セコムIS研究所
Intelligent Systems Laboratory

EUの技術標準

-- デジタル単一市場戦略の中核となるトラスト --

2019年　2月　7日

松本　泰　　セコム（株）ＩＳ研究所

EUの技術標準
デジタル単一市場戦略の中核となるトラスト

セコムIS研究所
Intelligent Systems Laboratory

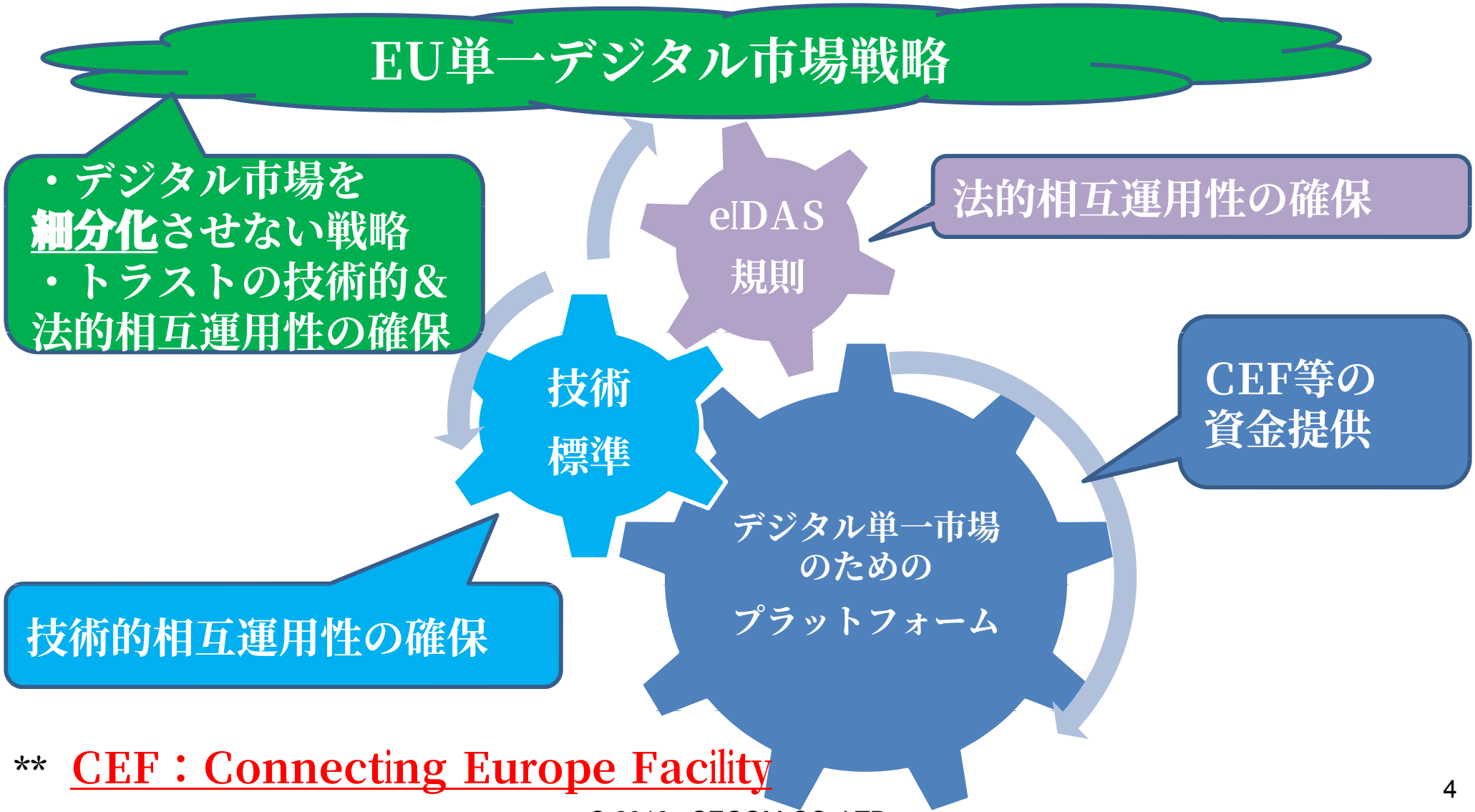
- (1) 技術標準とデジタルプラットフォームの関係
- (2) 事例から説明する技術標準
  - 欧州決済サービス指令(PSD2)に見られる技術標準
  - Adobe Acrobatに見られる技術標準
  - 欧州の新公的管理規則(OCR) に見られる技術標準
- (3) まとめ
- 参考
  - 適格Webサイト認証の事例
  - 技術標準の体系

「ＥＵの技術標準」の理解のためには バックグランドの知識として

セコムIS研究所 Intelligent Systems Laboratory

- 欧州のデジタル単一市場戦略
  - デジタル単一市場戦略におけるトラストの役割
    - GDPRと類似したところがある。　→　欧州域外への戦略でもある
- トラスト分野に限らず、欧州の標準化戦略　→　欧州域外への戦略でもある
- デジタル単一市場形成のための、国、分野を超えた相互運用性の確保
  - ４つの相互運用性の意味するところ－特に法的相互運用性の重要性
  - Legal interoperability、Organisational interoperability、Semantic interoperability、Technical interoperability
- デジタル社会への移行に伴う「技術標準」の要求(要求の変化)
  - 電子署名指令(1999年）からeIDAS規則(2016年）の決定的な違い??
  - （過去）人の目視による判断／検証　→　ヒューマンリーダブル
    - →　人の判断による曖昧な技術仕様を許容する
  - （現在）マシンが（構造化されたルール等により）検証・判断　→　（署名データが）マシンリーダブル　→　曖昧さをなるべく排除したい
    - →　そうした要求のための相互運用性を確保した技術標準の重要性
  - ICTの社会基盤化　->　技術的相互運用性と法的相互運用性の整合

ＥＵの技術標準とデジタルプラットフォームの関係



** CEF：Connecting Europe Facility

eIDAS前文 -- 技術標準の意味するところ

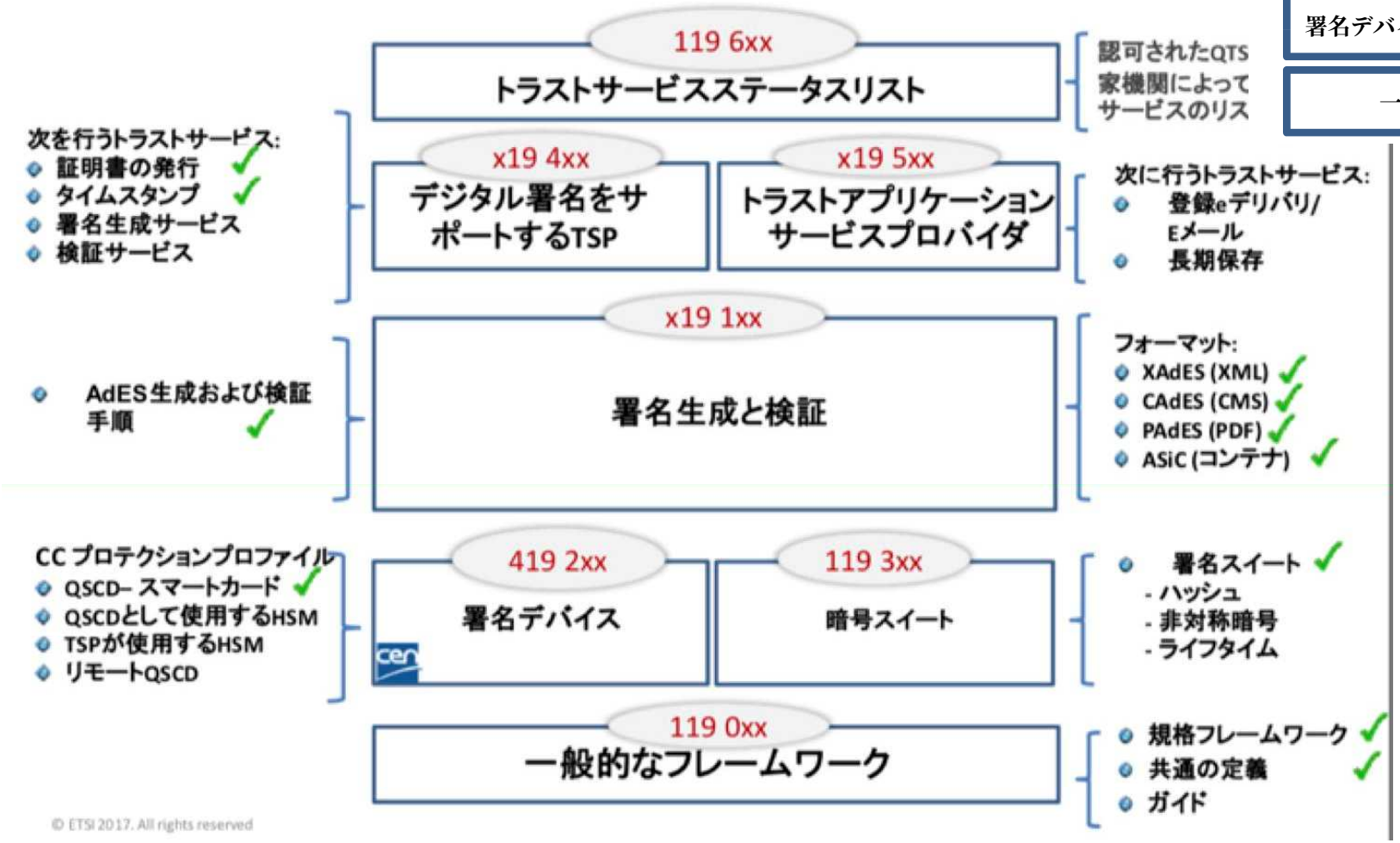
セコムIS研究所 Intelligent Systems Laboratory

- 「欧州デジタルアジエンダ」と題した2010年8月26日の欧州委員会コミュニケーションでは、**デジタル市場の細分化**、**相互運用性の欠如**、そして**サイバー犯罪の増加**を、デジタル経済の良好な循環にとって大きな障害となるものとして認定した。
- 委員会はさらに、２０１０年の「Dismantling the obstacles to EU citizens' rights (EU市民に対する障害の排除)」と題したEU市民活動レポートにおいて、連合市民が**デジタル単一市場**や国境を越えたデジタルサービスの恩恵を受けることの妨げとなっている問題を解決することの必要性について強調した。
- The Commission communication of 26 August 2010 entitled ‘ A Digital Agenda for Europe ’ identified the **fragmentation of the digital market**, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy.
- In its EU Citizenship Report 2010, entitled ‘ Dismantling the obstacles to EU citizens ’ rights ’, the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying

- 欧州において**デジタル単一市場**のためのデジタルプラットフォーム構築の障害となるのは、**デジタル市場の細分化**、**相互運用性の欠如**
- この障害を取り除くためには「トラスト」に関わる**相互運用性を確保した技術標準**が必要であり、更に、**デジタル市場を細分化（fragmentation）させないための規則（eIDAS規則）**が必要だった。
- eIDAS規則は、従来の紙台帳時代の法制度の単なるリプレースの話ではなく、デジタルプラットフォーム構築のための法制度。

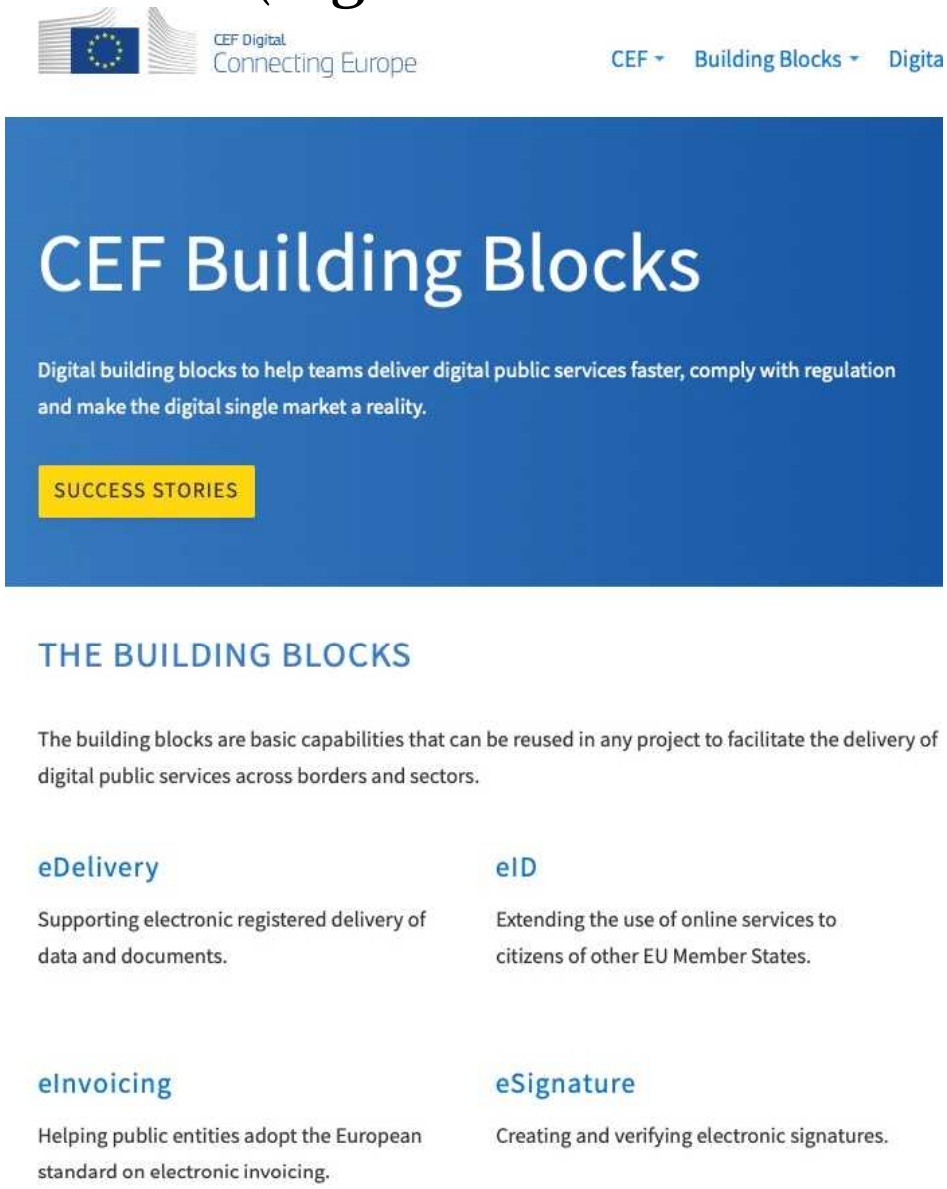
ETSIとCENが開発した「欧州標準」 EN

- 非常によく体系化され整備されている
- 法的な要求との整合が、よく考慮されている（法的相互運用性）
- 詳細な技術仕様からテストまでが仕様化されている（相互運用性の確保と実装可能、利用される標準）



出典：https://itc.jipdec.or.jp/common/images/kouensiryou_4.pdf

EUのデジタル単一市場プラットフォーム構築のための施策
CEF： Connecting Europe Facility -- EUの資金提供プログラム
CEFのDSI (Digital Service Infrastructures)のためのBuilding Blocks



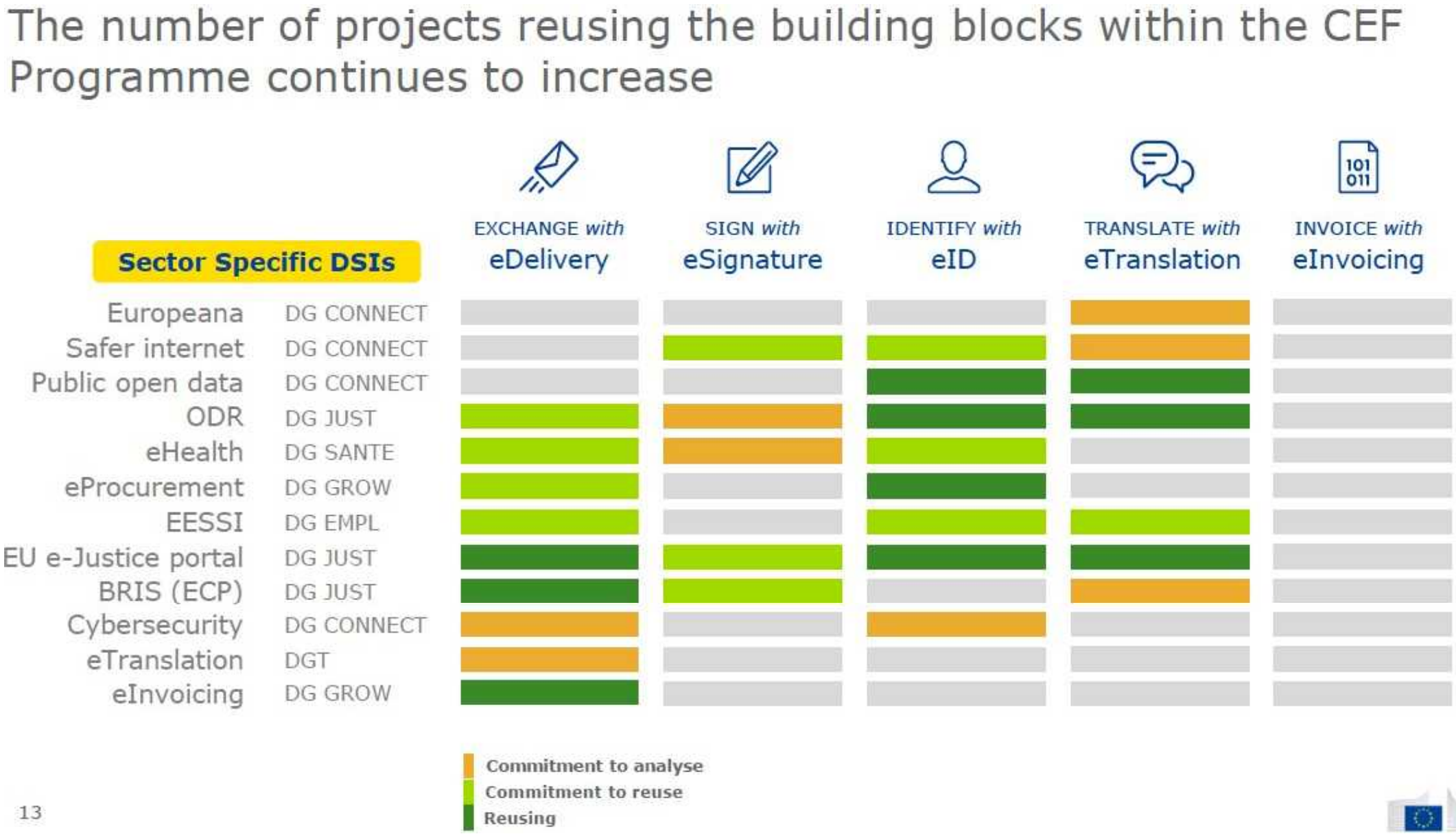
- ビルディングブロックの3つのレイヤ
  - 各ビルディングブロックの中核となる、準拠しなければならない技術仕様および規格のレイヤー
  - 技術仕様および標準の実装を容易にするために、それらに準拠し、再利用を目的としたサンプルソフトウェアのレイヤー
  - 技術仕様および標準の採用を容易にするために、使用を意図した一連のサービス（たとえば、適合性テスト、ヘルプデスク、オンボーディングサービスなど）。

- **Building Blocks に資金提供**
- **Building Blocksを再利用するプロジェクトに資金提供(??)**

出典：https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+a+building+Block

EUデジタル単一市場のプラットフォーム構築のための施策
CEFのDSIs（Digital Service Infrastructures）

セコムIS研究所 Intelligent Systems Laboratory

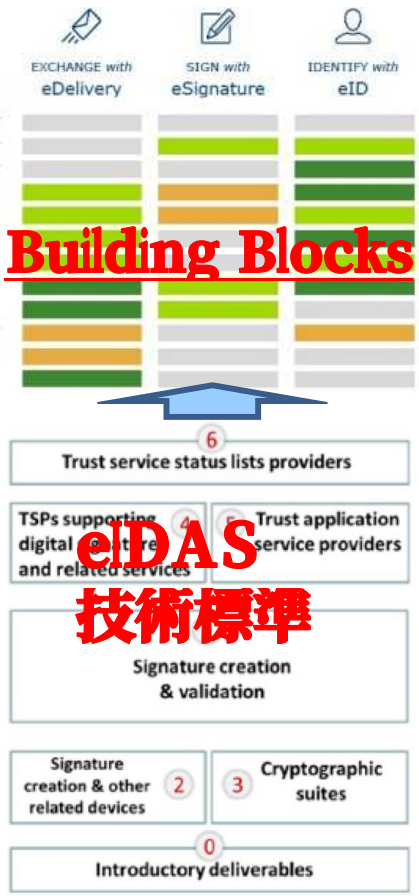


異なる分野に、共通の相互運用性が確保された**再利用可能**なパーツ等を提供

出典：
https://ec.europa.eu/cefdigital/wiki/download/attachments/46992269/%28CEF%20Building%20Blocks%29.%28DSF%29.%28v5.01%29.pdf

デジタルプラットフォームの構築に必要な技術アーキテクチャー

セコムIS研究所
Intelligent Systems Laboratory



eHealth　eJustice　OCR　PSD2

電子政府	健康	司法	動植物食品管理	金融	様々な分野

ここを薄くする

トラストサービスを利用する環境の開発
多くのオープンソースなど

技術標準(ETSI)に準拠した
トラストサービス(QTSP、non-QTSP)

技術標準(CEN)に
準拠し開発される製品群
(ICカード、HSM、etc..)

ここを厚くする

多くの公共財の提供　--　このことにより相互運用性の確保を推進
・技術標準(ETSI、CEN)
・トラストサービスに関連するガイドライン（ENISAなど）
・実装ガイドライン、レファレンス実装、オープンソースなど（CEF等）

技術的相互運用性に対して法的相互運用性の重要性
Technical interoperability & Legal interoperability

セコムIS研究所 Intelligent Systems Laboratory

法的相互運用性

eIDAS規則 ⟷ 欧州の様々な法制度との整合（サイバー空間とリアル空間の融合にとって重要）

技術的相互運用性

トラストリスト

監査スキーム

保証レベル　LoA

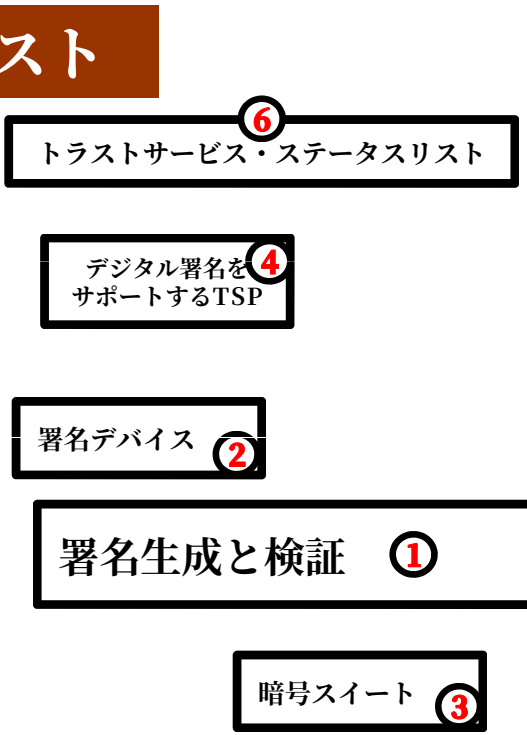
証明書ポリシー

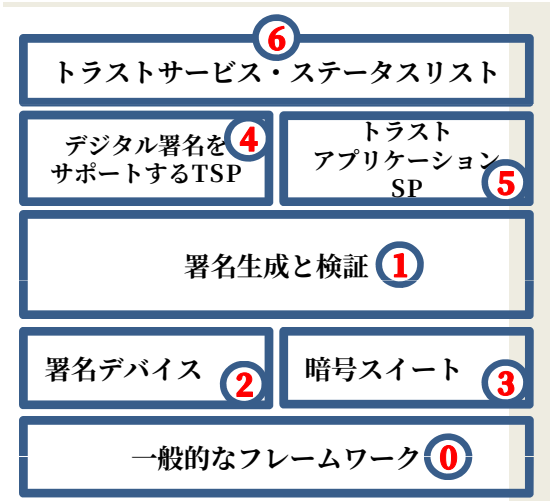
証明書プロファイル

QCプロファイル

データフォーマット

通信プロトコル　従来から技術標準

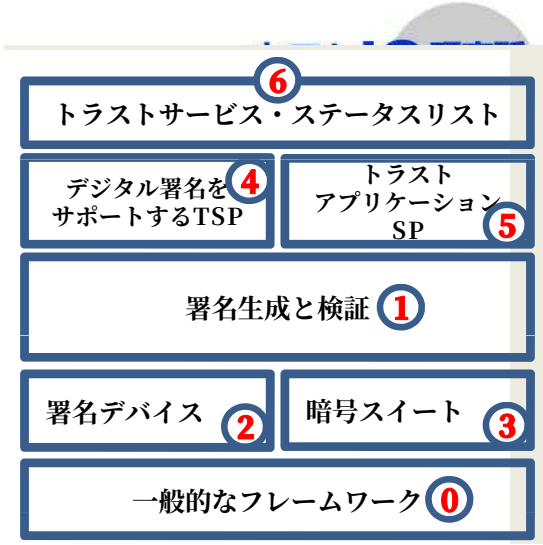




ICTが社会基盤化するほどに、技術的相互運用性と法的相互運用性の整合が重要になっている　-> EU技術標準を理解する上で非常に重要

eIDASトラストサービスの技術標準フレームワーク???

一般的なフレームワーク 0



署名デバイス 2

署名生成と検証 1

署名者
(自然人、法人)
署名環境

署名データ

署名検証者
署名検証環境

トラスト
アプリケーション
SP 5

6
トラストサービス・ステータスリスト

トラストリスト

QTSP/QCA
適格サービス
プロバイダー
(公開鍵証明書発行)

QTSP/QTA
適格サービス
プロバイダー
(時刻証明局)

デジタル署名を
サポートするTSP 4

全体で利用する
暗号アルゴリズム

暗号スイート 3

適合性評価機関

監督機関

用語と凡例

セコムIS研究所
Intelligent Systems Laboratory

署名環境

Qualified certificates for electronic signatures
適格電子署名用証明書 Qcert for ESig

Qualified certificates for electronic seals
適格電子シール用証明書 Qcert for ESeal

Qualified electronic signature creation devices
適格署名生成デバイス QSCD

Qualified Timestamp
適格タイムスタンプ QTimestamp

署名データ

Qualified electronic signature
適格電子署名 QESig

Qualified electronic seal
適格電子シール QESeal

Qualified Timestamp
適格タイムスタンプ QTimestamp

署名フォーマット
CAdES XAdES
PAdES ASiC

署名検証環境

EU/TL

TSP:Trust Service Provider

Qualified trust service provider
適格トラストサービスプロバイダー

Qualified Certificate Authority
適格認証局 QC/CA

Qualified Timestamp Authority
適格タイムスタンプ局 QTA

トラストリスト

EU/TL

QC/CA QTA

non-QC/CA non-QTA

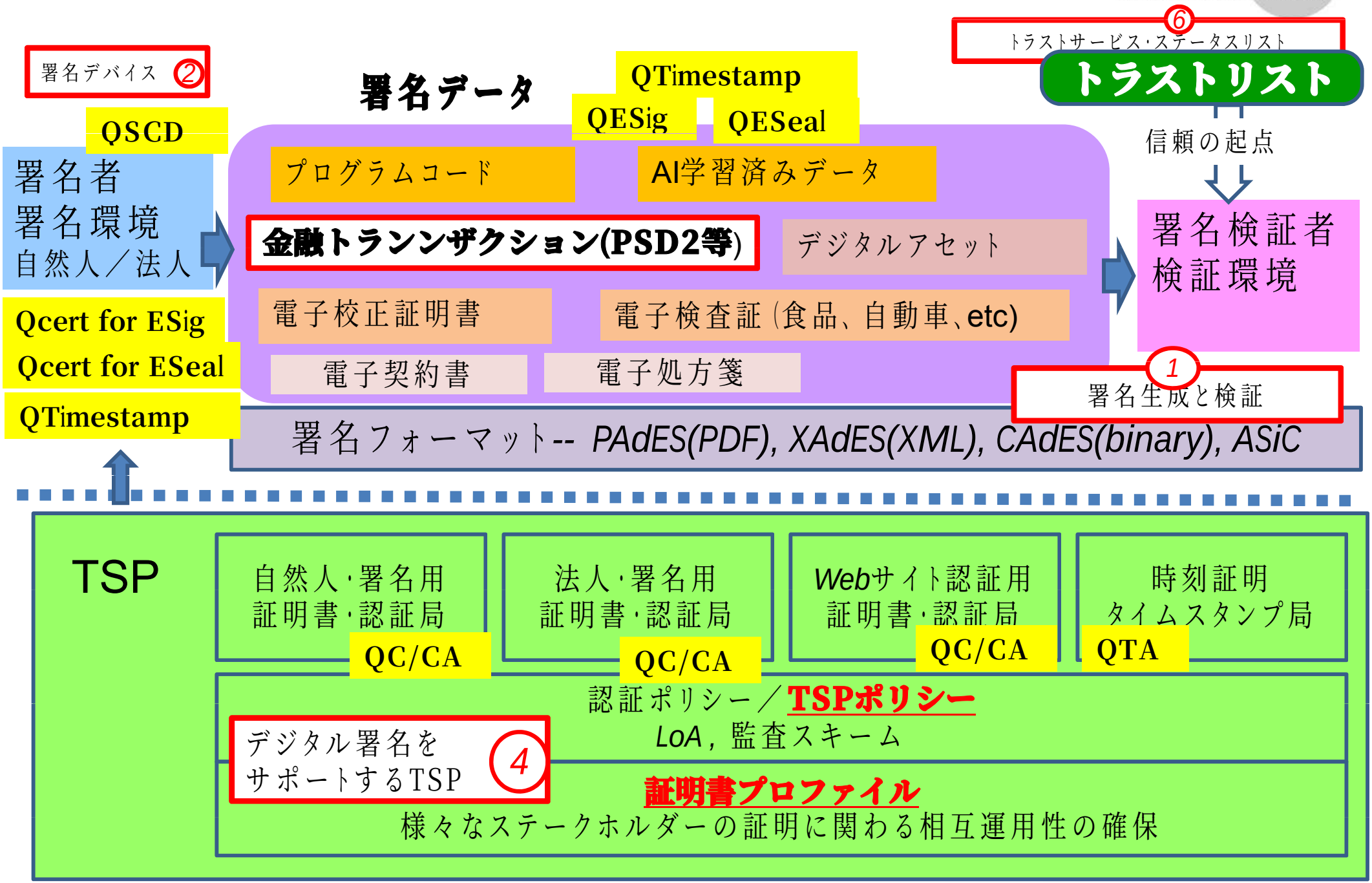
conformity assessment body
適合性評価機関

conformity assessment report
適合性評価レポート

Supervisory bodies
監督機関

TSP、署名者、署名データ、署名検証者の関係

セコムIS研究所 Intelligent Systems Laboratory



標準技術不在が招く、分野毎の細分化（fragmentation）
様々な分野で「誰が」、「何時」、「何を」を証明したい

セコムIS研究所 Intelligent Systems Laboratory

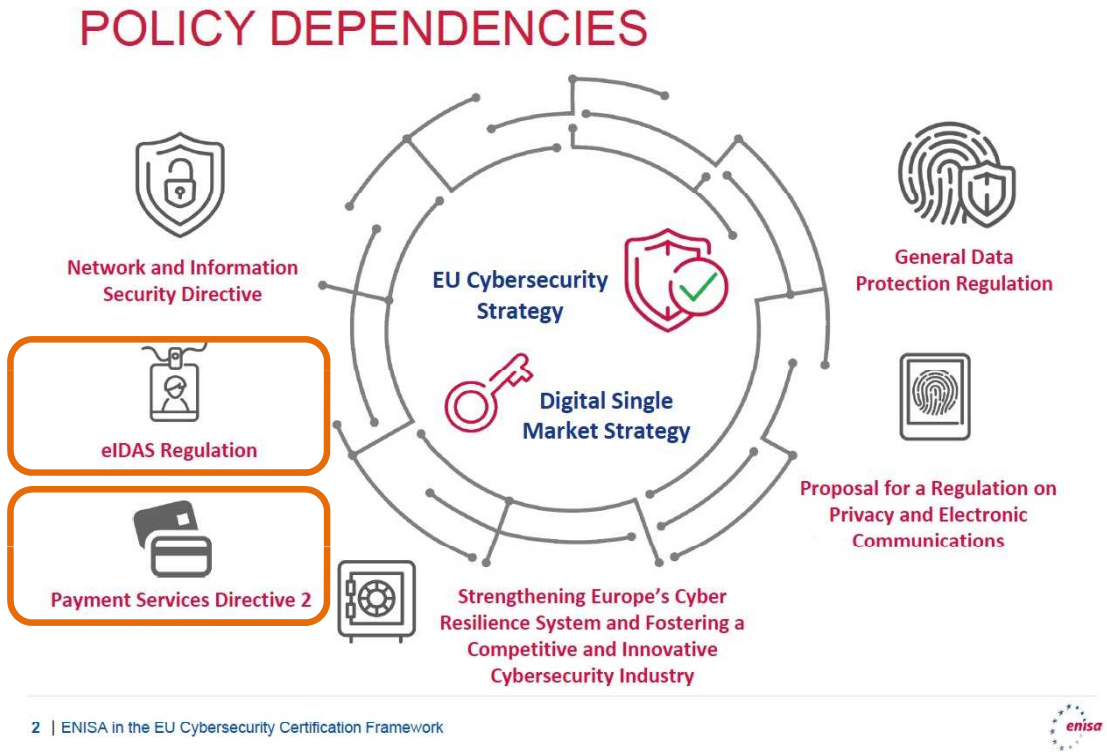
- 標準技術への要求
  - 署名検証者の多くは、マシン（コンピュータ）へ
    - Ex. 自動運転のための「学習済みデータ」や「ダイナミックマップ」の更新において、署名検証を行うのは、自動車内の自動運転を司るのECU
      -> リコール対応等の規制も必要
    - 類似する要求は、あらゆる分野に存在する（サイバー空間とフィジカル空間の高度な融合）
- 「誰が」、「何時」-> TSPの役割、ICT系の「DG CONNECT」が主導
  - 「何を」-> あらゆる分野におけるデジタル化の要求－＞ここに課題がある。
- 分野毎の細分化（fragmentation）の問題
  - 改正個人情報以前の主務官庁制の個人情報保護法の問題と類似
    - 細分化（fragmentation）された中の住人は、外のことは分からない -> このことが、後戻りの出来ない細分化を助長する。

様々な
分野毎の
様々な
署名データ

欧州決済サービス指令(PSD2)に見られる技術標準

「eIDASが提供するトラスト」と「OpenAPI」による金融サービス改革

- 欧州銀行監督局（EBA：European Banking Authority）が主導
- EBAの規制技術基準（RTS：Regulatory Technical Standards）よりeIDAS規則のQeSeal, QWACの利用を義務付け



1. 欧米における法制度の全体像

○ PSD2は、以下の業について、新たに規制の枠組みを整備。

① 決済指図伝達サービス提供者（PISP：Payment Initiation Service Provider）：
利用者の依頼により、他の決済サービス提供者（銀行、電子マネー事業者、決済サービス事業者）に開設されている利用者の決済口座に係る決済指図を伝達するサービス（第4条第15項）

② 口座情報サービス提供者（AISP：Account Information Service Provider）：
利用者が、他の決済サービス提供者（銀行、電子マネー事業者、決済サービス事業者）に開設されている1つ又は複数の決済口座の情報を統合して提供するオンラインサービス（第4条第16項）

	決済指図伝達サービス提供者(PISP)	口座情報サービス提供者(AISP)
業務内容	利用者の依頼による決済指図の伝達	利用者への口座情報の提供等
免許・登録	免許制（Authorisation ）	登録制（Registration ）
財務要件	資本金5万ユーロ以上	なし
資産保全	なし ※ 利用者からの資金預り禁止/※ 責任保険への加入義務あり	なし ※ 責任保険への加入義務あり

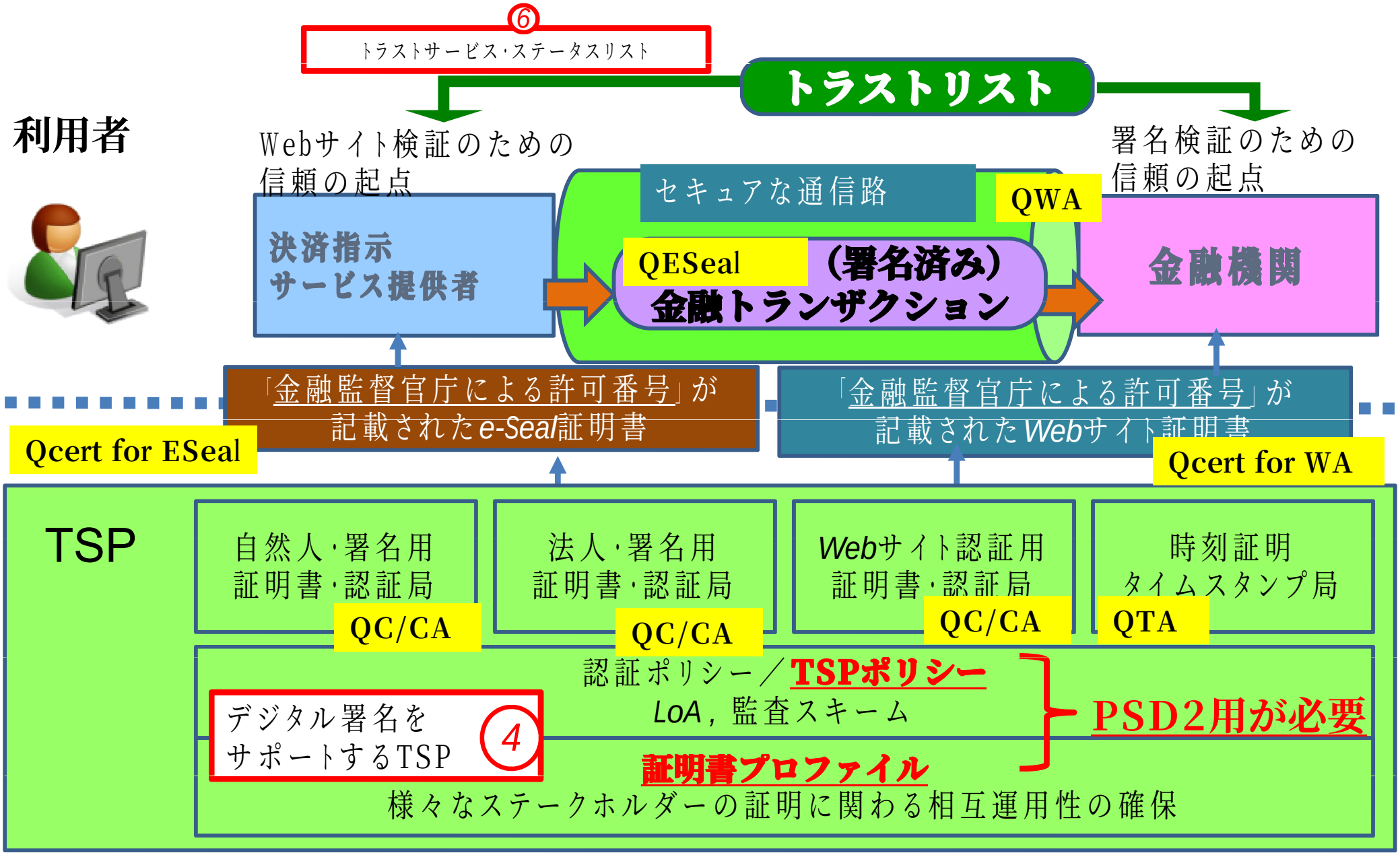
○ また、これに関連して、
① 無権限取引や決済の実行に瑕疵があった場合の中間的業者と銀行等の損失分担ルールや、
② 不正取引等の場合には、銀行等は、中間的業者からのアクセスを拒否できるといった規定を設ける一方、そうした場合以外では、銀行等が顧客による中間的業者経由の決済指図に応じるよう求めるとともに、銀行等による中間的業者の不当な取扱いを禁止するなど、オープンAPIの取組みと整合的な規定が整備されている。

出典：https://www.fsa.go.jp/singi/singi_kinyu/financial_system/siryou/20161028/01.pdf

欧州の決済サービス指令（PSD2)の場合

「eIDASが提供するトラスト」と「OpenAPI」による金融サービス改革

セコムIS研究所 Intelligent Systems Laboratory



欧州の決済サービス指令（PSD2)の場合

セコムIS研究所 Intelligent Systems Laboratory

- PSD2のステークホルダー
  - サービス利用者 – より便利で安全で多様な金融サービスを利用したい
  - 金融機関 -- サービス利用者の口座を保持し、OpenAPIを公開（義務）
  - 決済指示サービス提供者(PISP) -- 金融管轄官庁からの許可制
  - 欧州各国の金融管轄官庁
    - 金融サービス事業者に許可を与え「許可番号」を発行する
    - ＃許可の取り消しも行う（e-Seal証明書の失効→ QSTP）？？
  - QTSP -- 適格トラストサービスプラバイダー
    - 「金融監督官庁からの許可番号」が記載されたe-Seal証明書とWebサイト証明書の発行
- 金融サービス改革から見た（トラストサービスに関わる標準技術への要求）
  - 多対多の信頼関係と相互運用性の確保
  - 自動的な処理、機械判読可能な相互運用性
    - 署名者（金融サービス事業者）が、許可された事業者なのか（自動的に）検証可能なレベルの証明書プロファイル
  - 金融サービスの信頼
    - 金融サービス事業者としての信頼は、金融管轄官庁　-- 「許可番号」
    - 許可番号と、法人（Webサイト、金融トランザクション）との結合は、TSPの役割　→　多対多の信頼関係のためのLoA (証明書ポリシー)

PSD2の証明書プロファイル

デジタル署名を
サポートするTSP ④

セコムIS研究所
Intelligent Systems Laboratory

Internet X.509
Public Key
Infrastructure
Certificate and
CRL Profile

Internet X.509
Public Key
Infrastructure:
Qualified
Certificates
Profile

X.509証明書
v3拡張
フォーマット

RFC2459
1999年

RFC3280
2002年

RFC5820
2008年

RFC 3039
2001年

RFC 3739
2004年

Certificate Profiles;
Part 1: Overview and common data structures

ETSI EN
319 412-1

ETSI EN
319 412-2

eSig

ETSI EN
319 412-5

ETSI EN
319 412-3

eSeal

ETSI TS
119 412-1

ETSI EN
319 412-4

WAC

分野別の
証明書
プロファイル

eSeal

WAC

ETSI TS
119 495

Certificate Profiles;
Part 5: QCStatements

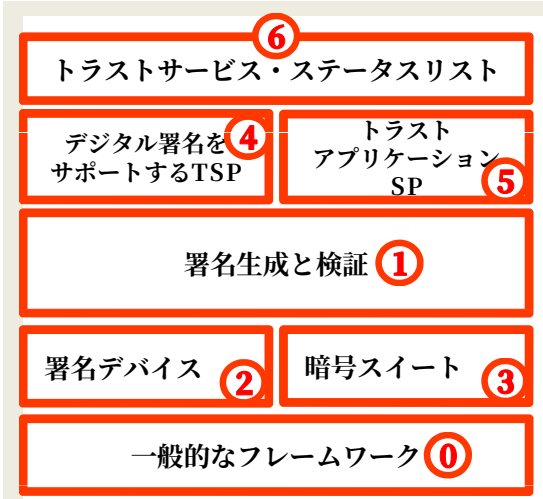
Certificate Profiles;
Part 1: Overview and common data structures

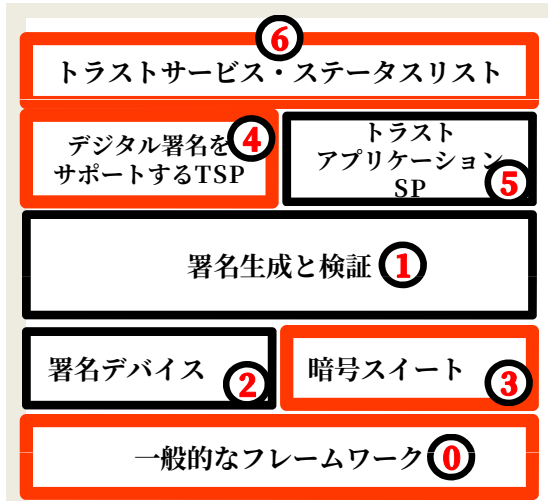
Sector Specific Requirements;
Qualified Certificate Profiles and TSP Policy Requirements
under the payment services Directive (EU) 2015/2366

ＥＵの技術標準からみた
電子署名、電子シール、Webサイト認証の関係

セコムIS研究所
Intelligent Systems Laboratory

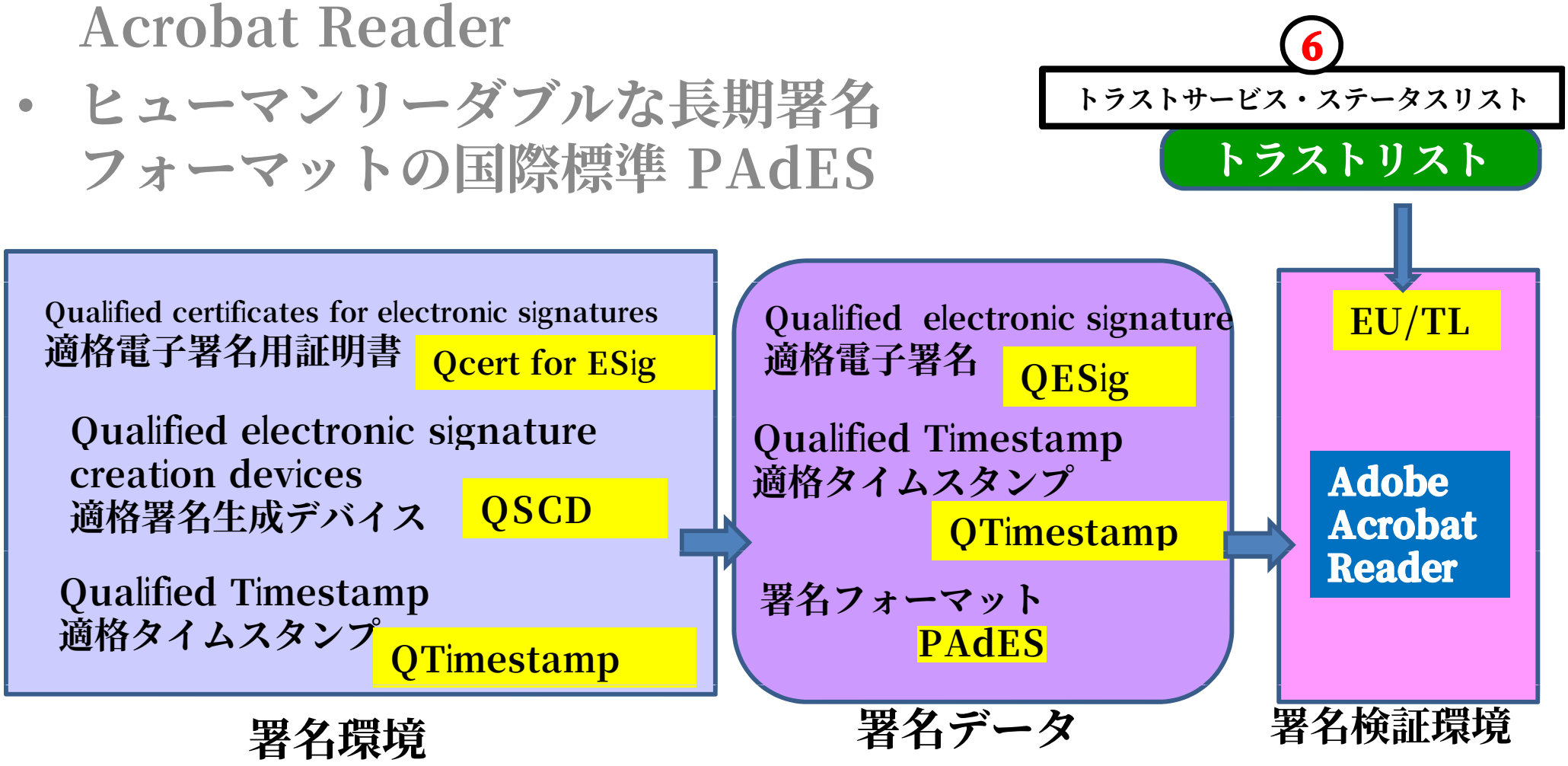
- 電子署名（自然人）と電子シール（法人）
  - TSPが発行する公開鍵証明書が、証明するエンティティ（自然人、法人）の違いのみ
  - 殆ど全ての欧州技術標準は、双方に適用できる
- 電子シール用証明書とWebサイト用証明書の関係
  - TSPから見ると、（ほとんどは）法人向けの公開鍵証明書の発行であり、TSPに関する多くの欧州技術標準は、双方に適用できる
    - PSD2的には（たぶん）電子シール用証明書とWebサイト用証明書は、セットで発行できる。
- おまけ
  - Webサイト認証とCAB/Fの関係
    - 同じETSIの監査スキームが適用できる





Acrobat Readerに見られる技術標準

- 日本語で、eIDAS規則＆欧州技術標準の署名検証が可能なAdobe Acrobat Reader
- ヒューマンリーダブルな長期署名フォーマットの国際標準 PAdES



ハンガリーのトラストサービスプロバイダーの証明書ポリシーを記述したPDF

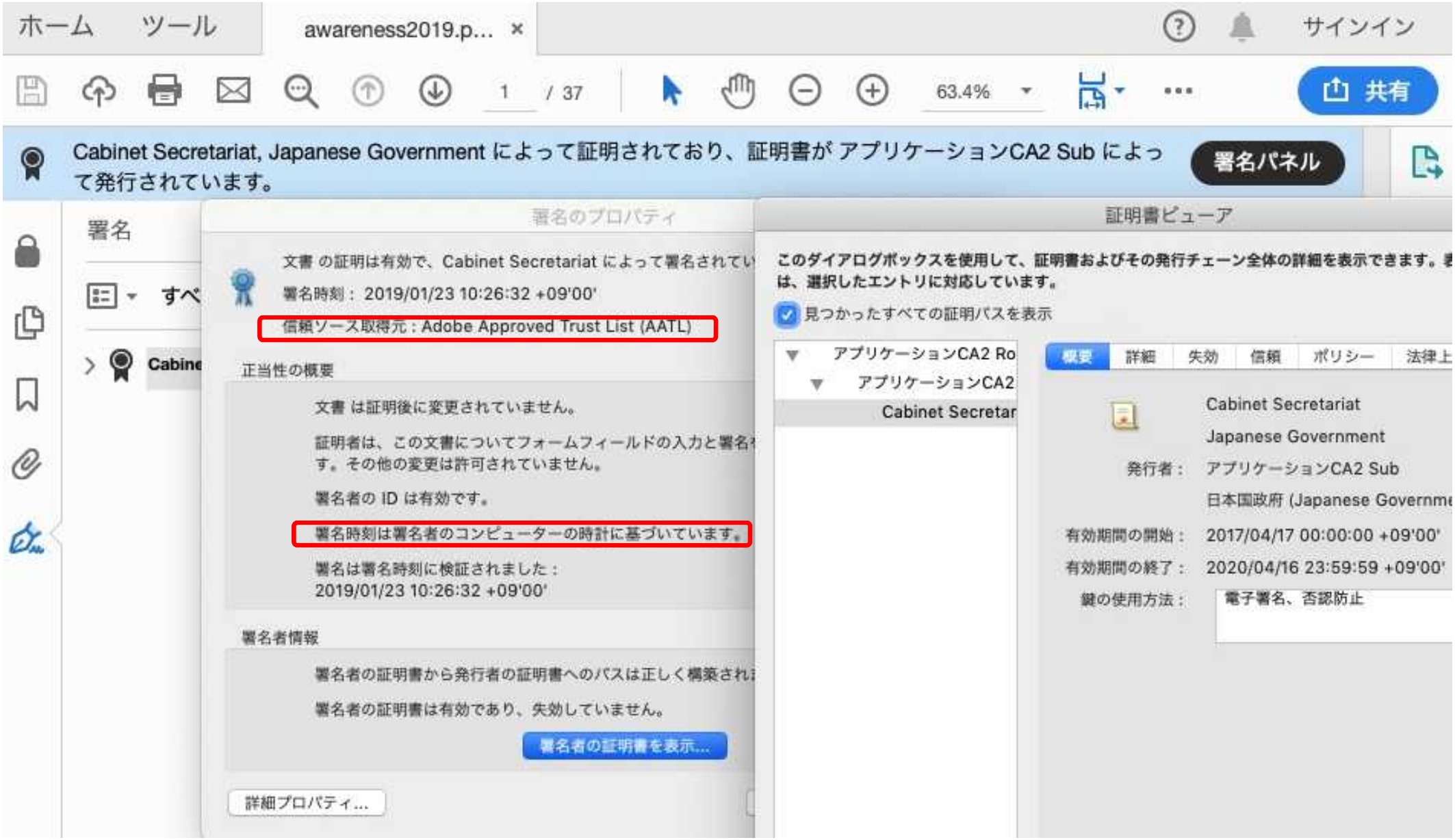
サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

Acrobat Reader が取り込んでいるEUトラストリスト

セコム IS 研究所
Intelligent Systems Laboratory

サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

参考　NISCの署名文書



サンプル署名ドキュメント　：https://www.nisc.go.jp/active/kihon/pdf/awareness2019.pdf

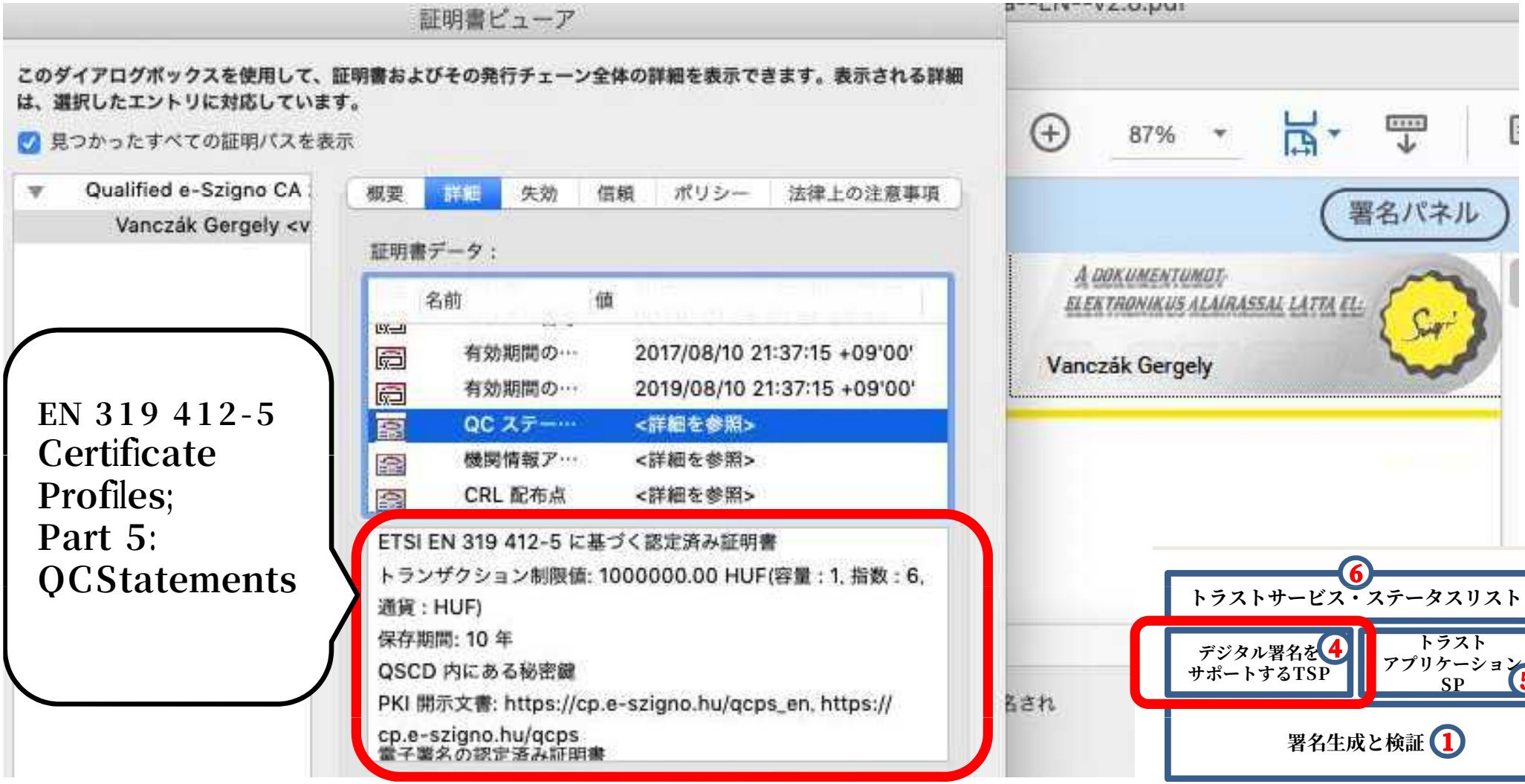
「適格署名生成デバイス」利用した署名

セコムIS研究所
Intelligent Systems Laboratory

サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

eIDAS証明書において非常に重要なQCステートメント
Acrobat Readerが解釈するQCステートメント

セコム IS研究所
Intelligent Systems Laboratory

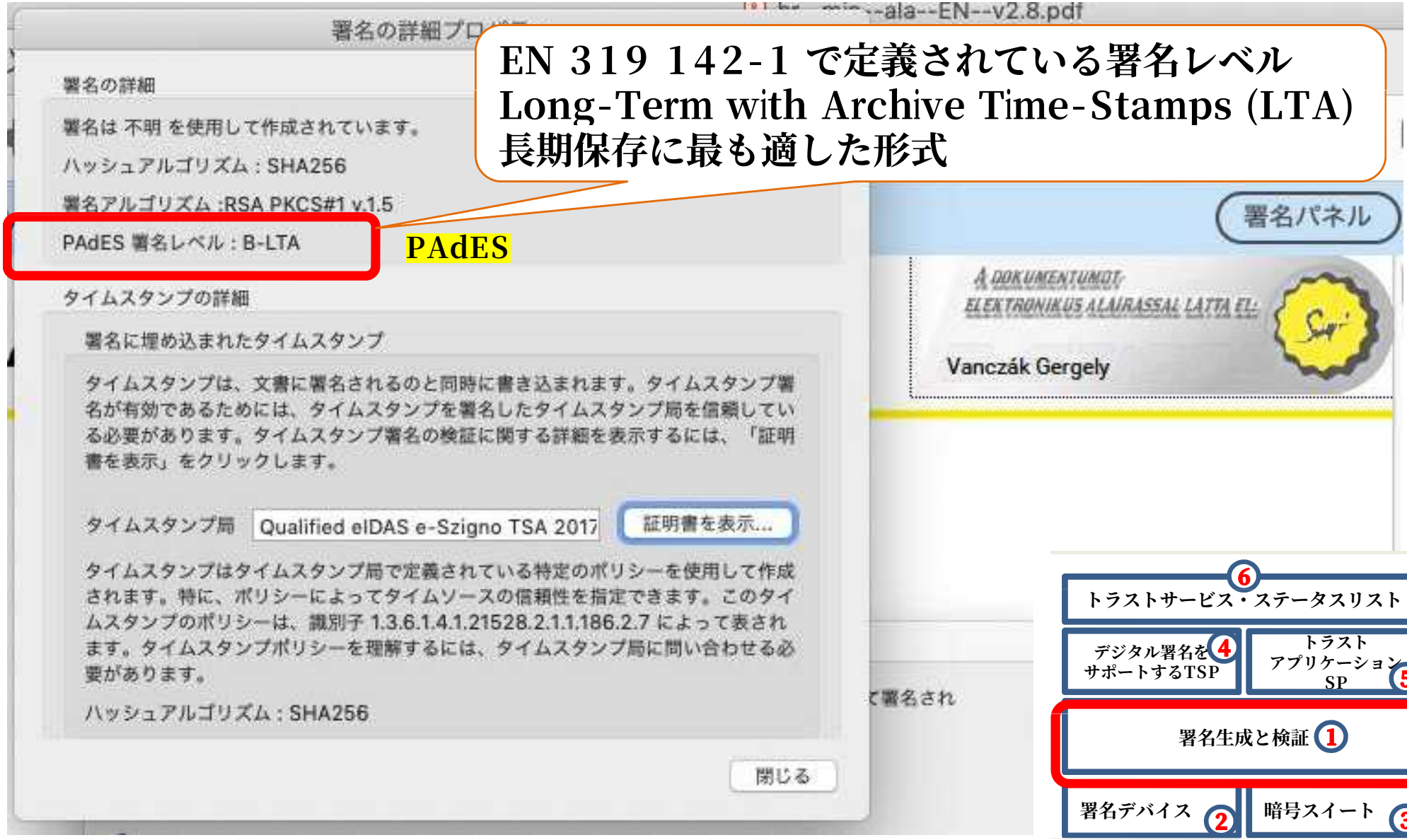


EN 319 412-5 Certificate Profiles; Part 5: QCStatements

サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

Acrobat Readerがサポートする PAdES

セコム IS 研究所
Intelligent Systems Laboratory



サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

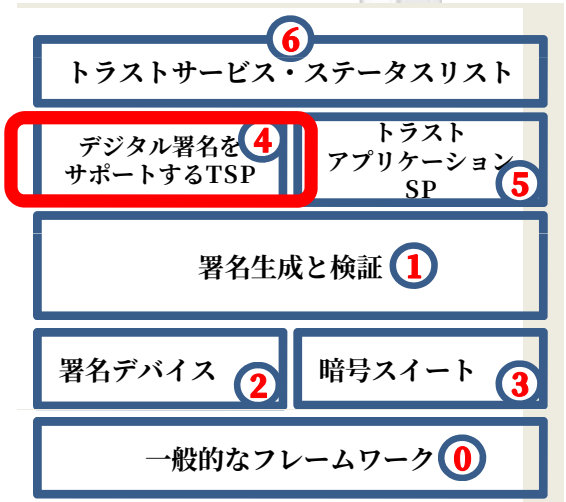
Acrobat Readerによる適格タイムスタンプの検証

セコムIS研究所
Intelligent Systems Laboratory

QTA　QTimestamp

附属書　Ⅲ
電子シールのための適格証明書の要件

ETSI EN 319 422
Time-stamping protocol and time-stamp token profiles
ETSI EN 319 421
Policy and Security Requirements for Trust Service Providers issuing Time-Stamps



サンプル署名ドキュメント：https://static.e-szigno.hu/docs/hr--min--bel--EN--v2.8.pdf

トラストリスト

CEF Digital
Connecting Europe

セコムIS研究所
Intelligent Systems Laboratory

CEF資金提供で開発、
運用されている
Trusted Listブラウザ

Trusted List Browser

Tool to browse the national Trusted Lists and the European List of Trusted Lists (LOTL).

Menu

European Commission > CEF Digital > eSignature > Trusted List Browser > Hungary > Trust service provider

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares

Trust services

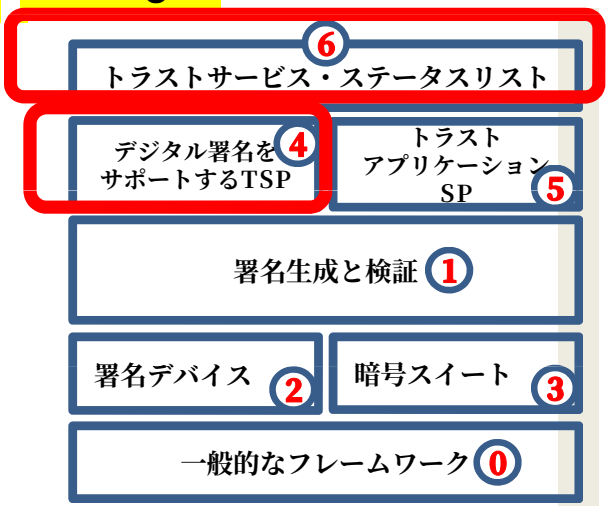
QC/CA　Qcert for ESig

- QCert for ESig — Qualified certificate for electronic signature
- QCert for ESeal — Qualified certificate for electronic seal
- QWAC — Qualified certificate for website authentication
- QPres for QESig — Qualified preservation service for qualified electronic signature
- QPres for QESeal — Qualified preservation service for qualified electronic seal
- QTimestamp — Qualified time stamp

QTA　QTimestamp

Acrobat Readerの署名検証が表示する署名者、署名時刻とeIDAS規則の関係

QTimestamp　QEsig



出典：https://webgate.ec.europa.eu/tl-browser/#/tl/HU/1

eIDASの適格認証局(eSign)と適格タイムスタンプ局の conformity assessment report　適合性評価レポート

セコムIS研究所 Intelligent Systems Laboratory

Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Microsec Ltd.
Záhony utca 7.
1031 Budapest, Hungary

to confirm that its trust service

e-Szignó Qualified Signature

QC/CA

fulfils all relevant requirements defined in regulation

Reg. (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures.

The appendix to the certificate is part of the certificate and consists of 3 pages.

The certificate is valid only in conjunction with the conformity assessment report.

eIDAS TÜVIT® 2018 Trusted Site
Certificate ID: 97120.18
© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Certificate valid until 2020-10-31

出典：
https://e-szigno.hu/assets/docs/e_Szigno_qualified_signature_2018.pdf

Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Microsec Ltd.
Záhony utca 7.
H-1031 Budapest, Hungary

to confirm that its trust service

e-Szignó Qualified Time-Stamp

QTA

fulfils all relevant requirements defined in

Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified electronic time stamps.

The appendix to the certificate is part of the certificate and consists of

The certifica
assessment

conformity assessment body
適合性評価機関

eIDAS TÜVIT® 2016 Trusted Site
Certificate ID: 9719.16
© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Certificate valid until 2018-10-31

出典：
https://e-szigno.hu/assets/docs/e_Szigno_qualified_time_stamp_2018.pd

欧州の新公的管理規則(OCR）に見られる技術標準
公的管理のための統合マネージメントシステム
(IMSOC-TRACES)とe-Certficate

- 1993年　EU加盟国間の「人、モノ、サービス、資本」の移動が自由化
- 1996年　牛海綿状脳症（BSE)問題発生
- 2005年　トレーサビリティ義務化、TRACES運用開始
  - 衛生証明書／獣医師証明書、植物検疫証明書等を扱う
- 2019年
  - 新公的管理規則(OCR）の実施と、公的管理のための統合マネージメントシステム(IMSOC)の稼働
  - eIDAS規則を適用した「デジタルがオリジナル文書（原本）」

欧州委員会　DG SANTE （保健衛生・食の安全総局）が主導

従来からのTRACES　TRAde Control and Expert System

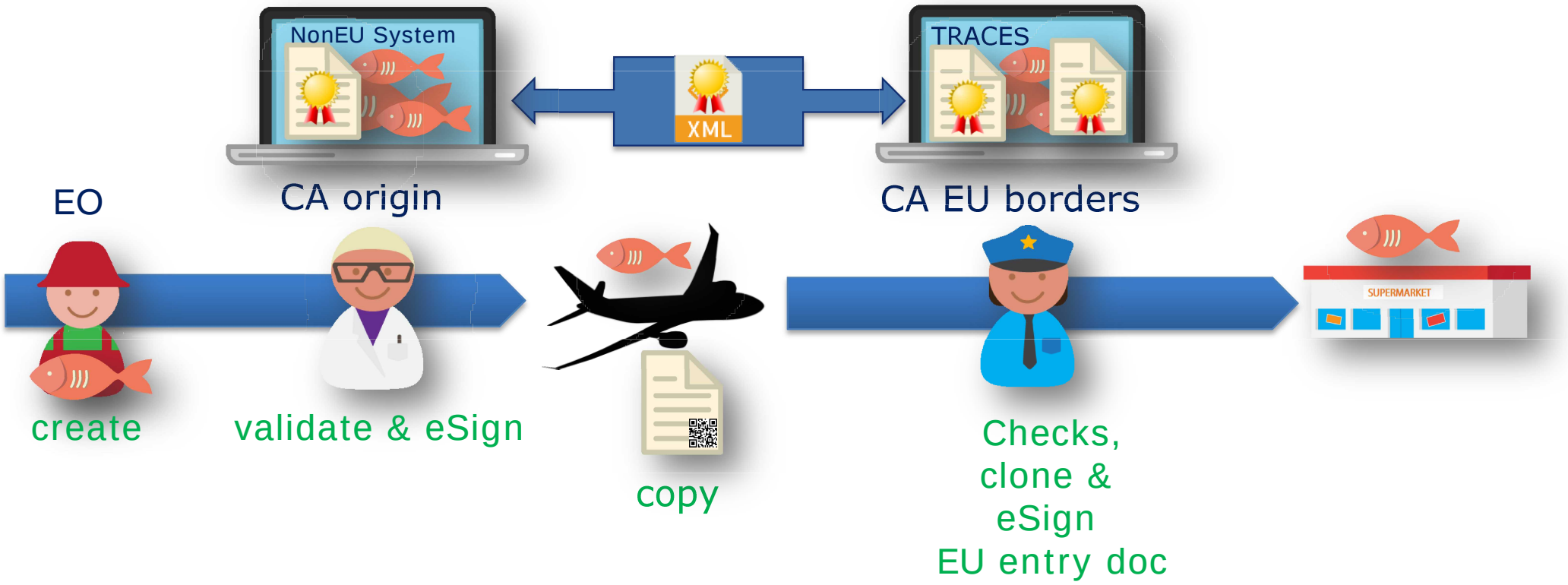
セコムIS研究所 Intelligent Systems Laboratory

- トレースの対象　　動植物
- ステークホルダー(TRACESの利用者）
  - 検査官等の行政官（40%)、EU域内事業者(50%)、EU域外の事業
- 関連する規制
  - 食品一般法（規則No.178/2002）第18条により義務づけられた食品、飼料などのトレーサビリティ確保の実施状況、課題、効果、および、モニタリング、罰則などの国内法令
  - 食品ロット識別のための表示の指令No.89/396/ECCについて、国内法令化、実施状況、効果、課題
- TRACES
  - 動物および動物製品に添付される「証明書」（certificate）を電子データベースで管理
  - 動物および動物製品に附帯が義務づけられている証明書を発行
  - 証明書は、パート１（荷の送付元、送付先）、パート２（健康情報）、パート３（コントロールの状態）からなる。
  - 証明書は、民間機関も許可を得て記載でき、当局がそれを査定し、証明書を発行し、さらに、発送通知書（送り状）を発行し、コントロールを行う。
  - 証明書が発行されると、許可をもらった民間業者はアクセスできる。

出典：欧州連合における 食品安全行政と食品産業団体、食品事業 者の取り組みに関する調査報告書
http://www.agribusiness.kais.kyoto-u.ac.jp/Europe.pdf

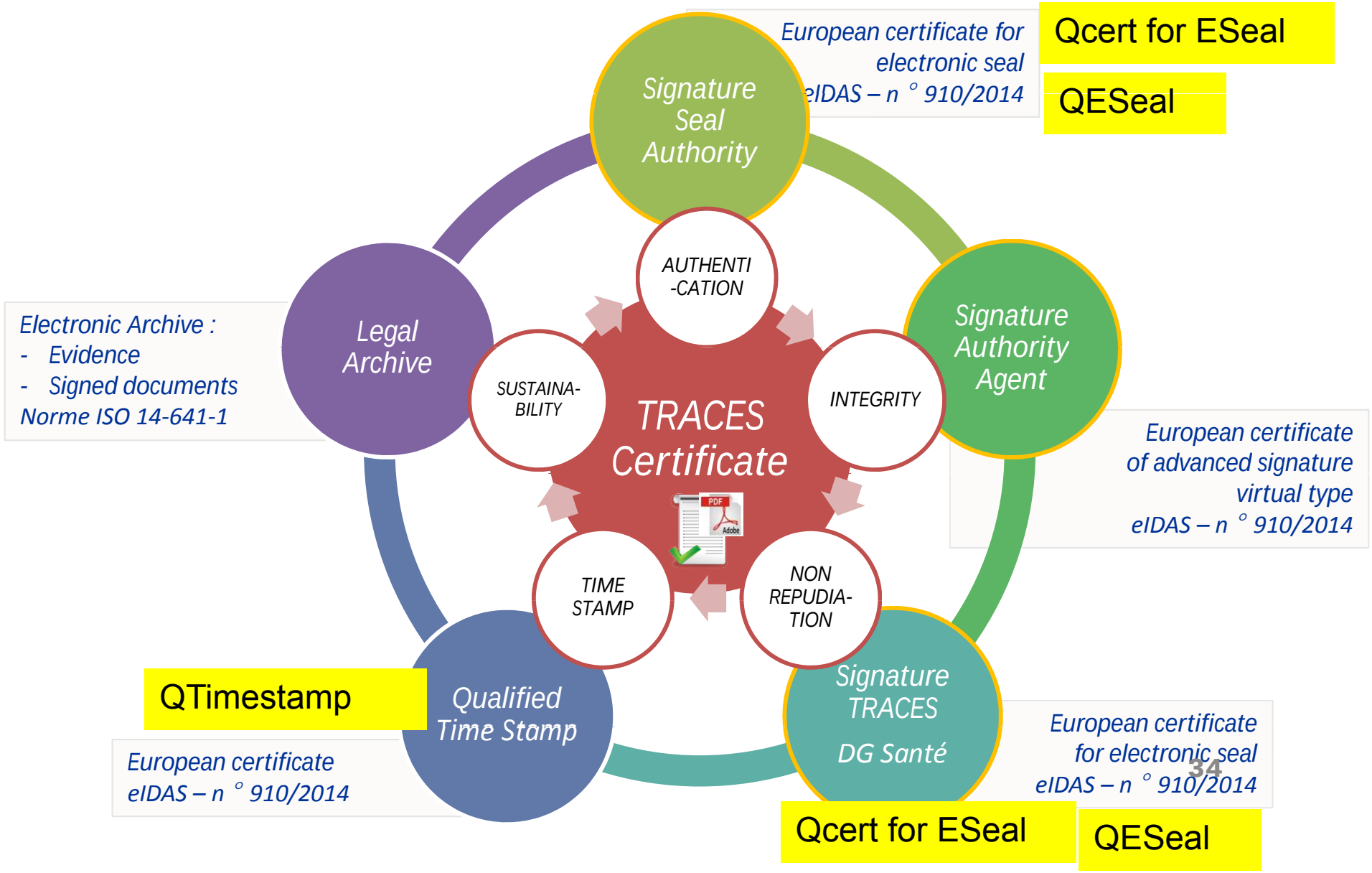
公的管理のための統合マネージメントシステム (IMSOC-TRACES)

The Official document is the digital one



出典:http://www.standardsfacility.org/sites/default/files/Ecert_Presentation_Carton_English.pdf

Sanitary certificate and key elements of legal evidence
衛生証明書（検疫証明書）と、法的エビデンスの重要な要素



出典:http://www.standardsfacility.org/sites/default/files/Ecert_Presentation_Carton_English.pdf

デジタルがオリジナル文書（原本）：IMSOCと他のシステム間のデータ交換のための方法

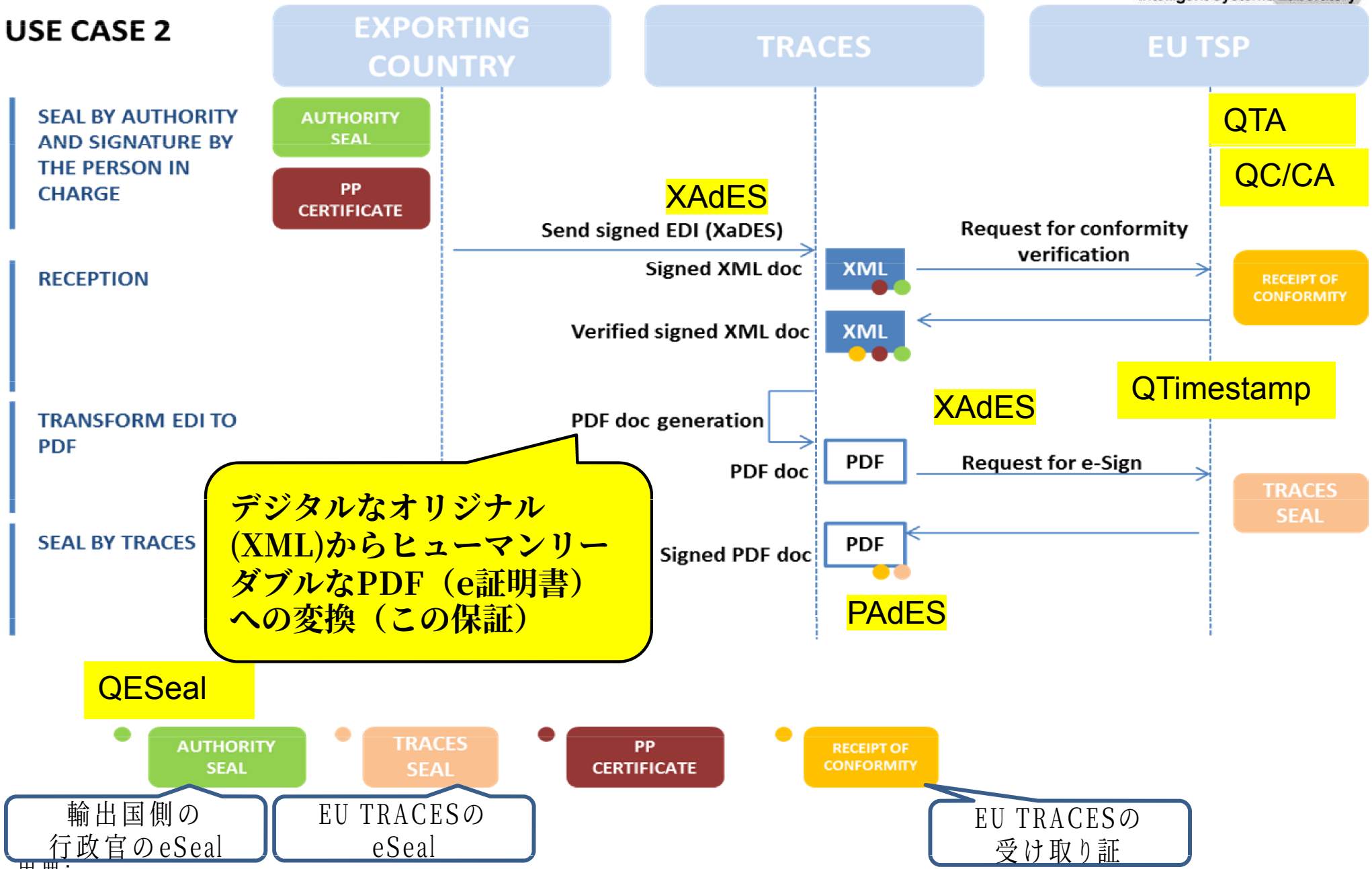
セコム IS 研究所 Intelligent Systems Laboratory

- 非EU国別システムとEU IMSOC間のデータ交換を確立
  - UN/CEFACT eCERT based XML exchanges + Validation rules
- データ交換において、適格電子署名（電子シール）と適格タイムスタンプを付す
  - 非EUシステムは、適格タイムスタンプを使用してXMLトランザクションに署名：
    - 自身（自国）のトラストサービスプロバイダーによるもの
    - IMSOCトラストサービスプロバイダーによるもの
  - 署名済みXMLが、オリジナル文書（原本）
  - ヒューマンリーダブルなe証明書(たぶん、PDF/PAdES)を再生成保証(コピーはオリジナルに準拠)

UN/CEFACT（United Nations Centre for Trade Facilitation and Electronic Business、貿易簡易化と電子ビジネスのための国連センター）

出典:
https://circabc.europa.eu/webdav/CircaBC/SANTE/Traces%20Toolkit/Library/Working%20groups%2c%20seminars%2c%20training%20sessions/TRACES%20Working%20Groups/2018-02-05%20TRACES%20Working%20Group/ TRACES WG Feb 2018 e-certification. EU approach and policy Final Export.pptx

IMSOC-TRACESによるデータ交換のための電子署名（電子シール）



出典:
https://circabc.europa.eu/webdav/CircaBC/SANTE/Traces%20Toolkit/Library/Working%20groups%2c%20seminars%2c%20trainings%20sessions/TRACES%20Working%20Groups/2018-02-05%20TRACES%20Working%20Group/ TRACES WG Feb 2018 e-certification. EU approach and policy Final Export.pptx

ＥＵの技術標準　まとめ

出典: https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Purser.pdf

ＥＵの技術標準　まとめ

セコムIS研究所
Intelligent Systems Laboratory

- eIDAS規則の施行に合わせて整備されてきたＥＵの技術標準は、非常によく整備され、多くは欧州標準(EN)となっている。
- こうした背景には、様々なモノ流通する第４次産業革命・超スマート社会において「トラスト」が重要になりつつあり、そして、様々な分野における相互運用性確保のために技術標準の重要さがある。
- 相互運用性に関して、サイバー空間とリアル空間が高度に融合する中、様々なシステムが連携が要求されており、そのためには、マシンリーダブルで自動的な処理に耐えられる、よりきめ細かい技術標準が必要となっている。
- また、ICT技術が、社会のありとあらゆるところに組み込まれる超スマート社会においては、法制度と技術の融合が求められており、法的相互運用性が考慮された技術標準が重要になっている。
- こうした要求に対して、欧州においては、 eIDAS規則、ETSI/CENの技術標準、更には、CEFのような資金提供プログラム等が一体となって、デジタル社会のインフラの整備を行っているように見受けられる。

欧州・米国・日本

セコムIS研究所
Intelligent Systems Laboratory

PKI day 2016 マイナンバー時代のPKI

欧州
規制モデル

米国
市場モデル

トラストが必要なサービス

一般データ
保護規則

個人情報の連携・個人情報の利活用と保護

eIDAS規則

トラストサービス・レイヤー

ハイパー
ジャイアント
による支配？

アイデンティティ管理（自然人、法人）
日本におけるマイナンバー制度等

日本の立ち位置は？？

出典：https://www.jnsa.org/seminar/pki-day/2016/data/2-4_panel_matsumoto.pdf

付録

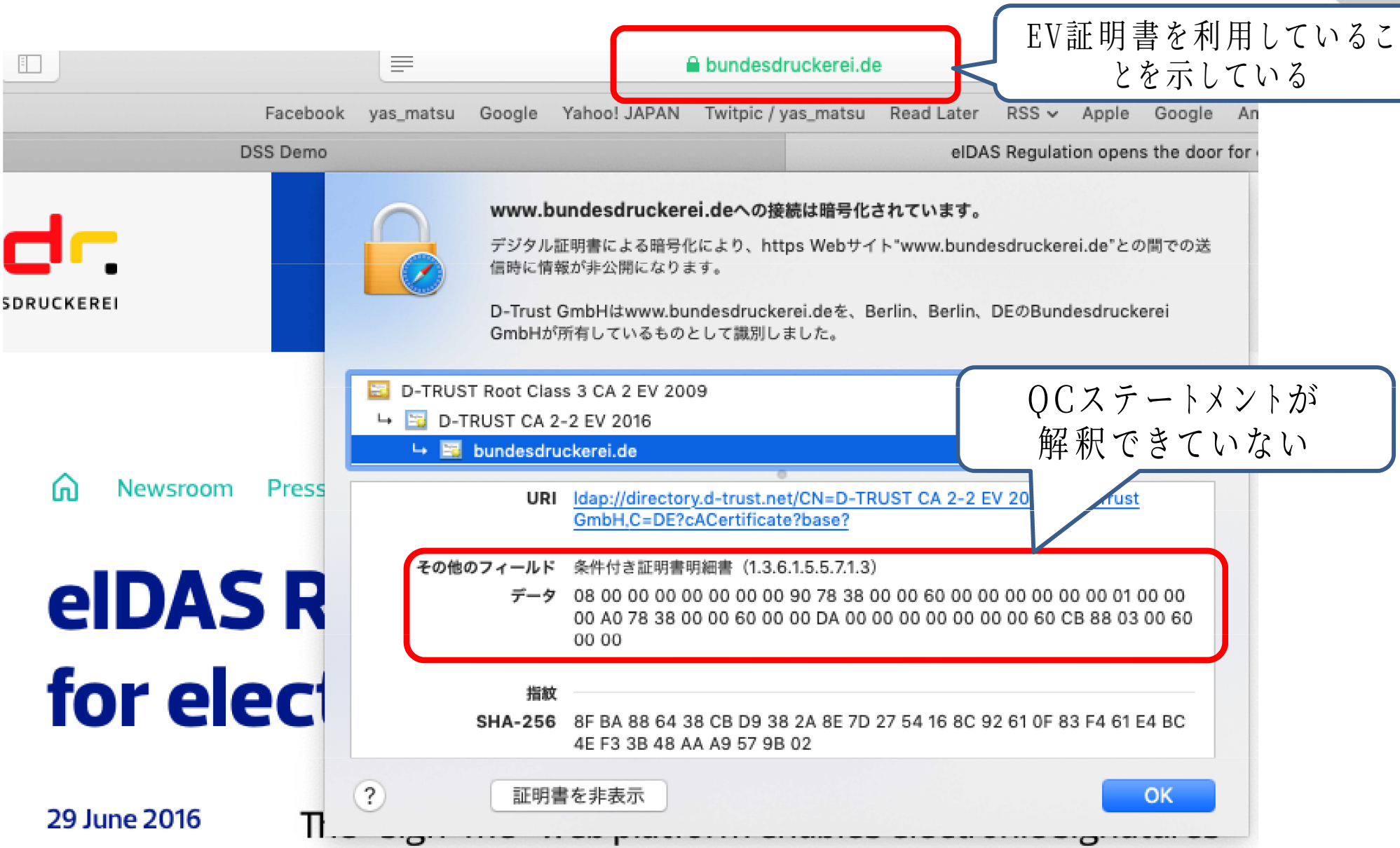
- 適格Webサイト認証の事例
- eIDAS技術標準の体系

適格Webサイト認証 QWAC

- CAB/Fとの関係
- eSealとの関係
- PSD2との関係
- → これらとの関係の理解が必要

適格Webサイト認証を利用したサイト

セコムIS研究所
Intelligent Systems Laboratory



参考URL:
https://www.bundesdruckerei.de/en/Press-room/eIDAS-Verordnung-macht-den-Weg-fur-Online-Unterschrift-frei

適格Webサイト認証を利用したサイト

セコムIS研究所
Intelligent Systems Laboratory

Webブラウザのトラストリストに登録されている

EUトラストリストに登録されている **QC/CA**

適格Webサイト証明書 かつ EV証明書 **QWAC**

QWAC

参考URL:
https://www.bundesdruckerei.de/en/Press-room/eIDAS-Verordnung-macht-den-Weg-fur-Online-Unterschrift-frei

適格Webサイト認証
conformity assessment report 適合性評価レポート

セコムIS研究所 Intelligent Systems Laboratory

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin, Germany

to confirm that its trust service

D-TRUST qualified EV SSL ID — QC/CA, QWAC

fulfils all relevant requirements defined in

Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for website authentication.

The appendix to the certificate is part of the certificate and consists of 3 pages.

The certificate is valid only in conjunction with the conformity assessment report.

Certificate

eIDAS TÜVIT 2017 Trusted Site
Certificate ID: 9729.17
© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Certificate valid until 2019-01-30

適合性評価機関
conformity assessment body

D-TRUST qualified Timestamp
fulfils all relevant requirements defined in
Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified electronic time stamps.
QTA, QTimestamp

D-TRUST qualified Signature ID card & D-TRUST qualified Signature HPC
fulfils all relevant requirements defined in regulation
Reg. (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures.
QC/CA, QESig

D-TRUST sign-me qualified
fulfils all relevant requirements defined in
Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures.
リモート署名
QC/CA, QESig

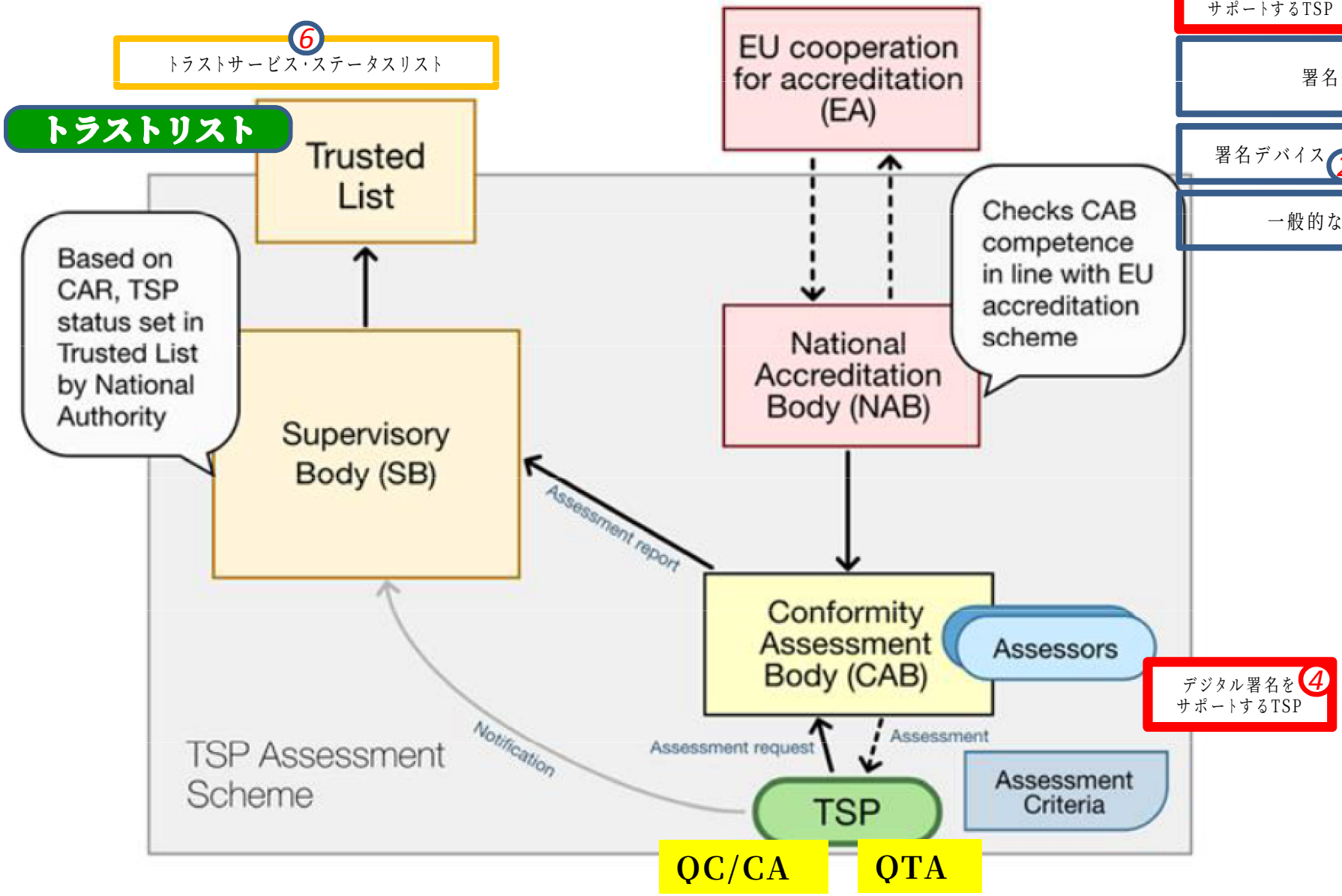
D-TRUST qualified Seal ID card
fulfils all relevant requirements defined in
Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic seals.
QC/CA, QESeal

出典： https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9729UE_s.pdf

eIDAS規則下のETSI監査スキーム

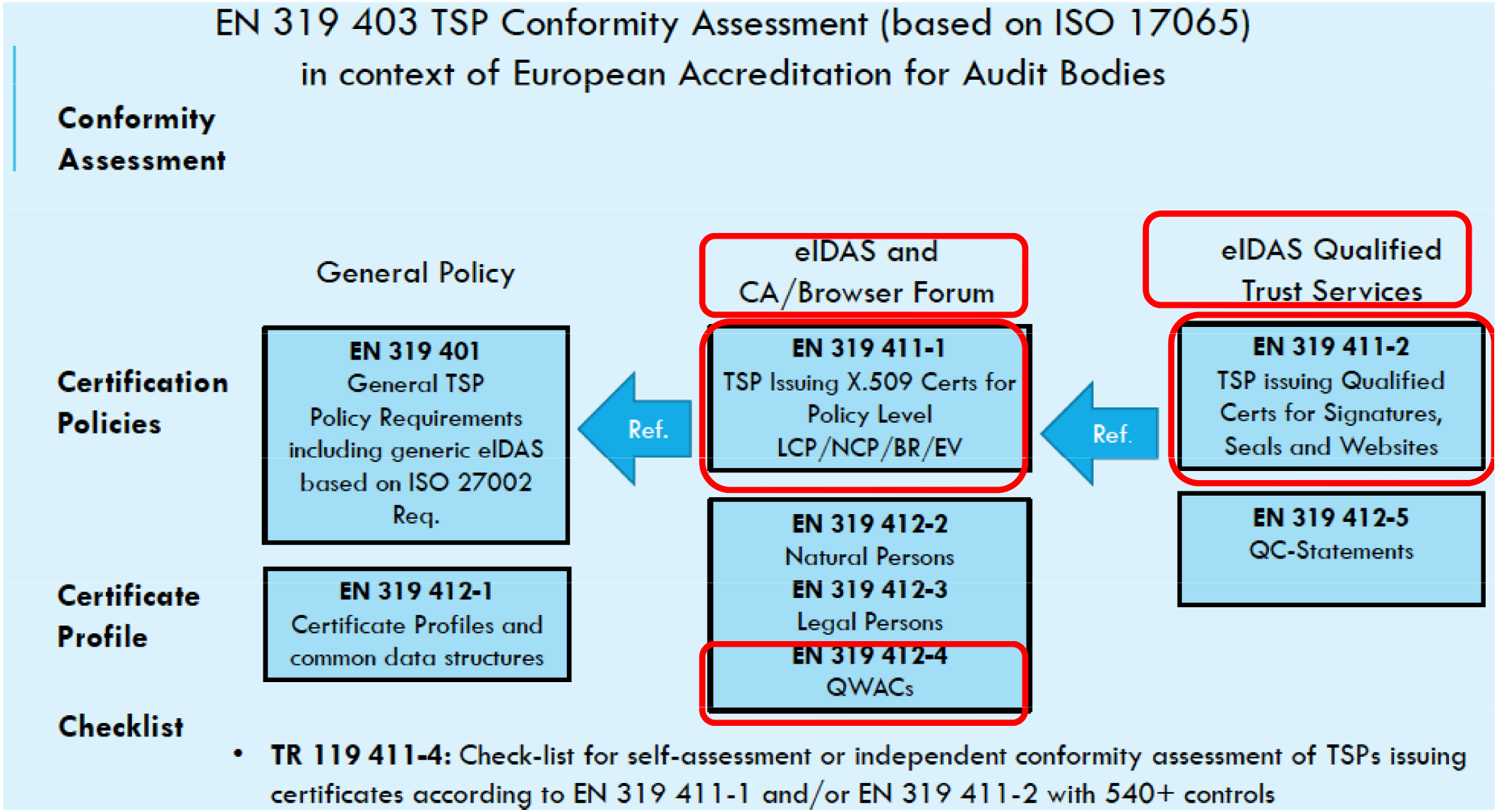
セコムIS研究所
Intelligent Systems Laboratory

6 トラストサービス・ステータスリスト
デジタル署名をサポートするTSP 4
トラストアプリケーションSP 5
署名生成と検証 1
署名デバイス 2
暗号スイート 3
一般的なフレームワーク 0



出典：https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/3a%20Fiedler.pdf

適格Webサイト認証に関する証明書ポリシー(TSPポリシー）（と証明書ポリシー）



出典：
https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/3a%20Fiedler.pdf

デジタル署名をサポートするTSP ④

CA/Browser Forum
Guidelines For The Issuance And Management Of Extended Validation Certificates

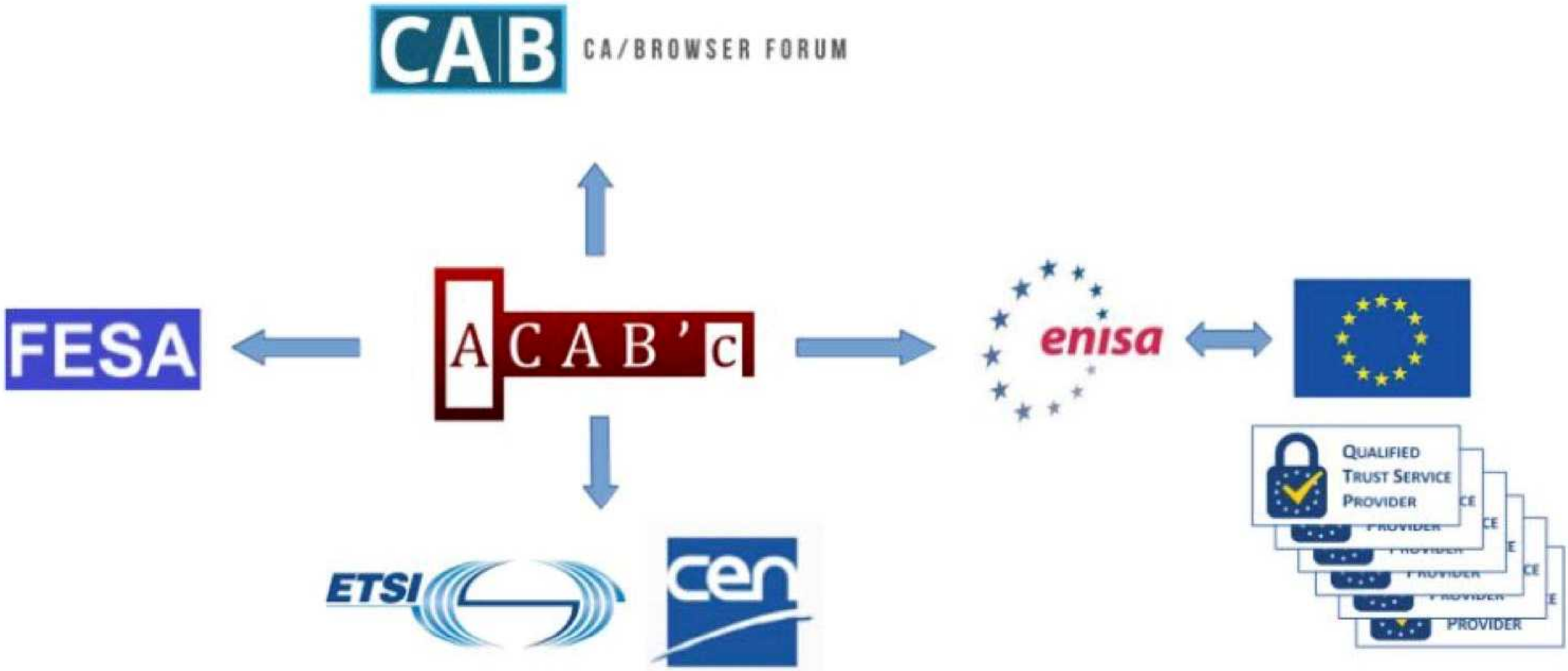
セコムIS研究所 Intelligent Systems Laboratory

- *17. Audit*
- *17.1. Eligible Audit Schemes*
- *A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:*
- *(i) WebTrust Program for CAs audit and WebTrust EV Program audit,*
  (ii) ETSI TS 102 042 audit for EVCP, or
  (iii) ETSI EN 319 411-1 audit for EVCP policy.
- *If the CA is a Government Entity, an audit of the CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.*

出典： https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf

- ETSI EN 319 411-2の記載　　--　証明書ポリシー
  - QCP-w
    - When the certificate is issued to a legal person the requirements for **QCP-w** include all the EVCP requirements,
  - QCP-l
- CAB/Fとの関係
- eSealとの関係
- PSD2との関係

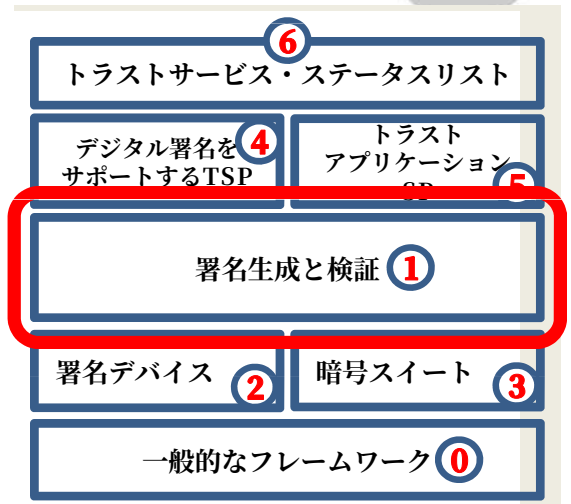
eIDAS規則・EU技術標準による監査スキームと監査スキームのグローバル化との関係



ACABs　Accredited Conformity Assessment Bodies
The Accredited Conformity Assessment Bodies' Council
https://www.acab-c.com
FESA　Forum of European Supervisory Authorities for trust service providers
http://www.fesa.eu

出典：https://www.enisa.europa.eu/events/tsforum-caday-2018/presentations/02_04_Gonnot.pdf

eIDAS技術標準の体系

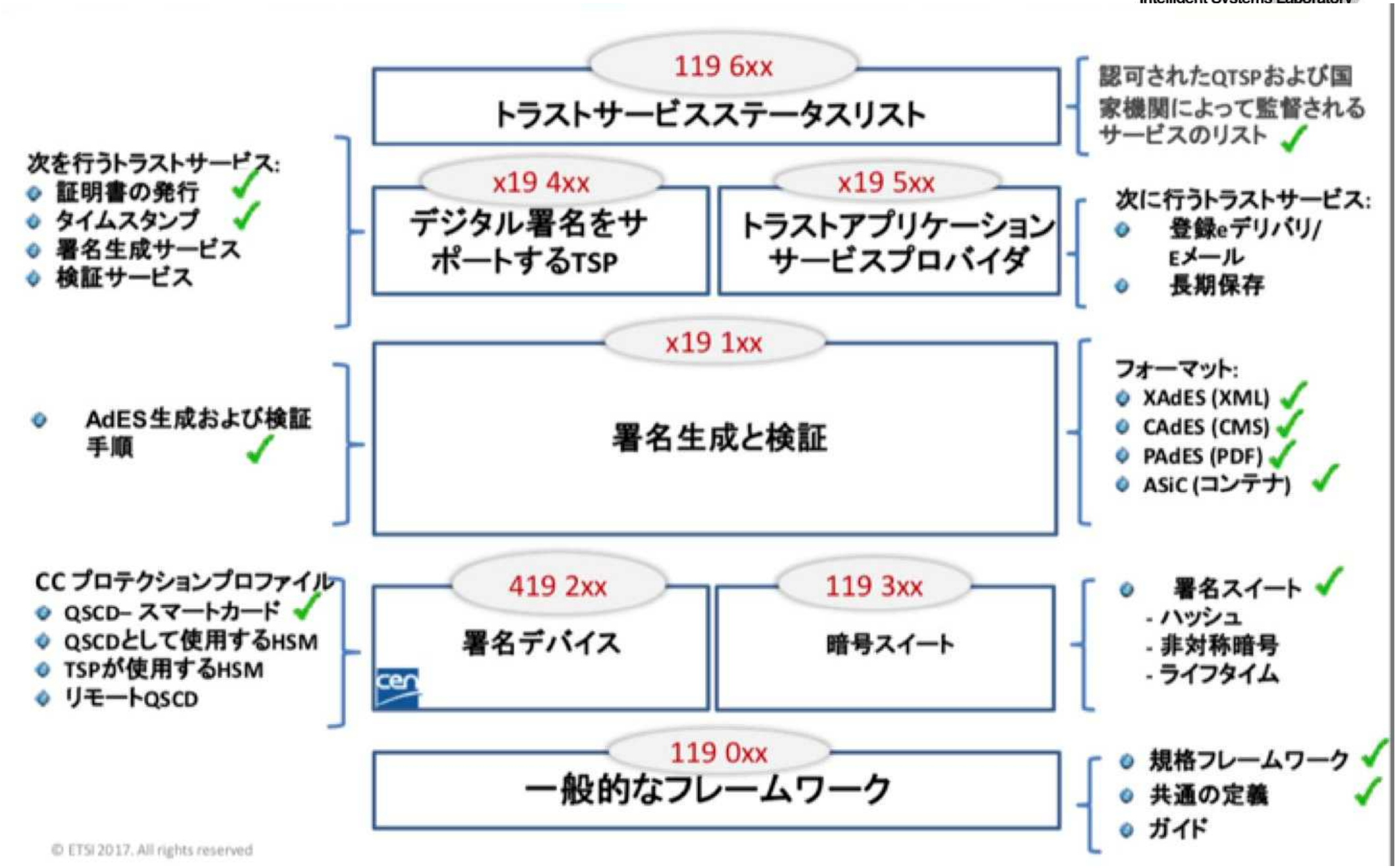


- 非常によく体系化され整備されている
- 法的な要求との整合が、よく考慮されている（法的相互運用性）
- 詳細な技術仕様からテストまでが仕様化されている（相互運用性の確保と実装可能、利用される標準）

出典：
https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf

eIDAS技術標準の体系

セコムIS研究所
Intelligent Systems Laboratory



出典：https://itc.jipdec.or.jp/common/images/kouensiryou_4.pdf

署名生成と検証

セコムIS研究所
Intelligent Systems Laboratory

						Signature creation and validation	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	1	0	0	Guidance on the use of standards for signature creation and validation		
						Policy & Security Requirements		
TS	1	19	1	0	1	Policy and security requirements for applications for signature creation and signature validation	(new)	published
EN	4	19	1	1	1	Protection profiles for signature creation and validation application - Part 1: Introduction to the European Norm - Part 2: Signature creation application - Core - Part 3: Signature creation application - Poss - Part 4: Signature verification application - Core PP - Part 5: Signature verification application - Possible Extensions	CWA/prEN 14170	All parts published certified in 2016-2017
						Technical Specifications		
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures - Part 1: Creation a - Part 2: Validation	TS 102 853,	art 1: Apr. 2016 art 2: undefined
EN	3	19	1	2	2	CAdES digital signa - Part 1: Building b - Part 2: Extended		arts 1 & 2: pr. 2016
EN	3	19	1	3	2	XAdES digital signa - Part 1: Building b - Part 2: Extended		arts 1 & 2: pr. 2016
EN	3	19	1	4	2	PAdES digital signat - Part 1: Building b - Part 2: Additiona - Part 3: Visual rep		arts pr. art 3: delayed
TS	1	19	1	5	2	Architecture for Ad		ndefined
EN	3	19	1	6	2	Associated Signatur - Part 1: Building b - Part 2: Additional ASiC containers		arts 1 & 2: Apr. 2016
TS	1	19	1	7	2	Signature policies - Part 1: Building blocks and table of contents for human readable signature policy documents - Part 2: XML format for signature policies - Part 3: ASN.1 format for signature policies - Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists	- TR 102 041 / 045 - TR 102 038 - TR 102 272	- Part1: published - Other parts: undefined
						Conformity Assessment		
EN	4	19	1	0	3	Conformity assessment for signature creation & validation (applications & procedures)	(new) (CWA 14172-	
						Testing Conformance & Interoperability		
TS	1	19	1	2	4	CAdES Testing conformance & interoperability	(new)	June 2016
TS	1	19	1	3	4	XAdES Testing conformance & interoperability		
TS	1	19	1	4	4	PAdES Testing conformance & interoperability		
TS	1	19	1	5	4	Testing conformance & interoperability of AdES in mobile enviro		
TS	1	19	1	6	4	ASiC Testing conformance & interoperability	(new)	June 2016

Guidance

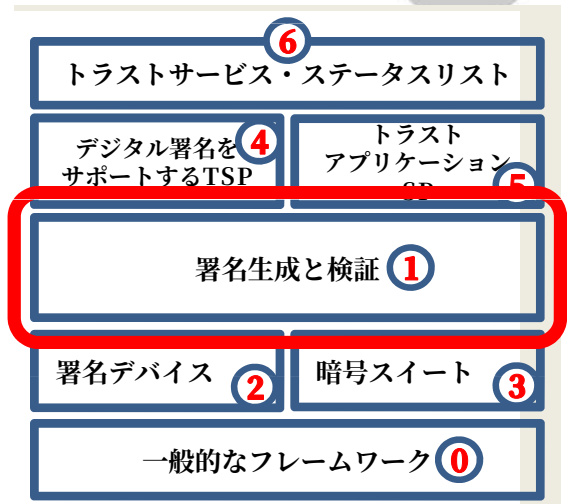
Policy & Security Requirements

CAdES 汎用
XAdES XML
PAdES PDF
ASiC コンテナ

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability



出典：https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf

署名デバイス -- QCSD by CEN

QSCD

セコムIS研究所 Intelligent Systems Laboratory

Signature creation and other related devices							Replaces	Expected publication
				Sub-areas				
				Guidance				
TR	4	19	2	0	0	Guidance on the use of standards for signature creation and other related devices	(new)	
				Policy & Security Requirements				
EN	4	19	2	1	1	Protection profiles for secure signature creation device		published
						- Part 1: Overview	- (new part)	
						- Part 2: Device with key generation	- prTS 14169-2	
						- Part 3: Device with key import	- prTS 14169-3	
						- Part 4: Extension for device with key generation and trusted communication with certificate generation application	- prTS 14169-4	
						- Part 5: Extension for device with key generation and trusted communication with signature creation application	- prEN 14169-5	
						- Part 6: Extension for device with key import and trusted communication with signature creation application	- (new part)	
EN	4	19	2	2	1	Protection Profiles for TSP cryptographic modules		
						- Part 1: Overview	- (new part)	Parts 1 to 4 in 2016
						- Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP)	- prTS 14167-2 - prTS 14167-3	Part 5 in 2017
						- Part 3: Cryptographic module for CSP key generation s		
						(CMCKG-PP)		
						- Part 4: Cryptographic module for CSP signing operation		
						Protection Profile (CMCSOPP)		
						- Part 5: Protection Profile for cryptographic module for TSPs		
EN	4	19	2	3	1	Protection profile for trustworthy systems support		
EN	4	19	2	4	1	Trustworthy systems supporting server signing		
						- Part 1: General system security requirements		
						- Part 2: Protection Profile for QSCD for Server Sig		
EN	4	19	2	5	1	Security requirements for device for authenticatio		
						- Part 1: Protection profile for core functionality		
						- Part 2: Protection profile for extension for trusted channel to certificate generation application		
						- Part 3: Additional functionality for security targets		
TS	4	19	2	6	1	Security requirements for trustworthy systems (incl. managing certificates for electronic signatures)	prTS 14167-1 prTS 419 221-1	published
				Technical Specifications				
EN	4	19	2	1	2	Application interfaces for secure elements used as qualified electronic signature (seal) creation devices	EN 14890	2016
						- Part 1: Introduction		
						- Part 2: Basic services		
						- Part 3: Device authentication		
						- Part 4: Privacy specific protocols		
						- Part 5: Trusted eServices		
				Conformity Assessment				
						no requirement identified		
				Testing Conformance & Interoperability				
-		-	-	-	-	*no requirement identified*		

Guidance

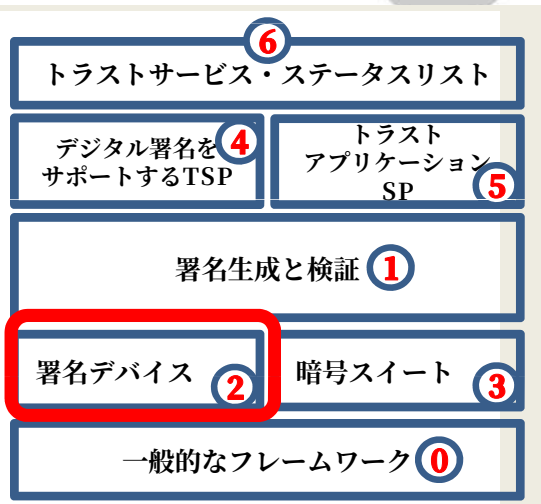
Policy & Security Requirements

署名デバイスの
プロテクションプロファイル

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability



出典：https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf

デジタル署名をサポートするTSP

QTA QTA

セコムIS研究所 Intelligent Systems Laboratory

TSPs supporting digital signatures and related services						Replaces	Expected publication
					Sub-areas		
					Guidance		
TR	1	19	4	0	0 Guidance on the use of standards for TSPs services		pu
					Policy & Security Requirements		
EN	3	19	4	0	1 General policy requirements for trust service providers	Replacing generic parts of TS 101 456, TS 102	pu
EN	3	19	4	1	1 Policy and security requirem - Part 1: General requirements - Part 2: Requirements for trust service providers issuing EU qualified certificates - Part 3: *To be withdraw* - Part 4: Requirements f	EN 319 411-3 - TS 101 456 (& TR 102 458), EN 319 411-3 - historical - (new)	- p - p - v - u
EN	3	19	4	2	1 Policy & security require	TS 102 023	pu
EN	3	19	4	3	1 Policy and security requi signature generation services	(new)	Undefined
EN	3	19	4	4	1 Policy and security requirements for trust service providers providing AdES digital signature validation services	(new)	Undefined
					Technical Specifications		
EN	3	19	4	1	2 Certificate profiles - Part 1: Overview - Part 2: Certificate - Part 3: Certificate - Part 4: Certifcate profile for web site certificates - Part 5: QCStatements	- (new part) - TS 102 280 & TS 101 - (new part) - TS 101 862	all parts published
EN	3	19	4	2	2 Time-stamping protocol and time-stamp token profiles	TS 101 861	published
EN	3	19	4	3	2 Protocol profiles for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	2 Protocol profiles for trust service providers providing AdES digital signature validation services	(new)	Undefined
					Conformity Assessment		
EN	3	19	4	0	3 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing trust service providers	TS 119 403	
					Testing Conformance & Interoperability		
-	-	-	-	-	- *no requirement identified for such a document*		

Guidance

Policy & Security Requirements

証明書ポリシー
TSPポリシー

証明書プロファイル

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability

6 トラストサービス・ステータスリスト

デジタル署名をサポートするTSP 4

トラストアプリケーションSP 5

署名生成と検証 1

署名デバイス 2

暗号スイート 3

一般的なフレームワーク 0

出典：https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf

トラストアプリケーション・サービスプロバイダー

セコムIS研究所 Intelligent Systems Laboratory

Trust application service providers							Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	5	0	0	Guidance on the use of standards for trust application service provid		
SR	0	19	5	1	0	Scoping study and framework for standardization of long term data p services, including preservation of/with digital signatures		
						Policy & Security Requirements		
EN	3	19	5	1	1	Policy & security requirements for trust service providers providing long term data preservation services, including preser	TS 102 573,	Undefined
EN	3	19	5	2	1	Policy & security requirements for elec		
EN	3	19	5	3	1	Policy & security requirements for regis		
						Technical Specifications		
EN	3	19	5	1	2	Long term data preservation services, including preservation of/with digital signatures		Undefined
EN	3	19	5	2	2	Electronic registered delivery services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings	(new)	Undefined
EN	3	19	5	3	2	Registered electronic mail (REM) services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles		
						Conformity Assessment		
-	-	-	-	-	-	*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*		
						Testing Conformance & Interoperability		
TS	1	19	5	0	4	General requirements for technical conformance and interoperability testing for trust application service providers and the services they provide		Undefined
TS	1	19	5	2	4	Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers	TR 103 071	Undefined
TS	1	19	5	3	4	Testing conformance & interoperability of registered electronic mail services. - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of providers using same format and transport protocols - Part 3: Test suites for interoperability testing of providers using different format and transport protocols		

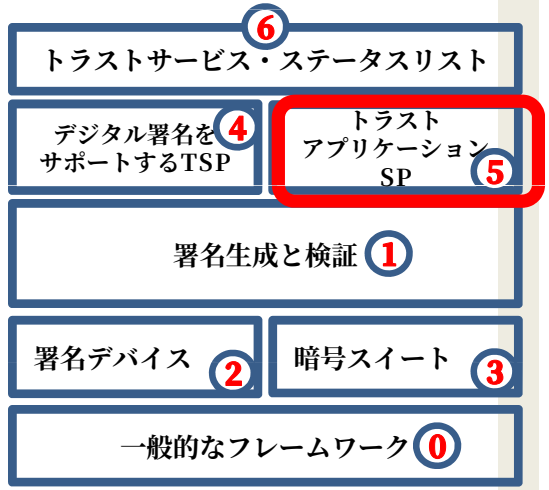
Guidance

Policy & Security Requirements

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability



出典：https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf

トラストサービス・ステータスリスト

セコムIS研究所
Intelligent Systems Laboratory

トラストリスト

⇑

信頼の起点

⇓

署名検証者
署名検証環境

					Trust service status lists provid		epiaces	Expected publication
					Sub-areas			
					Guidance			
TR	1	19	6	0	0 Guidance on the use of standards for trust service status lists providers	new		published
					Policy & Security Requirements			
TS	1	19	6	1	1 Policy & security requirements for trusted lists provide			
					Technical Specifications			
TS	1	19	6	1	2 Trusted lists			
					Conformity Assessment			
-	-	-	-	-	*no requirement identified for such a document - relying on*			
					Testing Conformance & Interoperability			
TS	1	19	6	1	4 Testing conformance & interoperability of trusted lists:			
					- Part 1: Test suites for testing interoperability of XML re			
					- Part 2: Specifications for testing conformance of XML representation of trusted lists			

Guidance

Policy & Security Requirements

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability

出典：https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf