Intra - ASEAN

Secure Transactions Framework

Final Report | July 2014

MINISTRY OF ICT Smart Thailand

ETDA สพธอ www.etda.or.th

List of Contributors

Project Advisors

Surangkana Wayuparb	Executive Director, ETDA
Chaichana Mitrpant	Deputy Executive Director, ETDA

Section 1: Overview

Section 2: e-Authentication Methodology

Lead Author

Werachai Prayoonpruk

Contributors

Pitinan Kooarmornpatana

Suntod Suriyan

Section 3: Legal Infrastructure and Readiness of ASEAN Member States

Lead Author

Nattawat Sukwongtrakul

Contributors

Kachida Meetortharn

Nubthong Wanawattanawong

Passamon Phutong

Warapan Seekomen

Table of Contents

List of Tables

1. Overview

1.1 Background

In 2015, the ASEAN Member States are looking forward to elevating themselves and forming the ASEAN Economic Community (AEC), which aims to strengthen relationships and cooperation and promote better flow of capital and human resources in order to enhance the regional economy, standard of living and social welfare of their people. It is obvious that information technology will play a critical role as a platform creating tool for digital economy development. One particularly powerful mechanism of information technology is the electronic transactions owing to its speed, convenience, and borderless characteristics.

The volume and value of electronic transactions among the member states have been increasing every year. This demonstrates increasing popularity of electronic transactions. However, to fully utilize potential and benefits of electronic transactions among ASEAN member states, it is necessary that we have solid legal, regulations and compliance apart from technical framework and standards so that we can build trust and promote secure electronic transactions.

The **Intra-ASEAN Secure Transactions Framework** is originated per ASEAN Cooperation Project Document as of May 4th, 2011 and is funded by the ASEAN ICT Fund. The project is a part of the ASEAN ICT Masterplan 2015; Strategic thrust 2, Initiative 2.4: Build trust and promote secure transaction within ASEAN, which ultimately aims to leverage information communication and technology as an enabler for improved economic growth of ASEAN member states.

The project aims to perform survey on the current state of the laws, policies and regulations related to electronic signature and digital certificate recognition as well as to develop a foundation framework for secure electronic transactions among ASEAN member states.

1.2 Objectives

The objectives of the framework are to:

- Provide guideline, technology-neutral framework, and legal consistency in secure transaction approaches across ASEAN member states
- Increase trust and promote secure and efficient electronic transactions through proper selection of e-authentication mechanism
- Initiate sharing of online identity and authentication across cross-border systems

1.3 Scope

The scope of this framework covers:

- Concept of secure electronic transactions and management of electronic authentication of identity
- Proposal on electronic authentication model and implementation guidelines
- Survey on laws, policies and regulations related to electronic signature and digital certificate recognition

1.4 Secure Electronic Transactions and e-Authentication

By mentioning the term "electronic transaction", it refers to an activity where a packet of data is transmitted online, which can be via any type of digital media. As cited earlier in this section, electronic transactions have become more popular judging from the growths in both their volume and value. However, it is important to note that when considering electronic methods for communication, there are four essential elements that should be addressed in order to ensure secure electronic transactions and enhance trust, including:

1. **Confidentiality** – the need to prevent the disclosure of information to unauthorized individuals or entities
2. **Data Integrity** – the need to maintain the accuracy and consistency of information transmitted through the network
3. **Authenticity** – the need to ensure that the parties involved in communication are actually who they are supposed to be
4. **Non-repudiation** – the need to prove and undeniable responsibility and accountability of the parties involved in communication

When referring to electronic authentication, it actually involves several aspects including but not limited to identity identification and verification, authentication mechanism, and credential issuance and management. Nonetheless, the implementation of these aspects is not simple at all especially in a cross-border manner as they inherit not only technical but also organizational and legal challenges. Though overcoming all challenges is almost impossible by any single document, this framework is developed as a Head Start to handle common challenges and to shed some ideas on what lie ahead. In this paper, we review international standards, best practices and the status of current practices by ASEAN member states and propose a framework for recognizing trustworthy electronic credential issuers or electronic authentication service providers. *Section 2: e-Authentication Methodology* will cover the suggestions and guideline to meet the requirements on technical and organizational aspects involving in electronic authentication. *Section 3: Legal Infrastructure and Readiness of ASEAN Member* will discuss on legal perspective regarding the electronic authentication.

All in all, for intra-ASEAN transactions to be trustworthy, a framework for electronic authentication needs to be developed and mutually agreed so that an electronic identity can be recognized and trusted by a relying party across physical boundaries within ASEAN.

1.5 Terms and Definitions

Term	Meaning
Assertion	Statement made by an entity without accompanying evidence of its validity. * Remark: see *Claim*. An assertion is considered to be a stronger statement than a claim. [ISO/IEC 29115:2013] [ITU-T X.1252]
Assurance level	The level of trust that is required from e-Authentication and/or the degree of trust related to a particular e-Authentication approach. [Australian National e-Authentication Framework]
Authentication	See *Electronic authentication*.
Claim	Statement that something is the case, without being able to give proof. * Remark: see *Assertion*. An assertion is considered to be a stronger statement than a claim. [ISO/IEC 29115:2013] [ITU-T X.1252]
Credential	An object that is verified when presented to the verifier in an authentication transaction. It binds an identity to a token possessed. [OMB M-04-04], [NIST SP 800-63-1]
Credential Service Provider	Trusted entity that issues and manages security tokens or electronic credentials to subscribers. [ISO/IEC 29115:2013] [NIST SP 800-63-1]
Electronic authentication (e-Authentication)	The process of establishing confidence in user identities that are electronically presented. [NIST SP 800-63-1]
e-Authentication approach	The collective of e-Authentication elements including the approach to registration and enrolment and the authentication mechanism. [Australian National e-Authentication Framework]
Entity	The person or "subject" (e.g. corporations, trusts, incorporated associations) associated with a digital identity. An entity may

Term	Meaning
	have multiple digital identities. [Australian National e-Authentication Framework]
Identification	See *Identity proofing*.
Identity verification	The process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. [ISO/IEC 29115:2013]
Identity proofing	The process of capturing and verifying sufficient information to identify an entity to a specified or understood level of assurance. [ISO/IEC 29115:2013]
Registration authority	Trusted actor that establishes and/or vouches for the identity of an entity to a credential issuer or service provider. [ISO/IEC 29115:2013]
Token	Something that is used to authenticate the user identity (typically a cryptographic module or password) [NIST SP 800-63-1]
Verification	See *Identity verification*.

Table 1: Definition of key terms

2. e-Authentication Methodology

E-Authentication is a global challenge that experts at organizational, national and international levels have looked at. Multiple authentication frameworks have been developed and referred to by many countries. Some frameworks have intentionally been developed for cross-border authentication. Nonetheless, from the studies of those frameworks, it appears that they all share the same core concepts, which are centered around risk-based analysis and assurance levels (LoA : Level of Assurance).

The idea behind the concepts suggests that for the decision makers to select among various choices of approaches and mechanisms, which possess different level of security strength and process stringency, they should assess and find a balance between the **acceptable level of risk** and **desired user experience**. Risk, according to ISO/IEC 31000: Risk Management is an effect of uncertainty on achieving one or more objectives. The level of risk is estimated by considering its consequences and likelihood of occurrence. In contrast, user experience takes into accounts several factors such as ease of usage, performance, reliability, availability, accessibility, and affordability.

Basically, a transaction that is associated with higher risk requires stricter registration and verification processes and stronger authentication mechanism. Of course, stricter registration processes and stronger authentication mechanism will create a credential that is more trustworthy, which will in turn lead to more reliable authentication process as well as the whole electronic transaction. But such level of strictness will be more difficult to implement and take more time to complete. Further, since authentication mechanism also depends on affordability and availability of the technology, the implementation of some mechanisms may be so costly that is unaffordable by consumers or, in some situations, its supporting technology is not at all available.

In addition, the key benefit of applying LoA is that it can be adapted to fit different types and forms of electronic transactions which inherit different level of risks and thus require different level of assurance. For example, the LoA model can be applied to electronic commerce transactions whose risk may be more associated with financial loss. It can also be applied to healthcare and medical transactions whose associated risks will be more on personal safety and unauthorized release of sensitive information. Moreover, the model can be applied to online social networking and web-board activities which can cause negative impact to standing and reputation of a person or an organization, and harm agency programs and public interests.

For the purpose of building a solid and applicable framework, the international standards, guidelines and best practices have been reviewed and three main components of e-authentication have been identified as follows:

- **Assurance Levels and Risk Assessments**

  Levels of assurance are defined so that different levels of importance of getting e-authentication right can be distinguished. For a transaction, risks are assessed and summarized in impact values of authentication failure associated with types of potential

impacts. Then, an appropriate level of assurance is chosen to reflect the potential impacts involved.

- **Identity Proofing and Verification**

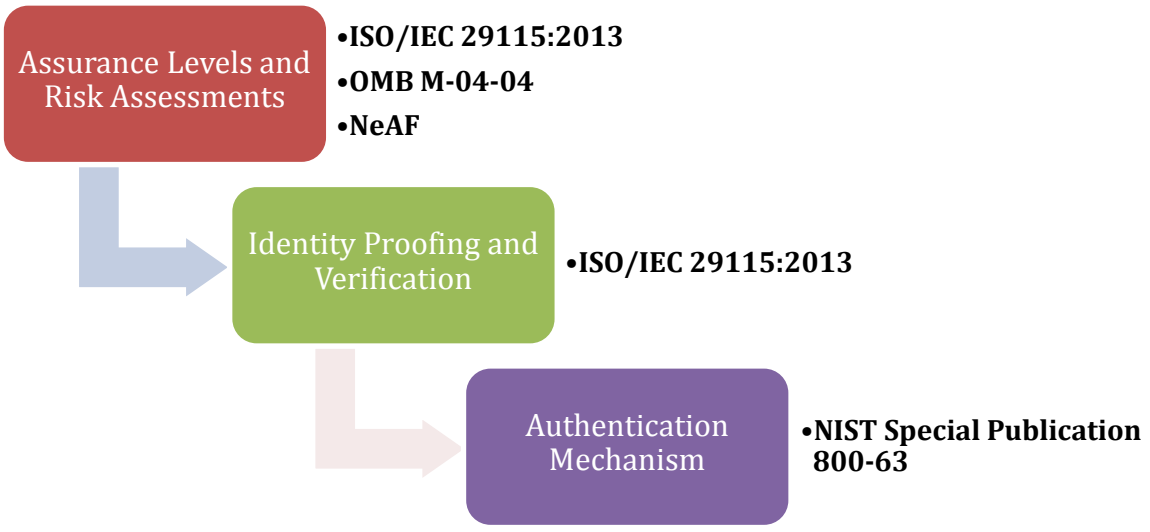
  For each level of assurance, an objective of authentication and a set of controls are defined. Then details about identity proofing and verification methods are provided for the registration process.

- **Authentication Mechanism**

  Different token technologies are listed and mapped to the levels of assurance. Moreover, how identity should be managed is recommended.

The international standard, guideline and best practices under review for the e-authentication methodologies consist of:

- **ISO/IEC 29115:2013** Information Technology – Security Techniques – Entity Authentication Assurance Framework;
- **NIST Special Publication 800-63-1** Electronic Authentication Guideline;
- **OMB M-04-04** E-Authentication Guidance for Federal Agencies;
- **National e-Authentication Framework (NeAF)** published by the Department of Finance and Deregulation, Australian Government.



The framework provides agencies with guidance on electronic authentication. Overall, it describes four levels of identity assurance for electronic transactions requiring authentication, and demands that agencies perform a risk assessment to determine the required level of assurance and ensure that the authentication processes of electronic transactions meet that level of assurance. The step-by-step direction on how to achieve this will be discussed in the following sections.

2.1 Assurance Levels and Risk Assessments

The studies of multiple international standards and guidelines have shown that they share the same core concepts which are risk-based analysis and assurance levels. They allow practitioners to adopt this framework to different scenarios which require different levels of assurance. Assurance levels, according to the Australian National e-Authentication Framework (NeAF), are used to describe the level of importance of getting e-Authentication right and the resultant level of robustness of the required solution.

A set of activities associated with risk assessment and identification of appropriate assurance level is considered to be the primary step of this framework. The method of defining assurance levels can be different depending on which international standard or framework you are referring to. For example, Australian NeAF defines five assurance levels ranging from Level 0 (for no assurance) to Level 4 (for high assurance). On the other hand, ISO/IEC 29115:2013, NIST SP 800-63-1 and United States' OMB M04-04 use four levels from Level 1 to Level 4; where Level 1 means little or no assurance and Level 4 means very high assurance.

Taking into consideration the benefits of standardization as well as availability and richness of explanations on each level of assurance for further references, this framework therefore adopts the ISO/IEC 29115: 2013's four-level approach. Four assurance levels for electronic transactions have been defined and represented in the table below.

Assurance Level	Description
LoA1	Little or no confidence in the asserted identity's validity
LoA2	Some confidence in the asserted identity's validity
LoA3	High confidence in the asserted identity's validity
LoA4	Very high confidence in the asserted identity's validity

Table 2: Levels of Assurance

Source: *ISO/IEC 29115: 2013, Table 6-1 page 7*

Each assurance level requires a particular degree of certainty of an identifier (or credential) that refers to the identity of an individual or entity. The term credential is used to refer to an object that is verified when presented to the verifier in an authentication transaction. As described earlier, higher assurance level will generally require higher degree of certainty and trustworthiness of a credential which acts on behalf of an individual or entity.

To determine the appropriate level of assurance, two steps should be followed:

- **Step 1: Assess the potential risks** will be discusses in *Section 2.1.1*, and;
- **Step 2: Map the risk assessment to the impact profiles** will be discussed in *Section 2.1.2.*

2.1.1 Step 1: Assess the potential risks

At the earliest stage, it is recommended that the decision makers begin with a clear understanding of their business requirements. This may include the identification of services to be provided, information to be accessed, users to consume such services and use the information, and the underlying need for authentication. The decision makers may also take into consideration security requirements at this stage.

To assess potential risks, it is proposed that the relative severity of the potential harm and likelihood of occurrence should be measured. Type of potential impact has been classified into six categories following the shared model of ISO/IEC 29115:2013 and OMB M-04-04. Basically, they consist of reputation damage, financial loss, harm to company operations, leak of sensitive information, personal safety, and violations of related laws and regulations. Then, the risk of authentication failure associated with each of these categories will be evaluated and assigned with appropriate impact values. Here, three impact values have been used and consist of low, moderate, and high. The criteria for assessment can be referred to Table 3 as represented below.

Impact Categories	Impact Values of Authentication Failure		
	Low	**Moderate**	**High**
1. Inconvenience, distress, or damage to standing or reputation	Limited and short-term inconvenience, distress or embarrassment to any party	Serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party
2. Financial loss or agency liability	Insignificant or inconsequential unrecoverable financial loss or agency liability to any party	Serious unrecoverable financial loss or agency liability to any party	Severe or catastrophic unrecoverable financial loss or agency liability to any party
3. Harm to agency programs or public interests	Limited adverse effect on organizational operations or assets, or public interests. Examples: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness (ii) minor damage to organizational assets or public interests	Serious adverse effect on organizational operations or assets, or public interests. Examples: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness (ii) significant damage to organizational assets or public interests	Severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions (ii) major damage to organizational assets or public interests
4. Unauthorized release of sensitive information	Limited release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199	Release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199	Release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199

Impact Categories	Impact Values of Authentication Failure		
	Low	Moderate	High
5. Personal safety	Minor injury not requiring medical treatment	Moderate risk of minor injury or limited risk of injury requiring medical treatment	Risk of serious injury or death
6. Civil or criminal violations	Risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts	Risk of civil or criminal violations that may be subject to enforcement efforts	Risk of civil or criminal violations that are of special importance to enforcement programs

Table 3: Potential impact categories and values

Source: *OMB M-04-04 Section 2.2. Risks, Potential Impacts, and Assurance Levels*

2.1.2 Step 2: Map the risk assessment to the impact profiles

From Step 1, the assessed impact values (Low, Moderate, and High) of six categories are then used to determine the required level of assurance by mapping them into Table 4: Assurance level impact .

Impact Categories	Assurance Level Impact Profiles			
	LoA1	LoA2	LoA3	LoA4
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interests	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

Table 4: Assurance level impact profiles

Source: *OMB M-04-04 Table 1 (no page number)*

The appropriate assurance level is the lowest level whose impact profile meets or exceeds the potential impact for every category. For example, if an electronic transaction has been assessed and the result of impact profile reveals that five categories (from #1 to #5) require Level 1, and one category is appropriate for Level 2. Therefore, this particular transaction would require at least identity proofing and authentication that meet Level 2 criterions.

Let's take a look at another example on an office lady's, whose name is Miss A, personal account login to a famous social networking application. From the basic assessment, it reveals that the impact will mostly be on reputation damage to the person, which is the first category. Since Miss A is neither a celebrity or high ranking business executive, impact caused from getting authentication wrong will be kept at low or moderate level and will not cause any severe

damage to her reputation. The impacts on other categories are low or no impact at all. Therefore, the impact profiles of this particular transaction as summarized below will require Assurance Level 2.

Impact Categories	Assurance Level Impact Profiles			
	LoA1	LoA2	LoA3	LoA4
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interests	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

Please note that the practice provided above is a guideline. In an actual application, decision makers may consider selecting implementation details such as registration process and authentication mechanism that are more appropriate for a higher level than the level suggested by the impact profile mapping so that they can achieve more reliable and trustworthy transaction. However, it is highly recommended that the decision makers not select any option lower than the minimum requirements.

Guideline on identify proofing and registration process will be discussed in the next section and authentication mechanism will be discussed in *Section 2.3*.

2.2 Identity Proofing and Verification Approach

Identity proofing is the process of capturing and verifying sufficient information to identify an entity to a specified or understood level of assurance. The major part of identity proofing involves the information verification process which will check identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. The stringency of identity proofing requirements is based on the objectives that must be met for each assurance level.

The proposed identity proofing requirements as described in the tables below and on the next pages have been studied and analyzed from related international standards as well as common practices of banking industry. The concept is that each level has its own set of objectives and controls which are consistent with the level of criticality of getting identity proofing and verification correct. Higher assurance levels will include all objectives of the lower levels with some additional requirements to solidify the process. Principally, higher assurance level will require more reliability and credibility of identity, which will also require more rigorous identity proofing process.

Table 5 explains the objectives of identity proofing of each assurance level and also specifies the registration methods which can either be local (in-person) or remote.

Assurance Level	Objectives	Control	Method of processing
LoA1	Identity is unique within a context	Self-claimed or self-asserted	In-person or remote
LoA2	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	In-person or remote
LoA3	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through 1. use of identity information from an authoritative source 2. identity information verification	In-person or remote
LoA4	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other context	Proof of identity through 1. use of identity information from multiple authoritative sources 2. identity information verification 3. entity witnessed in-person	In-person only

Table 5: Assurance level identity proofing objectives

Source: *ISO/IEC 29115: 2013, Table 8-1 page 13*

From the stated objectives, the following part discusses on identity proofing and verification approach for each assurance level. The identity proofing model is, in fact, under the development process by Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). However, since identity proofing is a non-negligible component of the electronic authentication, study and analysis have been performed based on equivalent framework as well as common practices of banking industry.

The concept is that a user who needs to have an electronic credential to be used in an authentication process must undergo some sort of registration procedure. The registration process is usually performed by a designated authority called Registration Authority or RA who can be the same entity as an issuer of credential or a separate entity depending on the implementation method and degree of stringency. The role of RA is to check identity information of the user who submits a request or application against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. Once the identity is confirmed to have sufficient trustworthiness, some form of electronic credential, for instance, username and password and security token, will be created by the Credential Service Provider and issued to the user.

Details of registration requirements have been defined and illustrated in Table 6 below. Note that the listed requirements are the minimum prerequisites. There is no constraint to include additional identity documents if necessary.

Assurance Level	**Registration Requirement**	
	In-Person	**Remote**
LoA1	Not Required	<u>Proof of Identity</u> • Email address <u>Verification Method</u> • Confirm the validity of email address and ensure that it uniquely identifies an individual.

Assurance Level	Registration Requirement	
	In-Person	**Remote**
LoA2	Not Required	Proof of Identity • Email address • Mobile telephone number Verification Method • Confirm the validity of email address and ensure that it uniquely identifies an individual. • Verify that the identity exists objectively, for example, by sending account activation link to the registered email and a verification code as SMS message to mobile telephone number. To completely activate the credential, both the activation link and the correct verification code are required.
LoA3	Proof of Identity • Government ID Card • Email address (if applicable) • Mobile telephone number • Another identification that contains current corroborating information such as House Registration Document or Resident Book, driving license, and passport Verification Method • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Record a photograph or other form of biometric i.e. fingerprint to ensure that applicant cannot repudiate application • Confirm possession of mobile telephone number by sending activation code required for completing the registration process as SMS message to that particular number.	Proof of Identity • Government ID Card (Color copy) • Email address • Mobile telephone number • A copy of House Registration Document or driving license or passport. Verification Method • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Verify that the identity exists objectively, truly lives in the registered address and owns the email address by, for example, sending activation link via email and username and password via registered mail to the address.

Assurance Level	Registration Requirement	
	In-Person	**Remote**
LoA4	<u>Proof of Identity</u> • Government ID Card • Certificate of Employment • Email address • Mobile telephone number • Other identifications that contain current corroborating information such as House Registration Document or Resident Book, driving license, and passport <u>Verification Method</u> • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Record a photograph • Record a current biometric i.e. fingerprint, palm print, and hand geometry to ensure that applicant cannot repudiate application • Verify that the identity exists objectively, truly lives in the registered address and owns the mobile telephone number and email address by sending elements required for completing the registration process via out-of-band channels. Example of scenario is - sending activation link via email - sending username and password via registered mail to the address - when login with the above elements, OTP will be generated and sent via SMS message to the mobile telephone number	Not Applicable

Table 6: Identity proofing and verification approach

2.3 Authentication Mechanism

Electronic authentication requires a certain degree of confidence in user identities electronically presented to an information system. The process involving with electronic authentication consists of three main components, which includes assurance levels and risk assessments, identity proofing and verification, and authentication mechanism. In the previous sections, we have discussed on how to evaluate the required level of confidence or assurance of any transaction through risk-based analysis and on how to achieve identity proofing and registration requirements of each assurance level.

In this section, authentication mechanism including available type of tokens or credentials and their life cycle management will be discussed. Essentially, tokens used as part of the authentication process consist of one or a combination of the three factors as follows:

- **Something you know**

  Knowledge factor or *something you know* is the most common form of authentication used. In this form, the user is required to prove knowledge of a secret in order to authenticate. Examples of this type are password and personal identification number (PIN).

  Using this authentication alone, however, has some drawbacks. First, if a person chooses a password that is hard to guess, it will be difficult to remember and may as well be forgotten. Contrarily, if the person chooses another password that is easy to remember such as his/her date of birth, car license plate numbers, or anything closely related to the person, it will also be easy to guess. In addition, using password or PIN requires the input of secret via some sort of keyboard. This keyboard input is prone to get captured by eavesdroppers who may either use “shoulder surfing” while the secret is being typed or intercept the input through a keyboard logging software installed on the victim’s machine.

  Anyway, knowledge factor is commonly used in combination with another factor, which will be discussed shortly hereafter, to form two-factor authentication techniques meaning that they rely on “something you know” secret as one factor of authentication.

- **Something you have**

  Something you have is also called Possession factor meaning that a user relies on some kind of objects or devices, such as smart card and cryptographic key, which contains a credential specific to that user and then uses it for authentication.

  Possession factor has an advantage over the knowledge-factor authentication in a way that there is no need to create a hard-to-guess password which can be easily forgotten. However, using the device alone would allow an attacker to impersonate its owner if the device got stolen. For this reason, it is more practical that the possession-factor authentication is used as part of as two-factor authentication along with another factor. This means the user is required not only to possess a device but also know some secret password.

- **Something you are**

  Inherence factor or *something you are* requires the use of physiological and behavioral characteristics of a user, which can also be referred to as biometrics. Examples of inherence-factor authentication include but not limited to fingerprint, face recognition, retinal scan, hand geometry, and voice print.

  This type of authentication has key benefits over the others as it requires much more efforts, if not at all impossible, to spoof an identity. In fact, biometric authentication also satisfies the regulatory definition of true multi-factor authentication. However, due to the complexity of the measurement method that normally requires high accuracy rate and, in the case of fingerprint, less than 5% false acceptance rate[1], this solution may become unacceptably slow and comparatively expensive especially when a large number of users are involved.

  Nonetheless, the biometric authentication techniques have still been under research and continuous development. Many related topics such as mobile biometrics and telebiometric authentication framework using biometric hardware security module have been under drafting period of the international standard committee.

Then, from the three factors described above, tokens may be characterized into single-factor and multi-factor tokens depending on the number and types of authentication factors they use.

- **Single-factor token**

  A single-factor token uses only one of the three factors to achieve authentication. Same as example given above, a password is a knowledge factor or *something you know*. If there is no requirement for additional factors to authenticate with the token, this is considered as a single-factor token.

- **Multi-factor token**

  A multi-factor token uses two or more factors to achieve authentication. For example, an ATM card (*something you have*) requires its associated PIN code (*something you know*) to activate. In this case, it is a multi-factor token.

In order to determine the type of authentication including token types, single-factor vs. multi-factor authentication, and credential usage and management to be employed, the assurance level assessed in the earlier stage will be used. The next section describes in detail the types of tokens for electronic authentication and management approaches based on the work of NIST Special Publication 800-63-1.

[1] Cornell University, Professor Fred B. Schneider, CS 513 System Security, http://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html

2.3.1 Token Types

From the study and analysis of NIST Special Publication 800-63-1, we propose six types of tokens to be used for electronic authentication. They have been identified based on the knowledge of three authentication factors and two categories of tokens and are listed as below:

1. **Memorized Secret Token**

   This type of token is more commonly referred to as password and PIN code and typically contains a combination of character and numerical strings. It also refers to pre-registered questions such as "What was your primary school?", "What was your first pet's name?" and etc. In both cases, they are secrets shared between the user and the service provider who provides an authentication service. Memorized secret tokens are *something you know*.

2. **Single-factor One-Time Password Token**

   This single-factor one-time password (OTP) type of token requires spontaneous generation of a password for one-time use. It can be implemented in two scenarios. In the first case, an authenticating party will generate a one-time password and send to a user via an out-of-band channel, which is uniquely addressable, such as an email or SMS to cellular phone. For example, e-Service website of a mobile network operator in Thailand asks users to input their mobile phone number. Its backend system will then generate a four-digit one-time password and send it as an SMS message to the inputted mobile phone number. When received, the user has only ten minutes to use the OTP to gain access to the e-Service. The benefit of having a short period of password validity is that it reduces a chance of having a potential intruder who manages to record an OTP to abuse it. Another benefit gained from this technique is that the user will immediately know if there is any malicious attempt to compromise his/her account.

   Another implementation scenario requires a user to possess a hardware device that supports generation of one-time passwords. The device has an embedded secret that is used as the seed for generation of OTP and does not require activation through a second factor. So the user can authenticate by providing an acceptable one-time password which proves possession and control of the device.

   In both cases, the single-factor one-time password tokens are *something you have*.

3. **Single-factor Cryptographic Token**

   This type of token requires the use of a hardware device that embeds symmetric or asymmetric cryptographic keys. Authentication is accomplished by proving possession of the device. A second factor of authentication is not required to activate the device. The most appropriate example of single-factor cryptographic token is a smart card that stores an encrypted digital certificate along with other relevant information based on a public key infrastructure (PKI). The credential contained in the card including the digital certificate and other information is then extracted with a specific

card reader to authenticate the identity of the owner. This type of token is, therefore, *something you have*.

4. Multi-factor Software Cryptographic Token

A multi-factor software cryptographic token uses a cryptographic key that is stored on disk or some other "soft" media. Similar to single-factor cryptographic token, authentication is accomplished by proving possession and control of the key. However, this type of token also requires activation through a second factor of authentication.

The multi-factor software cryptographic token is by itself *something you have*, and it may be activated by either *something you know* or *something you are*.

5. Multi-factor One-Time Password Token

Similar to single-factor one-time password token, this type of token requires a hardware device that generates one-time passwords for use in authentication and also requires activation through a second factor of authentication. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). Example of this type of token is RSA SecurID® which embeds a seed that not only makes each token unique but is also used for random generation of one-time password consisting of 6 numerical strings at a time. To achieve authentication with the generated OTP, it requires activation using an associated username and PIN code.

The multi-factor one-time password tokens are *something you have*, and may be activated by either *something you know* or *something you are*.

6. Multi-factor Hardware Cryptographic Token

A multi-factor hardware cryptographic token generates, stores, and protects cryptographic keys that require activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. Same as other multi-factor authentication mechanisms, the second factor of authentication may be achieved through some kind of entry pad, a biometric reader, or a direct computer interface. Example of this type of token is what is commercially known as Hardware Security Module or HSM which exhibits very secure cryptographic key generation mechanisms for strong authentication. It also safeguards the generated digital keys inside itself with high degree of logical and physical protection, such as tamper evidence, physical tamper resistance, and key zeroing mechanism. On the logical side, any interaction with the HSM requires multiple layers of security and access control including but not limited to username and password, USB tokens and PIN code.

The multi-factor hardware cryptographic tokens are *something you have*, and may be activated by either *something you know* or *something you are*.

The guideline of token type selection for different levels of assurance is presented in Table 7. Anyway, it is important to note that in order to achieve requirements and implementation details of each token type, reference to the source provided below should be made.

Token Type	Assurance Level			
	LoA1	LoA2	LoA3	LoA4
Memorized Secret Token	✓*	✓*		
Single-factor One-Time Password Token		✓		
Single-factor Cryptographic Token		✓		
Multi-factor Software Cryptographic Token			✓	
Multi-factor One-Time Password Token				✓
Multi-factor Hardware Cryptographic Token				✓

* Depend on implementation details

Table 7: Assurance levels and e-authentication schemes

Source: *Summarized from NIST Special Publication SP-800-63-1 Section 6.3: Token Assurance Levels, page 48*

2.3.2 Token and Credential Management

In the section, activities related to credential management, such as token verification and generation, token storage and security controls, will be discussed. Six types of activities and implementation requirements for each assurance level have been defined based on the analysis of NIST Special Publication 800-63-1. Basically, higher assurance levels will include all objectives of the lower levels with some additional requirements to add more controls and strictness to the process. Based on the same principal, higher assurance level will require more reliability and credibility of identity. As such, more rigorous processes regarding the token and credential management are definitely required.

The table on the next page describes a short summary of requirements for related activities.

Token and Credential Management Activity	Assurance Level			
	LoA1	LoA2	LoA3	LoA4
Credential storage	Access controls on files of shared secret	All requirements defined in lower level Protect shared secret files with password or encryption	All requirements defined in lower levels Shared secret files stored in a FIPS 140-2 Level 2 or higher hardware cryptographic module	All requirements defined in lower levels
Token and credential verification services	Token secrets should not be revealed	All requirements defined in lower level Verification processes through cryptographic channel(s)	All requirements defined in lower levels	All requirements defined in lower levels
Token and credential renewal / re-issuance	No requirement	Proof-of-possession of the current token Interact through protected session e.g. SSL/TLS	All requirements defined in lower levels Renew and re-issue token only before the current token is expired	All requirements defined in lower levels Sensitive data transfers are cryptographically authenticated using short-term key(s) that expire within 24 hours.
Token and credential revocation and destruction	No requirement	Revoke or destroy within 72 hours	Revoke within 24 hours	Revoke within 24 hours Destroy within 48 hours
Records retention	No requirement	7 years and 6 months	All requirements defined in lower levels	All requirements defined in lower levels
Security controls	No requirement	Employ security controls [SP 800-53] Satisfy the low baseline of the minimum assurance requirements	Employ security controls [SP 800-53] Satisfy the moderate baseline of the minimum assurance requirements	Employ security controls [SP 800-53] Satisfy the moderate baseline of the minimum assurance requirements

Table 8: Token and credential implementation requirements

Source: *Summarized from NIST Special Publication SP-800-63-1 Section 7.3: Token and Credential Management Assurance Levels, page 60*

3. Legal Infrastructure and Readiness of ASEAN Member States

In 2015, ASEAN members will be associated into ASEAN Economic Community with the purpose of seeking corporation for promoting economic and social living among Member States. It is envisaged that information technology, as mechanism and means, will play a pivotal role in developing economic system, especially in facilitating electronic transactions and improving business operations to be more effective.

In the era of information technology, electronic transactions among ASEAN Member States have been increased, largely owing to the increased awareness and interest of the citizens. This pattern will be remarkably clearer after the year 2015. Electronic transactions will not anymore be limited within a particular area or region but instead become widespread beyond any physical boundaries to create an interconnected, the so-called "Digital World". Such growing number of transactions is the crucial basis for fully connecting the member states.

Nonetheless, cross-border electronic transactions still have some limitations and not yet been fully utilized due to difference in user's cognition and legal infrastructure among ASEAN Member States. For this reason, all members have noted that creating security and trust through the development of related legal framework is a must to ensure reliable, secure, and smooth transactions, guarantee proper legal binding and court's acceptance of legal validity of the transaction in case of any dispute before the court, and to prevent against cybercrime issues. With this effort, it is expected that all member states will develop and share an equivalent legal standard and practices.

3.1 Information Technology Legal Infrastructure

Generally, the laws in relevant with Information Technology Legal Infrastructure and Secure E-transaction are as follows:

1. Electronic Transaction

Electronic Transaction Law specifies basic principles relating to the legal effect on Electronic Transactions. The Law focuses on the functional equivalency between electronic documents and traditional paper-based documents as required by laws or by an agreement between the parties. In case a transaction is created in electronic format, this Law values that the transaction has an equivalent legal binding as in written and paper-based format. Another important characteristic is the legal effects on electronic signature and evidence. This Law is, therefore, a vital part of the legal infrastructure required for promoting trust to parties involving in electronic transactions and enhancing the development of new innovation for supporting every format of electronic transactions created in the future.

2. Electronic Signature

Electronic Signature Law or Digital Signature Law is the other vital one created for supporting application of electronic signature in electronic transaction as it is a crucial part of Authentication that affects legal liability. The purpose of this Law is to provide standard by which the legal value of Electronic Signature, created by any technologies, can be equivalent to hand writing signature. However, the Electronic Signature Law in some countries is not enacted in a separate legislation, but contained as a part of Electronic Transaction Law.

The crucial role of Electronic Signature is to serve the security measurement requirements, such as the Identification, Authentication, Integrity, Non-repudiation and Confidentiality. Authentication is the important mechanism especially in this age at which the Authentication technology is developed in a variety of format. Considering the goal is security and safety, the format that is acceptable by international is 2-Factor Authentication, such as, the application of PKI: Public Key Infrastructure or TOKEN. Therefore, it will be necessary for ASEAN to develop the policy and relevant laws for enhancing such technology application and supporting cross border electronic transactions. This development should be made by encouraging each Member State to implement the legal principle on CA: Certificate Authority which is the important unit for impelling PKI technology. In addition, the qualification of Certificate Authority must be provided in order to establish the same level and standard for applying to Electronic Signature in cross border electronic transactions.

The status of Law on Certificate Authority of ASEAN member states is detailed in the *Appendix A: Certificate Authority Laws of ASEAN Member States*.

3. Personal Data Protection

With the characteristic of electronic transaction, large volumes of personal data are created, transmitted and stored especially by an electronic system service provider regardless of in private or public sector. Such data must be protected from unauthorized access which may

cause damage to the owner. For examples, identification number, passport number, social security number, credit card number, password and personal photograph. The Law therefore is necessary is to provide appropriate level of supervision and responsibility for personal data, including the protection of unauthorized access, amendment and misuse of personal data. As such, Personal Data Protection Law is the important Legal Infrastructure for sustaining and assisting the secured e-transaction in ASEAN member states.

4. Consumer Protection

With the proliferation of electronic commerce, various services and products are offered to the consumer via electronic transaction. The trader and advertising operator have applied both marketing and advertising practices for promoting their sale of goods and services. Electronic commerce is sometimes difficult for consumer to establish the reliability of the quality and prize of product/service or marketing environment. In case there is no Consumer Protection Law exists, the consumer may be damaged and usually be treated unfairly. In order to secure the consumer in electronic commerce, the Consumer Protection Law therefore must be created.

5. Cyber Crime

Cyber Crime Law (Computer Crime Law or Computer Misuse Law) is created to protect and eliminate criminal acts in which using computer and information technology as a tool or a target or a place of illegal activity to cause damage to others or to receive illegal returns. Examples include online trafficking, software piracy and virus spreading. The scope of Cyber Crime Law should include investigation mechanism and compilation of electronic evidence for initiating criminal procedure against an offender. There are 2 formats of legislative; i) to amend and add the new content in the existing Criminal Code or ii) to create new legislative particularly.

The Information Technology Legal Infrastructure as aforementioned above is the important mechanism for supporting electronic transaction can be operated stability and safety.

As there will be regional economic integration of ASEAN Members (AEC) in 2015 with the basis objective to have free flow of goods, trade, investment, and capital to improve ASEAN competitiveness by transforming the economic group into a single market and production base, it is thus necessary to harmonize national standard of each member states to be international standards. There are various model laws or guidelines which ASEAN member states can adopt the principle into its domestic laws regarding information technology and secure electronic transactions including UNITRAL model law on Electronic Commerce, UNICTRAL model law on Electronic Signature, the Council of Europe Convention on Cyber Crime, and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, etc.

3.2 Readiness of Legal Implementation

For the readiness of legal implementation in each ASEAN Member State, the details are summarized in the topics below:

1. Brunei Darussalam

Brunei Darussalam has Electronic Transaction Act revised in year 2008. The Act was drawn from UNCITRAL Model Law on Electronic Commerce. The Act deals with legal aspects of the recognition of Electronic contracts/records, Electronic signatures Retention of records by electronic means and the guidance for Legislative framework for Certification Authorities.

In respect of Cyber Crime Law, Brunei has Computer Misuse Act which has been revised in year 2007 and then promulgated in the same year.

However, for National Data Protection Policy, Brunei is now in the process of drafting by doing public hearing.

2. Cambodia

Cambodia is the new Member State of ASEAN called CLMV group (Cambodia, Laos, Myanmar, and Vietnam). Cambodia currently has several Laws that support the reliance on electronic transaction such as Draft Law on Electronic Commerce and Cyber Law 2012. Both Laws are now in the legislative process.

However, Consumer Protection Laws now exists in Cambodia for protecting consumer from purchasing any products and services, which is Law on the management of Quality and Safety of Products and Services, promulgated on June 21, 2000 (LMQSPS). The result of the research and study revealed that there is no Personal Data Protection Law available in Cambodia due to Cambodian people may not interesting and not have seen the necessity of personal data. Since Cambodia has just arranged the national election under a democracy system recently, it therefore necessary to take steps to enhance Cambodian people having legal knowledge evens more.

3. Republic of Indonesia

Politics of Indonesia takes place in a framework of a presidential representative democratic republic. In terms of the laws, the relevant legislation and supporting electronic transactions are Law of the Republic of Indonesia number 11 of 2008 concerning information and Electronic Transaction Bill of 2008 and Government Regulation Number 82 of 2012 on Electronic System and Electronic Transaction Operation (“ESETO”).

In respect of Cyber Crime Law, Indonesia has Cyber Crime Bill 2010 which has been enforced since 2010. In addition, Consumer Protection Law was enacted in year 1999. However, Personnel Data Protection Law has not yet been created separately in Indonesia, but it is available in Article 26 of the Law on Information and Electronic Transaction 2008.

4. Lao PDR

Currently, the Information Technology Law in Lao is extremely being developed especially in e-Government Services, e-Commerce, e-banking and e-taxation. With such development, the law relevant to Electronic Transaction has been drafted and now in the process of approval by the National Legislative before promulgating. Such draft of Electronic Transaction Law is expected to be approved within December 2012.

The draft is drawn from UNCITRAL Model Law on Electronic Commerce, which approves the legal status of electronic communication/message, electronic contracts, electronic signatures/digital signature and electronic records. The purpose of the draft of Electronic Transaction Law is to promote reliance on electronic transaction and to protect right and benefit of consumer and parties in electronic transaction. The Law therefore will enable electronic transaction to be completed even more effectively and will contribute to the development of social and economic.

However, Computer Crime Law is not yet available in Lao, only Consumer Protection Law which has been enacted since 2010. Also, there is still unclear in the matter of personal data protection.

The research revealed that Lao needs the assistance in Information Technology skills and training especially in policy and legal perspective as the majority of people have limitation of knowledge and understanding of electronic commerce. Furthermore, Lao also needs financial support for contributing in their electronic transaction activities in the near future.

5. Republic of Malaysia

Currently, there are several relevant legislations were enacted in Malaysia namely, i) Electronic Commerce Act 2006 that establishes legal status of electronic message, ii) Electronic Government Activities Act 2007 that relevant to an acceptance of electronic message contacted between government sector and private sector, iii) Digital Signature Act 1998 (was enacted separately from ETA) that recognizes the functional equivalency between handwriting signature in paper-based and electronic signature and iv) Digital Signature Regulation.

Malaysia has Computer Crime Act 1997 to provide principle of unauthorized access to computers and modification of the contents of the computer. To develop the creation of Information Technology Laws, Malaysia has provided a framework for physical operation and a plan for developing Cyber Crime Legal Infrastructure and International Telecommunication Law.

In terms of Consumer Protection Law, the Consumer Protection Act 1999 has been enacted in year 1999 and also has Personal Data Protection Act 2010.

The cross boarder electronic transactions have just been initiated in Malaysia for enhancing national services business. Presently, National Window for Trade Facilitation ASEAN Single Window, E-KL and Business Licensing Electronic Support Service (BLESS) are now being supported by the Government of Malaysia.

6. Republic of the Union of Myanmar

On November 24, 2002, Myanmar has signed e-ASEAN Framework Agreement. Currently, the legislation relating to Electronic Transactions is Electronic transaction Law 2004. The Law has provided Central Body accredited root certification authority since year 2008. With this respect, Authentication technology, Integrity technology, Confidentiality technology and Non-Repudiation technology are applied in CA.

In respect of Cyber Crime Law, Myanmar also has Computer Science Development Law 1996 and Wide Area Network Notification the Communications Law which was issued in notification for communication. However, neither specific law on Consumer Protection nor Personal Data Protection exists in Myanmar.

7. Republic of the Philippines

At the present moment, the Philippines has Electronic Commerce Act 2000 which is relevant to Electronic Transactions, Implementing Rules and Regulations on Electronic Authentication of Electronic Signatures Executive Order No. 810 which is relevant to Electronic Signature and enacted separately from Electronic Transaction, and Institutionalizing the Certificate Scheme for Digital Signature and Directing the Application of Digital Signatures in E-Government Service promulgated in year 2009.

With the proliferation of electronic services such as call centers service, therefore, the Data Personal Protection Law 2012 in Philippines is necessary to be in line with foreign requirement especially in respect of data processing.

The Philippines has also enacted the Cybercrime Prevention Act 2012 on September 12, 2012 to criminalize offenses against computer systems and computer data and to address legal issues concerning online transactions. The law is criticized for its definition of online libel, violation of personal rights and legal penalties for Internet defamation. In October 2012, the Supreme Court of the Philippines issued a temporary restrain order stopping implementation of the Act until further orders from the court to review whether the legislation violates civil rights or not.

8. Republic of Singapore

Currently, the available legislation on Electronic Transactions in Singapore is Electronic Transaction Act 2010, which was revised in order to be in line with United Nations Convention on the Use of electronic contracts (e-Contracts). The UN Convention is a model law providing standard provisions and standard format for Cross Border Electronic Transactions. The ratification for implementation of the model law was made in July 2010 and Singapore ETA Law promulgated on March 1, 2013.

The ETA Law was revised in i) e- Government in order to facilitate the use of electronic transactions in the public sector, ii) guidelines for controlling a Certification Authorities (CAs) in voluntary accreditation, iii) elimination of a requirement for Bank guarantee, iv) insurance, v) minimum capital requirement for applying a CA license as each CA in Singapore is not required to have the license, and vi) guidelines for modifying Information Technology security policy in Audit Checklist.

9. Kingdom of Thailand

Electronic Transaction Act B.E. 2544 and the second one B.E. 2551 are the Laws that facilitate the spread of Electronic Transaction. The reason for promulgation this Act is to provide i) legal recognition of electronic transactions by enabling them to have the same legal effect as that given to transactions made by traditional paper means, ii) recognition methods of dispatch and receipt of data messages, and iii) recognition of the use of electronic signatures and evidential admissibility of data messages.

In terms of Cyber Crime Law, Thailand has Computer Related Crime Act 2007 which is the important Law since computer system has played a vital role in daily life of Thai people. Therefore, it may cause a huge effect to national public order in case cyber-crime is committed. There are several regulations and notifications issued under the Computer Related Crime Act, namely, i) Regulations on the arresting ,confining, searching, investigating and instituting criminal prosecution against the offender under the Computer Crime Act B.E. 2550, ii) Notification of the Ministry of Information and Communication Technology on criteria on collection of computer traffic data of service provider B.E. 2550, iii) Ministerial Regulations providing form of letter on the seizure or attachment of computer system B.E.2551, and iv) Notification of the Ministry of Information and Communication Technology on criteria on qualification of authorized official under the Computer Crime Act B.E.2550.

For electronic Authentication, Thailand and Australia had agreed in mutual to sign in Thai-Australia Free Trade Agreement and it came into effect in year 2008. According to Article 1104 of the Agreement, each party shall maintain domestic legislation for electronic authentication, shall work towards the mutual recognition of digital certificates at government level, based on internationally accepted standards, and shall encourage the interoperability of digital certificates in the business sector. Such Articles represented that Thailand accepts and supports Cross boarder Electronic Transaction and corporate to support the Authentication and digital certificates for operating Electronic Transaction.

In terms of Electronic Data Protections, the Personal Data Protection Act has not yet become effective, as the draft is currently on its consideration and approval process of the parliament. This Act follows the principles set out under the worldwide accepted model, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

However, at present, the principle of Personal Data Protection was contained in several legislations, such as, i) the Official Information Act B.E. 2540 enforced on government sector and public agency, ii) the Royal Decree Prescribing Criteria and Procedures of Electronic Transactions in the Public Sectors B.E. 2549 provides the Government Sector is in charge of prescribing policy and guidelines on Personal Data Protection in case of compilation, storage, utilization, and publication of information or fact which may be able to, directly or indirectly, identify a person iii) Notification of the Electronic Transactions Commission on Policy and Practice Guideline on Maintenance of Information Security of a Government Agency B.E. 2553 provides basic guidelines and examples to Government Sector for applying as a framework when formulating policy and guidelines on Personal Protection, and iv) Regulation on Protection of Undisclosed Information Relating to Pharmaceutical.

10. The Socialist Republic Vietnam

Presently, Vietnam has Law on Information Technology 2006, Law on Electronic Transaction 2005, and the Management and use of internet services, which is dealing with security and safety in Electronic Transactions. In addition, Privacy Law is also available in Article 46 of E-Transactions 2005.

In terms of Cyber Crime, the Management and Use of Internet Services Decree 2001, a substitute law, has been issued in year 2001.

The status of Information Technology Legal Infrastructure needed to establish a confidence in Electronic Transactions among ASEAN Member States can be summarized in the *Appendix B: Information Technology Legal Infrastructure of ASEAN Member States*.

4. Conclusions and Recommendations

The ASEAN Economic Community (AEC) to be launched in 2015 will bring more capital flow and movement of resources among the member states in this region. Certainly, this opens extensive opportunities to both private and public sectors. Business executives may decide to open new branches or to penetrate markets in other member states as a part of their business growth strategies. Besides, government agencies within the Community may collaborate, join development efforts and introduce new cross-border public services to better promote standard of living and social welfare of the ASEAN people. For the most part, electronic transactions will play a key role in enabling these initiatives. As electronic transactions can happen in different forms and use different technologies, there exist both technical and legal challenges that should be put into considerations.

From the technical perspective, the challenge is how to appropriately and reliably authenticate involving parties in a way that everyone can trust and act upon the exchanged information. This has long been a global issue that experts and practitioners try to solve. As part of their efforts, several guidelines and international standards have been developed. From the analysis, they share the same principle of technology neutrality, which helps avoid technology mandates and allows the proposed framework to be widely adopted for different applications. As summarized in prior sections, this report suggests that ASEAN adopts the risk-based approach to authentication and methodologies for performing risk assessment (Section 2.1), identity proofing and verification (Section 2.2), and credential management (Section 2.3) required for intra-ASEAN secure transactions.

From the legal point of view, there exist differences in the capacity of legal infrastructure to support electronic transactions among ASEAN Member States. While some Member States have already had equivalent laws and regulations, the majority others' are under development. When looking deeper into mechanisms for supporting and enforcing the existing laws, there are still gaps to be bridged in terms of supporting standards and implementation procedures. Differences in criteria for acknowledging foreign CA and personal data protection standards are examples of critical factor that adversely affect people' confidence and also deters cross-border electronic transactions. However, almost all cases require judiciary's discretion. Therefore, harmonization of laws and regulations among the Member States is mandatory in order to raise confidence and acceptance.

Last but not least, this report provides a complete technical framework based on LoA model (LoA: Level of Assurance) and legal studies which give a leap towards long-term and sustainable cross-border electronic transactions in line with the Action Item "Promote secure transactions within ASEAN" under Initiative 2.4 Build trust. Nevertheless, there are some remaining steps which require active participation, which can be in the forms of seminar and workshop, from ASEAN Member States in order to address detailed implementation and legal issues. These remaining steps will be carried out during year 2014 and 2015 in order to produce agreed secure e-transaction classification, including the use of 2-factor authentication, for a selected sector in addition to recommendations for the intra-ASEAN secure transactions MRA model based on the agreed classification.

Appendix A: Certificate Authority Laws of ASEAN Member States

Country	Legislations on Electronic Signature	Regulations for Control of CA	Recognition of Foreign CA Clauses	Types of CA regulation
Brunei	Electronic Transactions Act (2008 edition)	Electronic Transactions Act (2008 edition), Part X Regulation of Certification Authority (Not yet effective)	Clause 43 of Electronic Transactions Act (2008 edition, Part X Regulation of Certification Authority on Recognition of Foreign Certification Authority provides that the minister may, by order published in the Gazette recognize certification authorities outside Brunei Darussalam that satisfy the prescribed requirements for any of the following purpose (a) The recommended reliance limit, if any, specify in the certificate issued by the certification authority; (b) The presumption referred to in section 20(b) (ii) and 21 (c) the standards to be maintained by certification authorities (d) …	Licensing
Cambodia	Draft Law on Electronic Commerce (as of 13 December 2007)	1. Draft Law on Electronic Commerce (as of 13 December 2007) 2. (Draft) Sub Decree on Electronic Transactions: Part X / Law on Electronic Transactions	Article 15 of Draft Law on Electronic Commerce (as of 13 December 2007) regarding Issuance of Regulations provides that (1) With the approval of the Prime Minister, and in consultation with other Ministerial Departments, the Ministry of Commerce is empowered, where it considers necessary, to draft and issue regulations governing all or any the following matters: (d) the legal recognition of foreign Certification Service Providers, any	Not specified

Country	Legislations on Electronic Signature	Regulations for Control of CA	Recognition of Foreign CA Clauses	Types of CA regulation
Cambodia (con't)			Certificates issued by them or the provision of other services. According to Article 30 of (Draft) Sub Decree on Electronic Transactions: Part X / Law on Electronic Transactions, the Controller may issue statements for the recognition of certification authorities outside Cambodia which may include a statement of the extent of the recognition.	
Indonesia	Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transaction Bill of 2008	1.Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transactions 2. Government Regulation Number 82 of 2012 on Electronic System and Electronic Transaction Operation ("ESETO")	Article 13 of Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transactions provides that Foreign Electronic Certification Service Provider that operates in Indonesia must be registered in Indonesia.	Not specified
Laos	(Draft) Electronic Commerce Law 2006	(Draft) Electronic Commerce Law 2006	A Recognition Clause has not been developed for foreign digital signatures, although it is envisaged that the legal recognition of foreign Certification Service Providers and any certificates issued by them may be the subject of future regulations	Not specified
Malaysia	1. Digital Signature Act of 1997 2. Digital Signature Regulations 1998 3. Digital Signature (Exemption) Order 1999	1. Digital Signature Act 1997 2. Digital Signature Regulations 1998	Section 19 of Digital Signature Act 1997 provides that the Commission may recognize CAs licensed or otherwise authorized by governmental entities outside Malaysia that satisfy the prescribed requirements under the Act Part 10 of the Digital Signature Regulations 1998 provide for procedures for recognizing a foreign CA.	Licensing

Country	Legislations on Electronic Signature	Regulations for Control of CA	Recognition of Foreign CA Clauses	Types of CA regulation
Myanmar	Electronic Transaction Law of 2004	Electronic Transaction Law of 2004	Section 10 of the Electronic Transaction Law 2004 provides that the Control Board shall exercise and carry out the following functions and powers under the guidance of the Central Body: (m) m) recognizing any foreign certification authority in accordance with the stipulations;.	Licensing
Philippines	1. Electronic Commerce Act 0f 2000 2. Joint Department Administrative Order No. 02 Series of 2001, Implementing Rules and Regulations on Electronic Authentication of Electronic Signatures (status-effective on 28 September 2001) 3. Executive Order No. 810, Institutionalizing the Certificate Scheme for Digital Signature and Directing the Application of Digital Signatures in E-Government Service (2009) (status-effective on 15 June 2009)	Executive Order No. 810, Institutionalizing the Certificate Scheme for Digital Signature and Directing the Application of Digital Signatures in E-Government Service (2009) (Section 3 d)	Section 15 of Joint Department Administrative Order No. 02 Series of 2001, Implementing Rules and Regulations on Electronic Authentication of Electronic Signatures expressly recognizes foreign certificates and electronic signatures as follows, (a) In determining whether, or the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the issuer had its place of business (b) Parties to commercial and other transactions may specify that a particular information certificate or supplier of certification services, class of supplies of certification service or class of certificates must be used in connection with messages or signature submitted to them (c) Where parties agree, as between themselves, to the use of certain types of electronic signatures and certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition.	Accreditation

Country	Legislations on Electronic Signature	Regulations for Control of CA	Recognition of Foreign CA Clauses	Types of CA regulation
Singapore	Electronic Transactions Act 2010	Electronic Transactions Act of 2010	Clause 22(3) (e) of 1. Electronic Transactions Act of 2010 provides that (3) Without prejudice to the generality of subsection (1), the Minister may make regulations to provide for the cross-border recognition of specified security procedure providers or specified security procedures or any processes or records related thereto, Including any requirements — (e) that ----- (i) the specified security procedure providers have been registered, accredited or licensed; (ii) the processes have been specified; or (iii) the records have been registered, under a particular registration, accreditation or licensing scheme (as the case may be) established outside Singapore;	Accreditation
Thailand	1. Electronic Transaction Act of 2001 2. Guideline of Certificate Policy and Certificate Practice Statement 2009 3. Notification of Electronic Transaction Commission on the guideline for preparation of Certificate Policy and Certificate Practice Statement of Certificate Authority B .E. 2552 (2009)	(Draft) The Royal Decree on CA Regulation (expected to be enacted shortly)	Section 31 of Electronic Transactions Act 2002 provides that an electronic signature created or used in a foreign country shall have the same legal effect as along as if the level of reliability is not lower than as prescribed in the Act.	Licensing

Country	Legislations on Electronic Signature	Regulations for Control of CA	Recognition of Foreign CA Clauses	Types of CA regulation
Vietnam	1. Electronic Transaction Law of 2005 2. Decree No. 26/2007/ND-CP dated 15/02/2007 of the Government providing in detail the implementation of the Law on electronic transaction on digital signature and service of digital signature certification.	1. Electronic Transaction Law of 2005 2. Decree No. 26/2007/ND-CP dated 15/02/2007 of the Government providing in detail the implementation of the Law on electronic transaction on digital signature and service of digital signature certification.	Article 27 of the Electronic Transaction Law 2005 provides for the government to recognize the validity of foreign e-certificates and e-signatures in condition that such e-signatures or e-certificates are equivalent to the reliability of e-signature and e-certificate in accordance with the legitimate provisions.	Not specified

Appendix B: Information Technology Legal Infrastructure of ASEAN Member States

Country	Legislations on Electronic Transactions	Legislations on Digital Signature	Legislations on Cybercrime	Legislations for Consumer Protection	Legislations for Data Protection
Brunei	1. Electronic Transactions Act (Revised 2008) 2. Electronic Transactions Act revised 2008 3. Telecommunications Order, 2001 4. Authority for Info-Communications Technology and Industry of Brunei Darussalam Order, 2001; 5. Broadcasting Order, 2000; 6. Telecommunications Successor Company Order, 2001;	Electronic Transactions Act (2008 edition)	Computer Misuse Act (Revised 2007)	Consumer Protection (Fair Trading) Order 2011	(Draft) National Data Protection Policy
Cambodia	1.(Draft) Law on Electronic Commerce (as of 13 December 2007) 2.(Draft) Sub Decree on Electronic Transactions: Part X / Law on Electronic Transactions	Draft Law on Electronic Commerce (as of 13 December 2007)	Cyber Crime Law (is Drafting – 2012) Information Technology Act	Law on the management of Quality and Safety of Products and Services (21 June 2000) "LMQSPS"	N/A
Indonesia Indonesia	1. Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transaction of 2008 2. Government Regulation Number 82 of 2012 on Electronic System and	1. Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transaction Bill of 2008 2. Government Regulation Number 82 of 2012 on	Cyber Crime Bill 2010	Consumer Protection Law (enacted in 1999)	The Law on information and Electronic Transaction 2008 (article 26)

Country	Legislations on Electronic Transactions	Legislations on Digital Signature	Legislations on Cybercrime	Legislations for Consumer Protection	Legislations for Data Protection
(con't)	Electronic Transaction Operation ("ESETO")	Electronic System and Electronic Transaction Operation ("ESETO")			
Laos	(Draft) Electronic Commerce Law Currently is in the process of National Assembly	N/A	N/A	Law on Consumer Protection 2010	N/A
Malaysia	1. Electronic Commerce Act of 2006 2. Electronic Government Activities 2007 3. Digital Signature Act 1997 4. Digital Signature Regulations 1998	1. Digital Signature Act of 1997 2. Digital Signature Regulations 1998 3. Digital Signature (Exemption) Order 1999	Computer Crime Act of 1997	The Consumer Protection Act 1999 ("CPA")	Personal Data Protection Act 2010
Myanmar	1. Electronic Transaction Law of 2004 2. Wide Area Network Notification 3. (Draft) The Communications Law	Electronic Transaction Law of 2004	Computer Science Development Law of 1996	N/A	N/A
Philippines	Electronic Commerce Act 2000	Implementing Rules and Regulations on Electronic Authentication of electronic signatures Executive order No.810	Cybercrime Prevention Act 2012 (currently, the supreme court of the Philippines issued a temporary restrain order and extended suspension of the Act until further orders from the court)	Republic Act No.7034 The Consumer Act of Philippines	Data Privacy Act 2012

Country	Legislations on Electronic Transactions	Legislations on Digital Signature	Legislations on Cybercrime	Legislations for Consumer Protection	Legislations for Data Protection
Singapore	1. Electronic Transactions Act 2010 2. Electronic Transactions (Certificate Authority) Regulations 1999	Electronic Transactions Act 2010	Computer Misuse Act of 1998	Consumer Protection Act (Amendment 2012)	Personal Data Protection Act 2012 ("PDPA")
Thailand	1.Electronic Transaction Act of 2001 The Royal Decree prescribing criteria and procedures for Electronic Transactions of the Government Sector B.E. 2549 (2006) 2 .Guideline of Certificate Policy and Certificate Practice Statement 2009 3.Notification of Electronic Transaction Commission on the guideline for preparation of Certificate Policy and Certificate Practice Statement of Certificate Authority B .E. 2552 (2009) 4. Notification of the Electronic Transactions Commission on Policy and Practice Guideline on Maintenance of Information Security of a Government Agency B.E. 2553 (2010) 5. Notification of the Electronic Transactions Commission on Policy and	1. Electronic Transaction Act of 2001 2. Guideline of Certificate Policy and Certificate Practice Statement 2009 3. Notification of Electronic Transaction Commission on the guideline for preparation of Certificate Policy and Certificate Practice Statement of Certificate Authority B .E. 2552 (2009)	1. Computer Related Crime Act of 2007 2. Regulations on the arresting ,confining, searching, investigating and instituting criminal prosecution against the offender under the Computer Crime Act B.E. 2550 (2007) 3. Notification of the Ministry of Information and Communication Technology on criteria on collection of computer traffic data of service provider B.E. 2550 (2007) 4. Ministerial Regulations providing form of letter on the seizure or attachment of computer system B.E.2551 (2008) 5. Notification of the Ministry of Information and Communication Technology on criteria on qualification of authorized official under the Computer	Consumer Protection Act B.E.2522 (1979)	1. (Draft) Personal Data Protection Act B.E… (under consideration) Trade Secret Act B.E. 2545 (Section 15) 2. (Draft) Regulation on Protection of undisclosed information relating to pharmaceutical data

Country	Legislations on Electronic Transactions	Legislations on Digital Signature	Legislations on Cybercrime	Legislations for Consumer Protection	Legislations for Data Protection
Thailand (con't)	Practice Statement on Personal Data Protection of a government agency B.E. 2553 (2010) 6. The Royal Decree Regulating Electronic Payment Services Business B.E. 2551 (2008) 7. The Royal Decree on Security Procedures for Electronic Transactions B.E. 2553 (2010)		Crime Act B.E.2550 (2007)		
Vietnam	1. Law on e-Transactions No.51/2005/QH11 2. Decree No. 26/2007/ND-CP dated 15/02/2007 of the Government providing in detail the implementation of the Law on electronic transaction on digital signature and service of digital signature certification. 3. Law on Information Technology 2006	1. Electronic Transaction Law of 2005 2. Decree No. 26/2007/ND-CP dated 15/02/2007 of the Government providing in detail the implementation of the Law on electronic transaction on digital signature and service of digital signature certification. 3. Decree No.106/2011 ND-CP Supplements and amends a number of articles in Decree No.26/2007/ND-CP	Management and Use of Internet Services Decree 2001	Consumer Protection Law of 2010	1.Vietnam has a short privacy section on E-Transactions 2005 (Article 46) 2.Circular No.25/2010/TT-BTTTT

Appendix C: Case Studies

Thailand

One of the most well-known electronic services in Thailand is internet banking. The latest statistical data from Bank of Thailand reveals that the country has about 8 million internet banking accounts out of 24 million internet users.

Since internet banking relates a great deal with monetary factors, impacts caused from authentication failure are perceived to be the highest on financial loss and unauthorized release of sensitive financial information. Besides, commercial banks who offer internet banking service are very concern about the security of the entire authentication process as a security flaw can seriously damage their reputation. Based on these factors, LoA4 (Very High Confidence) is therefore recommended for this type of transaction.

Impact Categories	Assurance Level Impact Profiles			
	LoA1	LoA2	LoA3	LoA4
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interests	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

From implementation viewpoint, below is the common practice of commercial banks in Thailand.

Activity	Mechanisms
Registration	Government ID card + In-person only
Login	username/password * Some with CAPTCHA
Add bank account	Login + OTP
Transfer	Login + OTP

European Union (EU) STORK Large-Scale Pilot

STORK (**S**ecure identi**T**y acr**O**ss bo**R**ders lin**K**ed) was launched by the European Commission in 2008. STORK's basic underlying principle is that systems that exist in the different Member States can be linked through an EU-wide eID management (eIDM) platform which leaves intact the national approach to identification and authentication.

Six pilots were put into production by STORK to demonstrate that this kind of eID environment can work in a user-friendly way. They consist of Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery, Change of Address and the European Commission Authentication System "ECAS" Integration.

The case study to be discussed here is Safer Chat. The project was initiated with the objective of providing safer Internet communication for children and teenagers. In Safer Chat, teachers in different countries will create projects in the classroom using the open source e-learning framework Moodle as an online platform for cross-border e-learning and safer chat rooms for their students within specified age groups. The students will work with their peers in other countries and create peer-to-peer educational packages.

From risk assessment on six impact categories as discussed in *Section 2.1: Assurance Levels and Risk Assessments*, authentication failure of this particular transaction can lead to unauthorized release of sensitive information such as name, address, and school name of teenagers, which can in turn increase the risk of criminal violations and personal safety. However, since the system does not collect and store complete information from the users, impacts caused from information leakage are limited and therefore categorized as having moderate risk.

Assurance level impact profiles are shown in the table below. It is recommended that this transaction requires at least LoA3 (High Confidence).

Impact Categories	Assurance Level Impact Profiles			
	LoA1	LoA2	LoA3	LoA4
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interests	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

Estonia

Estonia, officially the Republic of Estonia, is a state in the Baltic region of Northern Europe. Estonia is a democratic parliamentary republic divided into fifteen counties, with its capital and largest city being Tallinn. Estonia's population of 1.3 million makes it one of the least-populous member states of the European Union, Eurozone and the North Atlantic Treaty Organization. A developed country with an advanced, high-income economy, Estonia has the highest gross domestic product per person among the former Soviet republics, and is a member of the Organisation for Economic Co-operation and Development [2].

Estonia has by far the most highly-developed national ID card system in the world [3]. Multiple indicators have supported that Estonia is an information society. For example, ninety nine percent (99%) of bank transfers are performed electronically. Ninety five percent (95%) of income tax declarations made via the e-Tax Board. Sixty six percent (66%) of the population participated in the census via Internet. Numerous e-Services are offered such as e-Banking, e-Pension Account, e-Health, e-School, e-Police, and many more. Those services are integrated via Internet X-ROAD to form the Estonian Information System.

The example to be discussed is e-Prescription which was introduced in 2010. The objective is to save time for both patient and doctor by making medical appointments for routine refills unnecessary. At the pharmacy, all a patient needs to do is present an ID Card. The pharmacist then retrieves the patient's information from the system and fills the prescription. Since patients do not need to keep track of paper prescriptions, paperwork in hospitals and pharmacies are reduced. Speed and accuracy of the prescription process are expected to be greatly improved.

Since the prescription process involves health and well-being of the patients, impact on personal safety caused from authentication failure is recognized as high. As such, this type of transaction definitely requires LoA4.

Impact Categories	Assurance Level Impact Profiles			
	LoA1	LoA2	LoA3	LoA4
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interests	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

2 http://en.wikipedia.org/wiki/Estonia

3 http://e-estonia.com/component/electronic-id-card/

Appendix D: Intra-ASEAN Secure Electronic Transactions Questionnaire

Introduction

This survey is be part of the Intra-ASEAN Secure Transactions Framework project which is funded by ICT ASEAN fund. The project supports the ASEAN ICT Masterplan 2015, under Strategic thrusts 2, the Initiative 2.4. promoting the secure transaction within ASEAN.

This project will cover updating the current state of the laws, policies, and regulations related to electronic signature and digital certificate recognition in ASEAN member states as well as develop common recognition criteria of foreign electronic signature and digital certificate among ASEAN member states.

To update the existing status in ASEAN in year 2011,the questionnaire has been used as data collecting tools. The questionnaire comprises of four parts. Part 1 is respondent information; Part 2 is the business process requirement; Part 3 is the risk assessment; Part 4 is the legal policy and regulation updating.

The survey will start from 1 - 31 March 2012. All relevant agencies in each ASEAN member are encouraged to supply country information via the survey and returning it 15 of March 2012 in the following channels:

1. Your Country Focal Point

2. By e-mail at asean_survey2012@etda.or.th

By the additional documents or information are also welcome.

Your co-operation will benefit to the ASEAN members. If you have need any further information or any inquiry, please feel free to contact ASEAN_survey2012@etda.or.th or +66 2 142 2476

Part 1: Company/Organization Information

Name of Respondent:

_____

Company / Organization:

_____

Position / Job Title:

_____

Job Description:

- ☐ IT Management
- ☐ IT Staff
- ☐ Non-IT Management
- ☐ Software Developer
- ☐ Auditor
- ☐ Lawyer
- ☐ Researcher
- ☐ Others _____

Address:

_____

Telephone Number (country area number):

_____

Fax Number:

_____

E-mail address:

_____

Type of Organization:

- ☐ Govt. Ministry / Agency
- ☐ Govt./State Owned Enterprise
- ☐ University / Research Institution
- ☐ Local Owned Enterprise
- ☐ Multinational
- ☐ Others_____

Part 2: Business Requirements for e-Authentication Survey (Check all that apply)

No.	Services to be provided	Information to be accessed	User community	Assertion to be authenticated?	Registration Approach[4]	Authentication mechanism (current)	Authentication mechanism (planned)	Issues needed	Related Legal/Regulatory
1. e-Government Services									
1.1	e-Invoice ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
1.2	e-Tax Payment ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

4 Registration Approaches:
Evidence of identity (EoI) is an approach which requires individuals to present a range of documentation to validate their claim to identity.
Evidence of relationship (EoR) or "known customer" is an approach which requires individuals to establish they have an existing relationship with other agency, usually involves the presentation of documentary or knowledge-based evidence that relates to the context of the relationship between the subscriber and the relying party.
Pseudonymous registration doesn't require a user to go through either an EoI or EoR process to obtain an e-Authentication credential, but they use disguised name in order not to disclose their true name.

No.	Services to be provided	Information to be accessed	User community	Assertion to be authenticated?	Registration Approach[4]	Authentication mechanism (current)	Authentication mechanism (planned)	Issues needed	Related Legal/Regulatory
1.3	e-Customs ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
1.4	e-Passport ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
1.5	e-Voting ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

2. e-Services for Business									
2.1	Business registration ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
2.2	Online work/ resident permit ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
2.3	Online foreign business license ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

3. Online Banking/Trading									
3.1	e-Payment ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
3.2	e-Billing ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
3.3	Online Securities Trading ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

3.4	e-Procurement ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
4. Others									
4.1	e-Insurance Service ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
4.2	e-Healthcare (medical record, prescription) ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

4.3	e-Court/ Arbitration ☐ Yes ☐ No	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
4.4	Other - please identify _____	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No
4.5	Other - please identify _____	☐ Personal Info. ☐ Financial Info. ☐ _____ ☐ _____ ☐ _____	☐ Citizen ☐ Government ☐ Business ☐ Cross-border entity	☐ Identity ☐ Role ☐ Delegation ☐ Other _____	☐ Evidence of Identity ☐ Evidence of Relationship ☐ Pseudonymous Registration	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Memorised Password ☐ One-time Password ☐ PKI ☐ Biometrics ☐ Other _____	☐ Privacy ☐ Integrity ☐ Confidentiality ☐ Non-repudiation ☐ Protection of Identity ☐ Other _____	☐ Yes, please provide more information on Part 2.1 ☐ No

Part 2.1 Details for Legal/Regulatory under Part 2

Services to be provided	Name of law	Purpose of law	Relevant section	Regulatory Body	Status of the law
e.g. e Payment	The Royal Decree Regulating Electronic Payment Services Business B.E. 2551	The Royal Decree regulates the electronic payment service business provider. It prescribes that electronic payment service provider shall notify, register, or obtain a license prior to operation of service and that the Electronic Transaction Commission may prescribe regulations, procedures, and condition for service operation which may include the issues of disclosure of user's personal data, audit and maintenance of information.	All sections	Electronic Transaction Commission	Effective since 14 January 2009

Part 3: Risk Assessment

Consequence	(1.1) e-Invoice		(1.2) e-Tax Payment		(1.3) e-Customs		(1.4) e-Passport	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Inconvenience to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Risk to any party's personal safety	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Release of personally or commercially sensitive data to 3rd parties without consent	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to any client of the service provider or other 3rd party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(1.1) e-Invoice		(1.2) e-Tax Payment		(1.3) e-Customs		(1.4) e-Passport	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Financial loss to agency/service provider	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Impact on government finances or economic and commercial interests	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Damage to any party's standing or reputation	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Distress caused to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Threat to government agencies' systems or capacity to conduct their business	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(1.1) e-Invoice		(1.2) e-Tax Payment		(1.3) e-Customs		(1.4) e-Passport	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Assistance to serious crime or hindrance of its detection	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(1.5) e-Voting		(2.1) Business Registration		(2.2) Online Work/Resident Permit		(2.3) Online Foreign Bus. License	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Inconvenience to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Risk to any party's personal safety	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Release of personally or commercially sensitive data to 3rd parties without consent	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to any client of the service provider or other 3rd party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to agency/service provider	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(1.5) e-Voting		(2.1) Business Registration		(2.2) Online Work/Resident Permit		(2.3) Online Foreign Bus. License	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Impact on government finances or economic and commercial interests	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Damage to any party's standing or reputation	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Distress caused to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Threat to government agencies' systems or capacity to conduct their business	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Assistance to serious crime or hindrance of its detection	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(3.1) e-Payment		(3.2) e-Billing		(3.3) Online Securities Trading		(3.4) e-Procurement	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Inconvenience to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Risk to any party's personal safety	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Release of personally or commercially sensitive data to 3rd parties without consent	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to any client of the service provider or other 3rd party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(3.1) e-Payment		(3.2) e-Billing		(3.3) Online Securities Trading		(3.4) e-Procurement	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Financial loss to agency/service provider	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Impact on government finances or economic and commercial interests	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Damage to any party's standing or reputation	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Distress caused to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Threat to government agencies' systems or capacity to conduct their business	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(3.1) e-Payment		(3.2) e-Billing		(3.3) Online Securities Trading		(3.4) e-Procurement	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Assistance to serious crime or hindrance of its detection	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(4.1) e-Insurance Service		(4.2) e-Healthcare		(4.3) e-Court/Arbitration		Other___________________________	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Inconvenience to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Risk to any party's personal safety	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(4.1) e-Insurance Service		(4.2) e-Healthcare		(4.3) e-Court/Arbitration		Other_______________	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Release of personally or commercially sensitive data to 3rd parties without consent	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to any client of the service provider or other 3rd party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Financial loss to agency/service provider	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Impact on government finances or economic and commercial interests	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Damage to any party's standing or reputation	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Consequence	(4.1) e-Insurance Service		(4.2) e-Healthcare		(4.3) e-Court/Arbitration		Other______________________	
	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level	Likelihood	Severity level
Distress caused to any party	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Threat to government agencies' systems or capacity to conduct their business	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe
Assistance to serious crime or hindrance of its detection	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe	☐ Rare ☐ Unlikely ☐ Possible ☐ Likely ☐ Almost certain	☐ Insignificant ☐ Minor ☐ Moderate ☐ Major ☐ Severe

Part 4: Legal Update on e-Signature

Based on your answers/information on laws/legislation in your country as provided to Galaxia in 2011, as detailed in Annex A of this questionnaire, please response to the following question to update the status of relevant law and legislations of your country;

4.1 Legal Recognition of e-Signature	
4.1.1 Is there a law or regulation on electronic signature in your country?	☐ Yes, please specify information on the flowing; - Name of the law _____ - Purpose of the law _____ - Scope of implementation _____ - Amendment to such law (if any) _____ - Status of the law e.g. effective on [date], drafting, being amended _____ ☐ No (Please go to question 4.1.2)
4.1.2 What model law/foreign law is the electronic signature law based upon?	☐ UNCITRAL Model law on E-Commerce ☐ UNCITRAL Model law on Electronic Signature ☐ UN Convention on E-Contracting ☐ EC Directive on Electronic Signature ☐ Other (Please specify) _____

4.1.3 Is the electronic signature law technology neutral?	☐ Yes. Please provide supporting information. _____ ☐ No. Please provide supporting information. _____
4.1.4 What is legal effect of electronic signature under such law?	_____ _____
4.1.5 Does electronic signature under such law provide cross border functionality?	☐ Yes. Please provide supporting information. _____ ☐ No.
4.1.6 Are there any bilateral or multilateral agreement or legal framework between you and any ASEAN country in regard to electronic signature interoperability?	☐ Yes. Please provide information on key substance of the agreement and the country. _____ ☐ No.
4.2 Legal issues on Certification Authority	
4.2.1 Is there any law or legal framework on Certification Authority?	☐ Yes, please specify information on the flowing; - Name of the law _____ - Purpose of the law

	_____ - Scope of implementation _____ - Amendment to such law (if any) _____ - Status of the law □ effective date_____ □ drafting □ being amended □ No
4.2.2 What model law/foreign law is the Certification Authority law based upon?	□ UNCITRAL Model law on E-Commerce □ UNCITRAL Model law on Electronic Signature □ UN Convention on E-Contracting □ EC Directive (Please specify the name of directive/EU law) □ Other (Please specify) _____
4.2.3 What is the concept of such law/regulation?	□ Licensing □ Accreditation □ Voluntary licensing □ Other (Please specify) _____
4.2.4 Is there any authority/regulatory body responsible for supervision of Certification Authority under such law?	□ Yes. Please also provide supporting information. _____ □ No.

4.2.5 Is there requirements for Certification Authority under such law?	Requirements on; ☐ Appropriate means of verification ☐ Reliability ☐ Employment of personnel ☐ Use of trustworthy systems ☐ Measures against forgery of certificate ☐ Maintenance of financial resources ☐ Record of all relevant information ☐ Terms and conditions of service ☐ Data privacy ☐ Other (Please specify) _____
4.2.6 What are liabilities of Certification Authority for damage caused to any entity/person relying on the issued certificate under your relevant law (if any)?	_____ _____
4.2.7 How many types of Certification Authority under such law?	_____ _____
4.2.8 How many CAs have been passed?	_____ _____

4.2.9 Does your country recognize digital certificate or digital signature of foreign Certification Authority?	☐ Yes. Please provide supporting information. _____ ☐ No.
4.2.10 Is there any requirement in terms of format/form/technical tools for cross-bordered electronic documents?	☐ Yes. Please provide supporting information. _____ ☐ No.
4.2.11 Is there any law or implemented standard to facilitate cross bordered certification service?	☐ Yes. Please provide supporting information. _____ ☐ No.
4.2.12 Is there any international standards implemented to assess the reliability of cross-bordered certificates/document?	☐ Yes. Please provide supporting information. _____ ☐ No.

4.3 Data Privacy	
4.3.1 Is there a law or regulation governing the collection, use or other processing of personal information?	☐ Yes, please specify information on the flowing; - Name of the law _____ - Purpose of the law _____ - Scope of implementation _____ - Amendment to such law (if any) _____ - Status of the law □ effective on date _____ □ drafting □ being amended ☐ No
4.3.2 Under the relevant laws/regulations, how would the data privacy of a party be protected in the authentication process?	_____ _____
4.3.3 Is there any category of electronic transaction which requires protection of a party's identity?	☐ Yes. Please provide supporting information. _____ ☐ No.

4.3.4 What is the substance of data privacy provisions in relation to the authentication of identity or existence of a party/juristic person?	_____ _____

Thank for your kind co-operation for completing this survey.

(Please return your completed questionnaire to ASEAN_survey2012@etda.or.th)

Appendix E: Future Plan 2014 - 2015

Activity	Timeline											
	2014						2015					
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Focus group seminar												
Workshop												

Bibliography

1. Department of Finance and Deregulation, Australian Government Information Management Office. (2013).
National e-Authentication Framework.

2. Executive Office of the President, Office of Management and Budget. (2003).
OMB M-04-04 E-Authentication Guidance for Federal Agencies.

3. Interoperability Solutions for European Public Administrations (ISA). (2011).
Towards a Trusted and Sustainable European Federated eID system (Final Report).

4. ISO/IEC. (2013).
ISO/IEC 29115 Information technology - Security techniques - Entity authentication assurance framework.

5. National Institute of Standards and Technology. (2011).
NIST Special Publication 800-63-1 Electronic Authentication Guideline.

6. The Association of Southeast Asian Nations (ASEAN). (2011).
ASEAN ICT Masterplan 2015: We're Stronger When We're Connected.