendant was granted to use a service mark called "THE HIDE -AWAY" and LEMON BABY picture by Hide a way Co., Ltd. The Trademark licensing agreement was made in writing for 5 years but the agreement was not registered to the trademark registrar according to section 68 paragraph 2 and section 80 of Trademark Act. The defendant was claimed for unauthorized use of such service mark, the court held that the trademark licensing agreement was invalid but in this case some content, granted the defendant to use technical information under a service mark and trademark "The Hide Away Thai Herbal Steam Sauna", the action of the defendant was not made by intention or negligent and it did not cause damage to the plaintiff. The defendant did not infringe the plaintiff's service mark by advertising other service mark. Like the court decision in the Supreme

¹⁹⁰ Justice court electronic library, "*Specific Supreme Court Decision – Section 80*", p.1, http://www.library.coj.go.th/pongkun_68.php?idmain=102&&kotmaiyo=-&&mattra=80.

Court decision no.386/2549¹⁹¹, the court held that trademark licensing agreement was invalid due to it was not made as specific form under Trademark Act but it did not cause all content in such agreement invalid. But in case of DBD Registered, no provision stated about separate provisions or stated that some provision will survive, if some provision is invalid. Hence, it may be foreseen that regulation of use of DBD Registered will be interpreted totally invalid, if someone sue the e-merchants.

As for the authorized use of DBD Verified, when the Department allows the e-merchant to use its trustmark, the Department will issue an authorization of use in writing according to section 8 of the Regulation on the use of DBD Verified; this follows the concept of the authorization of a certification mark. The e-merchant must then display the certificate in their head office and on the first page of their website.

4.1.2.1 DBD Registered

DBD Registered is issued to e-merchants who have completed commercial registration with the objective of having a DBD Registered logo on their websites to guarantee their existence and commercial registration.¹⁹² See details in Appendix C.

The sample of DBD Registered is showed as:¹⁹³



4.1.2.2 DBD Verified

DBD Verified is issued to e-merchants who have registered with the DBD and possess all the required qualifications outlined by the Department.¹⁹⁴ This trustmark will certify

¹⁹¹ *Id.*

¹⁹² Department of Business Development, Ministry of Commerce, “*The Regulation of Use of DBD Registered*”, p.1, <http://www.trustmarkthai.com/ecm/forms/form010.pdf>.

¹⁹³ *Id* at 4.

¹⁹⁴ Department of Business Development, Ministry of Commerce, “*Issuance for E-commerce DBD Verified*”, p.1, <http://www.trustmarkthai.com/ecm/public/newsletter/view.html?id=382>.

the e-commerce reliability of the business and that the website has successfully met the e-commerce quality criteria of the Department.¹⁹⁵

The sample of DBD Verified is showed as:¹⁹⁶



In the early of Year 2016, DBD has announced new trustmarks, namely DBD Verified Silver, DBD Verified Gold, and DBD Verified Platinum. See details in Appendix D-F.

There are a number of advantages to DBD Registered and DBD Verified:

1. Entrepreneurs

- “Building confidence in the business as its website has been examined and approved for operations and good corporate practices
- Promoting good image and increasing competitiveness
- Building trust in products/services, resulting in a better opportunity to penetrate foreign markets
- Improving business opportunity by marketing/ public relations activities through various channels of the Department of Business Development.”¹⁹⁷

2. Consumers

- “Being confident that they buy products/services from a website that is reliable and has passed the E-commerce quality standards set by the Department of Business Development

¹⁹⁵ *Id.*

¹⁹⁶ Department of Business Development, Ministry of Commerce. “*The Regulation of Use of DBD Verified.*” p. 6, <http://www.trustmarkthai.com/ecm/forms/form015.pdf>.

¹⁹⁷ Department of Business Development, Ministry of Commerce, *supra* note 185, at 4.

- In case of any conflicts or problems, customers can file complaints to the Department of Business Development for settlement.”¹⁹⁸

4.2 Trustmark certification process

4.2.1 DBD Registered

The criteria for issuance of DBD Registered are as follows:

- “1. An applicant must own a website and has his/her own domain name.
2. The website must have had E-commerce registration in accordance with laws.
3. The website must show detailed information of the website owner, office address, landline and mobile phone numbers as well as channels for complaint filing and delivery of goods/services, both offline and online, or Contact Us menu.
4. Any products or services to be offered for sale through the E-commerce channel shall not be contrary to the laws and public order or good morals.
5. The products or services shall meet the objectives that have been electrically registered.
6. Presentation of the products and services must be clear and there shall be such data as types of the products or services, prices, and payment methods.
7. Customer care/service policy must be clearly stated on the website.”¹⁹⁹

In the application process, the applicant has to submit the following documents to the Bureau of E-Commerce, DBD.

- “1. A copy of commercial registration certificate (Form Phor Khor. 0403)
2. Details of the website (document attached to Form Thor Phor.)
3. A copy of domain name registration certificate”

¹⁹⁸ *Id.*

¹⁹⁹ Department of Business Development, Ministry of Commerce, “*Criteria for Awarding of DBD Registered*”, p.1, <http://www.trustmarkthai.com/ecm/public/newsletter/view.html?id=383>.

Upon the meeting the requirements, the Department will send the e-merchant a source code via email as specified during the commercial registration. A person granted permission to use the DBD Registered logo is required to display it on the first page of the website used for such e-commerce.

A summary of the steps for issuance of DBD Registered are given as follows:

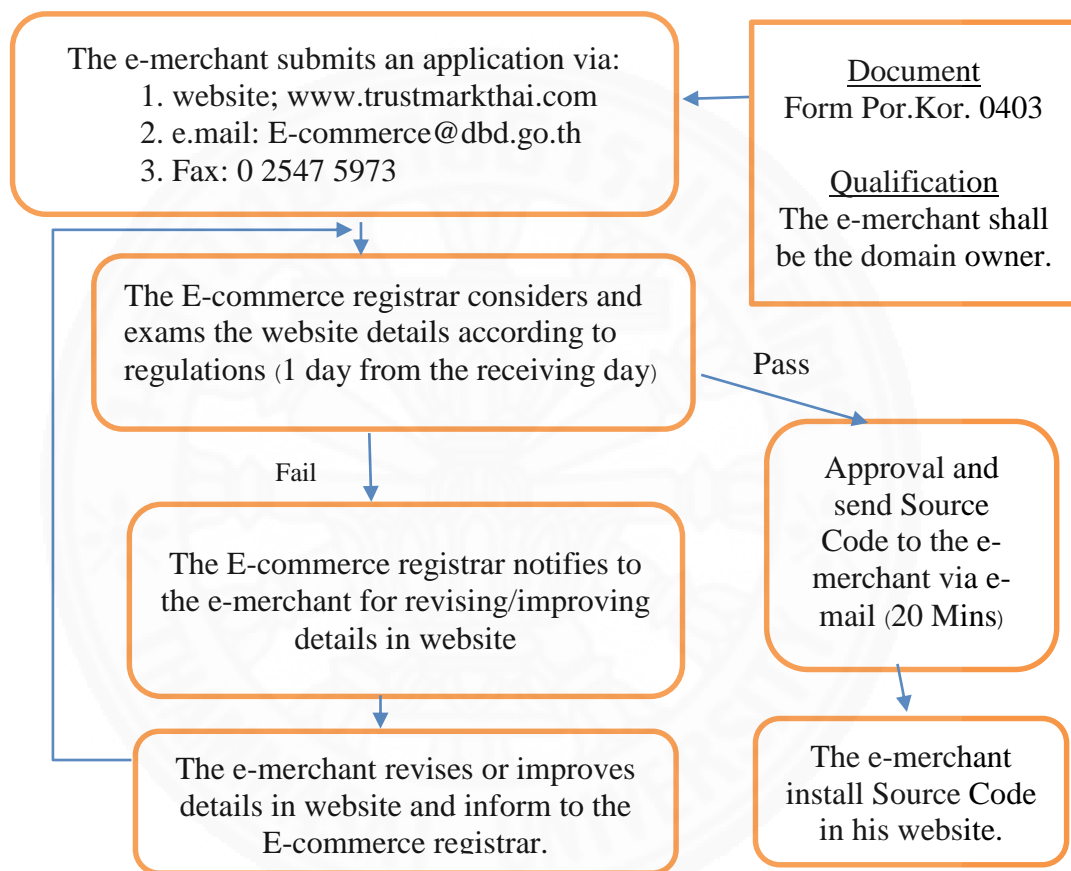


Figure 4.1 Steps for Issuance of the E-Commerce Trustmark (DBD Registered)²⁰⁰

After DBD Registered is issued, the e-merchant must comply with the rules under the Regulations on the use of DBD Registered of the DBD.

²⁰⁰ Department of Business Development, Ministry of Commerce, "the procedure of issuance of DBD Registered", <https://drive.google.com/file/d/0B76yJeKddP3QNUJYMW1YLWViT2c/view>.

4.2.2 DBD Verified

Qualifications of an eligible applicant and standard criteria for e-commerce quality are set out by the DBD as follows:

“Qualifications of an Eligible Applicant for DBD Verified

1. Being a juristic person incorporated in Thailand;
2. Having made E-commerce registration and been granted DBD Registered for not less than six months, or having made E-commerce registration for not less than 2 years;
3. Being a domain name owner;
4. Not being suspended from using the Trustmark; and
5. Never having his trust mark revoked, unless such revocation is more than five years old.

Standard Criteria for E-Commerce Quality

1. Data disclosure
2. Methods for cancellation or return of products and communication with customers
3. Security
4. Privacy
5. Complaint handling and conflict settlement²⁰¹

In the applying process, the applicant have to submit a copy of commercial registration certificate (Form Phor Khor. 0403) to Bureau of E-Commerce, Department of Business Development.

In the application process, the applicant has to submit a copy of the commercial registration certificate (Form Phor Khor. 0403) to the Bureau of E-Commerce, DBD.

²⁰¹ Department of Business Development, Ministry of Commerce, *Supra* 185.

To apply for a DBD Verified logo, e-merchants should have all the required qualifications and pass the quality evaluation processes as follows:

- “1) **Self-evaluation:** go to www.trustmarkthai.com to apply for DBD Verified logo. There, you need to complete the self-assessment for E-commerce entrepreneurs.
- 2) **Evaluation by Experts:** E-commerce experts will examine websites against the e-commerce quality standards.
- 3) **Evaluation by Committee:** DBD Verified Evaluation Committee will examine websites against the E-commerce quality standards.”²⁰²

The steps needed for issuance of DBD Verified can be summarized as follows:

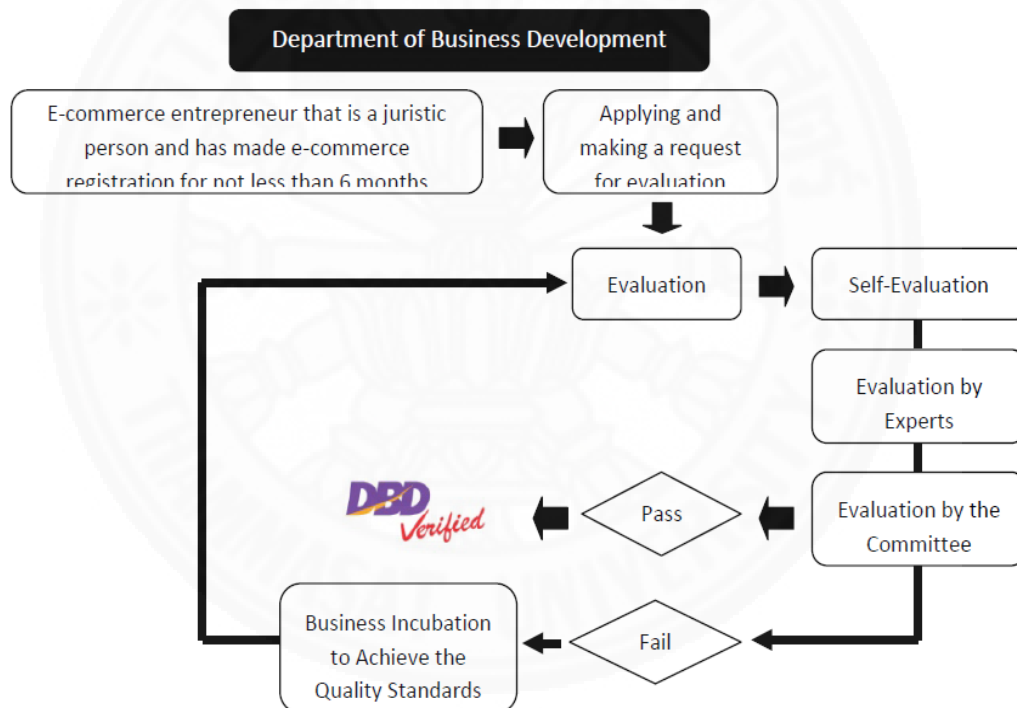


Figure 4.2 Steps for Issuance of E-Commerce Trustmark (DBD Verified)²⁰³

After DBD Verified is issued, the e-merchant must comply with the rules found in the regulations on the use of DBD Verified of the DBD.

²⁰² Department of Business Development, *Supra* 136.

²⁰³ Department of Business Development, Ministry of Commerce, *supra* note 139, at 4.

4.3 Fee

Before applying for DBD Registered, the e-merchants have to apply for E-commerce registration and the following fees are applied:

- “1) New commercial registration 50 Baht
- 2) Registration of changes to registered transactions 20 Baht/time
- 3) Registration of business dissolution 20 Baht”²⁰⁴

Otherwise, the e-merchants can apply for DBD Registered and DBD Verified for free by completing an online registered form.

4.4 The legal relationship with and liability of trustmark service providers

4.4.1 The legal relationship

The legal relationship between the DBD and e-merchants can be determined by understanding the meaning of administrative order.

Section 5 of the Administrative Procedure Act B.E. 2539 defines administrative order as:

"Administrative order" means an enforceable order issued by a public authority, which create a legal relationship between persons to create, change, assign, protect, cancel, to effect to other's rights or obligations, whether permanent or temporary such as an order, approval, authorization, appeal, certification and registration, exclude rule making.

The legal relationship between DBD and an e-merchant is created when DBD approves the authorization of a trustmark to an e-merchant. Such an action is an administrative order. E-merchants shall agree to perform according to DBD's standard criteria and

²⁰⁴ Department of Business Development, Ministry of Commerce, *supra* note 129, at 9.

DBD has a higher power to enforce e-merchants in case of suspension and revocation of the certificate. Otherwise, it seems to me that it is not an administrative contract because it does not meet all the conditions specified in section 3 of the Act on Establishment of Administrative Courts and Administrative Court Procedure B.E. 2542 (1999), which offers the following definition:

“Administrative contract” means including contract made between two parties which one party is a public agency or an authorized person and such contract has one of these characteristics; a concession contract, a public service system contract and a contract for the provision of public utilities or for the exploitation of natural resources.

In fact, DBD uses the power under section 82 of the Trademark Act to issue a certification mark to an e-merchant. It may be interpreted that this creates a commercial contract relationship, due to the regulation of using DBD certification mark is terms and conditions to use both DBD trademark.

In terms of the legal relationship between the e-merchant and e-consumers, the e-merchant has a responsibility to perform their obligations according to international principles. However, the legal relationship between DBD and an e-merchant will still be considered that seems to be a contractual relationship and a tortious relationship.

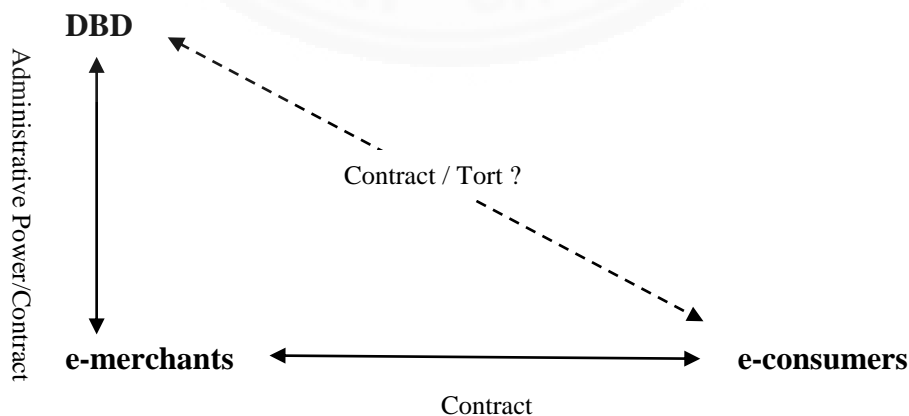


Figure 4.3 Thai Legal Relationship

4.4.2 Liability of trustmark service provider

It is necessary to determine the extent of liability that falls upon the DBD as a trustmark service provider if, for instance, an e-merchant breaches the contract made with an e-consumer by failing to send the goods or sending poor quality goods and this causes a commercial loss to the e-consumer who relies on the trustmark issued by DBD.

There are no specific provisions to apply in this case. The e-consumer may make a claim against DBD according to the administrative law on the basis that authorized use of both DBD trustmarks are made by an administrative order of a government agency. However, if the e-consumer can prove that it was caused by an intention or negligence of a government officer, a trustmark issuance procedure or the failure to monitor, then the e-consumer may make a claim against DBD under section 5 of the Government Officers Liability of Tort Act B.E. 2539. This states that:

“Agencies of the State must be liable for violations of the victim in the results that its officials have made in the implementation. In this case, the victim may sue the State agencies directly, but to sue the officers do not.”²⁰⁵

In the event that a government agency is held liable for damage claimed by a victim due to the abuse of officials, the government agency has the right to hold those officials liable who caused the damage to the victim if the acts were intentional or seriously negligent.²⁰⁶

It means that a government agency shall be liable towards third parties when officers act in breach of duty. However, the government agency has the right to recourse from the officials who commit violations, with intentional or serious negligent in their performance. If the violation occurred or non-action in action. The officers be liable for only one Department.

²⁰⁵ See section 5 of Government Officers Liability of Tort Act B.E. 2539.

²⁰⁶ See section 8 of Government Officers Liability of Tort Act B.E. 2539.

We may apply this idea developed in the Government Officers Liability of Tort Act B.E. 2539 to DBD officers or committees who are assigned by DBD to evaluate DBD Verified according to the definition of officials including government employees or workers in another category.

4.4.3 Damage and fault in case of breach of trust

In the relationship between e-consumers and DBD, there are also no specific provisions with which e-consumers can claim against DBD for damage when they rely on DBD Registered or DBD Verified. However, if we argue that there is a contractual relationship between them, then DBD shall be liable to the e-consumer as a guarantor if it can be proved that DBD failed to carry out controls or breached its obligation according to specific terms and conditions between DBD and the e-merchants.

In the event that occur dispute between an e-merchant and an e-consumer, subject to the international principles, an e-consumer can file a claim against an e-merchant via process, called dispute resolution service, a trustmark service provider will examine an e-merchant and punish it by suspending or cancelling the certificate, and/or enforcing an e-merchant to pay damage to an e-consumer. There are only dispute resolution services for DBD Verified is set, no provisions of Regulation of using DBD Registered are specified about dispute resolution services see at Appendix D. It means that an e-consumer shall file a lawsuit to an e-merchant for damage.

4.5 The monitoring of trustmark receivers

4.5.1 Passive monitoring

Section 7 of the regulation on the use of DBD Registered specifies that the DBD has the power to suspend the certificate mark if a trustmark receiver does not comply with the provision of section 5, i.e. the trustmark is not displayed in the first page of the e-commerce website or they do not disclose their business information (business name, brand name (if any), commercial certificate, company address and contact).

Revocation occurs if the DBD Registered receiver: commits an unlawful act or disturbs public order, morality or security; does any act that is unfair to the consumer under

section 8(1); misapplies the purpose of the certificate mark to the extent that the DBD, as the certificate mark owner, is harmed under section 8(2); does not consent or does not provide the required information to the Department officer under section 8(3); or its commercial registration certificate is revoked under the Business Registration Act B.E. 2499 (A.D. 1956) under section 8(4) or according to section 7 paragraph 3 as stated in section 8(5). Moreover, if the certificate mark is suspended or revoked by the Department officer, the DBD Registered receiver must stop using it immediately under section 9 paragraph 1. If anyone infringes this provision, they shall pay a penalty fee to the Department at a rate of Baht 5,000 per day until they stop doing so according to section 9 paragraph 2.

In the case of DBD Verified, it is specified in section 12 of the regulation on the use of DBD Verified that the DBD has the power to suspend the certificate mark if a trustmark receiver does not comply with the provision of section 6 (1) to (8)²⁰⁷ or section 8 paragraph 2. Moreover, the trustmark certificate will be revoked by the Department if the trustmark receiver breaches any provision of section 13 (1) to (5).²⁰⁸ The DBD Verified receiver must stop using it immediately as per section 14 paragraph 1. If anyone infringes this provision, they must pay a penalty fee to the Department at a rate of Baht 5,000 per day until they stop doing so as per section 14 paragraph 2, which reflects the DBD Registered rule.

4.5.2 Active monitoring

However, DBD provides only a passive monitoring system based on complaints reported by e-consumers about e-merchant practices. No active monitoring is performed. This cannot be considered a strong monitoring system worthy of e-consumers' trust.

²⁰⁷ See section 6 of the regulation of use of DBD verified.

²⁰⁸ See section 13 of the regulation of use of DBD verified.

4.6 Enforcement of laws in specific to trustmarks

There are no direct enforcement laws applied on the use of trustmarks in Thailand; both DBD trustmarks are registered as certificate marks under the Trademark Act B.E. 2534. If some concerns are raised, we may use the offline principles for interpretation and apply thereof.

4.7 Analysis of problems

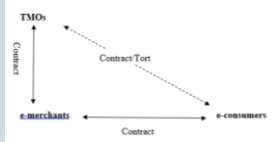

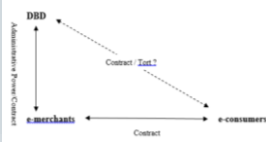
4.7.1 The characteristics of trustmarks

List	U.S	EU	Thailand
Operator	<ul style="list-style-type: none"> Non-profit organisation or private sector 	<ul style="list-style-type: none"> Non-profit organisation or private sector 	<ul style="list-style-type: none"> Government Sector
Character	<ul style="list-style-type: none"> Trust mark or Web seal 	<ul style="list-style-type: none"> Trust mark or Web seal 	<ul style="list-style-type: none"> Certificate mark under Trademark Act B.E. 2534

Most trustmark service providers in the US and EU are non-profit organisations or companies in the private sectors. However, trustmarks in Thailand are operated by the government sector, namely the DBD which does not follow the trustmark principles of developed countries. When the government sector acts as trustmark service provider, there is weak supervision and monitoring as it is difficult to assign such supervision over trustmark service providers. Because effective monitoring is also key for building trust in trustmarks, the use of hi-tech solutions are necessary.

The principle of a trustmark is specific, according to the OECD guidelines. In both the US and EU, they are set up as distinct from certificate marks and are not required to be registered as certificate marks under their trademark acts. This contrasts with Thai trustmarks which are registered as certificate marks under the Trademark Act B.E. 2534. It is therefore necessary for Thai trustmarks to stop being dealt with according to trademark rules as at present they cannot be enforced worldwide unless they are registered all around the world.

4.7.2 The legal relationship with and liability of trustmark service Providers

List	U.S	EU	Thailand
Legal relationship			
Liability of trustmark service provider	Yes	Yes (See Article 13 of the Regulation (EU) No 910/2014)	?

In US, no specific requirements are set out for a negligent action of trustmark service provider. Thus, off-line principles are applied in the case of torts and contracts laws.

In EU, trustmark service provider shall be liable for damages caused to any natural or legal person due to failure to comply with the obligations under the Regulation, as stated in Article 13 paragraph 1, except their limitations are informed to the consumers in advance, service provider will not be liable for damages arising from the use of service exceeding the indicated limitation according to Article 13 paragraph 2.

In Thailand, no specific law is announced, there are not stated in Regulation of using DBD Registered and DBD Verified. Thus, section 5 of Administrative Procedure Act B.E. 2539 “Administrative order” is applied to this case. I recommend that trust service provider (the DBD) should be liable to e-consumers for damage caused intentionally or negligently due to a failure to comply with their obligation.

4.7.3 The monitoring of trustmark receiver

List	US	EU	Thailand
Active monitoring	Yes	Yes	No
Passive monitoring	Yes	Yes	DBD Registered and DBD Verified

Active monitoring is a main required process which both US and EU set it as an essential method for building trustworthiness of online shopping. Effective monitoring should be set and applied to Thai trustmarks all well.

4.7.4 Enforcement of laws specific to trustmarks

U.S	EU	Thailand
<ul style="list-style-type: none"> • Yes (under the control of Federal Trade commission) 	<ul style="list-style-type: none"> • Yes (See Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market) 	<ul style="list-style-type: none"> • No Specific law • Present applying law: Trademark Act

The proper rules and regulations should be focus and concern, US and EU also follow and adopt the principles of OECD guidelines. Their laws are continually developed and educated for supporting an online economic. No specific law is applied for Thai trustmarks prepared by the BDB in Thailand. The specific act should be draft and set.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

E-commerce trustmarks are designed to be understandable to all e-consumers that websites meet the trustmark requirements under the standards of the trustmark service provider. The aim of issuing trustmarks is to overcome the lack of trust in online shopping which is the key element in e-commerce. Trustmark service providers will issue a trustmark to e-merchants only if the e-merchants meet their standards e.g. security, privacy, business practice. E-merchants hope that, by displaying the trustmark on their websites, e-consumers will trust their certified practice and feel more confident about parting with personal data and carrying out a transaction on the website. Mostly, trustmarks in the US and EU are administered by non-profit organizations and private organizations under their own official standards. Only a few trustmarks are operated by the government sector, such as in Thailand, as trustmark schemes by definition rely on self-regulation by the private sector. Trust in cross-border transactions is also a big concern. To address this, international trustmark alliances have been established, such as the GTA and WTA, in which their members mutually agree to enact the same code of conduct.

The standard certification process is divided into five stages. First, setting the standards, TMOs must draft standards or criteria to start the certification process in TMOs practice. Second, the e-merchants will be audited; this can be done in three ways: (1) internal audit based on internal standards, (2) internal audit based on third-party standards, and (3) the most reliable method, an external audit. Third, when the result of evaluation is concluded, the certifier will issue or deny the certificate. Fourth, after the certificate has been issued, the monitoring stage begins. Passive monitoring starts when the certifier receives a complaint, with the certified company being examined under the certifier's programme. In the case of active monitoring, the certifier and the certified company will agree on a periodical check. The last stage is that if the certified company still meets the standard of the certifier, the certificate will be confirmed.

The key elements of a trusted certification practice which are accepted by many countries are certifier independency, impartiality in the auditing procedure, active monitoring of the certified company, certifier enforcement power and certifier accountability.

Fees are another key point, especially in relation to TMO independence. Every trustmark service provider requires an annual fee from e-merchants. US trustmarks such as McAfee require annual fee from the e-merchant if the e-merchant wants more options like a daily scan. This is similar to Norton which offer many trustmark packages for e-merchants. Making it free of charge may not be a good way to build trust if it is not enough fund to support a trustmark operation and monitoring. The reasonable fee is preferable.

5.2 Recommendations

5.2.1 The characteristics of trustmarks

Thai trustmarks are arranged by the government sector. However, it would be better to encourage self-regulation and a code of practice for entrepreneurs. The government sector should support and arrange for non-profit organizations or the private sector to administer e-commerce trustmarks in Thailand according to international principles such as the OECD guidelines. The DBD should take on the role of supervisor of trustmark principles.

5.2.2 Trustmark certification process

For DBD Registered, if the Department proposes this trustmark to be protected under the Trademark Act, then it should change its issuance procedure. The authorized use of DBD Registered should be done in writing and signed by the authorized persons of the Department.

In the pre-certification phase of DBD Verified, the standard of certification should be set up by a specialist association and follow international practices, i.e. Regulation (EU) No. 910/2014. In the post-certification phase, the certified applicant who has had their trustmark revoked should not have the right to re-apply for certification for five years. A blacklist of e-merchants that cannot be trusted should be published.

5.2.3 The legal relationship with and liability of trustmark service Providers

It is unclear whether the DBD as a government body should be liable to e-consumers who rely on such trustmarks. There has been no specific law or reported legal cases about the liability of trustmark service provider. Regardless whether DBD Registered and DBD Verified are registered as certificate marks under the Trademark Act B.E. 2534, no provisions in this Act state the liability of the certification mark owner to the consumer who relies on such a certification mark.

As I mentioned above, no specific law deals with whether an e-consumer can recover directly from a trustmark service provider based either on the general principles of tort or contract law or other related acts that may apply by analogy to TMOs. In most of the cases in the US and EU, e-consumers will have to prove:

- “a) the damage occurred to them;
- b) TMOs fault in the issuance of the trustmark; and
- c) the causal link between TMOs fault and the damage occurred”²⁰⁹

²⁰⁹ Paolo Balboni, *supra* note 15, at 192.

In my opinion, the DBD, as a trust service provider, should be liable to the e-consumers for damage caused intentionally or negligently if they fail to comply with their obligations. The relationship between the DBD and e-consumer should be based on tort liability. To calculate the damages, the e-consumer could claim for damage as estimated by the parties at the time the contract between e-merchant and e-consumer was formed.

Otherwise, an adequate liability system for TMOs should be based on the liability rules that apply to surveyors, accountants, and auditors which then will have to be adjusted to TMOs. This would:

- “1. effectively protect what e-consumers’ value and the related expectations That e-consumers put into their trust relationship with TMOs;
2. take into account the difficulties that TMOs face by operating in a context Of action such as the Internet; and
3. bring TMOs practice up to the quality level which will give trustmarks the opportunity to extend their potential benefits to social, economic, and political levels.”²¹⁰

5.2.4 The monitoring of trustmark receiver

There is only a passive monitoring in both provisions on the regulation of the use of DBD Registered and DBD Verified. A periodic evaluation should be established instead as a necessary step of monitoring, the same as is specified for McAfee and Norton. We cannot overlook that the fee is also a key factor in the monitoring process; many trustmark service providers request an annual fee from e-merchants and provide an effective active monitoring. Being free of charge may not be a good method to build trust in e-commerce. The Department should request a reasonable fee or some funding to support improved monitoring.

²¹⁰ Paolo Balboni, *supra* note 15, at 229.

5.2.5 Enforcement of laws specific to trustmarks

There is no enforcement of a specific law; both DBD trustmarks are registered as certificate marks under the Trademark Act B.E. 2534. As argued above, this is problematic as there have different characteristics. They should be legislated according to the principle under the Regulation (EU) No 910/2014, especially with regard to a qualified trust service provider's liability and burden of proof, trustmark issuance procedure, and monitoring process including setting up a supervisory body to control all aspects of trustmarks.



REFERENCES

1. Books

1.1 English Books

Craig Allen Nard, David W. Barnes and Michael J. Madison. *The Law of Intellectual Property*. New York: Aspen Publishers, Inc., 2006.

Deborah E. Bouchoux. *Intellectual Property: the Law of Trademarks, Copyrights, Patents, and Trade Secrets*. New York: West Legal Studies, 2000.

Jeremy Philips & Lianah Simon. *Trade Mark Use*. New York: Oxford University Press, 2005.

Kate McGrath, Stephen Elias and Sarah Shena. *Trademark: how to name your business and product*. California: Nolo Press, 1996.

Pacini, C. & Sinason, D., ‘Auditor Liability for Electronic Commerce Transaction Assurance: the CPA/CA WebTrust’, *American Business Law Journal* 36 (1999). (Referred in Paolo Balboni. *Trustmarks in E-commerce: the Value of Web Seals and the Liability of their Providers*. The Hague: T.M.C. Asser Press, 2009.)

Paolo Balboni. *Trustmarks in E-commerce: the Value of Web Seals and the Liability of their Providers*. The Hague: T.M.C. Asser Press, 2009.

Przemyslaw Paul Polanski. *Customary Law of the Internet: in the Search for a Supranational Cyberspace Law*. The Hugue: T.M.C. Asser Press, 2007.

Lewis, C.T. *A Latin Dictionary*. New York: Oxford University Press, 1996.

1.2 Thai Books

ชัยยศ เหมะรัชตะ, *ลักษณะของกฎหมายทรัพย์สินทางปัญญา*. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2550. (Chaiyot Hemaratchata. *the principle of intellectual property*. Bangkok: Nititham, 2007)

วัด ดิงสมิตร, *คำอธิบายกฎหมายเครื่องหมายการค้า*. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2545. (Wat Tingsaming. *the explanation of trademark law*. Bangkok: Nititham, 2002)

2. Book Articles

Sunni Yuen, “Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross –Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry.”, **9 Colum. Sci. & Tech. L. Rev.** 41 (2007-2008).

Thesis

Chernovich, Elena. Trust in E-commerce: the moral agency of trustmarks. Master Degree, Philosophy of science. technology and society. University of Twente, 2012. In Theses, http://essay.utwente.nl/63443/1/Chernovich,_Elena_-_S1042726_-_Master_Thesis.pdf (accessed November 10, 2014).

Kongkaew, Natapong. Legal Problems of Liability for Trustmark Usage for Trustmark provider DBD Verified of Department of Business Development Ministry of Commerce. Master Degree, Law of International Business and Electronic Transaction. Bangkok University, 2009. In ProQuest Dissertations, http://dspace.bu.ac.th/bitstream/123456789/903/1/natapong_kong.pdf.

Electronic Media

Christian Holst. “Which site seal do People Trust the most? (2013 Surveys Results)”, <http://baymard.com/blog/site-seal-trust>. (accessed August 25, 2015).

Council of Better Business Bureaus. “*Programs and Services.*” BBB. <http://www.bbb.org/council/the-national-partner-program/programs-and-services/?id=234761> (accessed November 21, 2014).

Department of Business Development, Ministry of Commerce. “*Criteria for Awarding of DBD Registered.*” DBD. <http://www.trustmarkthai.com/ecm/public/newsletter/view.html?id=383> (accessed October 23, 2014).

Department of Business Development, Ministry of Commerce. “*Frequently Asked Questions.*” Trustmarkthai. <http://www.trustmarkthai.com/ecm/content/faq001.pdf> (accessed November 23, 2014).

Department of Business Development, Ministry of Commerce. “*The Regulation of Use of DBD Registered.*” <http://www.trustmarkthai.com/ecm/forms/form010.pdf> (accessed November 30, 2014).

Department of Business Development, Ministry of Commerce. “*The Regulation of Use of DBD Verified.*” DBD. <http://www.trustmarkthai.com/ecm/forms/form015.pdf> (accessed November 30, 2014).

Department of Business Development, Ministry of Commerce. “*Issuance for E-commerce DBD Verified.*” DBD. <http://www.trustmarkthai.com/ecm/public/newsletter/view.html?id=382> (accessed October 23, 2014).

Department of Business Development, Ministry of Commerce. “*The procedure of issuance of DBD Registered.*” <https://drive.google.com/file/d/0B76yJeKddP3QNUJYMW1YLWViT2c/view> (accessed August 22, 2015).

European Consumer Centre Denmark. “*E-Commerce Trustmarks in Europe.*” <http://dokumenter.forbrug.dk/forbrugereuropa/e-commerce-trustmarks-in-europe/kap04.htm> (accessed August 22, 2015).

European Consumer Centres' Network. "*Trust marks report 2013, "Can I trust the trust mark?ECC-NET"*". http://ec.europa.eu/dgs/health_consumer/sources/docs/trust_mark_report_2013_en.pdf (accessed December 3, 2014).

European Multi-channel and Online Trade Association. "*EMOTA European Trustmark*". <http://www.emota.eu/#!european-trustmark-/c1f52> (accessed August 3, 2015).

European Multi-channel and Online Trade Association. "*EMOTA European Trustmark Accreditation Criteria for national trustmark providers*". http://media.wix.com/ugd/b18286_9e22f83c2d8d491cb6_c5261a61db509d.pdf. (accessed August 3, 2015).

European Payments Council. "*Next Step to Create the Digital Single Market: EU Lawmakers Adopt the New Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.*" European Payments Council. http://www.europeanpaymentscouncil.eu/pdf/EPC_Article_338.pdf (accessed November 23, 2014).

European Union. "*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July on electronic identification and trust services for electronic transactions in the internal market.*" EUR-Lex. http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (accessed November 23, 2014).

E-marketer. "*Global B2C Ecommerce Sales to hit \$1.5 Trillion this year driven by growth in emerging markets*", <http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575> (accessed July 10, 2015).

Federal Trade Commission. "TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program." FTC. <http://www.ftc.gov/newsevents/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its> (accessed November 20, 2014).

Fredriksson, Torbjorn. "*E-commerce and Development Key Trend and Issues.*" WTO. http://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/fredriksson_ecommer_e.pdf (accessed November 10, 2014).

Gilad L. Rosner. "*Trustmarks in the Identity Ecosystem.*" p. 3, <http://oixuk.org/wp-content/uploads/2014/09/Trustmarks-paper-FINAL-v2.pdf>. (accessed August 19, 2015).

Investorwords. "*E-commerce definition.*" Investorwords. http://www.investorwords.com/1637/e_commerce.html (accessed November 12, 2014).

ISO. "*Standards.*" <http://www.iso.org/iso/home/standards.htm> (accessed November 20, 2014).

IT Law Wiki. "*Global Trustmark Alliance.*" IT Law Wiki. http://itlaw.wikia.com/wiki/Global_Trustmark_Alliance (accessed November 20, 2014).

Justice court electronic library. "*Specific Supreme Court Decision – Section 80.*" p.1, http://www.library.coj.go.th/pongkun_68.php?idmain=102&&kotmaiyo=-&&mattra=80. (accessed August 23, 2015).

Linux Information Project. "*De Facto Standard Definition.*" Linux. http://www.linfo.org/de_facto_standard.html, (accessed November 10, 2014).

McAfee Secure. "*We help websites sell more*". <https://www.mcafeesecure.com/>. (accessed August 3, 2015).

- Matthew, K. O. Lee and Efraim Turban. “*International Journal of Electronic Commerce*.” JSTOR. <http://www.jstor.org/discover/10.2307/27751003?uid=3739136&uid=2129&uid=2&uid=70&uid=4&sid=21104612913751> (accessed November 12, 2014).
- Nannariello, Guido. “*E-commerce and consumer protection a survey of codes of practice and certification processes*.” EU Bookshop. <http://bookshop.europa.eu/en/e-commerce-and-consumer-protection-pbLBNA19932/> (accessed December 6, 2014).
- National Statistical Office. “*The 2013 Survey on the Internet Users’ Profile in Thailand*.” The National Statistical Office. https://www.eta.or.th/internetuserprofile2013/Executive_Summary_IUP.pdf, (accessed November 10, 2014).
- National Statistical Office. “*The 2014 Household Survey on the Use of Information and Communication Technology*”. <http://service.nso.go.th/nso/nsopublish/service/survey/ICTFull57-1.pdf>, (accessed August 19, 2015).
- Organisation for Economic Co-operation and Development (OECD). “*Measuring the Information Economy 2002*.” OECD. <http://www.oecd.org/internet/ieconomy/2771174.pdf> (accessed November 10, 2014).
- Organisation for Economic Co-operation and Development (OECD). “*First Report: Government and Private Sector Initiatives to Promote and Implement the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*.” OECD. [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=DSTI/CP\(2000\)7/FINAL](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=DSTI/CP(2000)7/FINAL) (accessed May 17, 2016).
- SANS Institute Reading Room site. “*Comparison of Three Online Privacy Seal Programs*”. p.5, <https://www.sans.org/reading-room/whitepapers/privacy/comparison-online-privacy-seal-programs-685>. (accessed September 1, 2015).

Symantec. “*Compare SSL Certificates.*” <https://www.symantec.com/ssl-certificates/> (accessed August 3, 2015).

Top Alternatives. “*Top 3 trust seals/certificates to display on your website*”. <https://topalternatives.com/display-trust-seals-certificates-on-your-website/> (accessed August 8, 2015).

TRUSTe. “*TRUSTe Data Privacy Management Solution.*” TRUSTe. <http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=9GEA1GX6-488> (accessed November 20, 2014).

Vangie Beal. “*An E-Comm Buyers’ Guide to Choosing Trustmarks*”. <http://www.ecommerce-guide.com/article.php/3860526/An-EComm-Buyers-Guide-to-Choosing-Trustmarks.htm> (accessed August 3, 2015).

Wagemans, Ton. “*An Introduction to the labelling of websites*”. background paper for DG Information Society Conference “Quality Labels for Websites Alternative Approaches to Content Rating”, 27 February 2003, Luxembourg, http://www.europa.eu.int/information_society/activities/sip/docs/pdf/reports/qual_lab_bkgd.pdf.

Webtrust. “*Trust Services Principles, Criteria, and Illustrations.*” Webtrust. <http://www.webtrust.org/principles-and-criteria/item27818.pdf> (accessed November 20, 2014).

World Trustmark Alliance. “*About us.*” WTA. <http://www.wtaportal.org/aboutus.html> (accessed November 20, 2014).

World Trustmark Alliance. “*Code of Conduct.*” WTA. <http://www.wtaportal.org/code.html> (accessed November 20, 2014).



APPENDICES

APPENDIX A
OECD GUIDELINES FOR CONSUMER PROTECTION IN THE
CONTEXT OF ELECTRONIC COMMERCE (1999)

GUIDELINES

PART ONE

SCOPE

These Guidelines apply only to business-to-consumer electronic commerce and not to business-to-business transactions.

PART TWO

GENERAL PRINCIPLES

I. TRANSPARENT AND EFFECTIVE PROTECTION

Consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.

Governments, businesses, consumers and their representatives should work together to achieve such protection and determine what changes may be necessary to address the special circumstances of electronic commerce.

II. FAIR BUSINESS, ADVERTISING AND MARKETING PRACTICES

Businesses engaged in electronic commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices.

Businesses should not make any representation, or omission, or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair.

Businesses selling, promoting or marketing goods or services to consumers should not engage in practices that are likely to cause unreasonable risk of harm to consumers.

Whenever businesses make information available about themselves or the goods or services they provide, they should present such information in a clear, conspicuous, accurate and easily accessible manner.

Businesses should comply with any representations they make regarding policies or practices relating to their transactions with consumers.

Businesses should take into account the global nature of electronic commerce and, wherever possible, should consider the various regulatory characteristics of the markets they target.

Businesses should not exploit the special characteristics of electronic commerce to hide their true identity or location, or to avoid compliance with consumer protection standards and/or enforcement mechanisms.

Businesses should not use unfair contract terms.

Advertising and marketing should be clearly identifiable as such.

Advertising and marketing should identify the business on whose behalf the marketing or advertising is being conducted where failure to do so would be deceptive.

Businesses should be able to substantiate any express or implied representations as long as the representations are maintained, and for a reasonable time thereafter.

Businesses should develop and implement effective and easy-to-use procedures that allow consumers to choose whether or not they wish to receive unsolicited commercial e-mail messages.

Where consumers have indicated that they do not want to receive unsolicited commercial e-mail messages, such choice should be respected.

In a number of countries, unsolicited commercial e-mail is subject to specific legal or self-regulatory requirements.

Businesses should take special care in advertising or marketing that is targeted to children, the elderly, the seriously ill, and others who may not have the capacity to fully understand the information with which they are presented.

III. ONLINE DISCLOSURES

A. INFORMATION ABOUT THE BUSINESS

Businesses engaged in electronic commerce with consumers should provide accurate, clear and easily accessible information about themselves sufficient to allow, at a minimum:

- i) Identification of the business – including the legal name of the business and the name under which the business trades; the principal geographic address for the business; e-mail address or other electronic means of contact, or telephone number; and, where applicable, an address for registration purposes and any relevant government registration or licence numbers.
- ii) Prompt, easy and effective consumer communication with the business.
- iii) Appropriate and effective resolution of disputes.
- iv) Service of legal process.
- v) Location of the business and its principals by law enforcement and regulatory officials.

Where a business publicises its membership in any relevant self-regulatory scheme, business association, dispute resolution organisation or other certification body, the business should provide consumers with appropriate contact details and an easy method of verifying that membership and of accessing the relevant codes and practices of the certification body.

B. INFORMATION ABOUT THE GOODS OR SERVICES

Businesses engaged in electronic commerce with consumers should provide accurate and easily accessible information describing the goods or services offered; sufficient to enable consumers to make an informed decision about whether to enter into the transaction and in a manner that makes it possible for consumers to maintain an adequate record of such information.

C. INFORMATION ABOUT THE TRANSACTION

Businesses engaged in electronic commerce should provide sufficient information about the terms, conditions and costs associated with a transaction to enable consumers to make an informed decision about whether to enter into the transaction.

Such information should be clear, accurate, easily accessible, and provided in a manner that gives consumers an adequate opportunity for review before entering into the transaction.

Where more than one language is available to conduct a transaction, businesses should make available in those same languages all information necessary for consumers to make an informed decision about the transaction.

Businesses should provide consumers with a clear and full text of the relevant terms and conditions of the transaction in a manner that makes it possible for consumers to access and maintain an adequate record of such information.

Where applicable and appropriate given the transaction, such information should include the following:

- i) An itemisation of total costs collected and/or imposed by the business.
- ii) Notice of the existence of other routinely applicable costs to the consumer that are not collected and/or imposed by the business.
- iii) Terms of delivery or performance.
- iv) Terms, conditions and methods of payment.

- v) Restrictions, limitations or conditions of purchase, such as parental/guardian approval requirements, geographic or time restrictions.
- vi) Instructions for proper use including safety and health-care warnings.
- vii) Information relating to available after-sales service.
- viii) Details of and conditions related to withdrawal, termination, return, exchange, cancellation and/or refund policy information.
- ix) Available warranties and guarantees.

All information that refers to costs should indicate the applicable currency.

IV. CONFIRMATION PROCESS

To avoid ambiguity concerning the consumer's intent to make a purchase, the consumer should be able, before concluding the purchase, to identify precisely the goods or services he or she wishes to purchase; identify and correct any errors or modify the order; express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.

The consumer should be able to cancel the transaction before concluding the purchase.

V. PAYMENT

Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.

Limitations of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce.

VI. DISPUTE RESOLUTION AND REDRESS

A. APPLICABLE LAW AND JURISDICTION

Business-to-consumer cross-border transactions, whether carried out electronically or otherwise, are subject to the existing framework on applicable law and jurisdiction.

Electronic commerce poses challenges to this existing framework. Therefore, consideration should be given to whether the existing framework for applicable law and jurisdiction should be modified, or applied differently, to ensure effective and transparent consumer protection in the context of the continued growth of electronic commerce.

In considering whether to modify the existing framework, governments should seek to ensure that the framework provides fairness to consumers and businesses, facilitates electronic commerce, results in consumers having a level of protection not less than that afforded in other forms of commerce, and provides consumers with meaningful access to fair and timely dispute resolution and redress without undue cost or burden.

B. ALTERNATIVE DISPUTE RESOLUTION AND REDRESS

Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.

Businesses, consumer representatives and governments should work together to continue to use and develop fair, effective and transparent self-regulatory and other policies and procedures, including alternative dispute resolution mechanisms, to address consumer complaints and to resolve consumer disputes arising from business-to-consumer electronic commerce, with special attention to cross-border transactions:

- i)* Businesses and consumer representatives should continue to establish fair, effective and transparent internal mechanisms to address and respond to consumer complaints and difficulties in a fair and timely manner and without undue cost or burden to the consumer. Consumers should be encouraged to take advantage of such mechanisms.
- ii)* Businesses and consumer representatives should continue to establish co-operative self-regulatory programmes to address consumer

complaints and to assist consumers in resolving disputes arising from business-to-consumer electronic commerce.

- iii) Businesses, consumer representatives and governments should work together to continue to provide consumers with the option of alternative dispute resolution mechanisms that provide effective resolution of the dispute in a fair and timely manner and without undue cost or burden to the consumer.
- iv) In implementing the above, businesses, consumer representatives and governments should employ information technologies innovatively and use them to enhance consumer awareness and freedom of choice.

In addition, further study is required to meet the objectives of Section VI at an international level.

VII. PRIVACY

Business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998), to provide appropriate and effective protection for consumers.

VIII. EDUCATION AND AWARENESS

Governments, businesses and consumer representatives should work together to educate consumers about electronic commerce, to foster informed decision making by consumers participating in electronic commerce, and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

Governments, business, the media, educational institutions and consumer representatives should make use of all effective means to educate consumers and businesses, including innovative techniques made possible by global networks.

Governments, consumer representatives and businesses should work together to provide information to consumers and businesses globally about relevant consumer protection laws and remedies in an easily accessible and understandable form.

PART THREE

IMPLEMENTATION

To achieve the purpose of this Recommendation, Member countries should at the national and international level, and in co-operation with businesses, consumers and their representatives:

- i) Review and, if necessary, promote self-regulatory practices and/or adopt and adapt laws and practices to make such laws and practices applicable to electronic commerce, having in mind the principles of technology and media neutrality.*
- ii) Encourage continued private sector leadership that includes the participation of consumer representatives in the development of effective self-regulatory mechanisms that contain specific, substantive rules for dispute resolution and compliance mechanisms.*
- iii) Encourage continued private sector leadership in the development of technology as a tool to protect and empower consumers.*
- iv) Promote the existence, purpose and contents of the Guidelines as widely as possible and encourage their use.*
- v) Facilitate consumers' ability to both access consumer education information and advice and to file complaints related to electronic commerce.*

PART FOUR
GLOBAL CO-OPERATION

In order to provide effective consumer protection in the context of global electronic commerce, Member countries should:

- i) Facilitate communication, co-operation, and, where appropriate, the development and enforcement of joint initiatives at the international level among businesses, consumer representatives and governments.*
- ii) Through their judicial, regulatory and law enforcement authorities co-operate at the international level, as appropriate, through information exchange, co-ordination, communication and joint action to combat cross-border fraudulent, misleading and unfair commercial conduct.*
- iii) Make use of existing international networks and enter into bilateral and/or multilateral agreements or other arrangements as necessary and appropriate, to accomplish such co-operation.*
- iv) Work toward building consensus, both at the national and international levels, on core consumer protections to further the goals of enhancing consumer confidence, ensuring predictability for businesses, and protecting consumers.*
- v) Co-operate and work towards developing agreements or other arrangements for the mutual recognition and enforcement of judgements resulting from disputes between consumers and businesses, and judgements resulting from law enforcement actions taken to combat fraudulent, misleading or unfair commercial conduct.*

APPENDIX B
REGULATION (EU) No 910/2014 OF THE EUROPEAN
PARLIAMENT AND OF THE COUNCIL

28.8.2014

EN

Official Journal of the European Union

L 257/73

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND
OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the
internal market and repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Acting in accordance with the ordinary legislative procedure ⁽²⁾,

Whereas:

- (1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.
- (2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.
- (3) Directive 1999/93/EC of the European Parliament and of the Council ⁽³⁾, dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive.
- (4) The Commission communication of 26 August 2010 entitled ‘A Digital Agenda for Europe’ identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled ‘Dismantling the obstacles to EU citizens’ rights’, the Commission further highlighted the need to

- solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.
- (5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.
 - (6) In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.
 - (7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce [\(4\)](#), stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.
 - (8) Directive 2006/123/EC of the European Parliament and of the Council [\(5\)](#) requires Member States to establish 'points of single contact' (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.
 - (9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.
 - (10) Directive 2011/24/EU of the European Parliament and of the Council [\(6\)](#) set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.

- (11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council [\(7\)](#). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.
- (12) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.
- (13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.
- (14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the *Official Journal of the European Union*. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.
- (15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.
- (16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which

that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurance levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.

- (17) Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.
- (18) This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.
- (19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be

discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.

- (20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.
- (21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.
- (22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.
- (23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.
- (24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.
- (25) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.
- (26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.

- (27) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.
- (28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.
- (29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC ⁽⁸⁾, in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.
- (30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.
- (31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.
- (32) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.
- (33) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.
- (34) All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.
- (35) All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

- (36) Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market. Non-qualified trust service providers should be subject to a light touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.
- (37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.
- (38) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.
- (39) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).
- (40) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.
- (41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

- (42) To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.
- (43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.
- (44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council [\(9\)](#) which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.
- (45) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.
- (46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.
- (47) Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.
- (48) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC [\(10\)](#), electronic signatures with a lower security assurance should also be accepted.

- (49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.
- (50) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.
- (51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.
- (52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.
- (53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.
- (54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in

qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

- (55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.
- (56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.
- (57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.
- (58) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.
- (59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.
- (60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.
- (61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over

extended periods of time and guarantee that they can be validated irrespective of future technological changes.

- (62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.
- (63) Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.
- (64) When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU [\(11\)](#).
- (65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.
- (66) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.
- (67) Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

- (68)The concept of ‘legal persons’, according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, ‘legal persons’, within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.
- (69)The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.
- (70)In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.
- (71)In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council [\(12\)](#).
- (72)When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.
- (73)For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.
- (74)To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

(75)The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.

(76)Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(77)The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council [\(13\)](#) and delivered an opinion on 27 September 2012 [\(14\)](#),

HAVE ADOPTED THIS REGULATION:

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

- (a)lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- (b)lays down rules for trust services, in particular for electronic transactions; and
- (c)establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.
2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.
3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

- (1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- (2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- (3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- (4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
- (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- (6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;
- (7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- (8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council [\(15\)](#);
- (9) 'signatory' means a natural person who creates an electronic signature;
- (10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- (11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
- (12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
- (13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;
- (14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

- (15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
- (16) 'trust service' means an electronic service normally provided for remuneration which consists of:
- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
 - (b) the creation, verification and validation of certificates for website authentication; or
 - (c) the preservation of electronic signatures, seals or certificates related to those services;
- (17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;
- (18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
- (19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
- (20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
- (21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
- (22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
- (23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;
- (24) 'creator of a seal' means a legal person who creates an electronic seal;
- (25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- (26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;
- (27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
- (28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;

- (29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
- (30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;
- (31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;
- (32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;
- (33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- (34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;
- (35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
- (36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- (37) 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;
- (38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- (39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
- (40) 'validation data' means data that is used to validate an electronic signature or an electronic seal;
- (41) 'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

Article 4

Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

Article 5

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.
2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

CHAPTER II ELECTRONIC IDENTIFICATION

Article 6

Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:
 - (a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;
 - (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
 - (c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

Article 7

Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

- (a) the electronic identification means under the electronic identification scheme are issued:
 - (i) by the notifying Member State;
 - (ii) under a mandate from the notifying Member State; or
 - (iii) independently of the notifying Member State and are recognised by that Member State;
- (b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;
- (c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);
- (d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;
- (e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);
- (f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

- (g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);
- (h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

*Article 8***Assurance levels of electronic identification schemes**

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.
2. The assurance levels low, substantial and high shall meet respectively the following criteria:
 - (a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
 - (b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
 - (c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.
3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

- (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;
- (b) the procedure for the issuance of the requested electronic identification means;
- (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;
- (d) the entity issuing the electronic identification means;
- (e) any other body involved in the application for the issuance of the electronic identification means; and
- (f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 9

Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

- (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;
- (b) the applicable supervisory regime and information on the liability regime with respect to the following:
 - (i) the party issuing the electronic identification means; and
 - (ii) the party operating the authentication procedure;
- (c) the authority or authorities responsible for the electronic identification scheme;
- (d) information on the entity or entities which manage the registration of the unique person identification data;
- (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;
- (f) a description of the authentication referred to in point (f) of Article 7;
- (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10

Security breach

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.
2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.
3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11

Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.
2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.
3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.
4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.
5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 12

Cooperation and interoperability

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.
2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:
 - (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;
 - (b) it follows European and international standards, where possible;
 - (c) it facilitates the implementation of the principle of privacy by design; and
 - (d) it ensures that personal data is processed in accordance with Directive 95/46/EC.
4. The interoperability framework shall consist of:
 - (a) a reference to minimum technical requirements related to the assurance levels under Article 8;
 - (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
 - (c) a reference to minimum technical requirements for interoperability;
 - (d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
 - (e) rules of procedure;
 - (f) arrangements for dispute resolution; and
 - (g) common operational security standards.
5. Member States shall cooperate with regard to the following:
 - (a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and
 - (b) the security of the electronic identification schemes.
6. The cooperation between Member States shall consist of:
 - (a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;
 - (b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;
 - (c) peer review of electronic identification schemes falling under this Regulation; and
 - (d) examination of relevant developments in the electronic identification sector.
7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.
8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation

between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER III TRUST SERVICES

SECTION 1 General provisions

Article 13

Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

2. Agreements referred to in paragraph 1 shall ensure, in particular, that:

(a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service

providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;

- (b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Article 16

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

SECTION 2

Supervision

Article 17

Supervisory body

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State.

Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

3. The role of the supervisory body shall be the following:

(a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

(b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:
- (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;
 - (b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);
 - (c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);
 - (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;
 - (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);
 - (f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;
 - (g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;
 - (h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;
 - (i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);
 - (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.
5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.
6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).
7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.
8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 18

Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchanging good practice.
- A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can

be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:

- (a) the supervisory body is not competent to provide the requested assistance;
- (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;
- (c) providing the requested assistance would be incompatible with this Regulation.

3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

Article 19

Security requirements applicable to trust service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts,:

(a) further specify the measures referred to in paragraph 1; and

(b) define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

(a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b)auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 21

Initiation of a qualified trust service

1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 22

Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.
4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.
5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 23

EU trust mark for qualified trust services

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.
2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.
3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24

Requirements for qualified trust service providers

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

- (a) by the physical presence of the natural person or of an authorised representative of the legal person; or
- (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised

- representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’; or
- (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
 - (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.
2. A qualified trust service provider providing qualified trust services shall:
- (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
 - (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;
 - (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;
 - (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;
 - (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;
 - (f) use trustworthy systems to store data provided to it, in a verifiable form so that:
 - (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
 - (ii) only authorised persons can make entries and changes to the stored data,
 - (iii) the data can be checked for authenticity;
 - (g) take appropriate measures against forgery and theft of data;
 - (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;
 - (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);
 - (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;
 - (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.
4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.
5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

*Article 27***Electronic signatures in public services**

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.
4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).
5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 28***Qualified certificates for electronic signatures**

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.
2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.
3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.
4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

- (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;
 - (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.
2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.
3. The certification referred to in paragraph 1 shall be based on one of the following:
 - (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or
 - (b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32

Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the electronic signature was created by a qualified electronic signature creation device;

(g) the integrity of the signed data has not been compromised;

(h) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 33

Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

- (a) provides validation in compliance with Article 32(1); and
- (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 34

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 5

Electronic seals

Article 35

Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36

Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

- (a) it is uniquely linked to the creator of the seal;
- (b) it is capable of identifying the creator of the seal;
- (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

Article 37

Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.
4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).
5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define

reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38

Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.
2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:
 - (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;
 - (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.
3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

*Article 40***Validation and preservation of qualified electronic seals**

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

SECTION 6***Electronic time stamps****Article 41***Legal effect of electronic time stamps**

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

*Article 42***Requirements for qualified electronic time stamps**

1. A qualified electronic time stamp shall meet the following requirements:
 - (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
 - (b) it is based on an accurate time source linked to Coordinated Universal Time; and
 - (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7***Electronic registered delivery services****Article 43***Legal effect of an electronic registered delivery service**

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44

Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:
 - (a) they are provided by one or more qualified trust service provider(s);
 - (b) they ensure with a high level of confidence the identification of the sender;
 - (c) they ensure the identification of the addressee before the delivery of the data;
 - (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
 - (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
 - (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 8

Website authentication

Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER IV ELECTRONIC DOCUMENTS

Article 46

Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER V DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.
3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 48

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VI FINAL PROVISIONS

Article 49

Review

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

Article 50

Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.
2. References to the repealed Directive shall be construed as references to this Regulation.

Article 51

Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.
2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.
3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory

body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.

4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

Article 52

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from 1 July 2016, except for the following:

(a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;

(b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);

(c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).

3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 23 July 2014.

For the Parliament

The President

M. SCHULZ

For the Council

The President

S. GOZI

(¹) [OJ C 351, 15.11.2012, p. 73.](#)

(²) Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of 23 July 2014.

(³) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ([OJ L 13, 19.1.2000, p. 12](#)).

(⁴) [OJ C 50 E, 21.2.2012, p. 1.](#)

(⁵) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market ([OJ L 376, 27.12.2006, p. 36](#)).

(⁶) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare ([OJ L 88, 4.4.2011, p. 45](#)).

(⁷) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([OJ L 281, 23.11.1995, p. 31](#)).

(⁸) Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities ([OJ L 23, 27.1.2010, p. 35](#)).

(⁹) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 ([OJ L 218, 13.8.2008, p. 30](#)).

(¹⁰) Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market ([OJ L 274, 20.10.2009, p. 36](#)).

(¹¹) Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market ([OJ L 53, 26.2.2011, p. 66](#)).

(¹²) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers ([OJ L 55, 28.2.2011, p. 13](#)).

(¹³) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ([OJ L 8, 12.1.2001, p. 1](#)).

(¹⁴) [OJ C 28, 30.1.2013, p. 6.](#)

(¹⁵) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC ([OJ L 94, 28.3.2014, p. 65](#)).

ANNEX I

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,

- for a natural person: the person's name;
- (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
- (d) electronic signature validation data that corresponds to the electronic signature creation data;
- (e) details of the beginning and end of the certificate's period of validity;
- (f) the certificate identity code, which must be unique for the qualified trust service provider;
- (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
- (i) the location of the services that can be used to enquire about the validity status of the qualified certificate;
- (j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
 - (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
 - (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
 - (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
 - (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
- (a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

ANNEX III

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
- (c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;
- (d) electronic seal validation data, which corresponds to the electronic seal creation data;
- (e) details of the beginning and end of the certificate's period of validity;
- (f) the certificate identity code, which must be unique for the qualified trust service provider;
- (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
- (i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;
- (j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX IV**REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION**

Qualified certificates for website authentication shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;
 - (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
 - (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;
for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;
 - (d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
 - (e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;
 - (f) details of the beginning and end of the certificate's period of validity;
 - (g) the certificate identity code, which must be unique for the qualified trust service provider;
 - (h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
 - (i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;
 - (j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.
-

APPENDIX C

REGULATION OF USING “DBD REGISTERED”

ข้อบังคับ
ว่าด้วยการใช้เครื่องหมายรับรองการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์
“DBD Registered”
ของ กรมพัฒนาธุรกิจการค้า
พ.ศ. ๒๕๕๘

ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์นี้จัดทำขึ้นตามบทบัญญัติมาตรา ๘๒ แห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

หมวด ๑

บททั่วไป

ข้อ ๑ ข้อบังคับนี้ให้ใช้บังคับตั้งแต่วันที่ยื่นคำขอจดทะเบียนเป็นต้นไป

ข้อ ๒ ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์นี้ ถือเป็นส่วนหนึ่งของคำขอจดทะเบียนเครื่องหมายรับรองตามพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

ข้อ ๓ ข้อบังคับนี้หากมิได้กำหนดไว้เป็นอย่างอื่นให้นำบทบัญญัติแห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔ มาใช้บังคับ

ข้อ ๔ ในข้อบังคับนี้

“เครื่องหมายรับรอง” หมายถึง เครื่องหมายที่กรมพัฒนาธุรกิจการค้ากำหนดขึ้นท้ายข้อบังคับนี้เพื่อรับรองว่าเป็นผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ที่ได้จดทะเบียนพาณิชย์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์

“ผู้ประกอบการธุรกิจ” หมายถึง ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์

“การประกอบการพาณิชย์อิเล็กทรอนิกส์” หมายถึง การประกอบการดังต่อไปนี้

- (๑) การซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๒) การบริการอินเทอร์เน็ต
- (๓) การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย
- (๔) การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

(๕) การทำธุรกรรมโดยวิธีใช้สื่ออิเล็กทรอนิกส์อื่น ตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด

“กรม” หมายถึง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

หมวด ๒

เงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง

ข้อ ๕ ผู้ประกอบธุรกิจที่ประสงค์จะขอใช้เครื่องหมายรับรองต้องจดทะเบียนพาณิชย์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์

ข้อ ๖ ผู้ประกอบธุรกิจที่ได้รับเครื่องหมายรับรองตลอดระยะเวลาที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์

ข้อ ๗ ผู้ประกอบธุรกิจที่ได้รับเครื่องหมายรับรองต้องยินยอม อำนวยความสะดวก และให้ข้อมูลแก่เจ้าหน้าที่ของกรมพัฒนาธุรกิจการค้าเข้าตรวจสอบกำกับดูแลการใช้เครื่องหมายรับรองตามข้อบังคับนี้

หมวด ๓

การเพิกถอนการใช้เครื่องหมายรับรอง

ข้อ ๘ กรมพัฒนาธุรกิจการค้ามีอำนาจเพิกถอนการใช้เครื่องหมายรับรอง กรณีใดกรณีหนึ่งดังต่อไปนี้

(๑) จดทะเบียนเลิกประกอบพาณิชย์กึ่งประเภทพาณิชย์อิเล็กทรอนิกส์

(๒) ถูกถอนใบทะเบียนพาณิชย์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์

(๓) มีพฤติกรรมในการประกอบธุรกิจที่ขัดต่อกฎหมาย หรือความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน หรือความมั่นคงของประเทศ หรือไม่เป็นธรรมต่อผู้บริโภค

(๔) นำเครื่องหมายรับรองไปใช้ในลักษณะที่ผิดวัตถุประสงค์ของการประกอบธุรกิจอันอาจก่อให้เกิดความเสียหายกับกรมซึ่งเป็นเจ้าของเครื่องหมายรับรอง

(๕) ไม่ยินยอม หรือไม่อำนวยความสะดวก หรือไม่ให้ข้อมูลแก่เจ้าหน้าที่ของกรมตาม ข้อ ๗

ข้อ ๙ ผู้ถูกเพิกถอนการใช้เครื่องหมายรับรอง ต้องเลิกใช้เครื่องหมายรับรองในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ทันที

ในกรณีผู้ถูกเพิกถอนการใช้เครื่องหมายรับรองใดฝ่าฝืนใช้เครื่องหมายรับรองต้องรับผิดชอบใช้ค่าเสียหายให้กรมพัฒนาธุรกิจการค้าในอัตราวันละห้าพันบาทจนกว่าจะเลิกใช้

บทเฉพาะกาล

ข้อ ๑๐ ภายหลังจากข้อบังคับนี้มีผลใช้บังคับ ให้ผู้ประกอบธุรกิจที่ได้รับเครื่องหมายรับรองสามารถใช้ข้อบังคับฉบับเดิมได้อยู่ต่อไปจนกว่าจะมีการเลิกใช้เครื่องหมายรับรองหรือถูกเพิกถอนการใช้เครื่องหมายรับรองแล้วแต่กรณี

เครื่องหมายรับรอง

การจดทะเบียนพาณิชย์อิเล็กทรอนิกส์



APPENDIX D

REGULATION OF USING “DBD VERIFIED SILVER”

ข้อบังคับ

ว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดี “DBD Verified Silver”
ของ กรมพัฒนาธุรกิจการค้า

ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดี “DBD Verified Silver” นี้ จัดทำขึ้นตามบทบัญญัติมาตรา ๘๒ แห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

หมวด ๑

บททั่วไป

ข้อ ๑ ข้อบังคับนี้ให้ใช้บังคับตั้งแต่วันที่ยื่นคำขอจดทะเบียนเป็นต้นไป

ข้อ ๒ ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์นี้ ถือเป็นส่วนหนึ่งของคำขอจดทะเบียนเครื่องหมายรับรองตามพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

ข้อ ๓ ข้อบังคับนี้หากมิได้กำหนดไว้เป็นอย่างอื่น ให้มีบทบัญญัติแห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔ มาใช้บังคับ

ข้อ ๔ ในข้อบังคับนี้

“เครื่องหมายรับรอง” หมายถึง เครื่องหมายที่กรมพัฒนาธุรกิจการค้ากำหนดขึ้นท้ายข้อบังคับนี้ เพื่อรับรองความน่าเชื่อถือของการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดี “DBD Verified Silver” ของผู้ประกอบการ

“ผู้ประกอบการ” หมายถึง ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์

“การประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์” หมายถึง การประกอบธุรกิจ ดังต่อไปนี้

- (๑) การซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๒) การบริการอินเทอร์เน็ต
- (๓) การให้เข้าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย
- (๔) การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๕) การทำธุรกรรมโดยวิธีการใช้สื่ออิเล็กทรอนิกส์อื่น ตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด

“กรม” หมายถึง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

“เกณฑ์คุณภาพมาตรฐานธุรกิจ” หมายถึง ข้อกำหนดเกี่ยวกับคุณภาพและมาตรฐานการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ที่กรมกำหนด

“หน่วยตรวจประเมิน” หมายถึง ผู้ตรวจประเมินหรือคณะผู้ตรวจประเมินที่กรมมอบหมายให้ทำการตรวจประเมินเว็บไซต์และการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ ที่ขอใช้เครื่องหมายรับรอง และตรวจประเมินการประกอบธุรกิจในระหว่างที่ได้รับหนังสืออนุญาต

“หนังสืออนุญาต” หมายถึง หนังสืออนุญาตให้ใช้เครื่องหมายรับรอง

“ระบบตะกร้าสินค้า” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นเสมือนตะกร้าหรือรถเข็นสินค้าที่ลูกค้าใช้ระหว่างการเลือกสินค้าบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ ของสินค้า เช่น รหัสสินค้า ราคา จำนวนสินค้า และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบการจอง” หมายถึง ระบบการสั่งซื้อสินค้าประเภทงานบริการที่เป็นแบบฟอร์มให้ลูกค้าสามารถจองงานบริการบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของงานบริการเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบใบเสนอราคา” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นแบบฟอร์มให้ลูกค้าสามารถขอใบเสนอราคาบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น หรือสามารถ Print ใบเสนอราคาให้กับลูกค้าได้

หมวด ๒

หลักเกณฑ์ วิธีการ และเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง

ข้อ ๕ ผู้ประกอบธุรกิจที่ประสงค์จะขอใช้เครื่องหมายรับรอง ต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(๑) เป็นบุคคลธรรมดา หรือ ห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือ บริษัทมหาชนจำกัดที่ไม่เข้าข่ายเป็นคนต่างด้าวตามกฎหมาย ว่าด้วยการประกอบธุรกิจของคนต่างด้าว

(๒) จดทะเบียนพาณิชย์ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์ และได้รับเครื่องหมายรับรองการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์ของกรม

(๓) เป็นเจ้าของโดเมนเนม

(๔) มีระบบการสั่งซื้อ อย่างน้อย ระบบตะกร้าสินค้า หรือ ระบบการจอง หรือ ระบบใบเสนอราคา หรือ ระบบแบบฟอร์มสั่งซื้อสินค้าหรือบริการ

(๕) มีช่องทางการชำระเงิน อย่างน้อย โอนเงินผ่านธนาคาร หรือ เก็บเงินปลายทาง หรือ ผ่านตัวกลางทางการเงิน หรือ อิเล็กทรอนิกส์ แบงก์กิ้ง หรือ แคนเตอร์เซอร์วิส หรือ ผ่านบัตรเครดิต หรือ บัตรเดบิต

(๖) มีช่องทางการจัดส่ง

(๖.๑) ประเภทสินค้า เช่น ไปรษณีย์ บริษัทขนส่งเอกชน พนักงานส่งสินค้า

(๖.๒) ประเภทบริการ เช่น Download จัดส่งทางอีเมล

(๗) ปฏิบัติถูกต้องตามกฎหมายและไม่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

(๘) สินค้าหรือบริการ จะต้องเป็นไปตามประเภทธุรกิจของพาณิชย์กิจที่ได้จดทะเบียนพาณิชย์อิเล็กทรอนิกส์ และไม่ขัดต่อกฎหมายอื่นที่เกี่ยวข้อง

(๙) สินค้าหรือบริการที่อาจส่งผลกระทบต่อเด็กหรือเยาวชน จะต้องจัดให้มีข้อความเตือนบนเว็บไซต์ เพื่อให้ควบคุมครองสิทธิแก่เด็กและเยาวชน

(๑๐) ไม่เคยถูกเพิกถอนการใช้เครื่องหมายรับรอง เว้นแต่พ้นจากการเพิกถอนมาแล้วไม่น้อยกว่า ๕ ปีก่อนวันยื่นคำขออนุญาต

ข้อ ๖ ผู้ประกอบธุรกิจที่ประสงค์จะใช้เครื่องหมายรับรอง ต้องปฏิบัติตามหลักเกณฑ์ วิธีการและเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง โดยให้ยื่นคำขออนุญาตต่อกรมตามวิธีการที่กรมกำหนด

ข้อ ๗ ผู้ที่จะได้รับอนุญาตให้ใช้เครื่องหมายรับรองต้องผ่านการตรวจสอบว่าได้ประกอบธุรกิจตามหลักเกณฑ์ดังต่อไปนี้

(๑) ต้องเปิดเผยข้อมูลธุรกิจและรายละเอียดที่เกี่ยวข้องกับสินค้าหรือบริการ ได้แก่ ข้อมูลเกี่ยวกับชื่อชื่อทางการค้า (ถ้ามี) ชื่อเว็บไซต์ เลขทะเบียนพาณิชย์ ที่ตั้งสถานประกอบการหรือที่ตั้งของตัวแทนหรือบุคคลที่สามารถติดต่อได้ วิธีการติดต่อ หมายเลขโทรศัพท์ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) และเวลาทำการด้วยความถูกต้องชัดเจน และเข้าถึงได้ง่าย

(๒) การเสนอชื่อหรือขายสินค้าหรือบริการ ต้องมีรูปแบบที่เหมาะสมไม่ขัดต่อบทบัญญัติแห่งกฎหมายหรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ต้องแสดงรายละเอียดข้อมูลสินค้าหรือบริการ โดยพิจารณาจากสภาพการซื้อขายและลักษณะของสินค้าหรือบริการ ต้องระบุราคาให้ชัดเจน และกรณีที่มีค่าใช้จ่ายอื่นเพิ่มเติม เช่น ภาษี ค่าระวางบรรทุกสินค้า ค่าบริการจัดส่ง ให้ระบุไว้ด้วย รวมทั้ง ต้องแสดงรายละเอียดการซื้อหรือขายสินค้าหรือบริการ เพื่อให้ผู้สั่งซื้อหรือขายสินค้าหรือบริการ นำไปใช้ประกอบการตัดสินใจทำธุรกรรมเกี่ยวกับสินค้าหรือบริการนั้น ได้แก่

(๒.๑) สินค้าหรือบริการ และค่าบริการจัดส่ง ตลอดจนเงื่อนไขวิธีการสั่งซื้อหรือขายและตอบรับ หรือข้อมูลที่จำเป็นอื่นๆ

(๒.๒) วิธีการและระยะเวลาในการชำระราคาค่าสินค้าหรือบริการ ต้องกำหนดขั้นตอนวิธีการให้ชัดเจน วิธีการชำระเงินทั้งหมดหรือแบ่งเป็นงวด เงินสกุลที่รับชำระ นับแต่วันที่ได้รับเงินใช้บังคับ รวมทั้งการดำเนินการในกรณีที่มีการผิดนัดชำระราคา

(๒.๓) การส่งมอบสินค้าหรือการให้บริการต้องดำเนินการให้แล้วเสร็จภายในเวลาอันควรและต้องระบุให้ชัดเจนถึงวิธีการและระยะเวลาในการส่งมอบสินค้าหรือบริการ

(๓) ต้องมีข้อมูลแสดงนโยบายเงื่อนไขทางการค้าหรือบริการที่เป็นธรรม เช่น การยกเลิก การคืนสินค้าหรือบริการ มีระบบการยืนยันการสั่งซื้อ มีทางเลือกในการยกเลิกหรือยืนยันการตกลงทำธุรกรรม ก่อนที่จะมีการตกลง

ซื้อขาย เงื่อนไขและข้อตกลงของธุรกรรม เพื่อให้ผู้ซื้อหรือผู้ขายสามารถเข้าไปตรวจสอบได้ และมีรายละเอียดที่ติดต่อกันได้ของผู้ซื้อหรือผู้ขาย มีวิธีการตรวจสอบสถานะของสินค้าหรือบริการ และมีระบบแจ้งสถานะในการจัดส่งสินค้า และยกเลิกสินค้า

(๔) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมของผู้ซื้อหรือผู้ขาย โดยมีการรักษาความปลอดภัยของข้อมูลที่มีมาตรฐานเป็นที่ยอมรับ เหมาะสมกับข้อมูลที่มีการจัดเก็บและส่งผ่าน และมี การป้องกันรักษาความลับของผู้ซื้อหรือผู้ขาย

(๕) ต้องจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดรายละเอียดในการคุ้มครองข้อมูลดังกล่าว ประกอบด้วย ประเภทของข้อมูลส่วนบุคคลที่จะจัดเก็บ วัตถุประสงค์ในการจัดเก็บ เทคโนโลยีหรือวิธีการที่ใช้ในการจัดเก็บข้อมูล การนำไปใช้ หรือเปิดเผยต่อบุคคลที่สาม กรณีมีการส่งผ่านข้อมูลส่วนบุคคลไปยังบุคคลที่สามจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ รวมทั้งข้อมูลส่วนบุคคลที่นำมาใช้ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการนำไปใช้

(๖) ต้องจัดให้มีระบบในการแก้ไขปัญหาข้อร้องเรียนเกี่ยวกับการซื้อขายสินค้าหรือบริการ โดยมีช่องทางที่จะให้ผู้บริโภคสามารถร้องเรียนหรือสอบถามข้อมูลเกี่ยวกับสินค้า หรือบริการได้โดยมีการแจ้งรายละเอียดกระบวนการแก้ไขปัญหาและการแจ้งผลให้แก่ผู้ร้องเรียนโดยเร็ว

ทั้งนี้ การดำเนินการตามข้อ ๗ ต้องมีรายละเอียดการดำเนินการเป็นไปตามเกณฑ์มาตรฐานคุณภาพธุรกิจระดับดี “DBD Verified Silver” ที่กรมกำหนดไว้

ข้อ ๘ ผู้ซื้อใช้เครื่องหมายรับรองจะต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจประเมินเข้าทำการตรวจสอบการประกอบธุรกิจจนกว่าการตรวจสอบจะเสร็จสิ้น

ข้อ ๙ การอนุญาตให้ใช้เครื่องหมายรับรอง กรมจะออกหนังสืออนุญาตให้ไว้เป็นหลักฐานซึ่งผู้ประกอบการธุรกิจที่ได้รับอนุญาตต้องแสดงหนังสืออนุญาตไว้ ณ สถานที่ตั้งสำนักงานใหญ่ที่เห็นได้ง่าย และแสดงเครื่องหมายรับรองไว้บนหน้าแรกของเว็บไซต์ที่ใช้ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลาที่ได้รับอนุญาต

ในการอนุญาตตามวรรคหนึ่ง กรมอาจกำหนดเงื่อนไขให้ผู้ประกอบการธุรกิจที่ได้รับอนุญาตปฏิบัติเพิ่มเติมก็ได้

ข้อ ๑๐ หนังสืออนุญาตมีกำหนดระยะเวลาหนึ่งปี นับแต่วันที่ออกหนังสืออนุญาต

การต่ออายุหนังสืออนุญาต ให้ผู้ประสงค์จะขอต่ออายุหนังสืออนุญาต ยื่นคำขอต่ออายุต่อกรม ก่อนวันที่หนังสืออนุญาตสิ้นอายุ ๓๐ วัน และให้นำความในข้อ ๕ ข้อ ๗ และ ข้อ ๘ มาใช้บังคับกับการต่ออายุหนังสืออนุญาตโดยอนุโลม

ข้อ ๑๑ ในกรณีที่ผู้ได้รับหนังสืออนุญาตเปลี่ยนแปลงรายละเอียดข้อมูลที่แจ้งไว้ในคำขอใช้เครื่องหมายรับรองหรือคำขอต่ออายุหนังสืออนุญาต ให้ผู้รับหนังสืออนุญาตแจ้งข้อมูลที่เปลี่ยนแปลงต่อกรมภายใน ๗ วัน นับแต่วันที่เปลี่ยนแปลง

ข้อ ๑๒ ผู้รับหนังสืออนุญาตต้องประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ใน ข้อ ๗ ตลอดระยะเวลาของหนังสืออนุญาต

ในระหว่างที่ได้รับอนุญาต ผู้รับอนุญาตต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจประเมินเข้าทำการตรวจสอบการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลา

หมวด ๓

การพักใช้หนังสืออนุญาต และการเพิกถอนหนังสืออนุญาต

ข้อ ๑๓ กรณีมีอำนาจสั่งพักใช้หนังสืออนุญาตในกรณีผู้รับหนังสืออนุญาตไม่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขที่กำหนดในการอนุญาตตามข้อ ๔ วรรคสอง

ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาต ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไข และแจ้งกรมภายใน ๑๕ วัน นับแต่วันที่ถูกลงสั่งพัก

เมื่อกรมได้รับแจ้งตามวรรคสองและเมื่อได้มีการตรวจสอบแล้วพบว่าผู้ถูกสั่งพักใช้หนังสืออนุญาตได้ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไขแล้ว ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาตสามารถใช้อำนาจหนังสืออนุญาตได้ต่อไปจนสิ้นระยะเวลาที่กำหนด แต่ถ้าผู้ถูกสั่งพักใช้หนังสืออนุญาตไม่ปรับปรุง แก้ไขตามข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขภายในระยะเวลาที่กำหนด กรมมีอำนาจที่จะเพิกถอนหนังสืออนุญาตได้

ข้อ ๑๔ กรณีมีอำนาจเพิกถอนหนังสืออนุญาต ในกรณีดังต่อไปนี้

(๑) มีพฤติกรรมในการประกอบธุรกิจที่ขัดต่อกฎหมาย หรือความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน หรือความมั่นคงของประเทศ หรือไม่เป็นธรรมต่อผู้บริโภค หรือ

(๒) นำเครื่องหมายรับรองไปใช้ในลักษณะที่ผิดวัตถุประสงค์อันอาจก่อให้เกิดความเสียหายกับกรม ซึ่งเป็นเจ้าของเครื่องหมายรับรอง หรือ

(๓) ขาดคุณสมบัติตาม ข้อ ๕ หรือ

(๔) ไม่ยินยอม หรือไม่อำนวยความสะดวก หรือไม่ให้ข้อมูลแก่หน่วยตรวจประเมินตามข้อ ๑๒ หรือ

(๕) เพิกถอนตาม ข้อ ๑๓ วรรค สาม

ข้อ ๑๕ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ต้องเลิกใช้เครื่องหมายรับรองในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ทันที

ในกรณีผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาตได้ฝ่าฝืนใช้เครื่องหมายรับรอง ต้องรับผิดชอบใช้ค่าเสียหายให้กรมในอัตราวันละห้าพันบาทจนกว่าจะเลิกใช้

ข้อ ๑๖ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ไม่อาจขอใช้เครื่องหมายรับรองได้อีกภายในเวลา ๑ ปี

บทเฉพาะกาล

ข้อ ๑๗ ภายหลังจากข้อบังคับนี้มีผลใช้ข้อบังคับให้ผู้ที่ได้รับอนุญาตให้ใช้เครื่องหมายรับรองความน่าเชื่อถือ (DBD Verified) สามารถให้ใช้เครื่องหมายดังกล่าวต่อไปจนกว่าเครื่องหมายนั้นจะครบกำหนดระยะเวลาที่ได้รับอนุญาต

เครื่องหมายรับรองความน่าเชื่อถือ
ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดี “DBD Verified Silver”



APPENDIX E

REGULATION OF USING “DBD VERIFIED GOLD”

ข้อบังคับ
ว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดีมาก “DBD Verified Gold”
ของ กรมพัฒนาธุรกิจการค้า

ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดีมาก “DBD Verified Gold” นี้ จัดทำขึ้นตามบทบัญญัติมาตรา ๘๒ แห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

หมวด ๑
บททั่วไป

ข้อ ๑ ข้อบังคับนี้ให้ใช้บังคับตั้งแต่วันที่ยื่นคำขอจดทะเบียนเป็นต้นไป

ข้อ ๒ ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์นี้ ถือเป็นส่วนหนึ่งของคำขอจดทะเบียนเครื่องหมายรับรองตามพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

ข้อ ๓ ข้อบังคับนี้หากมิได้กำหนดไว้เป็นอย่างอื่นให้นำบทบัญญัติแห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔ มาใช้บังคับ

ข้อ ๔ ในข้อบังคับนี้

“เครื่องหมายรับรอง” หมายถึง เครื่องหมายที่กรมพัฒนาธุรกิจการค้ากำหนดขึ้นท้ายข้อบังคับนี้ เพื่อรับรองความน่าเชื่อถือของการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดีมาก “DBD Verified Gold” ของผู้ประกอบการ

“ผู้ประกอบการ” หมายถึง ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์

“การประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์” หมายถึง การประกอบธุรกิจ ดังต่อไปนี้

- (๑) การซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๒) การบริการอินเทอร์เน็ต
- (๓) การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย
- (๔) การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๕) การทำธุรกรรมโดยวิธีใช้สื่ออิเล็กทรอนิกส์อื่น ตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด

“กรม” หมายถึง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

“เกณฑ์คุณภาพมาตรฐานธุรกิจ” หมายถึง ข้อกำหนดเกี่ยวกับคุณภาพและมาตรฐานการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ที่กรมกำหนด

“หน่วยตรวจประเมิน” หมายถึง ผู้ตรวจประเมินหรือคณะผู้ตรวจประเมินที่กรมมอบหมายให้ทำการตรวจประเมินเว็บไซต์และการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ ที่ขอให้เครื่องหมายรับรอง และตรวจประเมินการประกอบธุรกิจในระหว่างที่ได้รับหนังสืออนุญาต

“หนังสืออนุญาต” หมายถึง หนังสืออนุญาตให้ใช้เครื่องหมายรับรอง

“ระบบตะกร้าสินค้า” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นเสมือนตะกร้าหรือรถเข็นสินค้าที่ลูกค้าใช้ระหว่างการเลือกสินค้าบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ ของสินค้า เช่น รหัสสินค้า ราคา จำนวนสินค้า และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบการจอง” หมายถึง ระบบการสั่งซื้อสินค้าประเภทงานบริการที่เป็นแบบฟอร์มให้ลูกค้าสามารถจองงานบริการบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของงานบริการเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบใบเสนอราคา” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นแบบฟอร์มให้ลูกค้าสามารถขอใบเสนอราคาบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น หรือสามารถ Print ใบเสนอราคาให้กับลูกค้าได้

หมวด ๒

หลักเกณฑ์ วิธีการ และเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง

ข้อ ๕ ผู้ประกอบธุรกิจที่ประสงค์จะขอให้เครื่องหมายรับรอง ต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(๑) ห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือ บริษัทมหาชนจำกัดที่ไม่เข้าข่ายเป็นคนต่างด้าวตามกฎหมาย ว่าด้วยการประกอบธุรกิจของคนต่างด้าว

(๒) จัดส่งงบการเงินมากกว่าหรือเท่ากับ ๑ ปี

(๓) จดทะเบียนพาณิชย์ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์มากกว่าหรือเท่ากับ ๑ ปี

(๔) เป็นเจ้าของโดเมนเนม

(๕) มีระบบการสั่งซื้อ อย่างน้อย ระบบตะกร้าสินค้า หรือ ระบบการจอง หรือ ระบบใบเสนอราคา หรือ ระบบแบบฟอร์มสั่งซื้อสินค้าหรือบริการ

(๖) มีช่องทางการชำระเงิน อย่างน้อย ผ่านตัวกลางทางการเงิน หรือ อิเล็กทรอนิกส์ แบงก์กึ่ง หรือ เคาน์เตอร์เซอร์วิส หรือ ผ่านบัตรเครดิต หรือ บัตรเดบิต

(๗) มีช่องทางการจัดส่ง

(๗.๑) ประเภทสินค้า เช่น ไปรษณีย์ บริษัทขนส่งเอกชน พนักงานส่งสินค้า

(๗.๒) ประเภทบริการ เช่น Download จัดส่งทางอีเมลล์

(๘) ปฏิบัติถูกต้องตามกฎหมายและไม่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

(๙) สินค้าหรือบริการ จะต้องเป็นไปตามประเภทธุรกิจของพาณิชย์กิจที่ได้จดทะเบียนพาณิชย์

อิเล็กทรอนิกส์ และไม่ขัดต่อกฎหมายอื่นที่เกี่ยวข้อง

(๑๐) สินค้าหรือบริการที่อาจส่งผลกระทบต่อเด็กหรือเยาวชน จะต้องจัดให้มีข้อความเตือนบนเว็บไซต์ เพื่อให้ความคุ้มครองสิทธิแก่เด็กและเยาวชน

(๑๑) ไม่เคยถูกเพิกถอนการใช้เครื่องหมายรับรอง เว้นแต่พ้นจากการเพิกถอนมาแล้วไม่น้อยกว่า ๕ ปีก่อนวันยื่นคำขออนุญาต

ข้อ ๖ ผู้ประกอบธุรกิจที่ประสงค์จะขอใช้เครื่องหมายรับรอง ต้องปฏิบัติตามหลักเกณฑ์ วิธีการและเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง โดยให้ยื่นคำขออนุญาตต่อกรมตามวิธีการที่กรมกำหนด

ข้อ ๗ ผู้ที่จะได้รับอนุญาตให้ใช้เครื่องหมายรับรองต้องผ่านการตรวจสอบว่าได้ประกอบธุรกิจตามหลักเกณฑ์ดังต่อไปนี้

(๑) ต้องเปิดเผยข้อมูลธุรกิจและรายละเอียดที่เกี่ยวข้องกับสินค้าหรือบริการ ได้แก่ ข้อมูลเกี่ยวกับชื่อชื่อทางการค้า (ถ้ามี) ชื่อเว็บไซต์ เลขทะเบียนพาณิชย์ ที่ตั้งสถานประกอบการหรือที่ตั้งของตัวแทนหรือบุคคลที่สามารถติดต่อได้ วิธีการติดต่อ หมายเลขโทรศัพท์ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) และเวลาทำการด้วยความถูกต้องชัดเจน และเข้าถึงได้ง่าย

(๒) การเสนอซื้อหรือขายสินค้าหรือบริการ ต้องมีรูปแบบที่เหมาะสมไม่ขัดต่อบทบัญญัติแห่งกฎหมายหรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ต้องแสดงรายละเอียดข้อมูลสินค้าหรือบริการ โดยพิจารณาจากสภาพการซื้อขายและลักษณะของสินค้าหรือบริการ ต้องระบุราคาให้ชัดเจน และกรณีที่มีค่าใช้จ่ายอื่นเพิ่มเติม เช่น ภาษี ค่าระวางบรรทุกสินค้า ค่าบริการจัดส่ง ให้ระบุไว้ด้วย รวมทั้ง ต้องแสดงรายละเอียดการซื้อหรือขายสินค้าหรือบริการ เพื่อให้ผู้สั่งซื้อหรือขายสินค้าหรือบริการ นำไปใช้ประกอบการตัดสินใจทำธุรกรรมเกี่ยวกับสินค้าหรือบริการนั้น ได้แก่

(๒.๑) สินค้าหรือบริการ และค่าบริการจัดส่ง ตลอดจนเงื่อนไขวิธีการสั่งซื้อหรือขายและตอบรับ หรือข้อมูลที่จำเป็นอื่นๆ

(๒.๒) วิธีการและระยะเวลาในการชำระราคาค่าสินค้าหรือบริการ ต้องกำหนดขั้นตอนวิธีการให้ชัดเจน วิธีการชำระเงินทั้งหมดหรือแบ่งเป็นงวด เงินสกุลที่รับชำระ นับแต่วันที่สัญญามีผลใช้บังคับ รวมทั้งการดำเนินการในกรณีที่มีการผิดนัดชำระราคา

(๒.๓) การส่งมอบสินค้าหรือการให้บริการต้องดำเนินการให้แล้วเสร็จภายในเวลาอันควรและต้องระบุให้ชัดเจนถึงวิธีการและระยะเวลาในการส่งมอบสินค้าหรือบริการ

(๓) ต้องมีข้อมูลแสดงนโยบายเงื่อนไขทางการค้าหรือบริการที่เป็นธรรม เช่น การยกเลิก การคืนสินค้าหรือบริการ มีระบบการยืนยันการสั่งซื้อ มีทางเลือกในการยกเลิกหรือยืนยันการตกลงทำธุรกรรม ก่อนที่จะมีการตกลง

ซื้อขาย เงื่อนไขและข้อตกลงของธุรกรรม เพื่อให้ผู้ซื้อหรือผู้ขายสามารถเข้าไปตรวจสอบได้ และมีรายละเอียดที่ติดต่อได้ของผู้ซื้อหรือผู้ขาย มีวิธีการตรวจสอบสถานะของสินค้าหรือบริการ และมีระบบแจ้งสถานะในการจัดส่งสินค้า และยกเลิกสินค้า

(๔) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมของผู้ซื้อหรือผู้ขาย โดยมีการรักษาความปลอดภัยของข้อมูลที่มีมาตรฐานเป็นที่ยอมรับ เหมาะสมกับข้อมูลที่มีการจัดเก็บและส่งผ่าน และมีการป้องกันรักษาความลับของผู้ซื้อหรือผู้ขาย

(๕) ต้องจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดรายละเอียดในการคุ้มครองข้อมูลดังกล่าว ประกอบด้วย ประเภทของข้อมูลส่วนบุคคลที่จะจัดเก็บ วัตถุประสงค์ในการจัดเก็บ เทคโนโลยีหรือวิธีการที่ใช้ในการจัดเก็บข้อมูล การนำไปใช้ หรือเปิดเผยต่อบุคคลที่สาม กรณีมีการส่งผ่านข้อมูลส่วนบุคคลไปยังบุคคลที่สามจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ รวมทั้งข้อมูลส่วนบุคคลที่นำมาใช้ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการนำไปใช้

(๖) ต้องจัดให้มีระบบในการแก้ไขปัญหาข้อร้องเรียนเกี่ยวกับการซื้อขายสินค้าหรือบริการ โดยมีช่องทางที่จะให้ผู้บริโภคสามารถร้องเรียนหรือสอบถามข้อมูลเกี่ยวกับสินค้า หรือบริการได้โดยมีการแจ้งรายละเอียดกระบวนการแก้ไขปัญหาและการแจ้งผลให้แก่ผู้ร้องเรียนโดยเร็ว

ทั้งนี้ การดำเนินการตามข้อ ๗ ต้องมีรายละเอียดการดำเนินการเป็นไปตามเกณฑ์มาตรฐานคุณภาพธุรกิจระดับดีมาก “DBD Verified Gold” ที่กรมกำหนดไว้

ข้อ ๘ ผู้ซื้อใช้เครื่องหมายรับรองจะต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจประเมินเข้าทำการตรวจสอบการประกอบธุรกิจจนกว่าการตรวจสอบจะเสร็จสิ้น

ข้อ ๙ การอนุญาตให้ใช้เครื่องหมายรับรอง กรมจะออกหนังสืออนุญาตให้ไว้เป็นหลักฐานซึ่งผู้ประกอบการธุรกิจที่ได้รับอนุญาตต้องแสดงหนังสืออนุญาตไว้ ณ สถานที่ตั้งสำนักงานแห่งใหญ่ที่เห็นได้ง่าย และแสดงเครื่องหมายรับรองไว้บนหน้าแรกของเว็บไซต์ที่ใช้ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลาที่ได้รับอนุญาต

ในการอนุญาตตามวรรคหนึ่ง กรมอาจกำหนดเงื่อนไขให้ผู้ประกอบการธุรกิจที่ได้รับอนุญาตปฏิบัติเพิ่มเติมก็ได้

ข้อ ๑๐ หนังสืออนุญาตมีกำหนดระยะเวลาหนึ่งปี นับแต่วันที่ออกหนังสืออนุญาต การต่ออายุหนังสืออนุญาต ให้ผู้ประสงค์จะขอต่ออายุหนังสืออนุญาต ยื่นคำขอต่ออายุต่อกรม ก่อนวันที่หนังสืออนุญาตสิ้นอายุ ๓๐ วัน และให้นำความในข้อ ๕ ข้อ ๗ และ ข้อ ๘ มาใช้บังคับกับการต่ออายุหนังสืออนุญาตโดยอนุโลม

ข้อ ๑๑ ในกรณีที่ผู้ได้รับหนังสืออนุญาตเปลี่ยนแปลงรายละเอียดข้อมูลที่แจ้งไว้ในคำขอใช้เครื่องหมายรับรองหรือคำขอต่ออายุหนังสืออนุญาต ให้ผู้รับหนังสืออนุญาตแจ้งข้อมูลที่เปลี่ยนแปลงต่อกรมภายใน ๗ วัน นับแต่วันที่เปลี่ยนแปลง

ข้อ ๑๒ ผู้รับหนังสืออนุญาตต้องประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ใน ข้อ ๗ ตลอดระยะเวลาของหนังสืออนุญาต

ในระหว่างที่ได้รับอนุญาต ผู้รับอนุญาตต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจประเมินเข้าทำการตรวจสอบการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลา

หมวด ๓

การพักใช้หนังสืออนุญาต และการเพิกถอนหนังสืออนุญาต

ข้อ ๑๓ กรมมีอำนาจสั่งพักใช้หนังสืออนุญาตในกรณีผู้รับหนังสืออนุญาตไม่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขที่กำหนดในการอนุญาตตามข้อ ๙ วรรคสอง

ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาต ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไข และแจ้งกรมภายใน ๑๕ วัน นับแต่วันที่ถูกลงสั่งพัก

เมื่อกรมได้รับแจ้งตามวรรคสองและเมื่อได้มีการตรวจสอบแล้วพบว่าผู้ถูกสั่งพักใช้หนังสืออนุญาตได้ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไขแล้ว ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาตสามารถใช้น้ำหนังสืออนุญาตได้ต่อไปจนสิ้นระยะเวลาที่กำหนด แต่ถ้าผู้ถูกสั่งพักใช้หนังสืออนุญาตไม่ปรับปรุง แก้ไขตามข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขภายในระยะเวลาที่กำหนด กรมมีอำนาจที่จะเพิกถอนหนังสืออนุญาตได้

ข้อ ๑๔ กรมมีอำนาจเพิกถอนหนังสืออนุญาต ในกรณีดังต่อไปนี้

(๑) มีพฤติกรรมในการประกอบธุรกิจที่ขัดต่อกฎหมาย หรือความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน หรือความมั่นคงของประเทศ หรือไม่เป็นธรรมต่อผู้บริโภค หรือ

(๒) นำเครื่องหมายรับรองไปใช้ในลักษณะที่ผิดวัตถุประสงค์อันอาจก่อให้เกิดความเสียหายกับกรม ซึ่งเป็นเจ้าของเครื่องหมายรับรอง หรือ

(๓) ขาดคุณสมบัติตาม ข้อ ๕ หรือ

(๔) ไม่ยินยอม หรือไม่อำนวยความสะดวก หรือไม่ให้ข้อมูลแก่หน่วยตรวจประเมินตามข้อ ๑๒ หรือ

(๕) เพิกถอนตาม ข้อ ๑๓ วรรค สาม

ข้อ ๑๕ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ต้องเลิกใช้เครื่องหมายรับรองในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ทันที

ในกรณีผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาตได้ฝ่าฝืนใช้เครื่องหมายรับรอง ต้องรับผิดชอบใช้ค่าเสียหายให้กรมในอัตราวันละห้าพันบาทจนกว่าจะเลิกใช้

ข้อ ๑๖ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ไม่อาจขอใช้เครื่องหมายรับรองได้อีกภายในเวลา ๑ ปี

บทเฉพาะกาล

ข้อ ๑๗ ภายหลังจากข้อบังคับนี้มีผลใช้ข้อบังคับให้ผู้ที่ได้รับอนุญาตให้ใช้เครื่องหมายรับรองความน่าเชื่อถือ (DBD Verified) สามารถให้ใช้เครื่องหมายดังกล่าวต่อไปจนกว่าเครื่องหมายนั้นจะครบกำหนดระยะเวลาที่ได้รับอนุญาต

เครื่องหมายรับรองความน่าเชื่อถือ
ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดีมาก “DBD Verified Gold”



APPENDIX F

REGULATION OF USING “DBD VERIFIED PLATINUM”

ข้อบังคับ

ว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดีเด่น “DBD Verified Platinum”
ของ กรมพัฒนาธุรกิจการค้า

ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดีเด่น “DBD Verified Platinum” นี้ จัดทำขึ้นตามบทบัญญัติมาตรา ๘๒ แห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

หมวด ๑

บททั่วไป

ข้อ ๑ ข้อบังคับนี้ให้ใช้บังคับตั้งแต่วันที่ยื่นคำขอจดทะเบียนเป็นต้นไป

ข้อ ๒ ข้อบังคับว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์นี้ ถือเป็นส่วนหนึ่งของคำขอจดทะเบียนเครื่องหมายรับรองตามพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔

ข้อ ๓ ข้อบังคับนี้หากมิได้กำหนดไว้เป็นอย่างอื่น ให้นำบทบัญญัติแห่งพระราชบัญญัติเครื่องหมายการค้า พ.ศ. ๒๕๓๔ มาใช้บังคับ

ข้อ ๔ ในข้อบังคับนี้

“เครื่องหมายรับรอง” หมายถึง เครื่องหมายที่กรมพัฒนาธุรกิจการค้ากำหนดขึ้นท้ายข้อบังคับนี้ เพื่อรับรองความน่าเชื่อถือของการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ระดับดีเด่น “DBD Verified Platinum” ของผู้ประกอบการ

“ผู้ประกอบการ” หมายถึง ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์

“การประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์” หมายถึง การประกอบธุรกิจ ดังต่อไปนี้

- (๑) การซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต
- (๒) การบริการอินเทอร์เน็ต
- (๓) การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย
- (๔) การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

(๕) การทำธุรกรรมโดยวิธีใช้สื่ออิเล็กทรอนิกส์อื่น ตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด

“กรม” หมายถึง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

“เกณฑ์คุณภาพมาตรฐานธุรกิจ” หมายถึง ข้อกำหนดเกี่ยวกับคุณภาพและมาตรฐานการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ที่กรมกำหนด

“หน่วยตรวจประเมิน” หมายถึง ผู้ตรวจประเมินหรือคณะผู้ตรวจประเมินที่กรมมอบหมายให้ทำการตรวจประเมินเว็บไซต์และการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ ที่ขอใช้เครื่องหมายรับรอง และตรวจประเมินการประกอบธุรกิจในระหว่างที่ได้รับหนังสืออนุญาต

“หนังสืออนุญาต” หมายถึง หนังสืออนุญาตให้ใช้เครื่องหมายรับรอง

“ระบบตะกร้าสินค้า” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นเสมือนตะกร้าหรือรถเข็นสินค้าที่ลูกค้าใช้ระหว่างการเลือกสินค้าบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ ของสินค้า เช่น รหัสสินค้า ราคา จำนวนสินค้า และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบการจอง” หมายถึง ระบบการสั่งซื้อสินค้าประเภทงานบริการที่เป็นแบบฟอร์มให้ลูกค้าสามารถจองงานบริการบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของงานบริการเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น

“ระบบใบเสนอราคา” หมายถึง ระบบการสั่งซื้อสินค้าที่เป็นแบบฟอร์มให้ลูกค้าสามารถขอใบเสนอราคาบนเว็บไซต์ ซึ่งระบบจะเก็บข้อมูลต่างๆ เช่น รหัสสินค้า ราคา จำนวน และการประมวลผลราคาของสินค้าเพื่อส่งข้อมูลให้กับผู้ประกอบการร้านค้าออนไลน์นั้น หรือสามารถ Print ใบเสนอราคาให้กับลูกค้าได้

หมวด ๒

หลักเกณฑ์ วิธีการ และเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง

ข้อ ๕ ผู้ประกอบธุรกิจที่ประสงค์จะขอใช้เครื่องหมายรับรอง ต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(๑) ห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือ บริษัทมหาชนจำกัดที่ไม่เข้าข่ายเป็นคนต่างด้าวตามกฎหมาย ว่าด้วยการประกอบธุรกิจของคนต่างด้าว

(๒) จัดส่งงบการเงินติดต่อกันมากกว่าหรือเท่ากับ ๒ ปี

(๓) จดทะเบียนพาณิชย์ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยทะเบียนพาณิชย์มากกว่าหรือเท่ากับ ๒ ปี

(๔) เป็นเจ้าของโดเมนเนม

(๕) มีระบบการสั่งซื้อ อย่างน้อย ระบบตะกร้าสินค้า หรือ ระบบการจอง หรือ ระบบใบเสนอราคา หรือ ระบบแบบฟอร์มสั่งซื้อสินค้าหรือบริการ

(๖) มีช่องทางการชำระเงิน อย่างน้อย ผ่านบัตรเครดิต หรือ บัตรเดบิต

(๗) มีช่องทางการจัดส่ง

(๗.๑) ประเภทสินค้า เช่น ไปรษณีย์ บริษัทขนส่งเอกชน พนักงานส่งสินค้า

(๗.๒) ประเภทบริการ เช่น Download จัดส่งทางอีเมลล์

(๘) ปฏิบัติถูกต้องตามกฎหมายและไม่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

(๙) สินค้าหรือบริการ จะต้องเป็นไปตามประเภทธุรกิจของพาณิชย์กิจที่ได้จดทะเบียนพาณิชย์อิเล็กทรอนิกส์ และไม่ขัดต่อกฎหมายอื่นที่เกี่ยวข้อง

(๑๐) สินค้าหรือบริการที่อาจส่งผลกระทบต่อเด็กหรือเยาวชน จะต้องจัดให้มีข้อความเตือนบนเว็บไซต์ เพื่อให้ความคุ้มครองสิทธิแก่เด็กและเยาวชน

(๑๑) ไม่เคยถูกเพิกถอนการใช้เครื่องหมายรับรอง เว้นแต่พ้นจากการเพิกถอนมาแล้วไม่น้อยกว่า ๕ ปี ก่อนวันยื่นคำขออนุญาต

(๑๒) เว็บไซต์ได้รับเครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ ระดับดีมาก “DBD Verified Gold” ต่อเนื่อง ๒ ปี

กรณีที่ไม่ได้รับเครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ ระดับดีมาก “DBD Verified Gold” หรือ ได้รับเครื่องหมายต่อเนื่องไม่ครบ ๒ ปี จะได้รับพิจารณาเป็นรายกรณี (กรณีเป็นธุรกิจได้รับการรับรอง หรือรางวัลด้านการบริหารจัดการจากสมาคมหรือหน่วยงานอื่น เช่น รางวัลธรรมาภิบาลของกรมพัฒนาธุรกิจการค้า จะได้รับการพิจารณาเป็นพิเศษ)

ข้อ ๖ ผู้ประกอบธุรกิจที่ประสงค์จะขอใช้เครื่องหมายรับรอง ต้องปฏิบัติตามหลักเกณฑ์ วิธีการและเงื่อนไขในการอนุญาตให้ใช้เครื่องหมายรับรอง โดยให้ยื่นคำขออนุญาตต่อกรมตามวิธีการที่กรมกำหนด

ข้อ ๗ ผู้ที่จะได้รับอนุญาตให้ใช้เครื่องหมายรับรองต้องผ่านการตรวจสอบว่าได้ประกอบธุรกิจตามหลักเกณฑ์ดังต่อไปนี้

(๑) ต้องเปิดเผยข้อมูลธุรกิจและรายละเอียดที่เกี่ยวข้องกับสินค้าหรือบริการ ได้แก่ ข้อมูลเกี่ยวกับชื่อชื่อทางการค้า (ถ้ามี) ชื่อเว็บไซต์ เลขทะเบียนพาณิชย์ ที่ตั้งสถานประกอบการหรือที่ตั้งของตัวแทนหรือบุคคลที่สามารถติดต่อได้ วิธีการติดต่อ หมายเลขโทรศัพท์ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) และเวลาทำการด้วยความถูกต้องชัดเจน และเข้าถึงได้ง่าย

(๒) การเสนอซื้อหรือขายสินค้าหรือบริการ ต้องมีรูปแบบที่เหมาะสมไม่ขัดต่อทบัญญัติแห่งกฎหมายหรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ต้องแสดงรายละเอียดข้อมูลสินค้าหรือบริการ โดยพิจารณาจากสภาพการซื้อขายและลักษณะของสินค้าหรือบริการ ต้องระบุราคาให้ชัดเจน และกรณีที่มีค่าใช้จ่ายอื่นเพิ่มเติม เช่น ภาษี ค่าระวางบรรทุกสินค้า ค่าบริการจัดส่ง ให้ระบุไว้ด้วย รวมทั้ง ต้องแสดงรายละเอียดการซื้อหรือขายสินค้าหรือบริการ เพื่อให้ผู้สั่งซื้อหรือขายสินค้าหรือบริการ นำไปใช้ประกอบการตัดสินใจทำธุรกรรมเกี่ยวกับสินค้าหรือบริการนั้น ได้แก่

(๒.๑) สินค้าหรือบริการ และค่าบริการจัดส่ง ตลอดจนเงื่อนไขวิธีการสั่งซื้อหรือขายและตอบรับ หรือข้อมูลที่เป็นอื่นๆ

(๒.๒) วิธีการและระยะเวลาในการชำระราคาสินค้าหรือบริการ ต้องกำหนดขั้นตอนวิธีการให้ชัดเจน วิธีการชำระเงินทั้งหมดหรือแบ่งเป็นงวด เงินสกุลที่รับชำระ นับแต่วันที่สัญญามีผลใช้บังคับ รวมทั้งการดำเนินการในกรณีที่มีการผิดนัดชำระราคา

(๒.๓) การส่งมอบสินค้าหรือการให้บริการต้องดำเนินการให้แล้วเสร็จภายในเวลาอันควรและต้องระบุให้ชัดเจนถึงวิธีการและระยะเวลาในการส่งมอบสินค้าหรือบริการ

(๓) ต้องมีข้อมูลแสดงนโยบายเงื่อนไขทางการค้าหรือบริการที่เป็นธรรม เช่น การยกเลิก การคืนสินค้าหรือบริการ มีระบบการยืนยันการสั่งซื้อ มีทางเลือกในการยกเลิกหรือยืนยันการตกลงทำธุรกรรม ก่อนที่จะมีการตกลงซื้อขาย เงื่อนไขและข้อตกลงของธุรกรรม เพื่อให้ผู้ซื้อหรือผู้ขายสามารถเข้าไปตรวจสอบได้ และมีรายละเอียดที่ติดต่อได้ของผู้ซื้อหรือผู้ขาย มีวิธีการตรวจสอบสถานะของสินค้าหรือบริการ และมีระบบแจ้งสถานะในการจัดส่งสินค้า และยกเลิกสินค้า

(๔) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมของผู้ซื้อหรือผู้ขาย โดยมีการรักษาความปลอดภัยของข้อมูลที่มีมาตรฐานเป็นที่ยอมรับ เหมาะสมกับข้อมูลที่มีการจัดเก็บและส่งผ่าน และมีการป้องกันรักษาความลับของผู้ซื้อหรือผู้ขาย

(๕) ต้องจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดรายละเอียดในการคุ้มครองข้อมูลดังกล่าว ประกอบด้วย ประเภทของข้อมูลส่วนบุคคลที่จะจัดเก็บ วัตถุประสงค์ในการจัดเก็บ เทคโนโลยีหรือวิธีการที่ใช้ในการจัดเก็บข้อมูล การนำไปใช้ หรือเปิดเผยต่อบุคคลที่สาม กรณีมีการส่งผ่านข้อมูลส่วนบุคคลไปยังบุคคลที่สามจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ รวมทั้งข้อมูลส่วนบุคคลที่นำมาใช้ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการนำไปใช้

(๖) ต้องจัดให้มีระบบในการแก้ไขปัญหาข้อร้องเรียนเกี่ยวกับการซื้อขายสินค้าหรือบริการ โดยมีช่องทางที่จะให้ผู้บริโภคสามารถร้องเรียนหรือสอบถามข้อมูลเกี่ยวกับสินค้า หรือบริการได้โดยมีการแจ้งรายละเอียดกระบวนการแก้ไขปัญหาและการแจ้งผลให้แก่ผู้ร้องเรียนโดยเร็ว

ทั้งนี้ การดำเนินการตามข้อ ๗ ต้องมีรายละเอียดการดำเนินการเป็นไปตามเกณฑ์มาตรฐานคุณภาพธุรกิจระดับดีเด่น “DBD Verified Platinum” ที่กรมกำหนดไว้

ข้อ ๘ ผู้ขอใช้เครื่องหมายรับรองจะต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจสอบประเมินเข้าทำการตรวจสอบการประกอบธุรกิจจนกว่าการตรวจสอบจะเสร็จสิ้น

ข้อ ๙ การอนุญาตให้ใช้เครื่องหมายรับรอง กรมจะออกหนังสืออนุญาตให้ไว้เป็นหลักฐานซึ่งผู้ประกอบการธุรกิจที่ได้รับอนุญาตต้องแสดงหนังสืออนุญาตไว้ ณ สถานที่ตั้งสำนักงานแห่งใหญ่ที่เห็นได้ง่าย และแสดงเครื่องหมายรับรองไว้บนหน้าแรกของเว็บไซต์ที่ใช้ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลาที่ได้รับอนุญาต

ในการอนุญาตตามวรรคหนึ่ง กรมอาจกำหนดเงื่อนไขให้ผู้ประกอบการธุรกิจที่ได้รับอนุญาตปฏิบัติเพิ่มเติมก็ได้

ข้อ ๑๐ หนังสืออนุญาตมีกำหนดระยะเวลาหนึ่งปี นับแต่วันที่ออกหนังสืออนุญาต การต่ออายุหนังสืออนุญาต ให้ผู้ประสงค์จะขอต่ออายุหนังสืออนุญาต ยื่นคำขอต่ออายุต่อกรม ก่อนวันที่หนังสืออนุญาตสิ้นอายุ ๓๐ วัน และให้นำความในข้อ ๕ ข้อ ๗ และ ข้อ ๘ มาใช้บังคับกับการต่ออายุหนังสือ อนุญาตโดยอนุโลม

ข้อ ๑๑ ในกรณีที่ผู้ได้รับหนังสืออนุญาตเปลี่ยนแปลงรายละเอียดข้อมูลที่แจ้งไว้ในคำขอใช้เครื่องหมาย รับรองหรือคำขอต่ออายุหนังสืออนุญาต ให้ผู้รับหนังสืออนุญาตแจ้งข้อมูลที่เปลี่ยนแปลงต่อกรมภายใน ๗ วัน นับแต่วันที่เปลี่ยนแปลง

ข้อ ๑๒ ผู้รับหนังสืออนุญาตต้องประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ ที่กำหนดไว้ใน ข้อ ๗ ตลอดระยะเวลาของหนังสืออนุญาต

ในระหว่างที่ได้รับอนุญาต ผู้รับอนุญาตต้องยินยอม อำนวยความสะดวกและให้ข้อมูลแก่หน่วยตรวจ ประเมินเข้าทำการตรวจสอบการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ตลอดระยะเวลา

หมวด ๓

การพักใช้หนังสืออนุญาต และการเพิกถอนหนังสืออนุญาต

ข้อ ๑๓ กรมมีอำนาจสั่งพักใช้หนังสืออนุญาตในกรณีที่ผู้รับหนังสืออนุญาตไม่ประกอบธุรกิจพาณิชย์ อีเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขที่กำหนดในการอนุญาต ตามข้อ ๔ วรรคสอง

ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาต ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไป ตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไข และแจ้งกรมภายใน ๑๕ วัน นับแต่วันที่ถูกสั่งพัก

เมื่อกรมได้รับแจ้งตามวรรคสองและเมื่อได้มีการตรวจสอบแล้วพบว่าผู้ถูกสั่งพักใช้หนังสืออนุญาตได้ ปรับปรุงแก้ไขการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ใน ข้อ ๗ หรือปฏิบัติตามเงื่อนไขแล้ว ให้ผู้ถูกสั่งพักใช้หนังสืออนุญาตสามารถใช้น้ำหนังสืออนุญาตได้ต่อไปจนสิ้นระยะเวลาที่กำหนด แต่ถ้าผู้ถูกสั่งพักใช้หนังสือ อนุญาตไม่ปรับปรุง แก้ไขตามข้อ ๗ หรือไม่ปฏิบัติตามเงื่อนไขภายในระยะเวลาที่กำหนด กรมมีอำนาจที่จะเพิกถอน หนังสืออนุญาตได้

ข้อ ๑๔ กรมมีอำนาจเพิกถอนหนังสืออนุญาต ในกรณีดังต่อไปนี้

(๑) มีพฤติกรรมในการประกอบธุรกิจที่ขัดต่อกฎหมาย หรือความสงบเรียบร้อย หรือศีลธรรมอันดี ของประชาชน หรือความมั่นคงของประเทศ หรือไม่ป็นธรรมต่อผู้บริโภค หรือ

(๒) นำเครื่องหมายรับรองไปใช้ในลักษณะที่ผิดวัตถุประสงค์อันอาจก่อให้เกิดความเสียหายกับกรม ซึ่งเป็นเจ้าของเครื่องหมายรับรอง หรือ

(๓) ขาดคุณสมบัติตาม ข้อ ๕ หรือ

(๔) ไม่ยินยอม หรือไม่อำนวยความสะดวก หรือไม่ให้ข้อมูลแก่หน่วยตรวจประเมินตามข้อ ๑๒ หรือ

(๕) เพิกถอนตาม ข้อ ๑๓ วรรค สาม

ข้อ ๑๕ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ต้องเลิกใช้เครื่องหมายรับรองในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ทันที

ในกรณีผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาตใดฝ่าฝืนใช้เครื่องหมายรับรอง ต้องรับผิดชอบค่าใช้จ่ายให้กรมในอัตราวันละห้าพันบาทจนกว่าจะเลิกใช้

ข้อ ๑๖ ผู้ถูกสั่งพักใช้หนังสืออนุญาต หรือเพิกถอนการใช้หนังสืออนุญาต ไม่อาจขอใช้เครื่องหมายรับรองได้อีกภายในเวลา ๑ ปี

บทเฉพาะกาล

ข้อ ๑๗ ภายหลังจากข้อบังคับนี้มีผลใช้ข้อบังคับให้ผู้ที่ได้รับอนุญาตให้ใช้เครื่องหมายรับรองความน่าเชื่อถือ (DBD Verified) สามารถให้ใช้เครื่องหมายดังกล่าวต่อไปจนกว่าเครื่องหมายนั้นจะครบกำหนดระยะเวลาที่ได้รับอนุญาต

เครื่องหมายรับรองความน่าเชื่อถือ
ในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์
ระดับดีเด่น “DBD Verified Platinum”

.....



APPENDIX G

SAMPLE OF “DBD VERIFIED SILVER” CERTIFICATE



เว็บไซต์นี้ได้รับการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์กับทางกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์
และได้รับอนุญาตให้ใช้เครื่องหมายรับรองความน่าเชื่อถือ DBD Verified ระดับ Silver

This Web Site is registered with the Department of Business Development, the Ministry of Commerce of Thailand

ชื่อผู้ประกอบการ : บริษัท สื่อเดินทาง จำกัด

(Owner name) : Travel Mart Company Limited

ชื่อที่ใช้ในการประกอบพาณิชย์กิจ : บริษัท สื่อเดินทาง จำกัด

(Company name) : Travel Mart Company Limited

เลขทะเบียนพาณิชย์อิเล็กทรอนิกส์ (E-commerce
Registration ID) : 7100803001410

บริการเว็บไซต์ (Website name) : www.e-travelmart.com

ชนิดแห่งพาณิชย์กิจ : กีฬา/อุปกรณ์

(Type of business) : Sport/Accessory

ที่อยู่ : 127/21-22 ถนนราชปรารภ แขวงมักกะสัน เขตราชเทวี
จังหวัดกรุงเทพมหานคร 10400

(Address) : 127/21-22 Ratchaprarop ROAD,MAKKASAN,
RATCHATHEWI, BANGKOK 10400

โทรศัพท์ (Telephone) : 022475371-2

โทรสาร (Fax) : 026400020

E-mail : info@e-travelmart.com

วันที่ได้รับ DBD Registered : 22 กันยายน 2546

Registered date : 22 September. 2003

วันที่ได้รับ DBD Verified : 17 กันยายน 2558

Verified date : 17 September. 2015

วันที่หมดอายุ DBD Verified : 17 กันยายน 2559

DBD Verified Expire date : 17 September. 2016

ข้อมูล ณ วันที่ : 19 พฤษภาคม 2559

ดูรายละเอียดได้ที่ www.trustmarkthai.com

Details can be found at www.trustmarkthai.com

สอบถามข้อมูลได้ที่ กองพาณิชย์อิเล็กทรอนิกส์ โทร.02 547 5959-61 E-mail : e-commerce@dbd.go.th

BIOGRAPHY

Name	Ms.Chatanut Khiewcham
Date of Birth	October 31, 1986
Educational Attainment	2015: LL.M-Legal Institutions Degree, University of Wisconsin 2010: Bachelor of Laws Degree, Thammasat University
Work Position	Senior Legal Officer Univentures Public Company Limited
Work Experiences	2011-2014: Legal Executive, SF Development Co., Ltd. 2010-2011: Transactional Lawyer, Narit & Associates