Japan-Europe
Comparison of Legal Frameworks for Electronic Signatures

July 4th, 2017@Japan-Europe Internet Trust Symposium

Soshi Hamaguchi, Cosmos Corporation

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Definition of Electronic Signature in eIDAS Regulation

eIDAS Regulation
Article 3 (10)(11)(12)
'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

Advanced electronic signature（Article 26）

it is uniquely linked to the signatory ;

it is capable of identifying the signatory ;

It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;

it is linked to the data signed therewith in such a way that any subsequent change in the data i s detectable.

➡ PKI-based electronic signature

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Qualified Electronic Certificate

eIDAS Regulation Article 3 (15)
'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

Qualified trust service provider
➡Trust service provider who is granted the qualified status by supervisory body (government) for their facilities, identification methods and operations meeting the eIDAS regulations.

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Definition of Electronic Signature in eIDAS Regulation

eIDAS Regulation
Article 3(10)(11)(12)
'electronic signature'
➡Signature in electronic form

'advanced electronic signature'
➡PKI-based electronic signature (digital signature) which meets the requirements (ETSI standards)

'qualified electronic signature'
➡Advanced electronic signature created by a secure device such as qualified electronic certificate or a IC card.

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Definition of Electronic Signature in Japan

Act on Electronic Signatures and Certification Business

Article 2
The term ‘electronic signature’ as used in this Act means a measure taken with respect to information that can be recorded in an electromagnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers; hereinafter the same shall apply in this Act), and which falls under both of the following requirements:

(i) A measure to indicate that such information was created by the person who has taken such measure

(ii) A measure to confirm whether such information has been altered.

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Definition of Specified Certification Business in the e-Signature Act

Article 2

2 The term “Certification Business” as used in this Act means a service that, in response to either the request of any person who uses the business (hereinafter referred to as the “User”) with respect to the Electronic Signature that he/she himself/herself performs or the request of another person, certifies that an item used to confirm that such User performed the Electronic Signature pertains to such User.

3 The term “Specified Certification Business” as used in this Act means a Certification Business that, among Electronic Signatures, is performed with respect to an Electronic Signature that confirms to the criteria prescribed by ordinance of the competent minister as an Electronic Signature that can be performed by that person in response to the method thereof.

＊PKI-based

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

eIDAS Regulation and e-Signature Act

Accredited Certification Business in the e-Signature Act

Article 4

Any person who intends to perform the Specified Certification Business may obtain accreditation from competent minister.

（Criteria for Accreditation）

(i) The facilities provided for use of the business pertaining to the application conform to the criteria, as provided by ordinance of the competent minister;

(ii) The confirmation of identity of the user in the business pertaining to the application is implemented by a method, as provided by ordinance of the competent minister;

(iii) In addition to what is listed in the preceding item, business pertaining to the application is performed by a method that conforms to the criteria, as provided by ordinance of the competent minister.

Certification Business

➡A service proves that the electronic signature was made by the signer

Specified Certification Business

➡certification business which is PKI-based service and conforms to the criteria (related guidelines)

Accredited Certification Business

➡Specified certification business that has obtained the accreditation from the competent minister

eIDAS Regulation and e-Signature Act

Legal Effects of Electronic Signatures

eIDAS Regulation
Article 25
An electronic signature shall not be denied lega
l
effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signature.

A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

Act on Electronic Signatures and Certification Business
Article 3
Any electromagnetic record that is made in order to express information (except for that prepared by a public official in the course of duties) shall be presumed to be established authentically if the Electronic Signature (limited to that which can be performed by the principal through appropriate management of codes and properties necessary to perform this) is performed by the principal with respect to information recorded in such electromagnetic record.

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

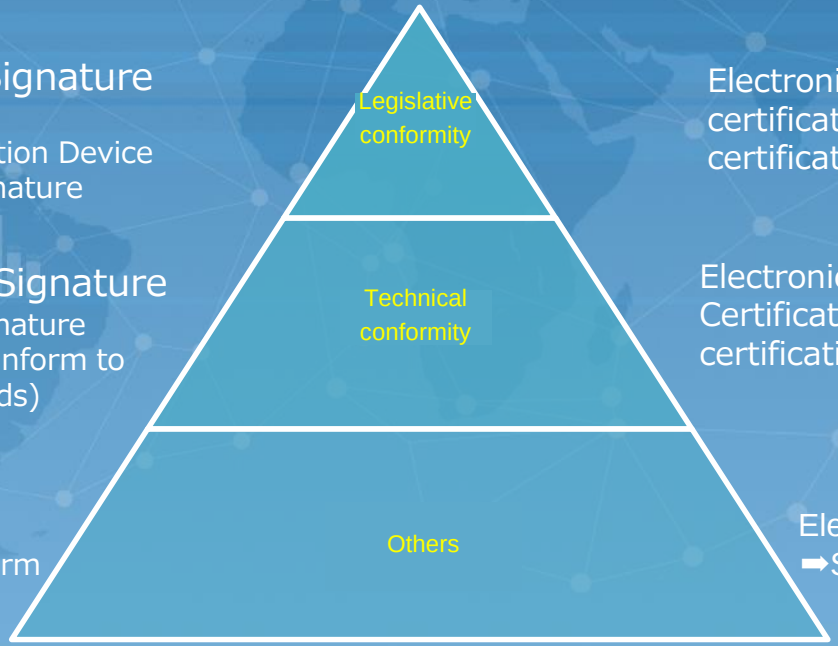
Comparison of Definitions of Electronic Signatures in Japan and Europe

EU

Qualified Electronic Signature
➡Qualified certificate
＋Qualified Signature Creation Device
＋Advanced Electronic Signature

Advanced Electronic Signature
➡PKI-based Electronic Signature
（digital signature）that conform to
The criteria (ETSI standards)

Electronic Signature
➡Signature in electronic form



Japan

Electronic signature based on electronic certificates issued by accredited certification business

Electronic signature based on electronic Certification issued by specified certification business

Electronic Signature
➡Signature in electronic form

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Product Evaluation Scheme

Product Evaluation for Compliance with the eIDAS Regulation

HSM and Qualified Electronic Signature Creation Device
➡CC EAL4+ and Protection Profile
＊FIPS 140-2?

Issues on Common Criteria Evaluation/Certification
➡Mutual recognition of CCRA is up to EAL2

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Comparison of Accreditation Scheme

Qualified Trust Service Provider

➡Accreditation and renewal of accreditation every 24 months

➡Accreditation criteria : ETSI EN Standards and eIDAS Regulation

➡Accreditation results are published in the Trust List

Accredited Certification Service Provider

➡renewal of Accreditation every year

➡Accreditation criteria: Implementing Regulations/Guidelines

➡Accreditation results are published in the Official Journal

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

Supervisory Scheme

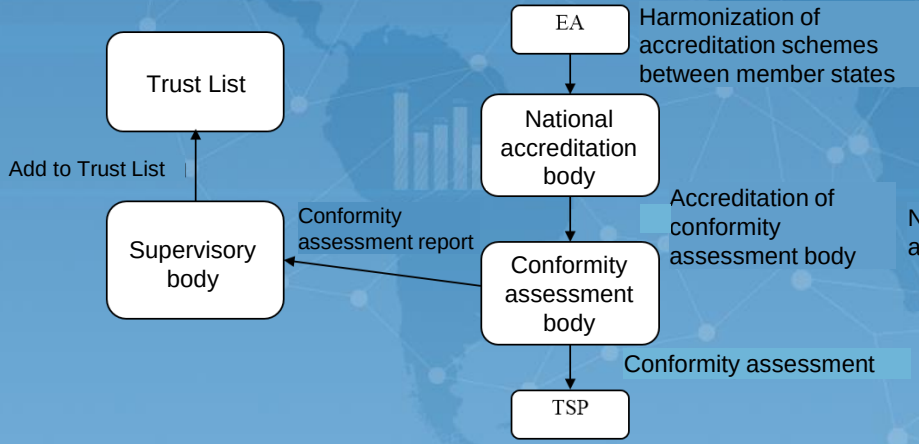
Supervision of Trust Service Provider

Qualified Trust Service Provider ≒ Accredited Certification Service Provider

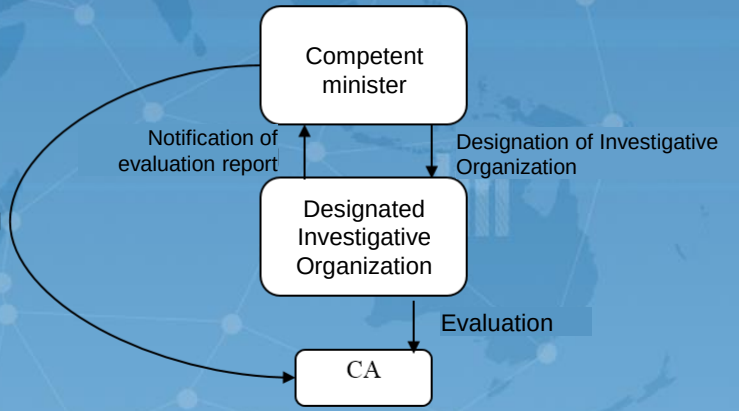
In EU, non-qualified trust service providers are also subject to the supervision

Comparison of Accreditation Schemes

EU



JAPAN



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Comparison of Accreditation Criteria

Comparison of Requirements of EN 319 401, 411-1,-2 and Implementing Regulations/Guidelines

EN 319 411-1,2	施行規則	指針
5 認証業務運用規定及び証明書ポリシーに関する一般規定	1. 業務の用に供する設備の基準	1.1 認証設備室への入出場を管理するために必要な措置
6 トラストサービスプロバイダの運用	2 利用者の真偽の確認の方法	1.2 認証業務用設備への不正なアクセス等を防止するために必要な措置
6.1 公開及び保管の責任	3 その他の業務の方法	1.3 正当な権限を有しない者による認証業務用設備の作動を防止するための措置等
6.2 識別及び認証	4 帳簿書類	1.4 発行者署名符号の生成管理に使用する暗号装置
6.3 証明書のライフサイクル運用要件		1.5 認証業務用設備等の災害の被害を防止するために必要な措置
6.4 施設、管理、及び運用管理		
6.5 技術的セキュリティマネジメント		
6.6 証明書、CRL、及びOSCPプロファイル		2.1 認証業務の利用申込み等
6.7 適合性の監査及びその他の評価		2.2 利用者の真偽の確認方法等
6.8 その他の事業及び法的事項		
6.9 その他の規定		3.1 利用申込者に対する説明事項
		3.2 利用申込書等の記載事項等
		3.3 利用者署名符号及び利用者識別符号の生成等
		3.4 電子証明書に係る事項
		3.5 認定認証業務と他の業務との誤認を防止するための措置
EN 319 401		3.6 電子証明書への属性の記録
5 リスクアセスメント		3.7 署名検証者への情報提供
6 ポリシー及び運用		3.8 電子証明書の失効に係る事項
6.1 トラストサービス運用規定		3.9 認証業務の実施に関する規程
6.2 契約条件		3.10 認証業務の廃止
6.3 情報セキュリティポリシー		3.11 電子証明書名義人への情報の開示
7 TSPの管理及び運営		3.12 認証業務実施のための組織及び体制等
7.1 内部組織		3.13 認証業務用設備の操作等に関する許諾等
7.2 人的資源		3.14 発行者署名符号の漏えいを防止するために必要な措置
7.3 資産管理		
7.4 アクセスコントロール		4.1 認証業務利用申込に関する帳簿書類関係
7.5 暗号管理		4.2 電子証明書の失効に関する帳簿書類関係
7.6 物理および環境セキュリティ		4.3 認証事業者の組織管理に関する帳簿書類関係
7.7 運用セキュリティ		4.4 設備及び安全対策措置に関する帳簿書類関係
7.8 ネットワークセキュリティ		
7.9 インシデント管理		
7.10 証拠の収集		
7.11 事業継続マネジメント		
7.12 TSPの終了および終了計画		
7.13 コンプライアンス		

Comparison of Accreditation Criteria

Characteristics of ETSI EN Standards

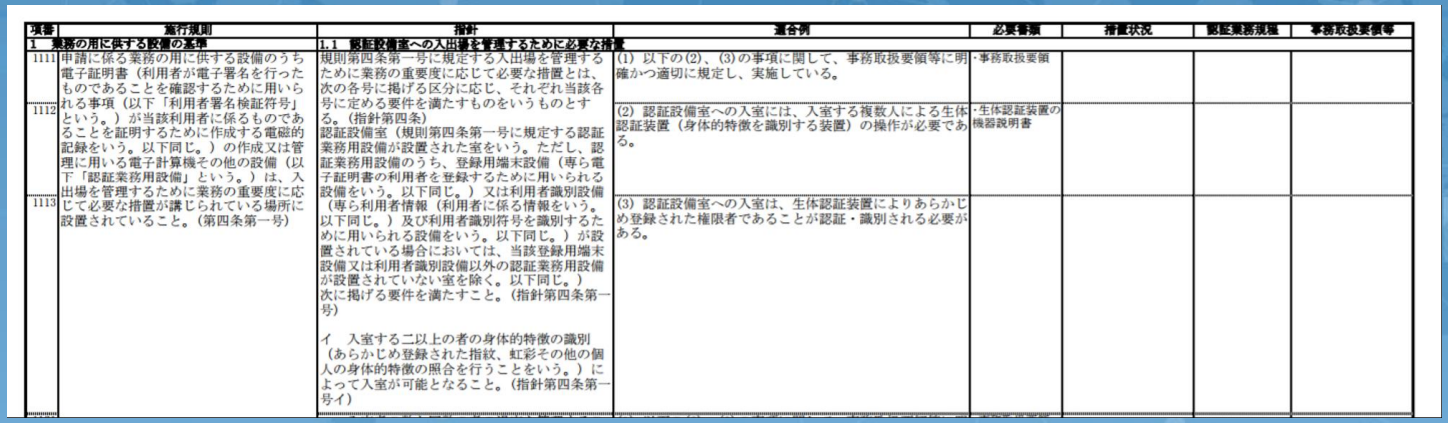
- Management system base（27002）
  - Risk assessment
  - Demonstration of process
- Financial requirements
- Personnel background checks
- Penalties
- Requirements upon termination
- Requirements of CA/B Forum

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Comparison of Accreditation Criteria

Characteristics of Implementing Regulations/Guidelines

- Specification of Examples of Conformance



項番	施行規則	指針	適合例	必要書類	措置状況	認証業務規程	事務取扱要領等
1	業務の用に供する設備の基準	1.1 認証設備室への入出場を管理するために必要な措置					
1111	申請に係る業務の用に供する設備のうち電子証明書（利用者が電子署名を行ったものであることを確認するために用いられる事項（以下「利用者署名検証符号」という。）が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。以下同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。（第四条第一号）	規則第四条第一号に規定する入出場を管理するために業務の重要度に応じて必要な措置とは、次の各号に掲げる区分に応じ、それぞれ当該各号に定める要件を満たすものをいうものとする。（指針第四条） 認証設備室（規則第四条第一号に規定する認証業務用設備が設置された室をいう。ただし、認証業務用設備のうち、登録用端末設備（専ら電子証明書の利用者を登録するために用いられる設備をいう。以下同じ。）又は利用者識別設備（専ら利用者情報（利用者に係る情報をいう。以下同じ。）及び利用者識別符号を識別するために用いられる設備をいう。以下同じ。）が設置されている場合においては、当該登録用端末設備又は利用者識別設備以外の認証業務用設備が設置されていない室を除く。以下同じ。）次に掲げる要件を満たすこと。（指針第四条第一号） イ　入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。（指針第四条第一号イ）	(1) 以下の(2)、(3)の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施している。	・事務取扱要領			
1112			(2) 認証設備室への入室には、入室する複数人による生体認証装置（身体的特徴を識別する装置）の操作が必要である。	・生体認証装置の機器説明書			
1113			(3) 認証設備室への入室は、生体認証装置によりあらかじめ登録された権限者であることが認証・識別される必要がある。				

- Detailed requirements for cryptographic modules
- Sample check

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Conclusion

Gap of Legislative Systems for Electronic Signature between Japan and EU

1. Qualified electronic signature creation device

In EU, it is required to use a qualified electronic signature creation device to create a qualified electronic signature.

In Japan, key management is signer's own responsibility.

➡Possibilities of remote signature

Not just convenient, but also more secure

2. Product evaluation of HSM and signature creation device

3. Trust List

Trust list or bridge certification authority for interoperability/mutual recognition between multiple schemes.

4. Gap of accreditation criteria

Cultural differences, harmonization with IETF RFC3647

5. Other trust services such as time stamping

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

Thank you very much for your attention

If you have any questions, Please contact

Cosmos Corporation
IT Security Department
Soshi Hamaguchi
s.hamaguchi@cosmos-corp.com

Cosmos
POFESSIONALS OF SAFETY ENGINEERING