



# Welcome to the World of Standards



## **E-COMMERCE USING ELECTRONIC SIGNATURES IN JAPAN AND EUROPE**

*Keio University Tokyo – 4 July 2017*

### **The European Member States Trusted Lists**

Sylvie Lacroix – ETSI Electronic Signatures & Infrastructures expert, Signature Validation STF leader



# Welcome to the World of Standards



**電子署名を利用した電子商取引の日本と欧州の事例と課題**  
**慶応義塾大学 – 2017年7月4日**  
**欧州加盟国のトラストリスト**

Sylvie Lacroix – ETSI Electronic Signatures & Infrastructures expert, Signature Validation STF leader

## eIDAS Regulation

**eID**

**Trust  
Services**

(eDocuments)

Notification of  
schemes

Assurance  
levels – low,  
substantial,  
high

Closed list at  
EU level

Non-  
discrimination  
and legal  
value

Non-  
discrimination

Mutual  
recognition

Public sector

Qualified and  
nonqualified

Supervision –  
conformity  
assessment

Shall not be  
denied legal  
effect

Source: European Commission

## eIDAS規則

eID

トラストサービス

e文書

スキーム  
の通知

保証レベル-  
Low(低)、  
Substantial(十  
分)、High(高)

EUレベルでの  
クローズドリスト

非差別  
および  
法的価値

非差別

相互承認

公共部門

適格・非適格

監督-適合性  
評価


法的効力が否  
定されないこと

Source: European Commission

# QTSPs/QTSSs and their legal benefits



🔒 Provision of QC for eSignatures

→ QESig ≡ 



🔒 Provision of QC for eSeals

→ QESeal ≡ Data integrity & Proof of data origin



🔒 Provision of QC for website auth<sup>o</sup>



🔒 Qualified validation of QESig

→ 🔒 Trustworthy results for validation of QESig/QESeal

🔒 Qualified validation of QESeal

🔒 Qualified preservation of QESig

→ 🔒 Trustworthy assurance of long term evidentiary value of QESig/QESeal

🔒 Qualified preservation of QESeal

🔒 Provision of qualified time stamps

→ 🔒 presumption of the accuracy of the date & time and integrity of the time stamped data

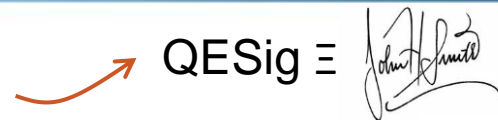
🔒 Qualified electronic registered delivery services

→ 🔒 presumption of integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of date & time of sending and receipt

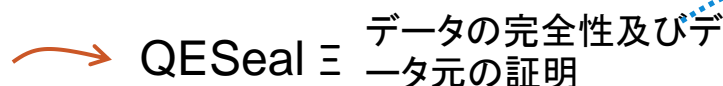
# QTSP/QTSおよびその法的メリット



🔒 電子署名のためのQCの提供



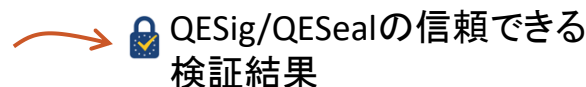
🔒 eシールのためのQCの提供



🔒 ウェブサイト認証のためのQCの提供

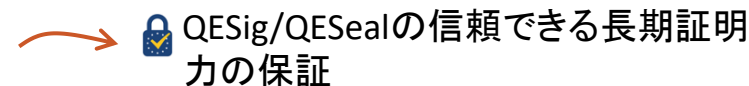


🔒 QESigの適格検証



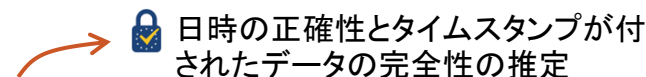
🔒 QESealの適格検証

🔒 QESigの適格保存

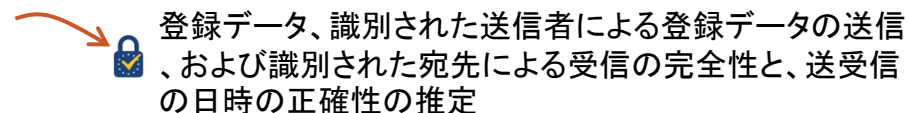


🔒 QESealの適格保存

🔒 適格タイムスタンプの提供



🔒 適格電子eデリバリサービス



# Where we come from

Directive  
1999/93/EC



eIDAS  
Regulation



## 指令 1999/93/EC



適格電子署名

## eIDAS 規則

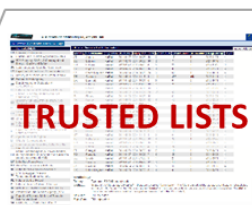




# Pyramid of trust



EU trust mark for QTS  
may only be used by QTSP



Constitutive list to state who is a “qualified” TSP and for what “qualified” trust service(s) can be used as trust anchors list for automatized validation (e.g. signature validation)

## SUPERVISORY REGIME

### Initiation

(initial assessment by eIDAS accredited CAB)

Termination

QTSP & QTS  
they provide

Ad-hoc  
audits  
(at any time)

Regular Assessments  
(at least every 24m  
by eIDAS accredited CAB)



### [eIDAS Observatory/Library](#)

Compiled list of eIDAS accredited CABs



(1) for all types of QTSP/QTS



(3) for all types of QTSP/QTS



(3) for CA/QC eSig & TSA/QTST



(2) for all types of QTSP/QTS  
but QERDS



(1) for all types of QTSP/QTS

(Any CAB can be used by any (Q)TSP)

QTSP & QTS RELATED eIDAS PROVISIONS

BEST PRACTICES & STANDARDS



QTSのためのEUトラストマークは  
QTSPによってのみ使用される

## トラストリスト

誰が「適格」TSPであるか、またどの「適格」トラストサービスがトラストアンカーリストとして自動化された検証(署名検証など)に使用されるかを示す構成リスト

## 監督制度

### 開始

(eIDAS認定CABIによる  
初回評価)

終了

QTSP & QTS  
they provide

Ad-hoc  
監査  
(随時)






### 定期評価

(eIDAS認定CABIによる少  
なくとも24カ月毎の評価)



## eIDAS監視所/ライブラリ

eIDAS認定CABのコンパイルドリスト

-  (1) すべてのタイプの QTSP/QTSPについて
-  (3) すべてのタイプのQTSP/QTSPについて
-  (3) CA/QC eSigおよびTSA/QTSTについて
-  (2) QERDSを除くすべてのタイプのQTSP/QTSPについて
-  (1) すべてのタイプのQTSP/QTSPについて

QTSPおよびQTSに関するeIDAS規定

ベストプラクティスおよび規格

(すべての(Q)TSPは  
どのCABでも使用することができる)

## Key elements

🌐 Legal basis – Article 22.5 of the eIDAS Regulation and procedures and format specified by CID (EU) 2015/1505

- National TLs have a constitutive effect for QTSP and QTS
- Ensure legal certainty with regards to QTS

## 🌐 Mandatory

- MS to establish, maintain and publish TL in a Form suitable for automated processing
- Member States to include information on qualified trust service providers

## 🌐 Voluntary

- MS to establish, maintain and publish TL in human readable format (signed or sealed PDF/A)
- MS to include info on other trust service providers (not qualified)

## 重要な要素

● 法的基盤 – eIDAS規則の22.5条およびCID(EU) 2015/1505で規定されている手順およびフォーマット

- 国家TLにはQTSPおよびQTSについての構成的効果がある
- QTSに関する法的確実性を保証する

● 必須

- MSは、自動プロセスに適した形式でTLを策定、維持および公開する
- 加盟国は、適格トラストサービスプロバイダに関する情報を含める

● 任意

- MSは、可読フォーマット(署名済みもしくはシールを付したPDF/A)でTLを策定、維持および公開する
- MSは、その他のトラストサービスプロバイダ(非適格)に関する情報を含める

## Key principles

- Allow citizens, businesses and public administrations to easily verify nature and status of a trust service
- Procedures and format specified by CID (EU) 2015/1505 building upon (profiling) technical specifications of ETSI TS 119 612 v2.1.1: machine processable by validation applications or services
- Foster cross border recognition of qualified trust services by facilitating a.o. the validation of e-signatures and e-seals
- Ensure continuity with the existing TLs established under the Service Directive

## 基本原則

- 国民、ビジネスおよび行政機関がトラストサービスの性質およびステータスを簡単に検証することを認める
- ETSI TS 119 612 v2.1.1 の技術仕様に基づく(プロフィール)CID(EU) 2015/1505で規定されている手順および形式: 検証アプリケーションまたはサービスによる機械処理が可能である
- すべての電子署名およびeシールの検証を容易にすることにより適格トラストサービスの国境を越えた承認を促進する
- サービス指令の下で策定された既存のTLの継続を保証する

# Trusted Lists – trusted source of info

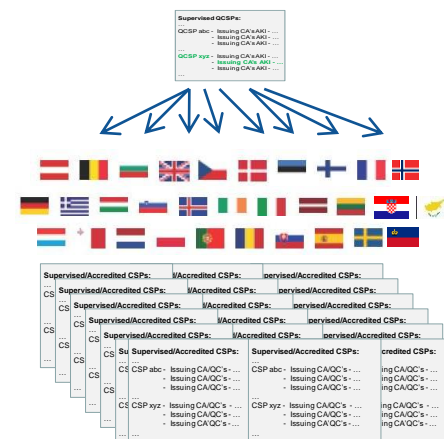


## QC ? on SSCD (QSCD) ?

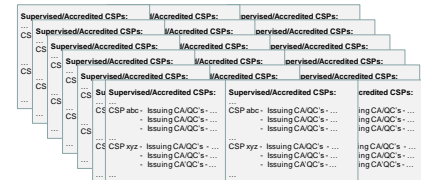
- First usual source of info is certificate content
  - Claimed as “qualified” (for eSig, for eSeal, for website)
  - Claimed as “on SSCD (QSCD)”
- Confirmation/compensation in national trusted list
- Check (qualified) status of issuing service
- Check additional qualifier statement for certificate when applicable, e.g.:
  - qualified or not,
  - on (Q)SSCD or not,
  - QC type (for eSig, for eSeal, for web site authentication)
- Full history of status and qualifier: time info is essential – Q-status, i.e. granted / withdrawn / t.o.b. is adapted and traceability is provided



## Centralised List of pointers to MS/EEA TLs (LOTL- signed/sealed XML)



## National Trusted Lists (TLs - signed/sealed XML)

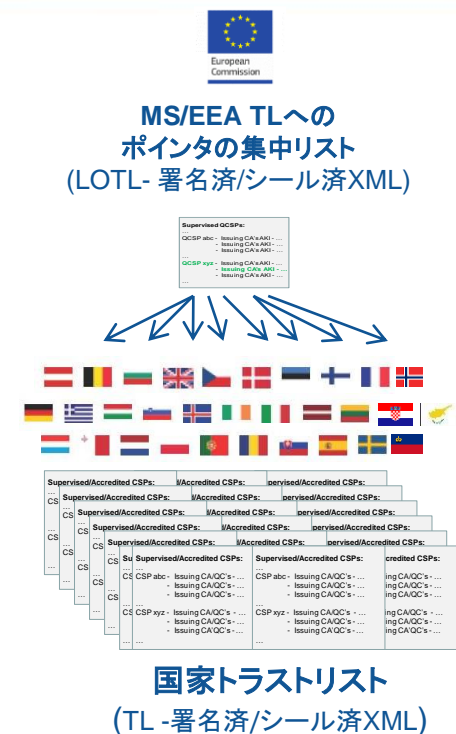


# トラストリスト – 信頼できる情報源



## QC ? On SSCD (QSCD) ?

- 最初の通常情報源は証明書コンテンツである
  - (電子署名、eシール、ウェブサイトについて)「適格」と主張するもの
  - 「on SSCD (QSCD)」と主張するもの
- 国家トラストリストにおける確認/補償
- 発行サービスの(適格)ステータスを確認
- 必要に応じて、次にあげるものなどの証明書の追加修飾子記述を確認
  - 適格か否か
  - on (Q)SSCDか否か?
  - QCタイプ(電子署名、eシール、ウェブサイト認証用)
- ステータスおよび修飾子の全履歴: 時間情報は必須である-適格ステータス(付与/廃止/t.o.b.)が適応され、トレーサビリティが提供されている





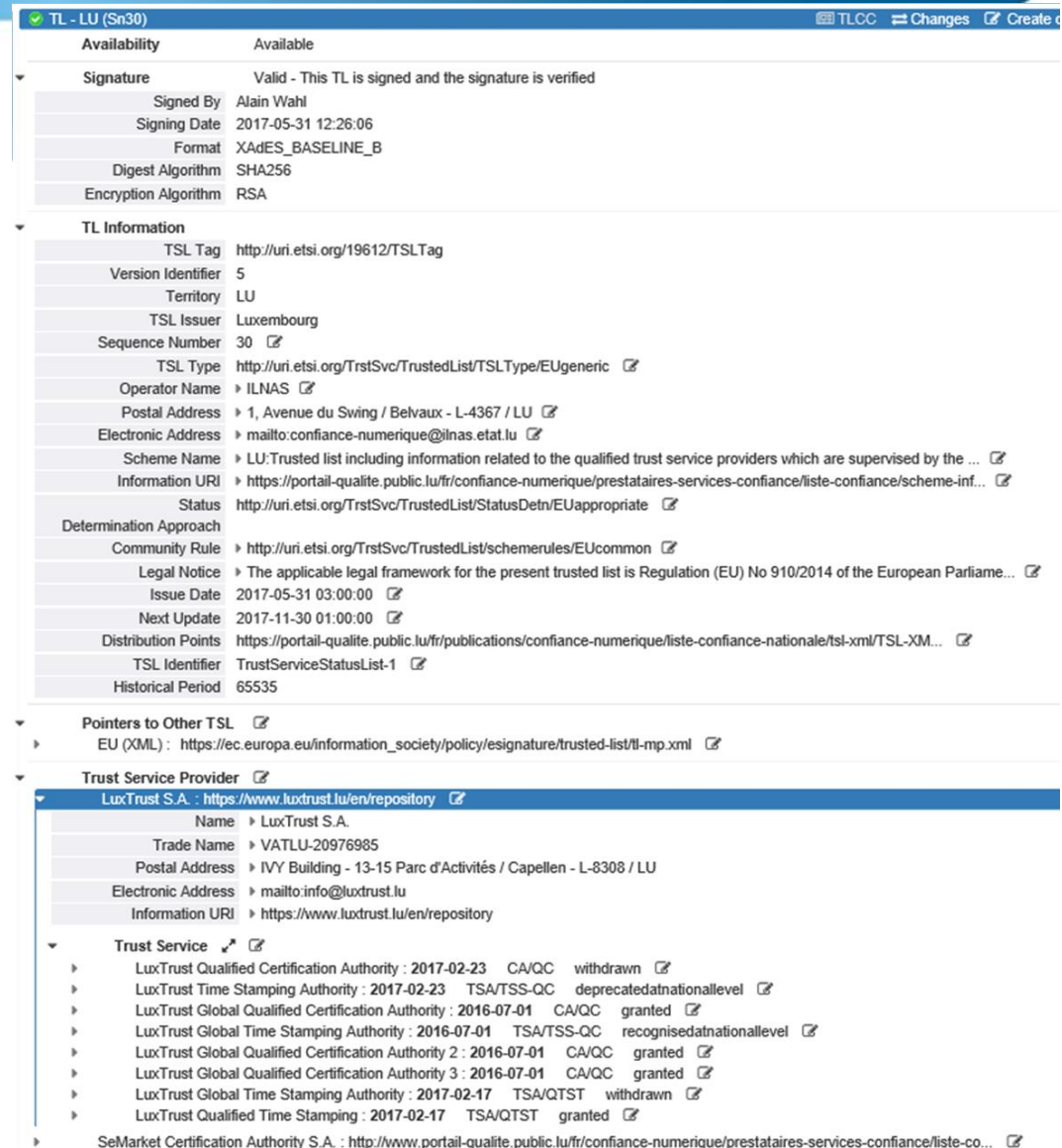
## TLSO & scheme information

- TL Issuer
  - Name
  - Postal & eAddresses
- Scheme information
  - Territory
  - National URI incl. info on national supervision scheme
  - TL Type, Scheme name, Legal Notice
  - Date of issuance & expiry
  - Status determination
  - Community rules (EU & national):  
**how to use and interpret the trusted lists**

## Pointer to the LOTL

## List of TSPs and their services

- TSP (Name, postal & eAddresses)
- URI to info on TSP practices
  - CPS/CP, GTC, legal, customer care, etc.
- TSP services (per service)
  - “Digital identity” (trust anchor)
  - Current status & full status history



**TL - LU (Sn30)** TLCC Changes Create d

**Availability** Available

**Signature** Valid - This TL is signed and the signature is verified

Signed By	Alain Wahl
Signing Date	2017-05-31 12:26:06
Format	XAdES_BASELINE_B
Digest Algorithm	SHA256
Encryption Algorithm	RSA

**TL Information**

TSL Tag	<a href="http://uri.etsi.org/19612/TSLTag">http://uri.etsi.org/19612/TSLTag</a>
Version Identifier	5
Territory	LU
TSL Issuer	Luxembourg
Sequence Number	30
TSL Type	<a href="http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUGeneric">http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUGeneric</a>
Operator Name	ILNAS
Postal Address	1, Avenue du Swing / Belvaux - L-4367 / LU
Electronic Address	<a href="mailto:confiance-numerique@ilnas.etat.lu">mailto:confiance-numerique@ilnas.etat.lu</a>
Scheme Name	LU:Trusted list including information related to the qualified trust service providers which are supervised by the ...
Information URI	<a href="https://portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/liste-confiance/scheme-inf...">https://portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/liste-confiance/scheme-inf...</a>
Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate">http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate</a>
Determination Approach	
Community Rule	<a href="http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</a>
Legal Notice	The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliame...
Issue Date	2017-05-31 03:00:00
Next Update	2017-11-30 01:00:00
Distribution Points	<a href="https://portail-qualite.public.lu/fr/publications/confiance-numerique/liste-confiance-nationale/tsl-xml/TSL-XM...">https://portail-qualite.public.lu/fr/publications/confiance-numerique/liste-confiance-nationale/tsl-xml/TSL-XM...</a>
TSL Identifier	TrustServiceStatusList-1
Historical Period	65535

**Pointers to Other TSL**

- EU (XML) : [https://ec.europa.eu/information\\_society/policy/esignature/trusted-list/tl-mp.xml](https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml)

**Trust Service Provider**

**LuxTrust S.A.** : <https://www.luxtrust.lu/en/repository>

Name	LuxTrust S.A.
Trade Name	VATLU-20976985
Postal Address	IVY Building - 13-15 Parc d'Activités / Capellen - L-8308 / LU
Electronic Address	<a href="mailto:info@luxtrust.lu">mailto:info@luxtrust.lu</a>
Information URI	<a href="https://www.luxtrust.lu/en/repository">https://www.luxtrust.lu/en/repository</a>

**Trust Service**

- LuxTrust Qualified Certification Authority : 2017-02-23 CA/QC withdrawn
- LuxTrust Time Stamping Authority : 2017-02-23 TSA/TSS-QC deprecatedatnationallevel
- LuxTrust Global Qualified Certification Authority : 2016-07-01 CA/QC granted
- LuxTrust Global Time Stamping Authority : 2016-07-01 TSA/TSS-QC recognisedatnationallevel
- LuxTrust Global Qualified Certification Authority 2 : 2016-07-01 CA/QC granted
- LuxTrust Global Qualified Certification Authority 3 : 2016-07-01 CA/QC granted
- LuxTrust Global Time Stamping Authority : 2017-02-17 TSA/QTST withdrawn
- LuxTrust Qualified Time Stamping : 2017-02-17 TSA/QTST granted

SeMarket Certification Authority S.A. : <http://www.portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/liste-co...>

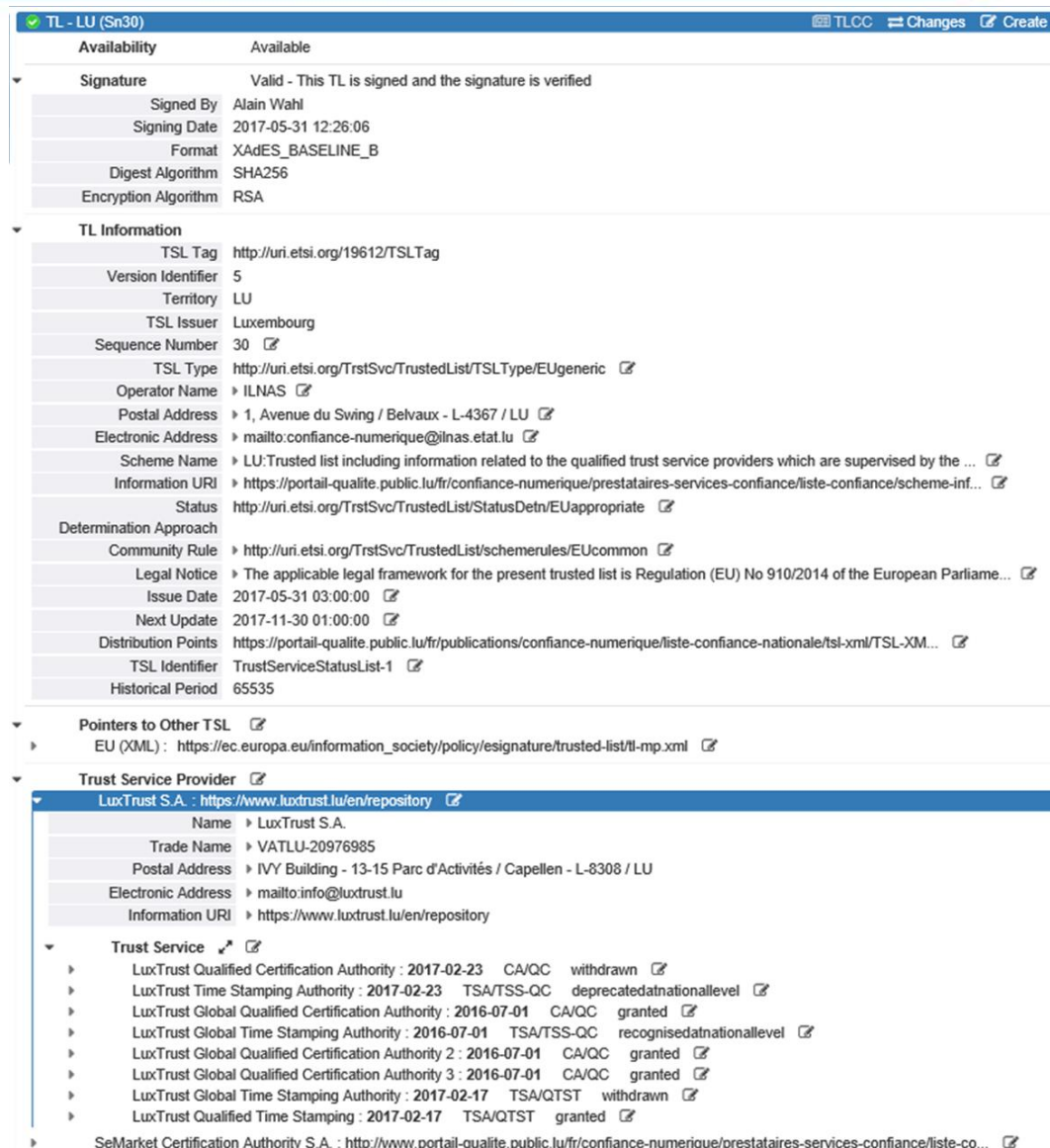
## TLSO およびスキームリスト

- TL発行者
  - 名称
  - 郵便および電子アドレス
- スキーム情報
  - 領域
  - 国家監督スキームに関する情報を含む国家URI
  - TLタイプ、スキーム名、法的通知
  - 発行および有効期間終了の日付
  - ステータス決定
  - コミュニティ規則 (EU & 国家): トラストリストの使用および解釈の方法

## LOTLへのポインタ

## TSPとそのサービスのリスト

- TSP (名称、郵便および電子アドレス)
- TSPの運用に関する情報へのURI
  - CPS/CP、GTC、法律、カスタマーケア等
- TSPサービス(サービス別)
  - 「デジタルアイデンティティ(トラストアンカー)
  - 現在のステータスおよびステータスの全履歴



The screenshot displays the details for a Trust List (TL) identified as 'TL - LU (Sn30)'. The interface is in Japanese and shows the following information:

- Availability:** Available
- Signature:** Valid - This TL is signed and the signature is verified.
  - Signed By: Alain Wahl
  - Signing Date: 2017-05-31 12:26:06
  - Format: XAdES\_BASELINE\_B
  - Digest Algorithm: SHA256
  - Encryption Algorithm: RSA
- TL Information:**
  - TSL Tag: <http://uri.etsi.org/19612/TSLTag>
  - Version Identifier: 5
  - Territory: LU
  - TSL Issuer: Luxembourg
  - Sequence Number: 30
  - TSL Type: <http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUGeneric>
  - Operator Name: ILNAS
  - Postal Address: 1, Avenue du Swing / Belvaux - L-4367 / LU
  - Electronic Address: <mailto:con fiance-numerique@inas.etat.lu>
  - Scheme Name: LU:Trusted list including information related to the qualified trust service providers which are supervised by the ...
  - Information URI: <https://portail-qualite.public.lu/fr/con fiance-numerique/prestataires-services-con fiance/liste-con fiance/scheme-inf...>
  - Status: <http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate>
  - Determination Approach: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>
  - Community Rule: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>
  - Legal Notice: The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliame...
  - Issue Date: 2017-05-31 03:00:00
  - Next Update: 2017-11-30 01:00:00
  - Distribution Points: <https://portail-qualite.public.lu/fr/publications/con fiance-numerique/liste-con fiance-nationale/tsl-xml/TSL-XM...>
  - TSL Identifier: TrustServiceStatusList-1
  - Historical Period: 65535
- Pointers to Other TSL:**
  - EU (XML): [https://ec.europa.eu/information\\_society/policy/esignature/trusted-list/ll-mp.xml](https://ec.europa.eu/information_society/policy/esignature/trusted-list/ll-mp.xml)
- Trust Service Provider:**
  - LuxTrust S.A.:** <https://www.luxtrust.lu/en/repository>
    - Name: LuxTrust S.A.
    - Trade Name: VATLU-20976985
    - Postal Address: IVY Building - 13-15 Parc d'Activités / Capellen - L-8308 / LU
    - Electronic Address: <mailto:info@luxtrust.lu>
    - Information URI: <https://www.luxtrust.lu/en/repository>
  - Trust Service:**
    - LuxTrust Qualified Certification Authority: 2017-02-23 CA/QC withdrawn
    - LuxTrust Time Stamping Authority: 2017-02-23 TSA/TSS-QC deprecatedatnationallevel
    - LuxTrust Global Qualified Certification Authority: 2016-07-01 CA/QC granted
    - LuxTrust Global Time Stamping Authority: 2016-07-01 TSA/TSS-QC recognisedatnationallevel
    - LuxTrust Global Qualified Certification Authority 2: 2016-07-01 CA/QC granted
    - LuxTrust Global Qualified Certification Authority 3: 2016-07-01 CA/QC granted
    - LuxTrust Global Time Stamping Authority: 2017-02-17 TSA/QTST withdrawn
    - LuxTrust Qualified Time Stamping: 2017-02-17 TSA/QTST granted
- SeMarket Certification Authority S.A.:** <http://www.portail-qualite.public.lu/fr/con fiance-numerique/prestataires-services-con fiance/liste-co...>

## The EU Trust Mark for Qualified Trust Services, Commission Implementing Regulation (EU) 2015/806

- Can only be used by a qualified trust service provider
- Can only "label" its qualified trust services
- Helps Customers distinguish between qualified trust services and non-qualified ones



## 適格トラストサービスのEUTラストマーク、委員会規則 (EU) 2015/806

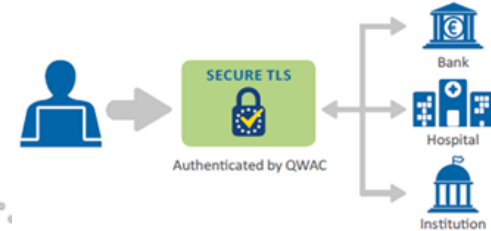
- 適格トラストサービスプロバイダのみが使用することができる
- 適格トラストサービスの「表示」のみができる
- 顧客が適格トラストサービスと非適格トラストサービスを区別する場合に役立つ



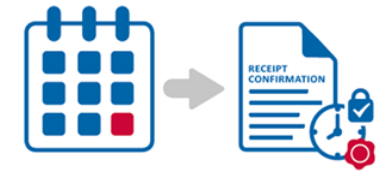
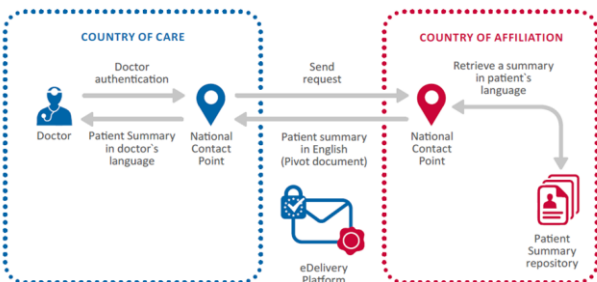
# Use cases of QTSPs/QTSs ?



Electronic signatures or seals are not required as such by the VAT Directive. However *“authenticity of the origin, the integrity of the content and the legibility of an invoice, whether on paper or in electronic form, shall be ensured from the point in time of issue until the end of the period for storage of the invoice”*



Directives encourage Member States to adopt use of electronic procurement processes, and allowing them to require the use of QES





# Trusted Lists – technical support (1/2)



🌐 Read TSL: <https://webgate.ec.europa.eu/tl-manager/home>

🌐 Interpretation of trusted lists:  
<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/Eucommon>:

EU Member States Trusted Lists Scheme Type Community Rules: Common statement

**Participation in a scheme**

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

**Policy/rules for the assessment of the listed services**

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation. The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505. The trusted lists include both current and historical information about the status of listed trust services. Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

**Interpretation of the Trusted List**

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows: The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("SdID") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable. Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication: A "CA/QC" "Service type identifier" ("SdID") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("SdID") additionalServiceInformation Extension)

- indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("SdID") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:
  - the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
  - the 0.4.0.1499.1.1 (QCP+) ETSI defined certificate policy OID,
  - the 0.4.0.1499.1.2 (QCP-) ETSI defined certificate policy OID, and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. "undersupervision", "supervisioninaccession", "accredited" or "granted") for that entry.
- and if "SdID" "Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of "SdID" "Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the "SSCD support" and/or "Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of "Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:
- to indicate the qualified certificate nature:
  - "QCStatement" meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;
  - "QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;
  - "QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;
  - "QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.
- to indicate that the certificate is not to be considered as qualified:
- "NoQualified" meaning the identified certificate(s) is(are) not to be considered as qualified; and/or
- to indicate the nature of the SSCD support:
  - "QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or
  - "QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or
  - "QCSSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does/do contain proper machine processable information about whether or not their private key residing in an SSCD;
- to indicate the nature of the QSCD support:
  - "QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or
  - "QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or
  - "QCQSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does/do contain proper machine processable information about whether or not their private key is residing in a QSCD;
  - "QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or
- to indicate issuance to Legal Person:
  - "QCForLegalPerson" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

- if none of the id-etsi-qcs 1 statement, QCP OID or QCP + OID information is included in an end-entity certificate, and
- if no "SdID" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "QCStatement" qualifier, or
- an "SdID" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "NoQualified" qualifier,

then the certificate is not to be considered as qualified.

"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other "SdID" type entry is that, for that "SdID" identified service type, the listed service named according to the "Service name" field value and uniquely identified by the "Service digital identity" field value has the current qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time".

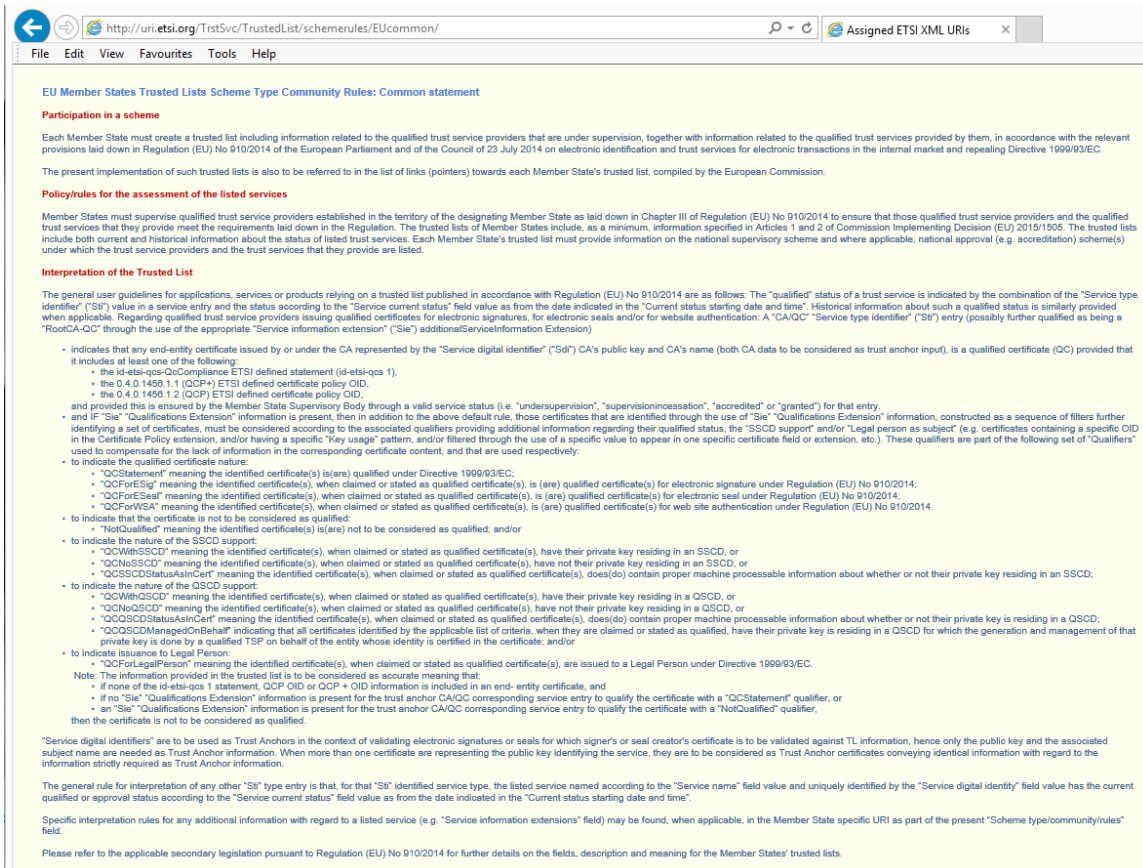
Specific interpretation rules for any additional information with regard to a listed service (e.g. "Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present "Scheme type/community/rules" field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.

🌐 TSLを確認: <https://webgate.ec.europa.eu/tl-manager/home>

🌐 トラストリストの解釈:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/Eucommon>:



The screenshot shows a web browser window displaying the ETSI website page titled "EU Member States Trusted Lists Scheme Type Community Rules: Common statement". The page content includes sections for "Participation in a scheme", "Policy/rules for the assessment of the listed services", and "Interpretation of the Trusted List".

**Participation in a scheme**

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/03/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

**Policy/rules for the assessment of the listed services**

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation. The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505. The trusted lists include both current and historical information about the status of listed trust services. Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

**Interpretation of the Trusted List**

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows: The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("ST") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable. Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication: A "CA/QC" "Service type identifier" ("ST") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("SIE") additionalServiceInformation Extension)

- indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("SDI") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:
  - the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
  - the 0.4.0.1456.1.1 (QCPA) ETSI defined certificate policy OID,
  - the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. "undersupervision", "supervisionincessation", "accredited" or "granted") for that entry.
- and if "SIE" "Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of "SIE" "Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the "SSCD support" and/or "Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of "Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:
  - to indicate the qualified certificate nature:
    - "QCStatement" meaning the identified certificate(s) is(are) qualified under Directive 1999/03/EC;
    - "QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;
    - "QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;
    - "QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.
  - to indicate that the certificate is not to be considered as qualified:
    - "NoQualified" meaning the identified certificate(s) is(are) not to be considered as qualified; and/or
  - to indicate the nature of the SSCD support:
    - "QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or
    - "QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or
    - "QCSSCDStatusInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does/do contain proper machine processable information about whether or not their private key residing in an SSCD;
  - to indicate the nature of the QSCD support:
    - "QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or
    - "QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or
    - "QCQSCDStatusInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does/do contain proper machine processable information about whether or not their private key is residing in a QSCD,
    - "QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or
  - to indicate issuance to Legal Person:
    - "QCForLegalPerson" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/03/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

  - if none of the id-etsi-qcs 1 statement, QCP, CID or QCP + CID information is included in an end- entity certificate, and
  - if no "SIE" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "QCStatement" qualifier, or
  - an "SIE" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "NoQualified" qualifier,

then the certificate is not to be considered as qualified.

"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other "ST" type entry is that, for that "ST" identified service type, the listed service named according to the "Service name" field value and uniquely identified by the "Service digital identity" field value has the current qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time".

Specific interpretation rules for any additional information with regard to a listed service (e.g. "Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present "Scheme type/community/rules" field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.



## ENISA guidelines

- End-user manuals on QTS
- Guidelines for (Q)TSPs
- Initiation & supervision, Security measures, Technical guidelines, Adequacy of standards, ...

## European Commission – eIDAS Observatory/Library



- Art.31 QSCD List
- Compilation of information notified by EUMS on eIDAS state of play
- Compilation of accredited CABs information as notified by NABs

## CEF building blocks

- eSiG
- OSS Libraries to implement eSig/eSeal creation & validation
- TLManager
- eID, eDelivery, ...

## 🌐 ENISA ガイドライン

- QTSに関するエンドユーザマニュアル
- (Q)TSPのガイドライン
- 開始/監督、セキュリティ措置、技術的ガイドライン、規格の妥当性、...

## 🌐 欧州委員会 – eIDAS監視所/ライブラリ

- 第31条 QSCDリスト
- eIDASの現在の状況についてのEUMSが通知した情報の編集
- NAB(国家認定機関)が通知した認定CAB情報の編集



## 🌐 CEF構成要素

- eSiG
- eSig/eSeal生成および検証を実施するためのOSSライブラリ
- TLManager
- eID、電子デリバリ、...

# Trusted Lists – much more than just a certificate store



- Full history of qualified (or “approval”) status grant
- International *mutual* recognition only possible through agreement concluded between the Union and the candidate third country or international organisation in accordance with Article 218 TFEU (cfr Art.14 of the eIDAS Regulation) but ...
- everybody may use TSLs; e.g. Adobe AATL endorses TSL and others (US FED Bridge). International interoperability created de facto.
- ETSI TS 119 612 allows for non EU countries, international organisations and/or application domain owners to set-up trusted list using the same standard as EU MS trusted lists
  - European Payment Council
  - Perú
  - Brazil
  - Etc.

- 付与された適格(または「認可」)ステータスの全履歴
- 第218条TFEU(cfr(連邦規則集) eIDAS規則の第14条)に従って連合と候補となる第三国または国際組織の間で締結した合意を通してのみ実行可能な国際相互承認であるが...
- だれでも、Adobe AATLを指示するTSLおよびその他(US FEDブリッジ)などのTSLを使用することができる。国際的な相互運用性が事実上実現された。
- ETSI TS119 612は、非EU加盟国、国際組織および/またはアプリケーションドメインオーナーが、EU加盟国のトラストリストと同じ規格を使用してトラストリストをセットアップすることを許可している。
  - 欧州決済協議会
  - ペルー
  - ブラジル
  - その他

- eIDAS QTSP/QTS as huge opportunity to secure/boost cross-border eTransactions & digital market
  
- Trusted lists have constitutive value for validating the qualified status of a QTSP/QTS
  - E.g. validate that an AdES is a QES according to the Regulation
  
- Still in growing phase
  - Today 157 QTSP over 29 states
    - 150 QCA issuing Q\_certificates for eSignature
    - 13 QCA issuing Q\_certificates for eSeal
    - 30 QTSA issuing Q\_timestamps
    - 4 Q\_eDelivery Providers, 4 Qualified Signatures Validation Providers, 3 Qualified Signatures Preservation Providers, 3 QCA issuing Q\_certificates for Web.Authentication

- eIDAS QTSP/QTSは、国境を越えた電子商取引およびデジタル市場を保護および促進するための非常に大きな機会である
- トラストリストには、QTSP/QTSの適格ステータスの検証についての構成価値がある
  - 例：規則に従いAdESがQESであることを検証する
- いまだ成長の過程である
  - 現在29か国に157のQTSP
    - 電子署名の適格証明書を発行している150の QCA
    - eシールの適格証明書を発行している13の QCA
    - 適格タイムスタンプを発行している30の QTSA
    - 4つの適格eデリバリプロバイダ、4つの適格署名検証プロバイダ、3つの適格署名保存プロバイダ、ウェブサイト認証の適格証明書を発行している3つの QCAがある

# Questions ? - Contact information



Sylvie LACROIX (CISA, CSXF)

Mobile: +32 477 78 79 75

Email: [sylvie.lacroix@sealed.be](mailto:sylvie.lacroix@sealed.be)

Web: [www.sealed.be](http://www.sealed.be)

Sylvie LACROIX (CISA, CSXF)

Mobile: +32 477 78 79 75

Email: [sylvie.lacroix@sealed.be](mailto:sylvie.lacroix@sealed.be)

Web: [www.sealed.be](http://www.sealed.be)