

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



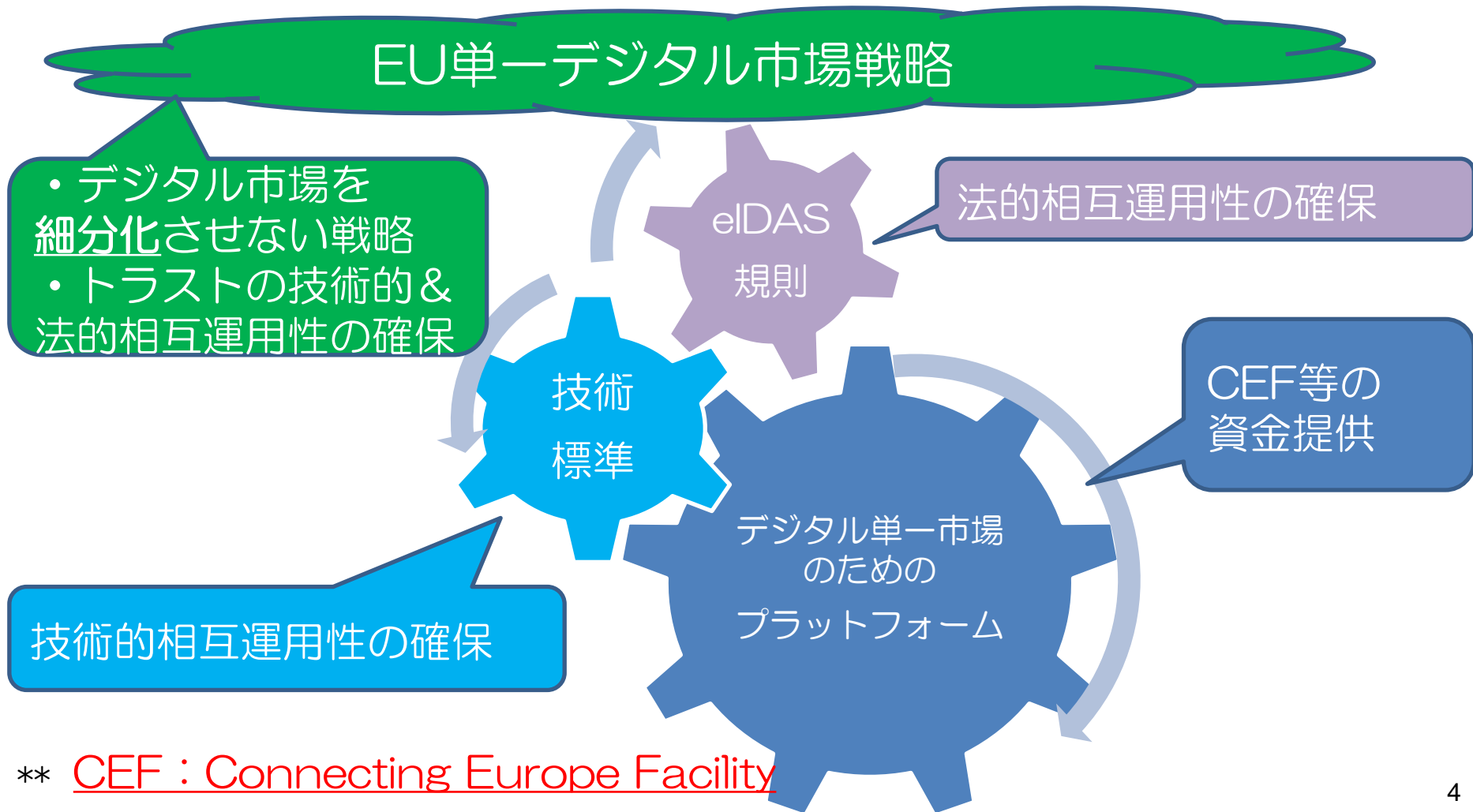
デジタル単一市場戦略の中核となるトラスト

- (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 バックグラウンドの知識として

- 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

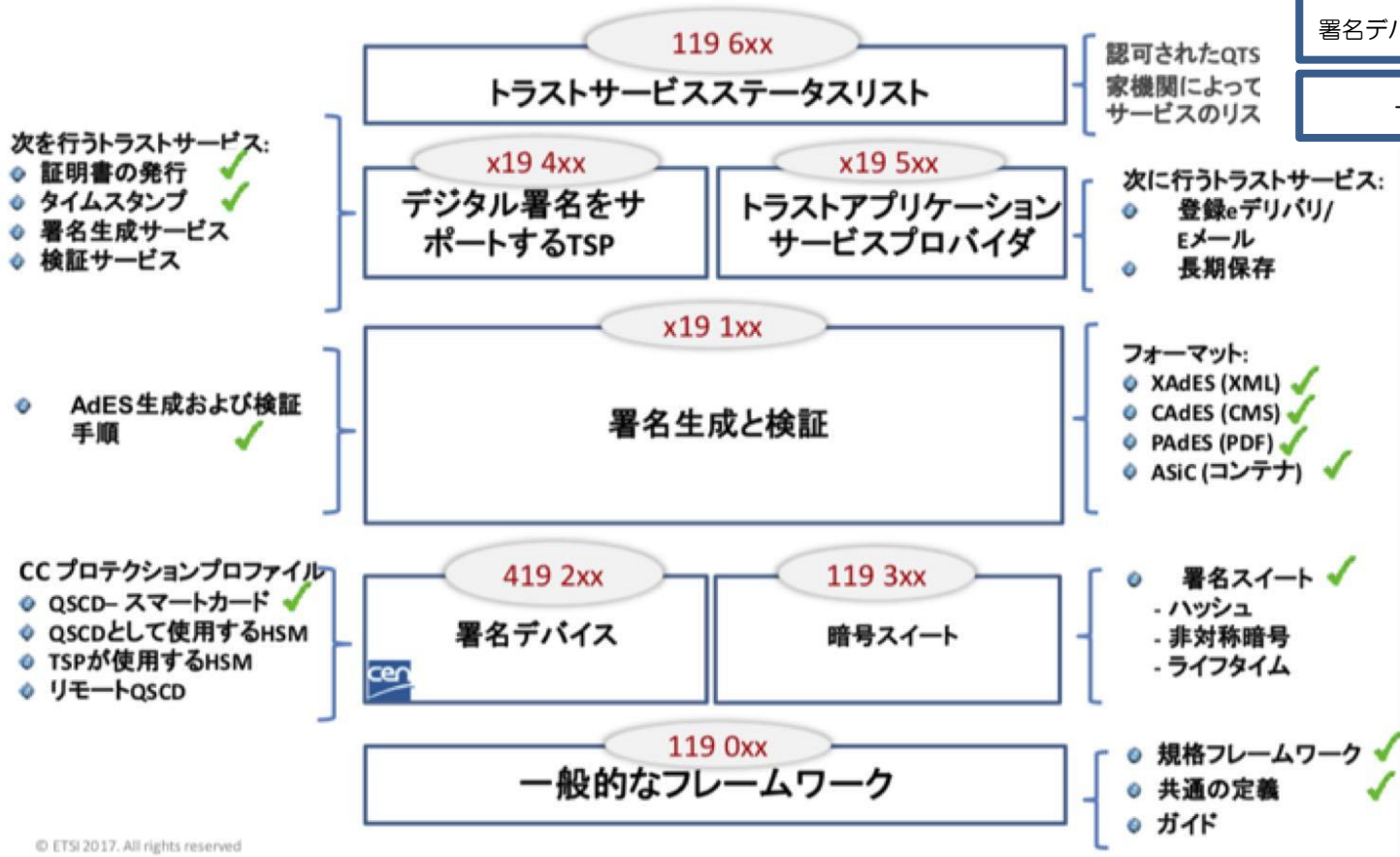
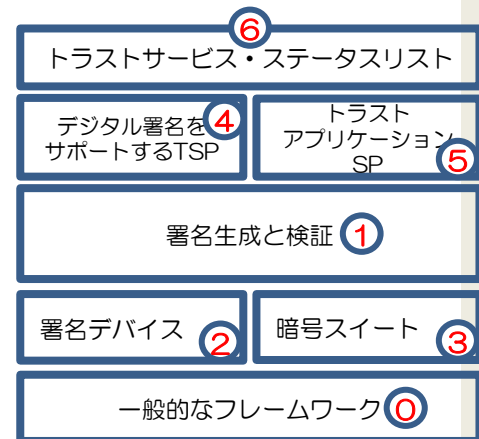
eIDAS前文 -- 技術標準の意味するところ

- 「欧州デジタルアジェンダ」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）



© ETSI 2017. All rights reserved

出典: https://itc.jpdec.or.jp/common/images/kouensiryuu_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



CEF ▾ Building Blocks ▾ Digita

CEF Building Blocks

Digital building blocks to help teams deliver digital public services faster, comply with regulation and make the digital single market a reality.

SUCCESS STORIES

THE BUILDING BLOCKS

The building blocks are basic capabilities that can be reused in any project to facilitate the delivery of digital public services across borders and sectors.

eDelivery

Supporting electronic registered delivery of data and documents.

eID

Extending the use of online services to citizens of other EU Member States.

eInvoicing

Helping public entities adopt the European standard on electronic invoicing.

eSignature

Creating and verifying electronic signatures.

- 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(??)

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)

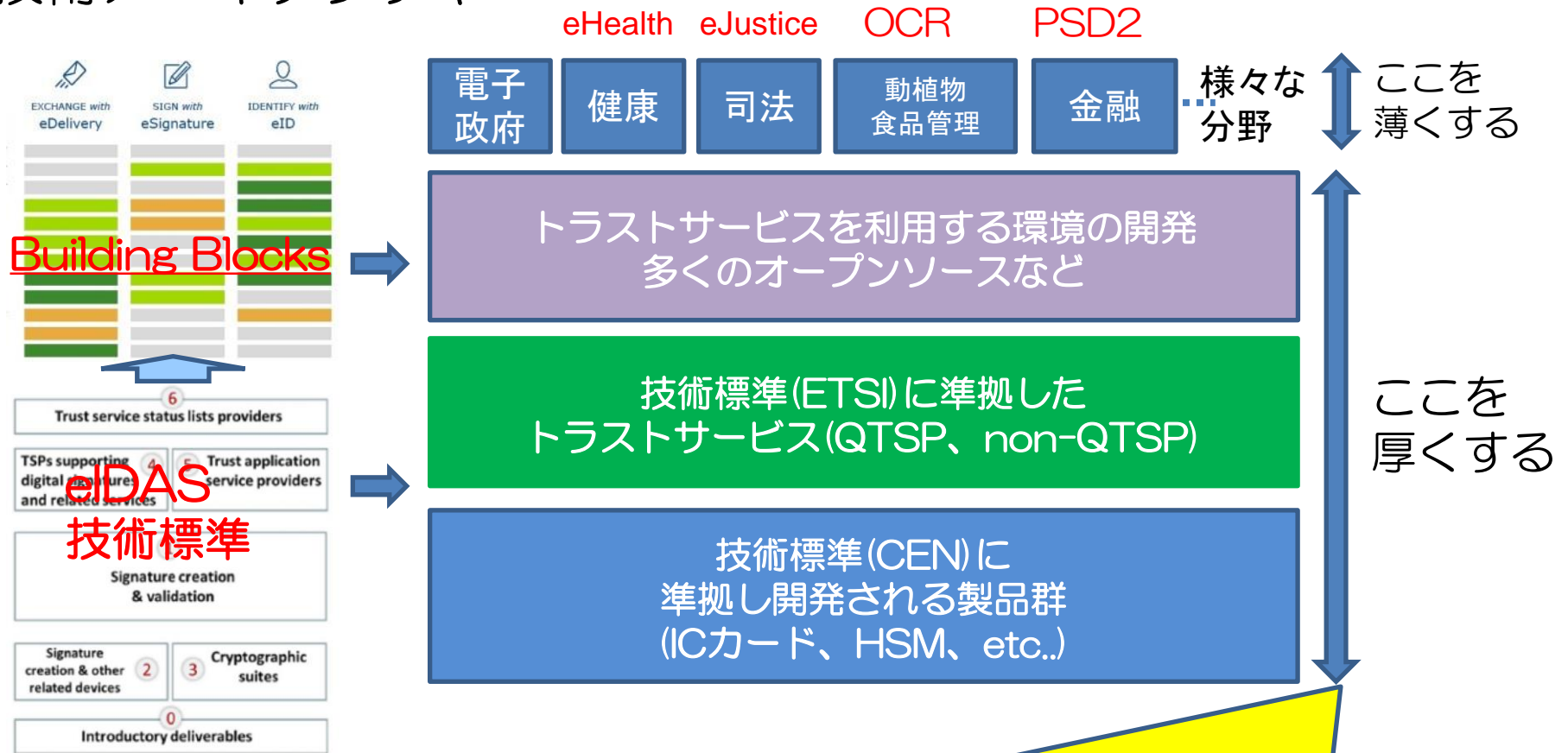
The number of projects reusing the building blocks within the CEF Programme continues to increase



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



- 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

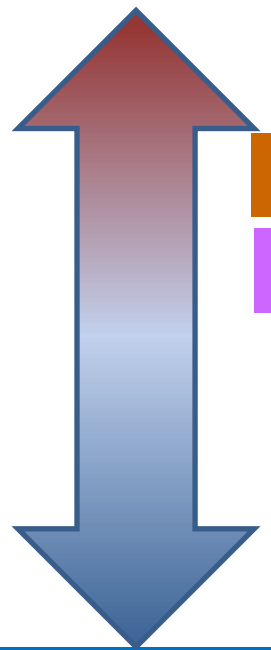
Technical interoperability & Legal interoperability

法的
相互運用性

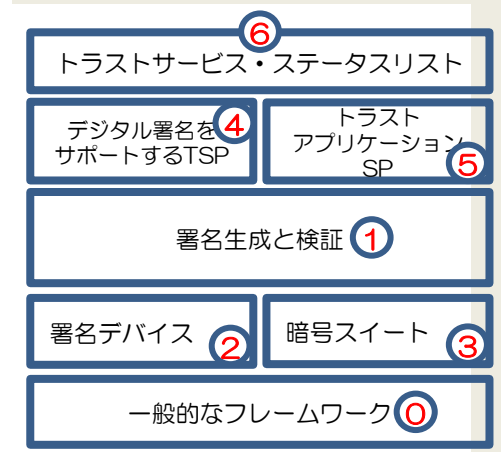
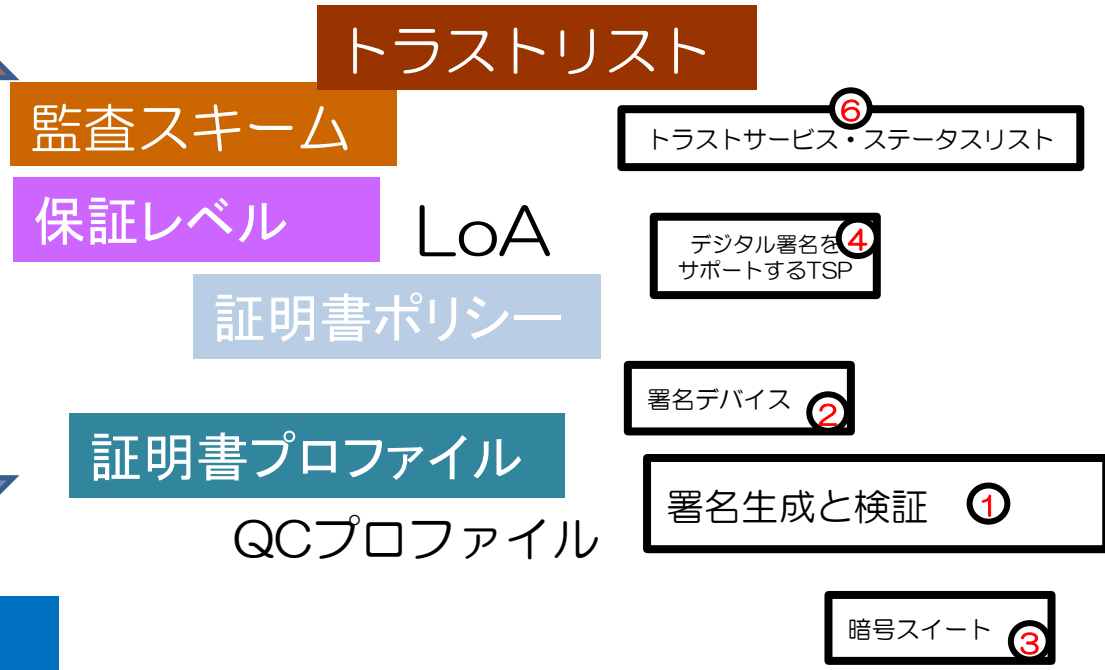
eIDAS規則



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



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 ①



署名デバイス ②

署名生成と検証 ①



トラストアプリケーション SP ⑤

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)

トラストリスト 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

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

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
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**

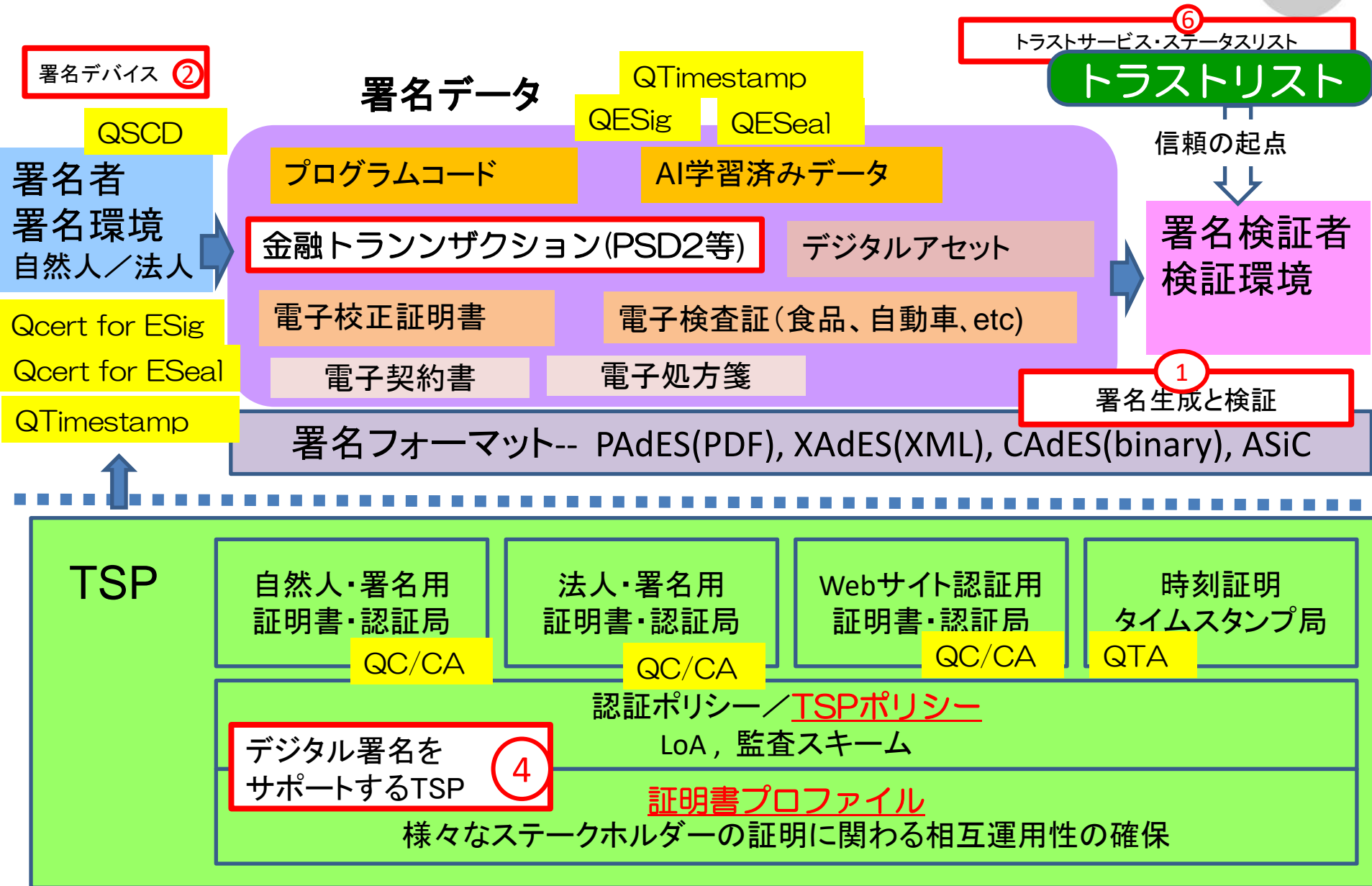
non-QC/CA **non-QTA**

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

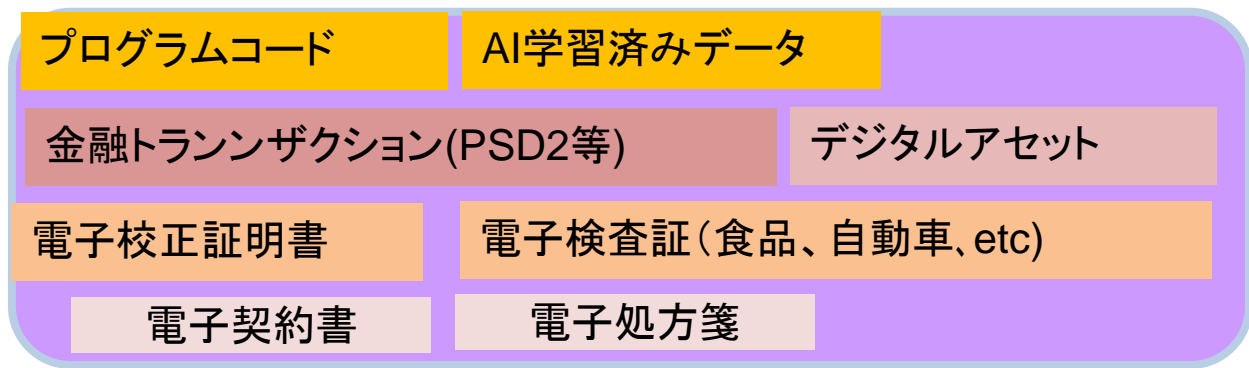
TSP、署名者、署名データ、署名検証者の関係



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

- 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。

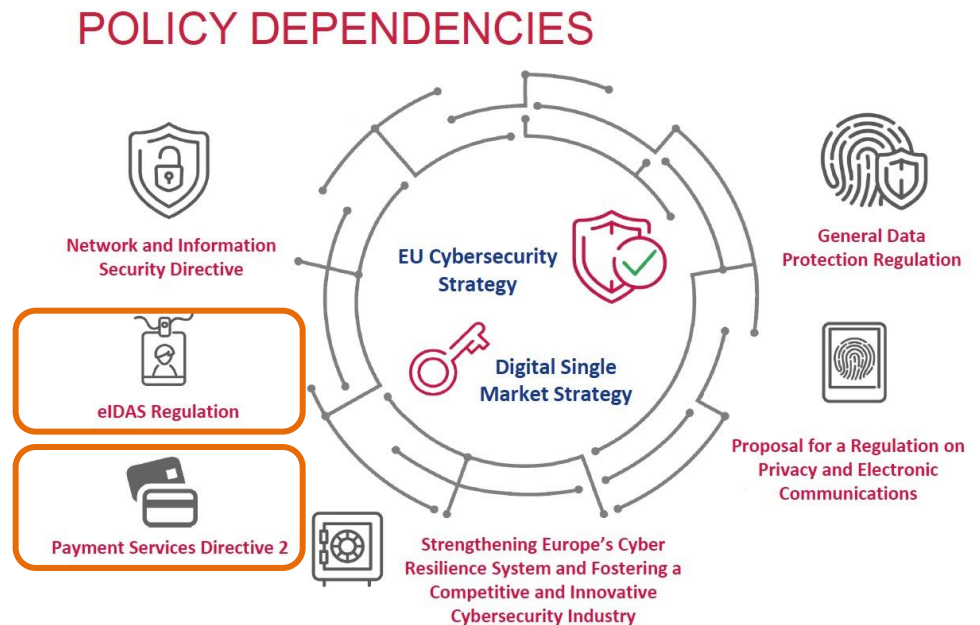
様々な
分野毎の
様々な
署名データ



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

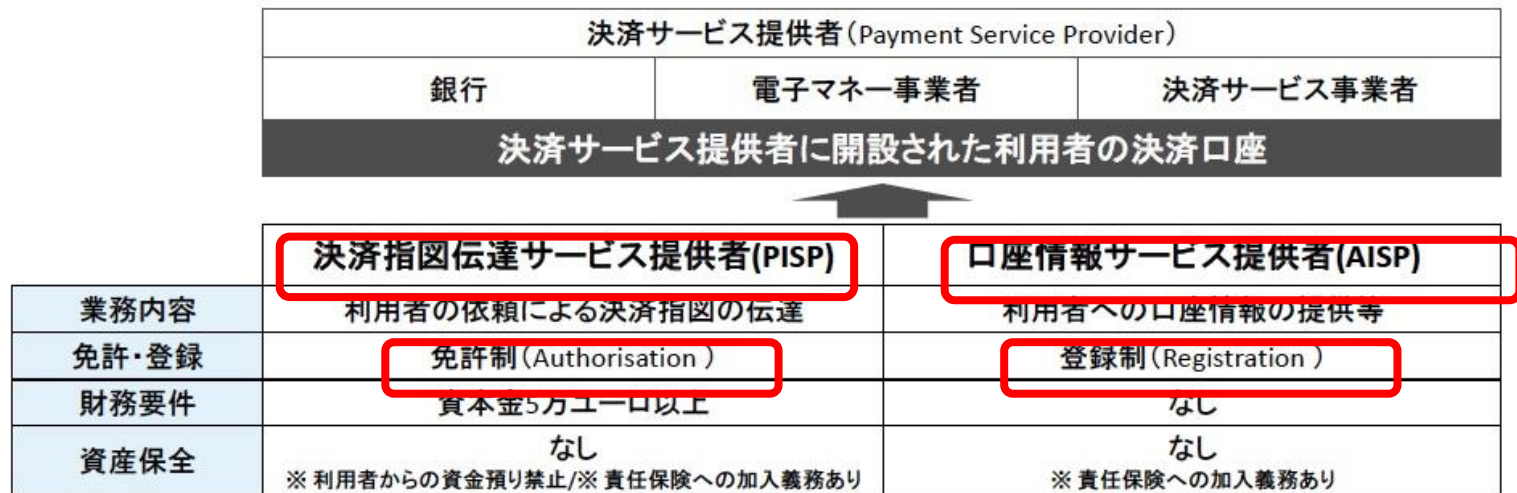
- 欧州銀行監督局 (EBA : European Banking Authority) が主導
- EBAの規制技術基準 (RTS : Regulatory Technical Standards) よりeIDAS規則のQeSeal, QWACの利用を義務付け



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)



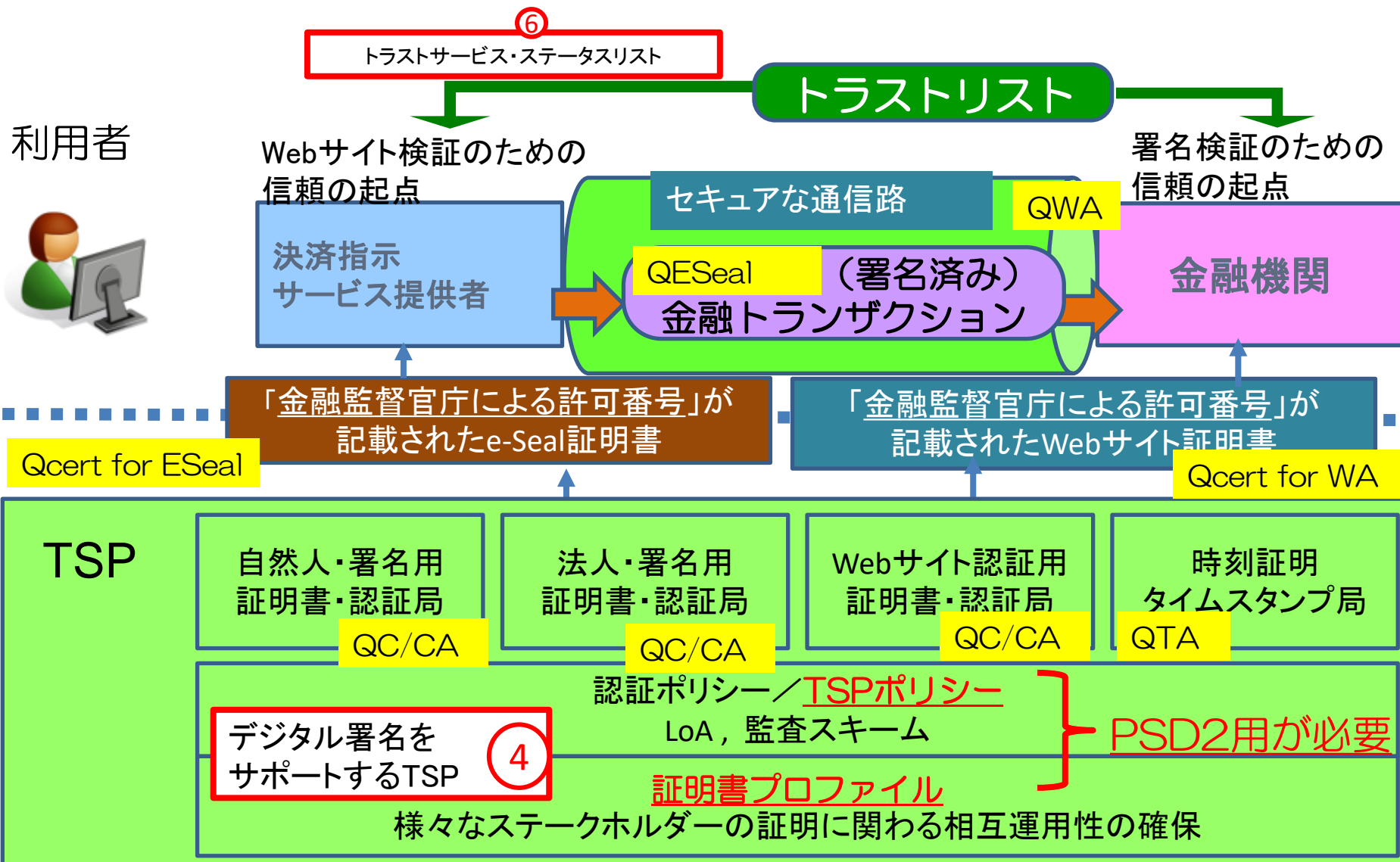
○ また、これに関連して、

- 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



欧州の決済サービス指令（PSD2）の場合

- 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ロバイダー
 - 「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



Internet X.509
Public Key
Infrastructure
Certificate and
CRL Profile

Internet X.509
Public Key
Infrastructure:
Qualified
Certificates
Profile

Certificate Profiles;
Part 1: Overview and common data structures

X.509証明書
v3拡張
フォーマット

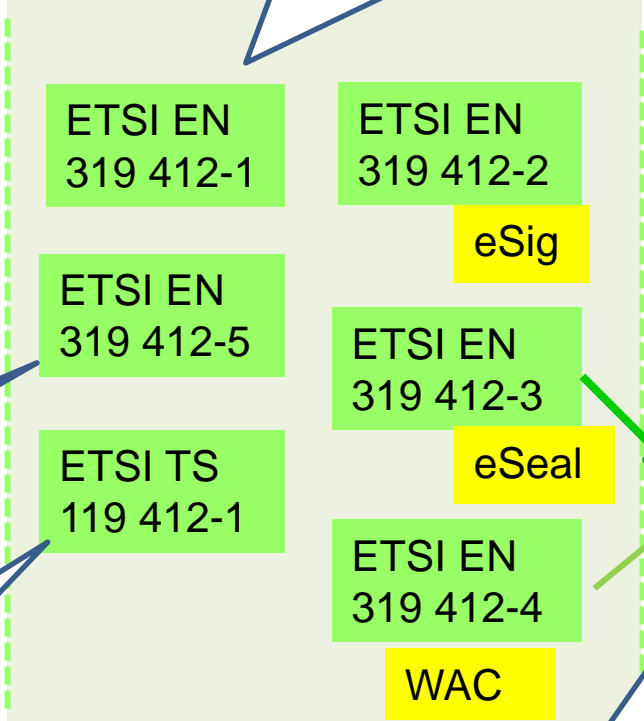
RFC2459
1999年

RFC3280
2002年

RFC5820
2008年

RFC 3039
2001年

RFC 3739
2004年



分野別の
証明書
プロファイル

eSig
eSeal
WAC

ETSI TS
119 495

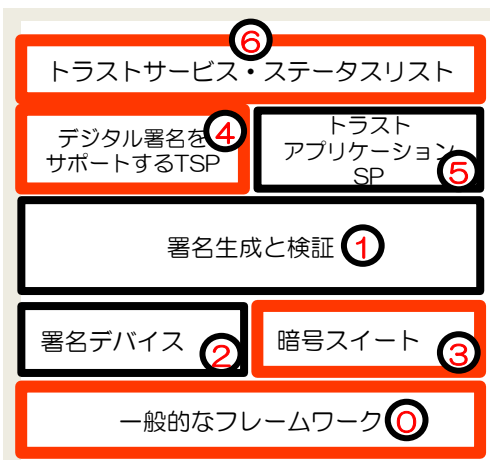
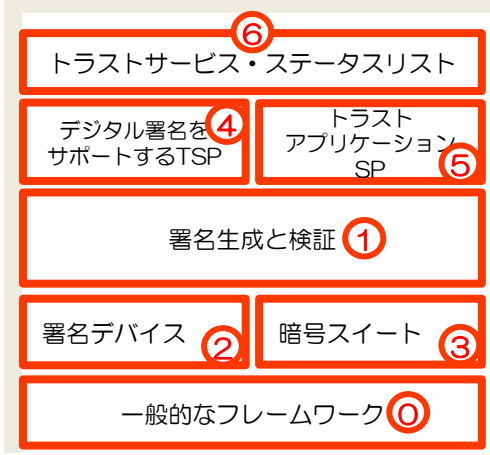
Certificate Profiles;
Part 5: QCStatements

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

- 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



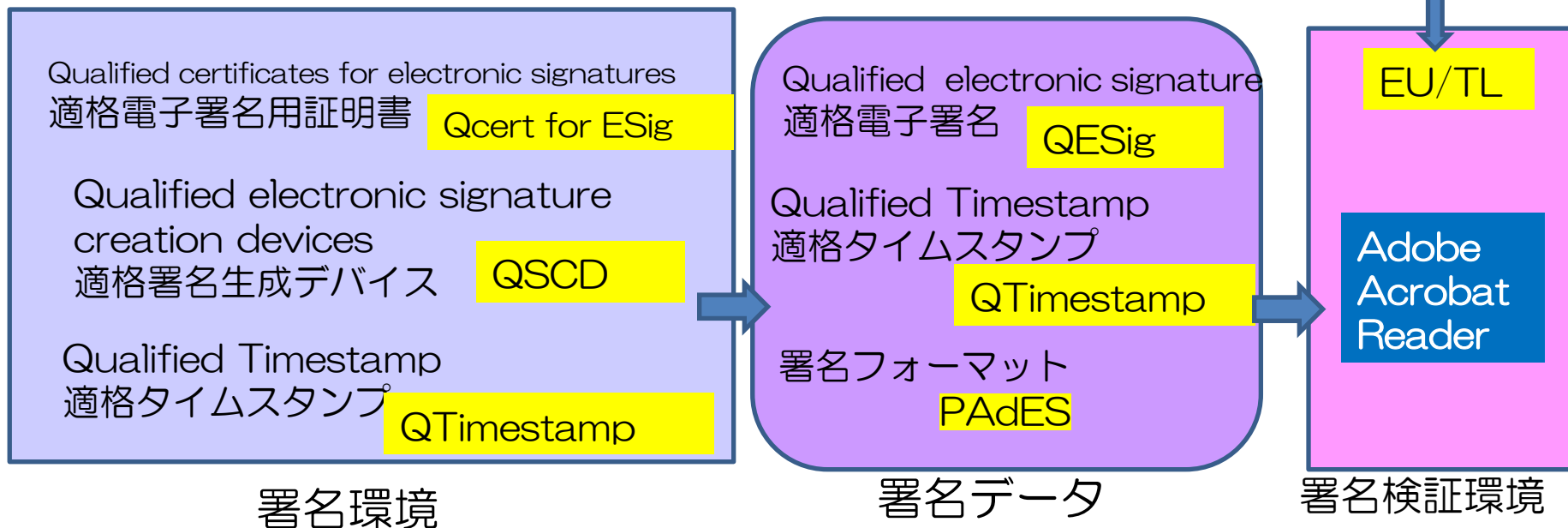
Acrobat Readerに見られる技術標準

- 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

6

トラストサービス・ステータスリスト

トラストリスト



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>

トラストリスト

署名のプロパティ

署名は有効で、Vanczák Gergely <vanczak.gergely@microsec.hu> によって署名されています。

署名時刻：2018/12/13 23:19:46 +09'00'

信頼ソース取得元：European Union Trusted Lists (EUTL)

EU/TL

これは、EU 規則 910/2014 に従って認定された電子署名です

正当性の概要

文書は、この署名が適用された後、変更されていません。

証明者は、この文書についてフォームフィールドの入力、署名、および注釈の作成を許可することを指定しています。その他の変更は許可されていません。

署名者の ID は有効です。

埋め込みタイムスタンプが署名に含まれています。タイムスタンプ時刻：2018/12/13 23:19:53 +09'00'

署名は保証された (タイムスタンプ) 時刻に検証されました：2018/12/13 23:19:53 +09'00'

署名者情報

署名者の証明書から発行者の証明書へのパスは正しく構築されました。

署名者の証明書は有効であり、失効していません。

署名者の証明書を表示...

詳細プロパティ... 閉じる 署名を検証

署名パネル

Á DOKUMENTUMOT ELEKTRONIKUS ALÁÍRASSAL LÁTTA EL: Vanczák Gergely

ion A

DAS

nic S

6 トラストサービス・ステータスリスト

4 デジタル署名をサポートするTSP

5 トラストアプリケーションSP

1 署名生成と検証

2 署名デバイス

3 暗号スイート

0 一般的なフレームワーク

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>

ホーム ツール awareness2019.p... x

1 / 37 63.4%

共有

Cabinet Secretariat, Japanese Government によって証明されており、証明書がアプリケーションCA2 Sub によって発行されています。 **署名パネル**

署名のプロパティ

文書の証明は有効で、Cabinet Secretariat によって署名されています。

署名時刻: 2019/01/23 10:26:32 +09'00'

信頼ソース取得元: Adobe Approved Trust List (AATL)

正当性の概要

文書は証明後に変更されていません。

証明者は、この文書についてフォームフィールドの入力と署名しています。その他の変更は許可されていません。

署名者のIDは有効です。

署名時刻は署名者のコンピューターの時計に基づいています。

署名は署名時刻に検証されました:
2019/01/23 10:26:32 +09'00'

署名者情報

署名者の証明書から発行者の証明書へのパスは正しく構築されています。

署名者の証明書は有効であり、失効していません。

[署名者の証明書を表示...](#)

証明書ビューア

このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。選択したエントリに対応しています。

見つかったすべての証明パスを表示

アプリケーションCA2 Root
アプリケーションCA2
Cabinet Secretariat

概要 詳細 失効 信頼 ポリシー 法律上

Cabinet Secretariat
Japanese Government

発行者: アプリケーションCA2 Sub
日本国政府 (Japanese Government)

有効期間の開始: 2017/04/17 00:00:00 +09'00'

有効期間の終了: 2020/04/16 23:59:59 +09'00'

鍵の使用法: 電子署名、否認防止

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

証明書ビューア

このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示される詳細は、選択したエントリに対応しています。

見つかったすべての証明パスを表示

Qualified e-Szigno CA
Vanczák Gergely <v>

概要 詳細 失効 信頼 ポリシー 法律上の注意事項

Vanczák Gergely
Microsec zrt.
発行者: Qualified e-Szigno CA 2009 <info@e-Microsec Ltd.
有効期間の開始: 2017/08/10 21:37:15 +09'00'
有効期間の終了: 2019/08/10 21:37:15 +09'00'
鍵の使用法: 否認防止

この証明書は、EU 規則 910/2014 Annex I に従って認定されています

この証明書に関連する秘密鍵は、QSCD (Qualified Signature Creation Device) にあります

書き出し...

選択した証明書パスは有効です。

パスの検証および失効確認は、保証された (タイムスタンプ) 時刻に行われました:
2018/12/13 23:19:53 +09'00'
検証モデル: シェル

OK

署名パネル

A DOKUMENTUMOT ELEKTRONIKUS ALÁÍRÁSSAL LÁTTA EL:

Vanczák Gergely

附属書 | 電子署名のための適格証明書の要件

「適格電子署名生成デバイス」内のプライベート鍵で署名を生成

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

トラストアプリケーション SP

署名生成と検証

署名デバイス

署名スイート

一般的なフレームワーク

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

証明書ビューア

このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示される詳細は、選択したエントリに対応しています。

見つかったすべての証明バスを表示

Qualified e-Szigno CA
Vanczák Gergely <v>

概要 詳細 失効 信頼 ポリシー 法律上の注意事項

証明書データ:

名前	値
有効期間の…	2017/08/10 21:37:15 +09'00'
有効期間の…	2019/08/10 21:37:15 +09'00'
QC ステータス	<詳細を参照>
機関情報ア…	<詳細を参照>
CRL 配布点	<詳細を参照>

ETSI EN 319 412-5 に基づく認定済み証明書
トランザクション制限値: 1000000.00 HUF(容量: 1, 指数: 6, 通貨: HUF)
保存期間: 10 年
QSCD 内にある秘密鍵
PKI 開示文書: https://cp.e-szigno.hu/qcps_en, <https://cp.e-szigno.hu/qcps>
電子署名の認定済み証明書

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

87%

署名パネル

A DOKUMENTUMOT
ELEKTRONIKUS ALÁÍRASSAL LÁTTA EL:

Vanczák Gergely

6
トラストサービス・ステータスリスト

4
デジタル署名を
サポートするTSP

5
トラスト
アプリケーション
SP

1
署名生成と検証

2
署名デバイス

3
暗号スイート

0
一般的なフレームワーク

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

EN 319 142-1 で定義されている署名レベル
Long-Term with Archive Time-Stamps (LTA)
長期保存に最も適した形式

署名の詳細

署名は 不明 を使用して作成されています。

ハッシュアルゴリズム : SHA256

署名アルゴリズム : RSA PKCS#1 v1.5

PAdES 署名レベル : B-LTA

タイムスタンプの詳細

署名に埋め込まれたタイムスタンプ

タイムスタンプは、文書に署名されるのと同時に書き込まれます。タイムスタンプ署名が有効であるためには、タイムスタンプを署名したタイムスタンプ局を信頼する必要があります。タイムスタンプ署名の検証に関する詳細を表示するには、「証明書を表示」をクリックします。

タイムスタンプ局

タイムスタンプはタイムスタンプ局で定義されている特定のポリシーを使用して作成されます。特に、ポリシーによってタイムソースの信頼性を指定できます。このタイムスタンプのポリシーは、識別子 1.3.6.1.4.1.21528.2.1.1.186.2.7 によって表されます。タイムスタンプポリシーを理解するには、タイムスタンプ局に問い合わせる必要があります。

ハッシュアルゴリズム : SHA256

署名パネル

A DOKUMENTUMOT
ELEKTRONIKUS ALÁÍRASSAL LÁTTA EL:

Vanczák Gergely

6 信頼サービス・ステータスリスト

4 デジタル署名をサポートするTSP

5 信頼アプリケーションSP

1 署名生成と検証

2 署名デバイス

3 暗号スイート

0 一般的なフレームワーク

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

QTA

QTimestamp

証明書ビューア

このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示される詳細は、選択したエントリに対応しています。

見つかったすべての証明パスを表示

Qualified eIDAS e-Szigno

概要 詳細 失効 信頼 ポリシー 法律上の注意事項

証明書データ:

名前	値
サブジェクト	cn=Qualified eIDAS e-Szigno...
発行者	email=info@e-szigno.hu, c...
シリアル番号	00 B4 F5 45 57 FC FE AA...
有効期間の開始	2018/05/31 19:00:00 +09'...
有効期間の終了	2029/12/15 19:00:00 +09'...
QC ステータス	<詳細を参照>

ETSI EN 319 412-5 に基づく認定済み証明書
トランザクション制限値: 100000.00 HUF(容量: 1, 指数: 5, 通貨: HUF)
保存期間: 10 年

cp.e-szigno.hu/qcps
電子印鑑の認定済み証明書

証明書ビューア

このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示される詳細は、選択したエントリに対応しています。

見つかったすべての証明パスを表示

Qualified eIDAS e-Szigno

概要 詳細 失効 信頼 ポリシー 法律上の注意事項

Qualified eIDAS e-Szigno TSA 2017 02
Microsec Ltd.

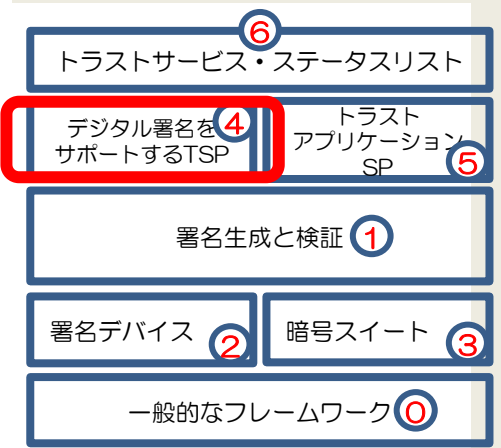
発行者: Microsec e-Szigno Root CA 2009
Microsec Ltd.

有効期間の開始: 2018/05/31 19:00:00 +09'00'
有効期間の終了: 2029/12/15 19:00:00 +09'00'
鍵の使用法: 電子署名、否認防止、タイムスタンプ

この証明書は、EU 規則 910/2014 Annex III に従って認定されています

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>

Trusted List Browser

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

Menu ▾

CEF資金提供で開発、
運用されている
Trusted Listブラウザ

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

署名は有効で、Vanczák Gergely <vanczak.gergely@microsec.hu> によって署名されています。
署名時刻 : 2018/12/13 23:19:46 +09'00'
信頼ソース取得元 : European Union Trusted Lists (EUTL)
 これは、EU 規則 910/2014 に従って認定された電子署名です

QTimestamp

QESig

⑥ トラストサービス・ステータスリスト

④ デジタル署名を
サポートするTSP

⑤ トラスト
アプリケーション
SP

① 署名生成と検証

② 署名デバイス

③ 暗号スイート

⑦ 一般的なフレームワーク

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

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

QC/CA

e-Szignó Qualified Signature

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.



Certificate ID: 97120.18

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

20
Certificate valid until
2020-10-31

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 2 pages.

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

conformity assessment body
適合性評価機関



Certificate ID: 9719.16

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

18
Certificate valid until
2018-10-31

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

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

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ジメントシステム (IMSOC-TRACES)とe-Certificate

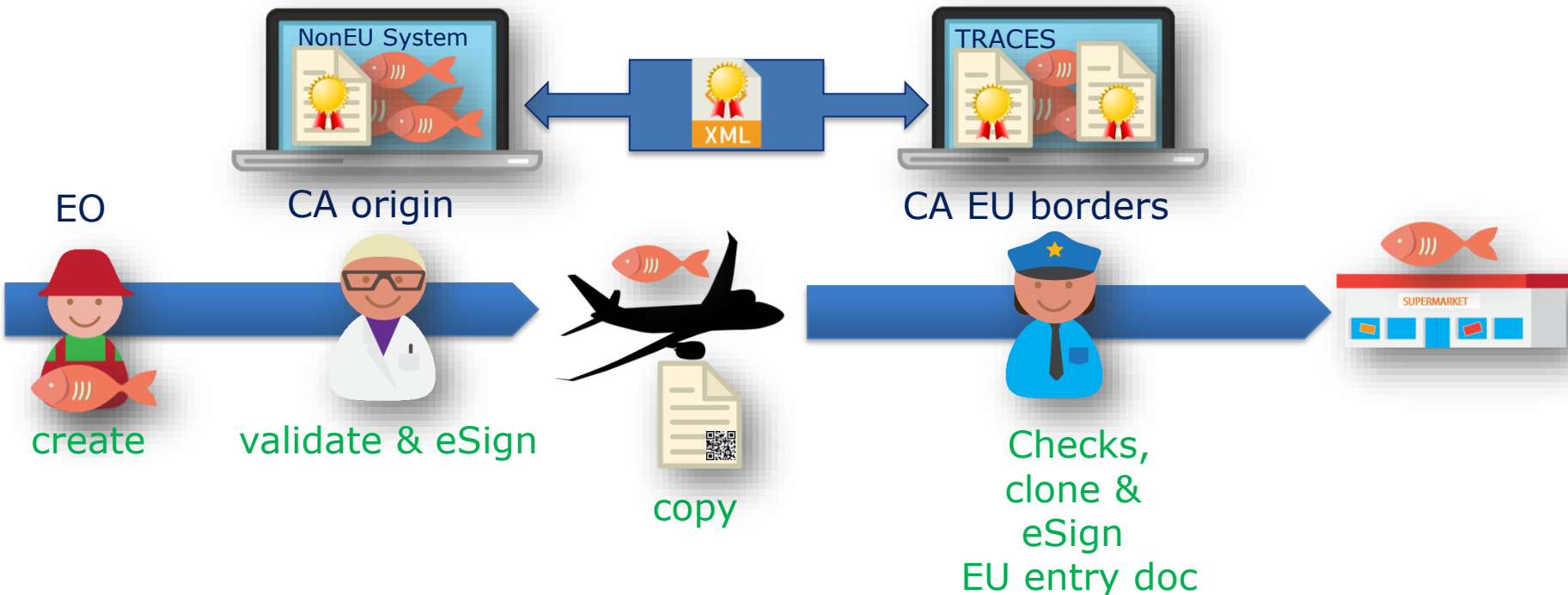
- 1993年 EU加盟国間の「人、モノ、サービス、資本」の移動が自由化
- 1996年 牛海綿状脳症 (BSE)問題発生
- 2005年 トレーサビリティ義務化、TRACES運用開始
 - 衛生証明書/獣医師証明書、植物検疫証明書等を扱う
- 2019年
 - 新公的管理規則(OCR)の実施と、公的管理のための統合マネジメントシステム(IMSOC)の稼働
 - eIDAS規則を適用した「デジタルがオリジナル文書(原本)」

欧州委員会 DG SANTE (保健衛生・食の安全総局) が主導

- 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。

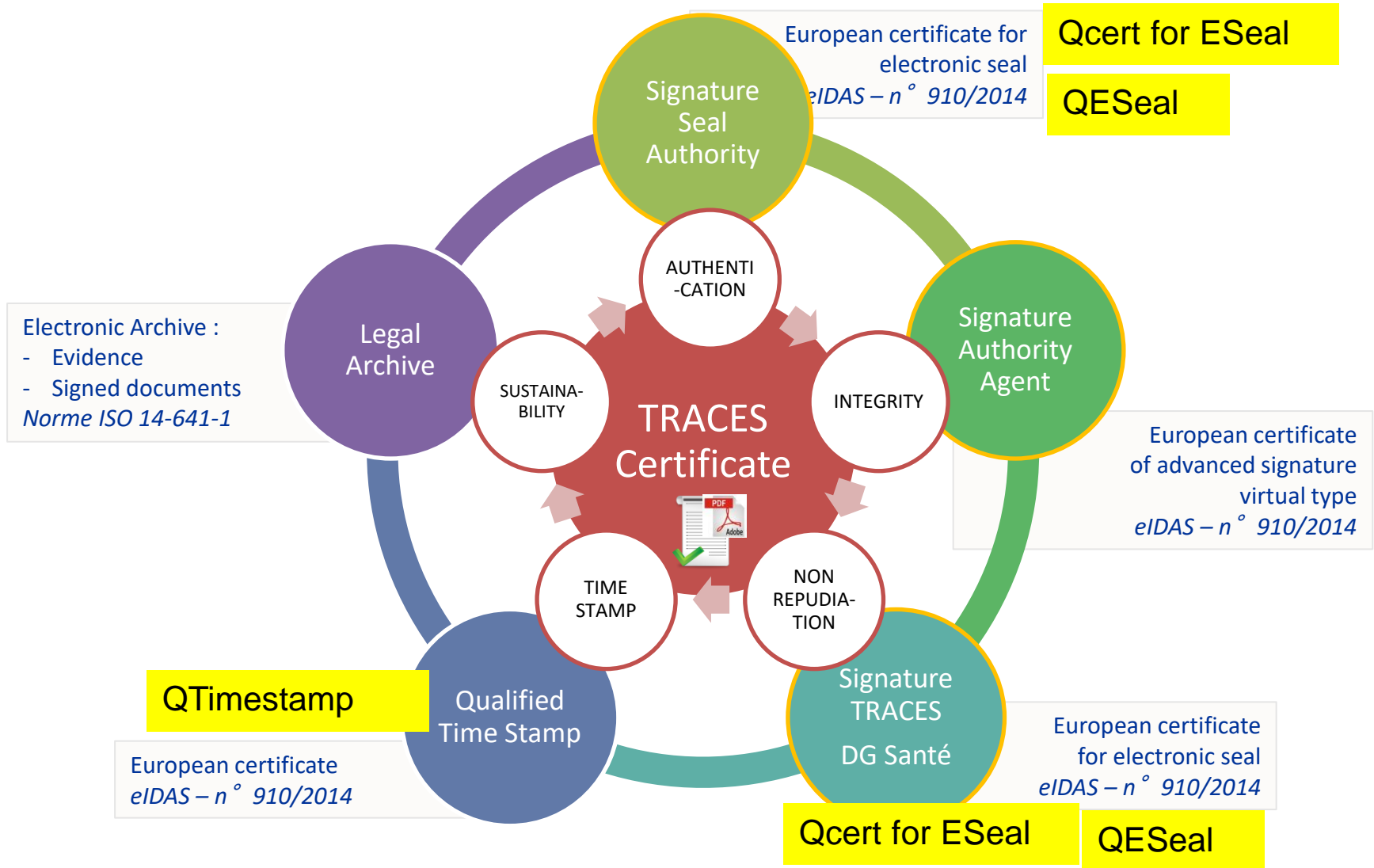
公的管理のための統合マネージメントシステム (IMSOC-TRACES)

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

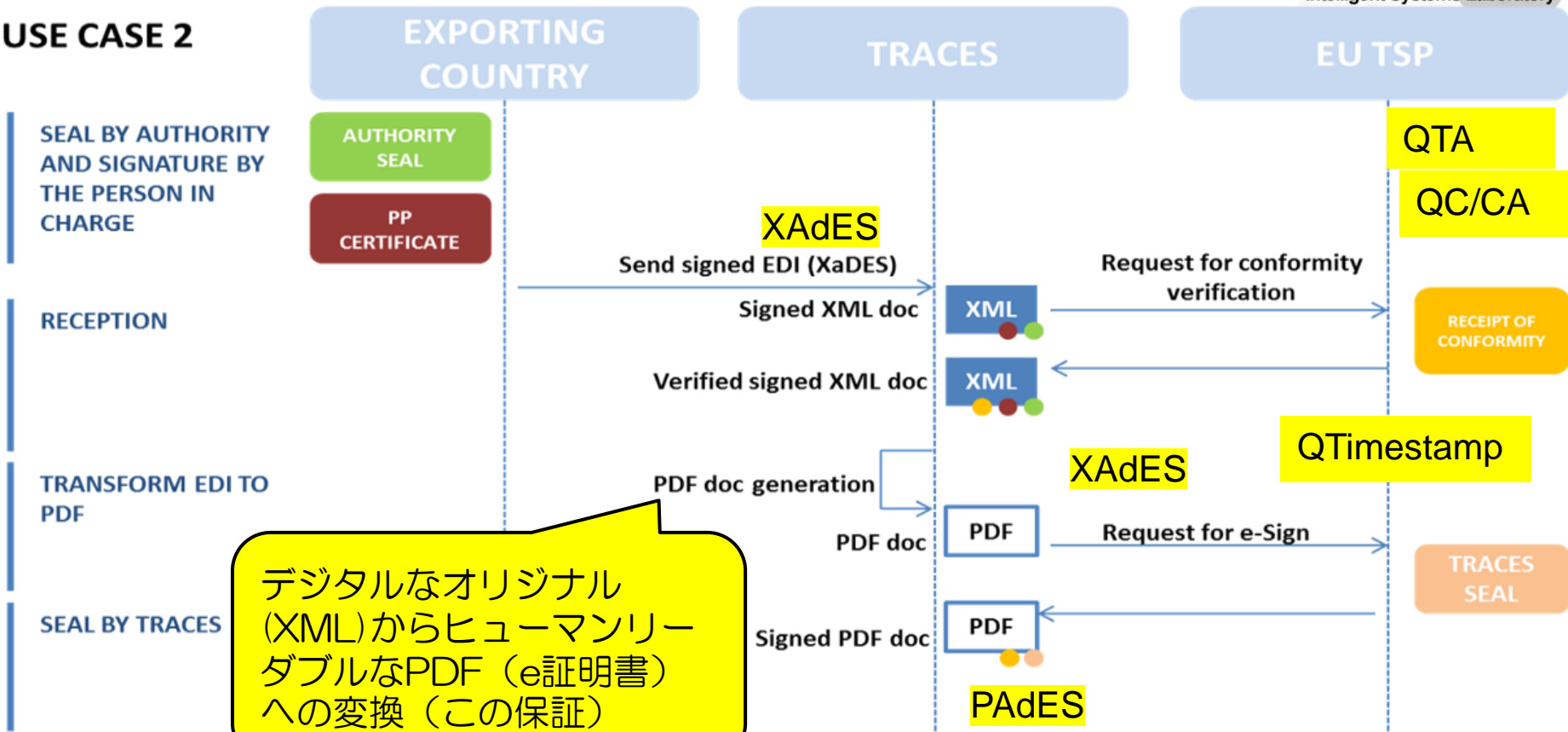
- 非EU国別システムとEU IMSOC間のデータ交換を確立
 - UN/CEFACT eCERT based XML exchanges + Validation rules
- データ交換において、適格電子署名（電子シール）と適格タイムスタンプを付す
 - 非EUシステムは、適格タイムスタンプを使用してXMLトランザクションに署名：
 - 自身（自国）のトラストサービスプロバイダーによるもの
 - IMSOCトラストサービスプロバイダーによるもの
 - 署名済みXMLが、オリジナル文書（原本）
 - ヒューマンリーダブルなe証明書（たぶん、PDF/PAdES）を再生成保証（コピーはオリジナ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

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%20WG%20Feb%202018%20e-certification%20EU%20approach%20and%20policy%20Final%20Export.pptx>

USE CASE 2



デジタルなオリジナル (XML) からヒューマンリーダブルなPDF (e証明書) への変換 (この保証)

QESeal

AUTHORITY SEAL

TRACES SEAL

PP CERTIFICATE

RECEIPT OF CONFORMITY

輸出国側の行政官のeSeal

EU TRACESのeSeal

EU TRACESの受け取り証

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

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

- 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、様々なモノが流通する第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。

PKI day 2016 マイナンバー時代のPKI

欧州

米国

規制モデル

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??

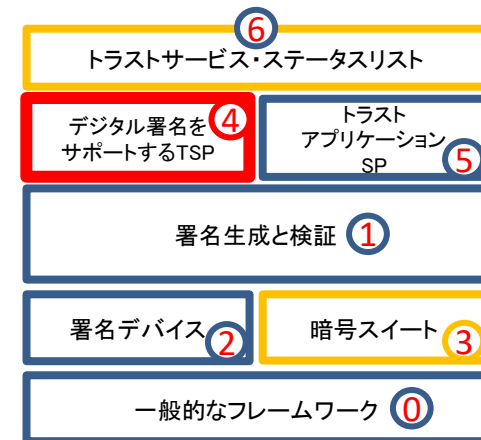
付録

- 適格Webサイト認証の事例
- eIDAS技術標準の体系

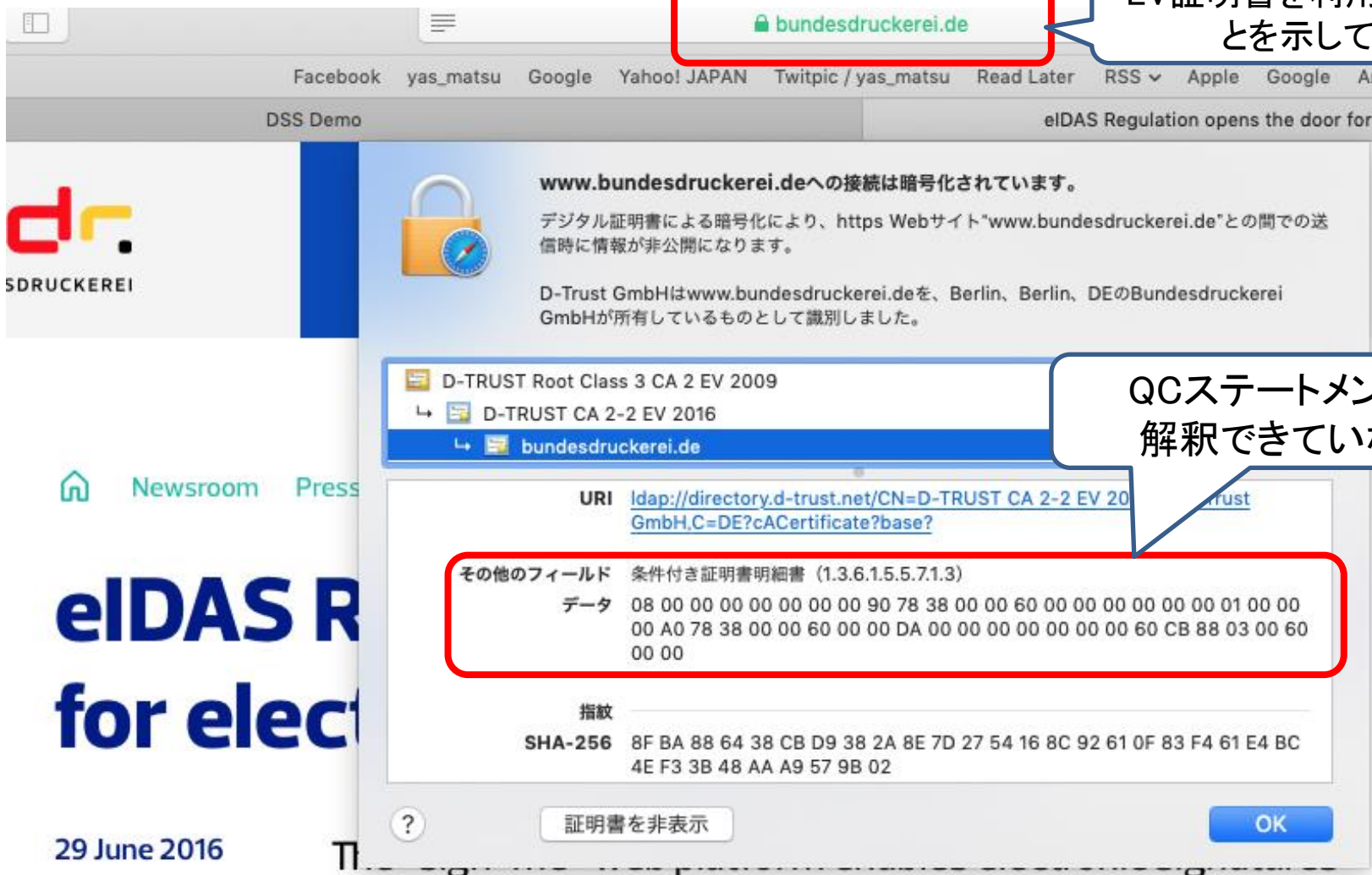
適格Webサイト認証

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

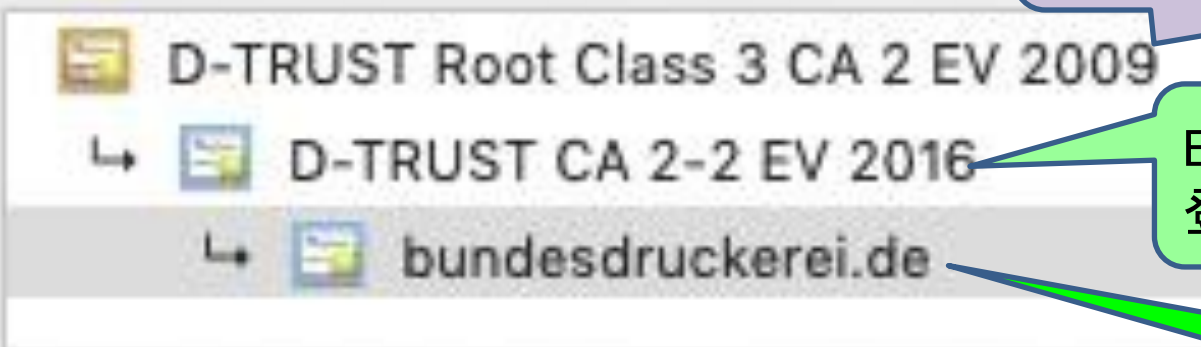


参考URL:

<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

Webブラウザのトラストリストに登録されている



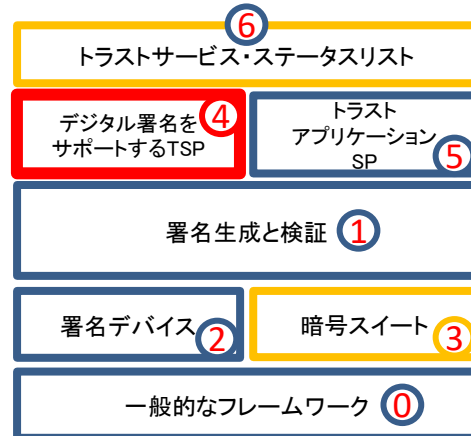
EUTラストリストに登録されている **QC/CA**

適格Webサイト証明書
かつ
EV証明書 **QWAC**



bundesdruckerei.de
発行元: D-TRUST CA 2-2 EV
有効期限: 2020年4月27日 月曜
✔ この証明書は有効です

- ▶ 信頼
- ▶ 詳細な情報



参考URL:

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

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

fulfills all relevant requirements defined in

QC/CA

QWAC

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 valid until
 2019-01-30

Certificate

D-TRUST qualified Timestamp

fulfills all relevant requirements defined in

QTA

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

QTimestamp

D-TRUST qualified Signature ID card & D-TRUST qualified Signature HPC

fulfills all relevant requirements defined in regulation

QC/CA

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

QESig

D-TRUST sign-me qualified

fulfills all relevant requirements defined in

リモート署名

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

QC/CA

QESig

D-TRUST qualified Seal ID card

fulfills all relevant requirements defined in

QC/CA

Regulation (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic seals.

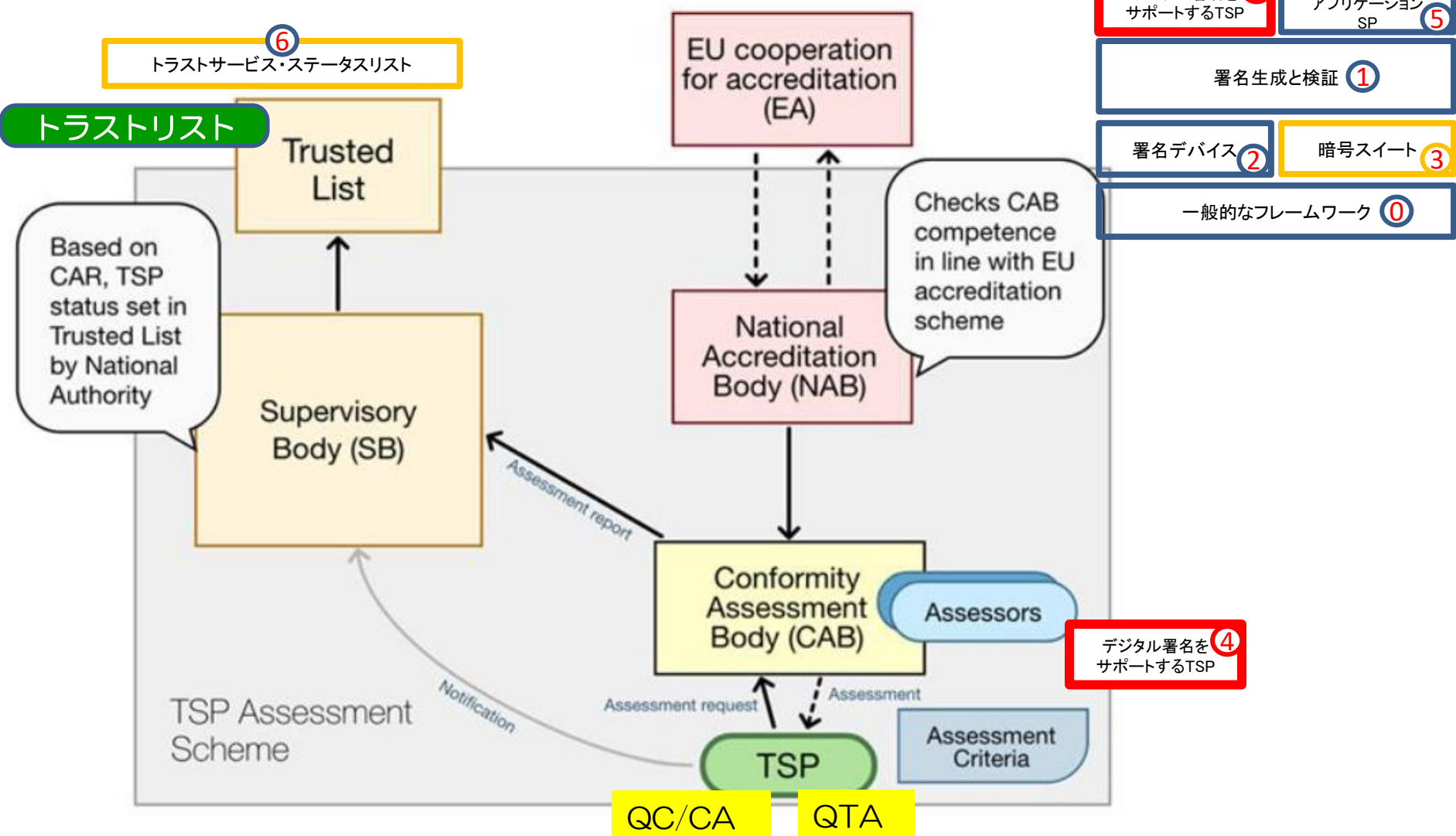
QESeal

適合性評価機関

conformity assessment body

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

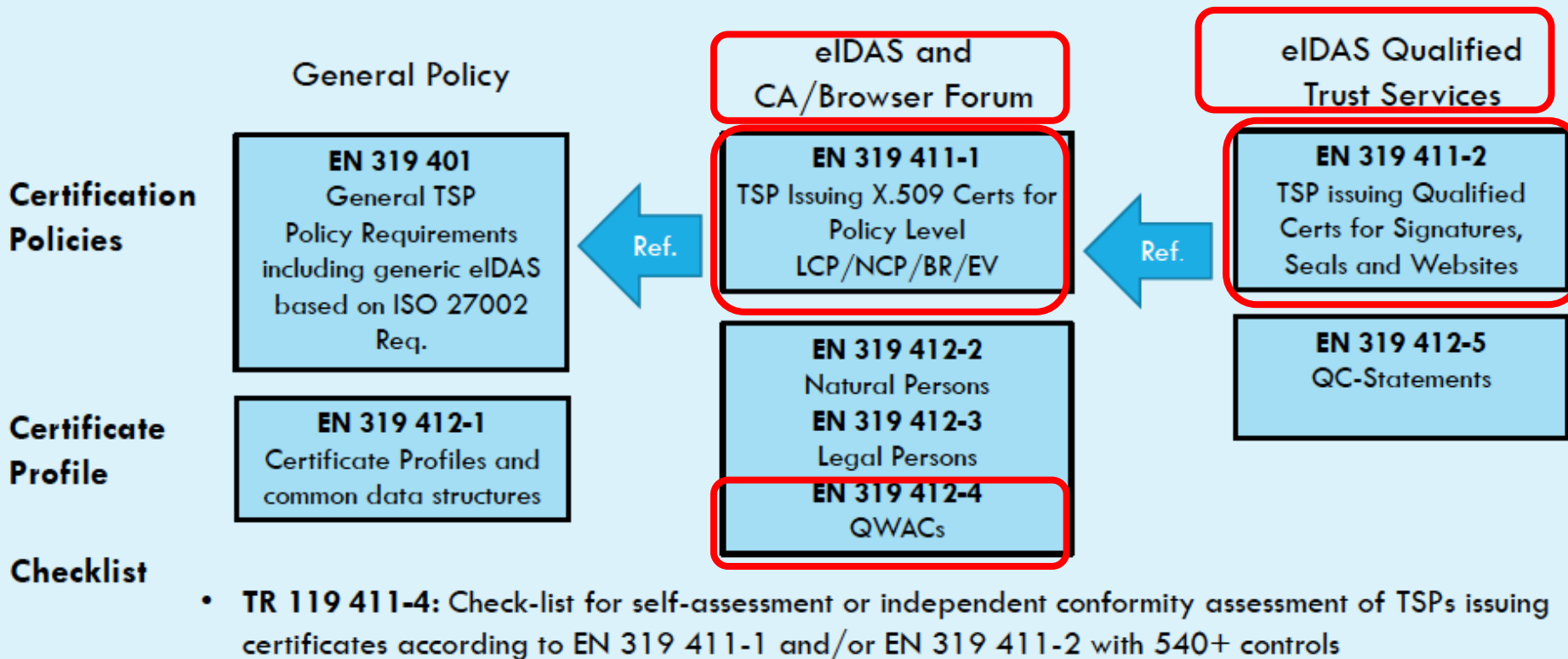


出典: https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/3a%20Fiedler.pdf

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)

EN 319 403 TSP Conformity Assessment (based on ISO 17065)
in context of European Accreditation for Audit Bodies

Conformity Assessment



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

デジタル署名を
サポートするTSP 4

CA/Browser Forum

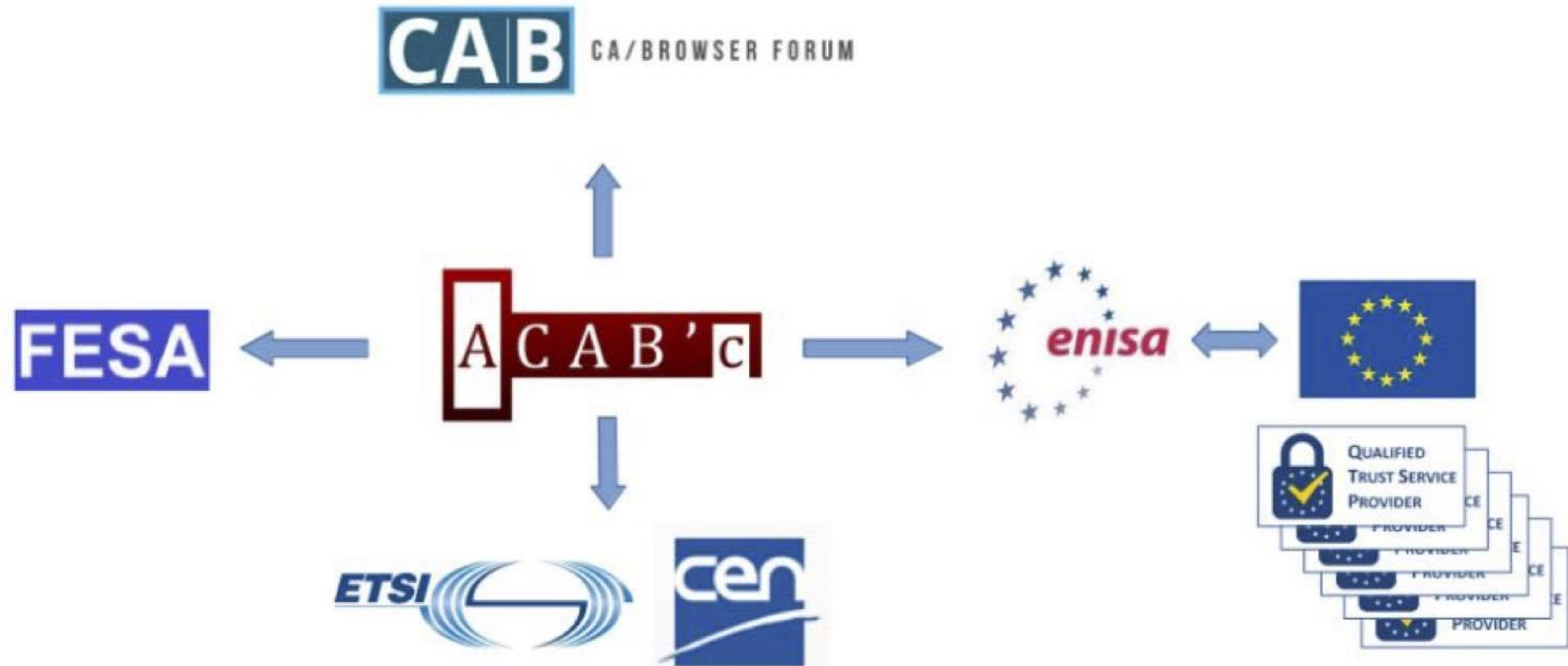
Guidelines For The Issuance And Management Of Extended Validation Certificates

- **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-I
 - 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

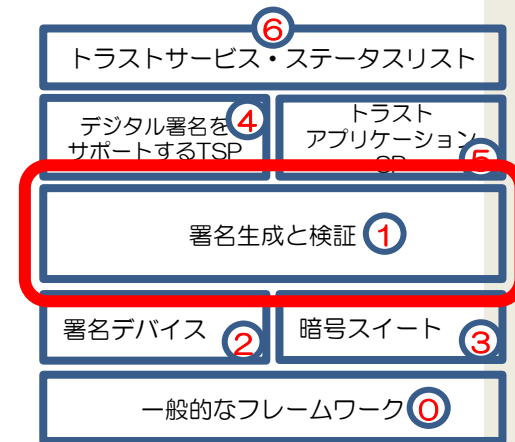
<https://www.acab-c.com>

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）



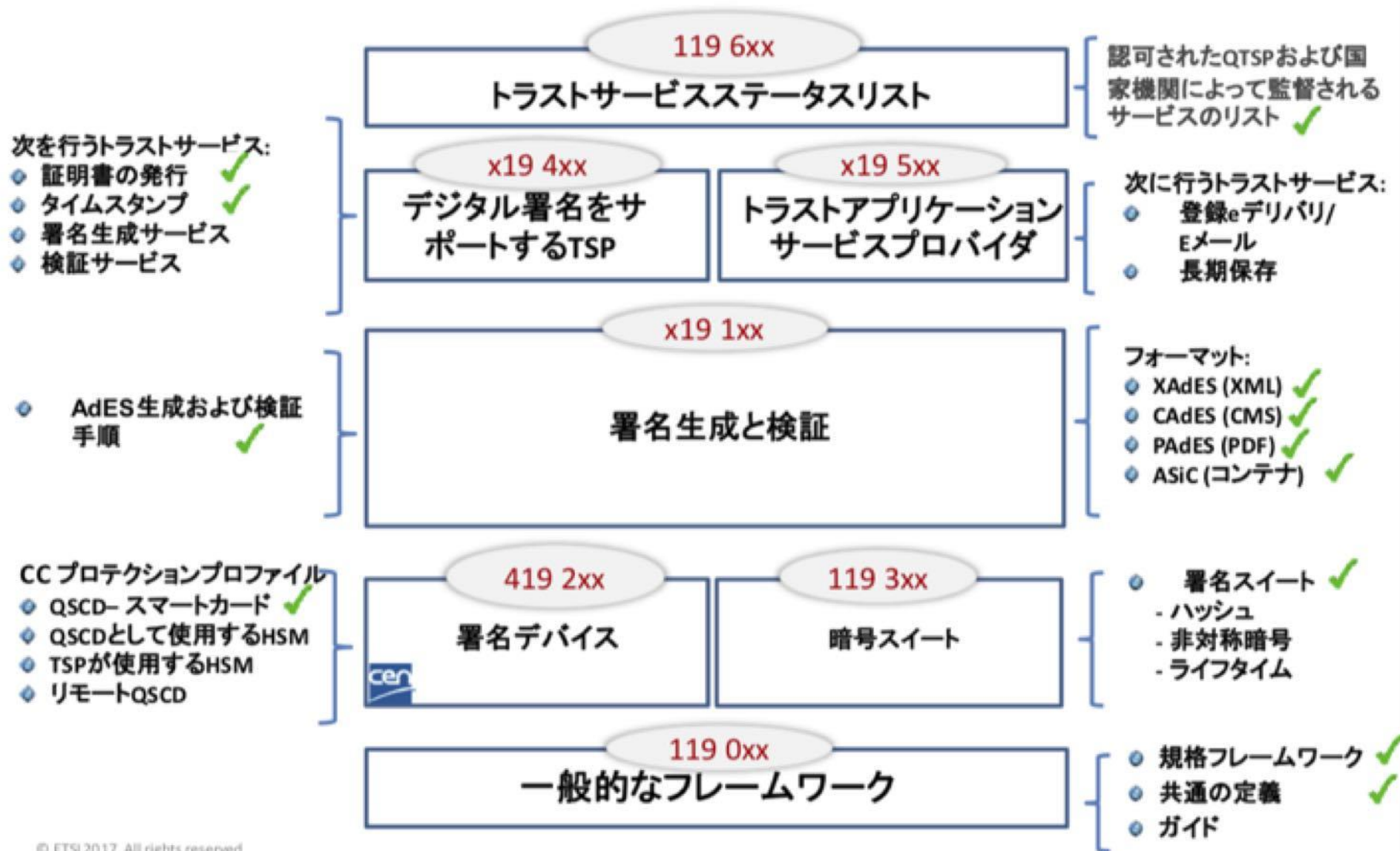
ETSI TR 119 000 V1.2.1 (2016-04)



Electronic Signatures and Infrastructures (ESI);
The framework for standardization of signatures: overview

出典:

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



© ETSI 2017. All rights reserved

出典: https://itc.jipdec.or.jp/common/images/kouensiryoku_4.pdf

© 2019 SECOM CO.,LTD.

署名生成と検証

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	CWA/prEN 14170	All parts published
Technical Specifications								
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures	TS 102 853,	Part 1: Apr. 2016 Part 2: undefined
EN	3	19	1	2	2	CAdES digital signature		parts 1 & 2: pr. 2016
EN	3	19	1	3	2	XAdES digital signature		parts 1 & 2: pr. 2016
EN	3	19	1	4	2	PADES digital signature		parts 1 & 2: pr. 2016
TS	1	19	1	5	2	Architecture for AdES		part 3: delayed undefined
EN	3	19	1	6	2	Associated Signatures		parts 1 & 2: Apr. 2016
TS	1	19	1	7	2	Signature policies	- 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 & procedure)	(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 environment		
TS	1	19	1	6	4	ASiC Testing conformance & interoperability	(new)	June 2016

Guidance

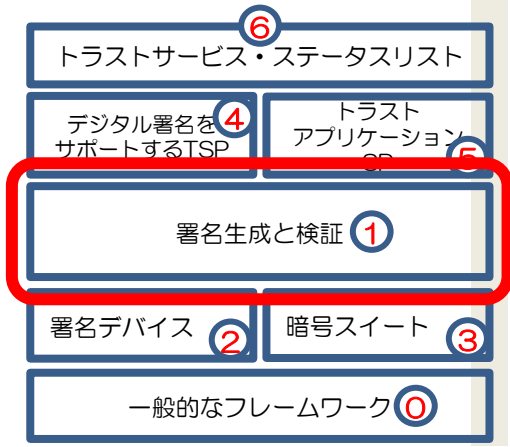
Policy & Security Requirements

CAdES 汎用
XAdES XML
PADES PDF
ASiC コンテナ

Technical Specification

Conformity Assessment

Testing Conformance & Interoperability



署名デバイス -- QCSD by CEN

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)	Guidance	
Policy & Security Requirements							
EN	4	19	2 1	1	Protection profiles for secure signature creation device - Part 1: Overview - Part 2: Device with key generation - Part 3: Device with key import - Part 4: Extension for device with key generation and trusted communication with certificate generation application - Part 5: Extension for device with key generation and trusted communication with signature creation application - Part 6: Extension for device with key import and trusted communication with signature creation application	(new part) - prTS 14169-2 - prTS 14169-3 - prTS 14169-4 - prEN 14169-5 - (new part)	published
EN	4	19	2 2	1	Protection Profiles for TSP cryptographic modules - Part 1: Overview - Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP) - Part 3: Cryptographic module for CSP key generation and signing operations (CMCKG-PP) - Part 4: Cryptographic module for CSP signing operations – Protection Profile (CMCSOPP) - Part 5: Protection Profile for cryptographic module for TSPs	(new part) - prTS 14167-2 - prTS 14167-3	Parts 1 to 4 in 2016 Part 5 in 2017
EN	4	19	2 3	1	Protection profile for trustworthy systems supporting server signing		
EN	4	19	2 4	1	Trustworthy systems supporting server signing - Part 1: General system security requirements - Part 2: Protection Profile for QCSD for Server Signing		
EN	4	19	2 5	1	Security requirements for device for authentication - 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 - Part 1: Introduction - Part 2: Basic services - Part 3: Device authentication - Part 4: Privacy specific protocols - Part 5: Trusted eServices	EN 14890	2016
Conformity Assessment							
no requirement identified							
Testing Conformance & Interoperability							
no requirement identified							

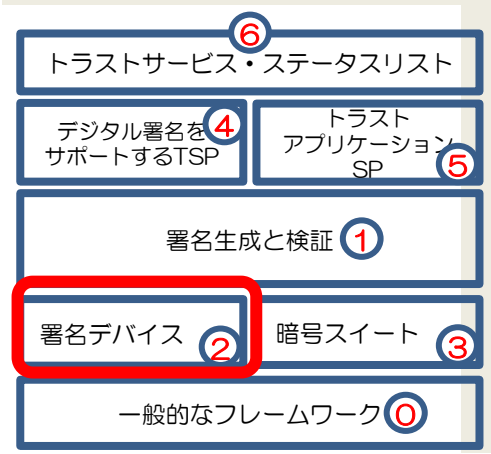
Policy & Security Requirements

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

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	pu
EN	3	19 4 1	1	Policy and security requirements for trust service providers - Part 1: General requirements - Part 2: Requirements for trust service providers issuing EU qualified certificates - Part 3: <i>To be withdrawn</i> - Part 4: Requirements for trust service providers providing AdES digital signature generation services	pu
EN	3	19 4 2	1	Policy & security requirements for trust service providers providing AdES digital signature validation services	pu
EN	3	19 4 3	1	Policy and security requirements for trust service providers providing AdES digital signature generation services	pu
EN	3	19 4 4	1	Policy and security requirements for trust service providers providing AdES digital signature validation services	pu
Technical Specifications					
EN	3	19 4 1	2	Certificate profiles - Part 1: Overview - Part 2: Certificate profile for web site certificates - Part 3: Certificate profile for X.509 certificates - Part 4: Certificate profile for web site certificates - Part 5: QCStatements	pu
EN	3	19 4 2	2	Time-stamping protocol and time-stamp token profiles	pu
EN	3	19 4 3	2	Protocol profiles for trust service providers providing AdES digital signature generation services	pu
EN	3	19 4 4	2	Protocol profiles for trust service providers providing AdES digital signature validation services	pu
Conformity Assessment					
EN	3	19 4 0	3	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing trust service providers	pu
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

④ デジタル署名をサポートするTSP

⑤ トラストアプリケーションSP

① 署名生成と検証

② 署名デバイス

③ 暗号スイート

⑦ 一般的なフレームワーク

トラストアプリケーション・サービスプロバイダー

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 providers	(new)	Undefined
SR	0	19	5	1	0	Scoping study and framework for standardization of long term data preservation 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 preservation of/with digital signatures	TS 102 573,	Undefined
EN	3	19	5	2	1	Policy & security requirements for electronic registered delivery services		
EN	3	19	5	3	1	Policy & security requirements for registered electronic mail (REM) service providers	TS 102 640	Undefined
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	TS 102 640	Undefined
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

6
トラストサービス・ステータスリスト

4
デジタル署名をサポートするTSP

5
トラストアプリケーションSP

1
署名生成と検証

2
署名デバイス

3
暗号スイート

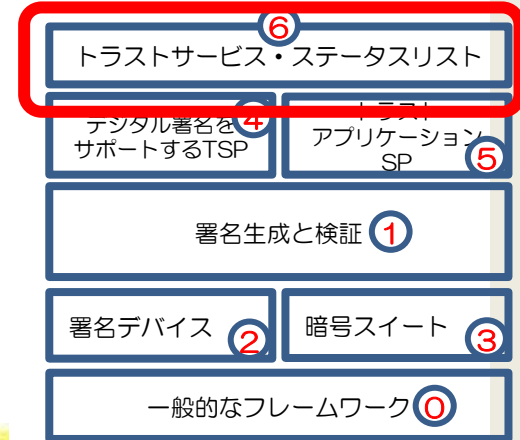
0
一般的なフレームワーク

トラストサービス・ステータスリスト

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 provided				Guidance	replaces	expected publication
Sub-areas						
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 providers		
				Technical Specifications		
TS	1	19	6 1	2 Trusted lists		
				Conformity Assessment		
				<i>no requirement identified for such a document - relying on</i>		
				Testing Conformance & Interoperability		
TS	1	19	6 1	4 Testing conformance & interoperability of trusted lists: - Part 1: Test suites for testing interoperability of XML representations of trusted lists - Part 2: Specifications for testing conformance of XML representations of trusted lists	(new)	Undefined
				Testing Conformance & Interoperability		