Welcome to the World of Standards

ETSI

World Class Standards

E-COMMERCE USING ELECTRONIC SIGNATURES IN JAPAN AND EUROPE

Keio University Tokyo – 4 July 2017

Setting the Context: Remote signing & eIDAS

Nick Pope – Vice Chair ETSI Electronic Signatures & Infrastructures
Principal consultant -Thales

Welcome to the World of Standards

ETSI

World Class 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

コンテキストの設定 – リモート署名とeIDAS

Nick Pope – Vice Chair ETSI Electronic Signatures & Infrastructures
Principal consultant -Thales

Topics

- Example requirements for Digital Signatures
- EU eIDAS Regulation 910/2014
- ETSI Standards on Digital Signatures and Trust Infrastructures
- The EU Trust Framework
- Remote Signing

トピックス

- デジタル署名に関する要件例
- EU eIDAS 規則910/2014
- デジタル署名およびトラスト基盤に関するETSI規格
- EUトラストフレームワーク
- リモート署名

Examples of Digital Signature Usage

- Dematerialisation of customer documents
  example bank has 2.5 million documents per year

デジタル署名の使用例

- 顧客文書の電子化
  例：ある銀行では年間250万部の文書を電子化している

Examples of Digital Signature Usage

- Dematerialisation of customer documents
  example bank has 2.5 million documents per year

- E-Commerce: Digital signatures supporting
  global tax compliance

デジタル署名の使用例

- 顧客文書の電子化
  例：ある銀行では年間250万部の文書を電子化している

- 電子商取引: デジタル署名が世界的な納税制度への適合性をサポートしている

Examples of Digital Signature Usage

- Dematerialisation of customer documents
  example bank has 2.5 million documents per year

- E-Commerce: Digital signatures supporting
  global tax compliance

- Regulatory requirements for security of records:
  e.g. US FDA / EU Medicines Agency

デジタル署名の使用例

- 顧客文書の電子化
  例：ある銀行では年間250万部の文書を電子化している

- 電子商取引: デジタル署名が世界的な納税制度への適合性をサポートしている

- 記録文書のセキュリティに関する規制要件:
  例： 米国FDA（連邦食品医薬品局） / EU医薬品庁

Examples of Digital Signature Usage

- Dematerialisation of customer documents
  example bank has 2.5 million documents per year

- E-Commerce: Digital signatures supporting
  global tax compliance

- Regulatory requirements for security of records:
  e.g. US FDA / EU Medicines Agency

- eContracts: e.g. Loan agreement, car hire, insurance

Examples of Digital Signature Usage

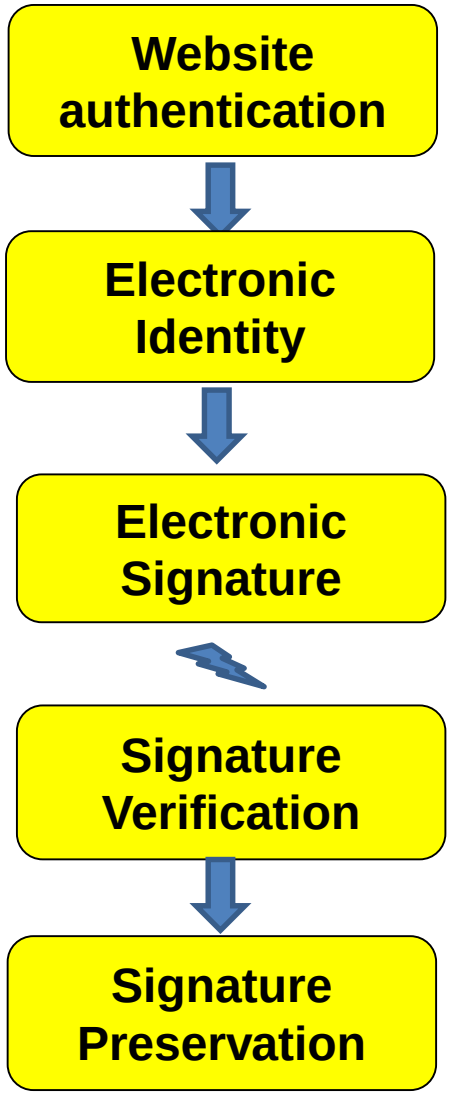
- 顧客文書の電子化
  例：ある銀行では年間250万部の文書を電子化している

- 電子商取引: デジタル署名が世界的な納税制度への適合性をサポートしている

- 記録文書のセキュリティに関する規制要件:
  例： 米国FDA（連邦食品医薬品局） / EU医薬品庁

- 電子契約: 借款契約、レンタカー、保険など

eID and trust services supporting full transaction cycle



Web site authentication certificate confirms web site identity

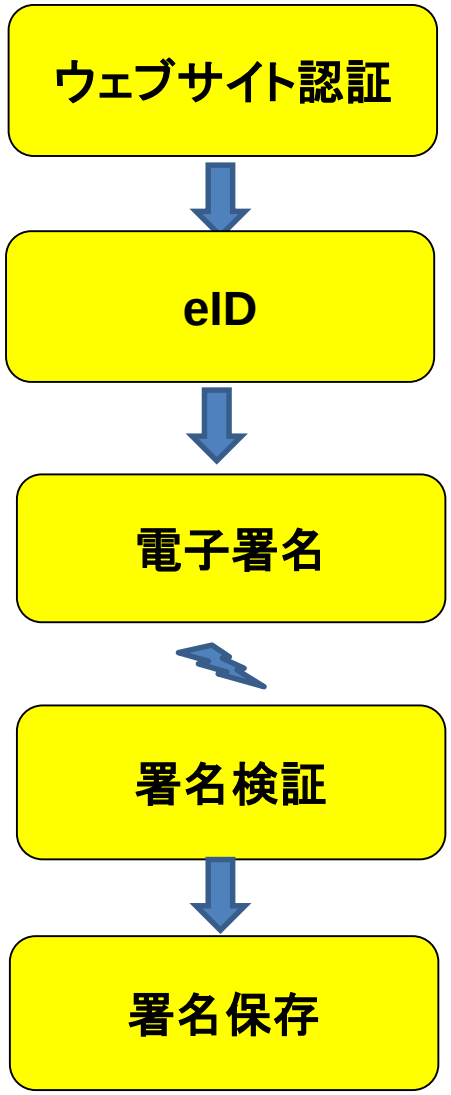
Electronic identity confirms user identity

User identity bound to document using Digital signature

Digital signature verified by document recipient

Validity of signature maintained by time-stamping service.

トランザクションサイクル全体をサポートする eIDおよびトラストサービス



ウェブサイト認証証明書は
ウェブサイトのアイデンティティを裏付ける

eIDはユーザのアイデンティティを裏付ける

デジタル署名の使用で文書に結び付く
ユーザアイデンティティ

文書の受信者が検証するデジタル署名

タイムスタンプサービスが保全する
署名の有効性

EU eIDAS regulation 910/2014

- eIDAS covers two main topics:
  - Electronic identities
  - Trust services

- eIDAS provides legal framework for two main areas trust services :
  - Recognition of electronic signatures (physical persons) and electronic seals (equivalent for organisations)
  - Assuring trust in Trust Service Providers

EU eIDAS規則910/2014

- eIDASの対象は2つの主要トピックス
  - eID
  - トラストサービス

- eIDASは2つの主なトラストサービス分野についての法的なフレームワークを規定している：
  - 電子署名（自然人）およびeシール（組織に対応）の承認
  - トラストサービスプロバイダの信頼性の保証

EU eIDAS regulation 910/2014
Recognition of electronic signatures

- Electronic Seal vs Signature
  - Signature: Created by a physical person
  - Seal: Created by a legal person (e.g. company, governmental body)

- Forms of electronic signatures / Seals
  - Electronic Signature / Seal : No restriction on form of signature
  - Advanced Electronic Signature / Seal: form meets requirements relating to use of digital signature technology
  - Qualified Electronic Signature / Seal:
    digital signatures supported by
    - "qualified" signature creation device – certified against requirements
    - "qualified" trust service provider – audited against requirement

EU eIDAS規則910/2014
電子署名の承認

- 電子シールVS 署名
  - 署名：自然人が生成する
  - シール: 法人（企業、政府機関など）が生成する
- 電子署名/シールの形式
  - 電子署名/シール： 署名の形式に関する制約はない
  - 先進電子署名/シール: デジタル署名技術の使用に関連する要件を満たす形式
  - 適格電子署名/シール:
    次によってサポートされるデジタル署名
    - 「適格」署名生成装置 – 要件に対して認証されている
    - 「適格」トラストサービスプロバイダ–要件に対して監査されている

Recognised signature formats

- Specific signature formats to be recognised by government systems
  - Secondary legislation reference ETSI standards (PAdES, CAdES, XAdES, ASIC)

認められている署名の形式

- 政府のシステムによって認められる特定の署名フォーマット
  - 二次法はETSI規格を参照している
    (PAdES, CAdES, XAdES, ASIC)

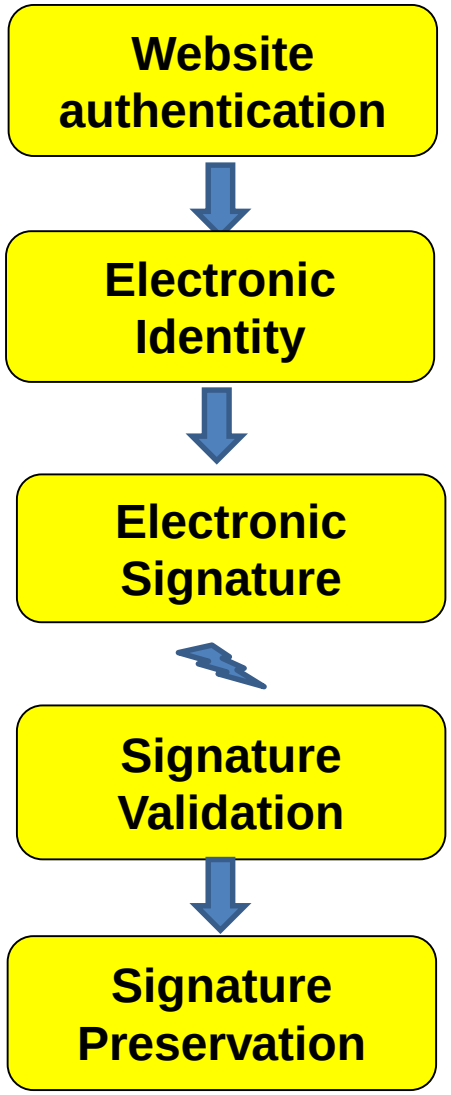
EU eIDAS regulation 910/2014
Trust services

- Trust Services covered by eIDAS
  - Trust services supporting electronic Signatures / Seals:
    - Certification authorities
    - Cloud / remote signature creation
    - Signature validation
    - Signature preservation
  - Time-stamping authority
  - Registered electronic delivery

EU eIDAS規則910/2014
トラストサービス

- eIDASの適用対象であるトラストサービス
  - 電子署名/シールをサポートするトラストサービス:
    - 認証局
    - クラウド / リモート署名生成
    - 署名検証
    - 署名保存
  - タイムスタンプ局
  - 登録eデリバリ

eID and trust services supporting full transaction cycle



TSP issuing web site certificates

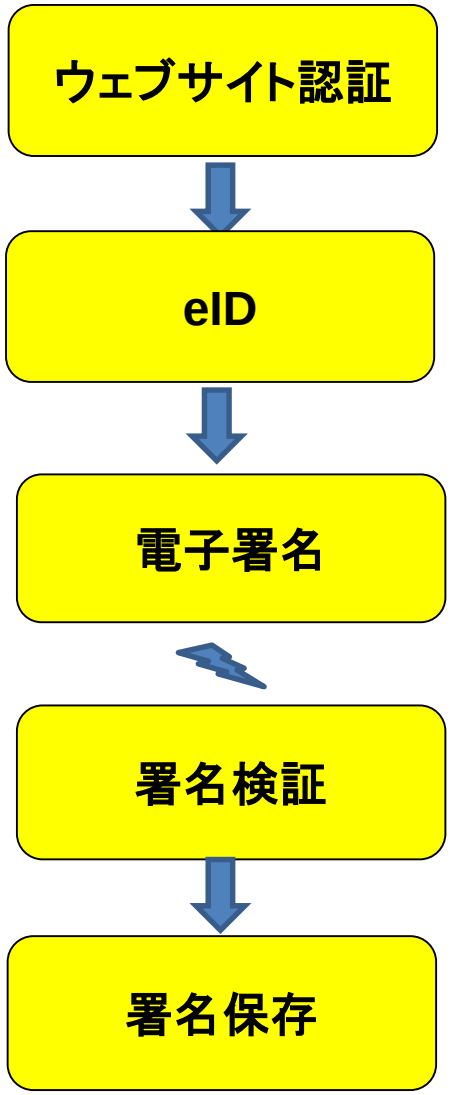
eID provider

TSP issuing signing certificate,
TSP time-stamping proving signing time
TSP providing remote signing

TSP providing signature validation

TSP time-stamp / preservation service maintaining signature & document integrity

トランザクションサイクル全体をサポートする eIDおよびトラストサービス



ウェブサイト証明書を発行するTSP

eID プロバイダ

署名証明書を発行するTSP

署名の時刻を証明するTSPタイムスタンプ

リモート署名を提供するTSP

署名検証を提供するTSP

署名および文書の完全性を保全する

TSP タイムスタンプ / 保存サービス

EU eIDAS regulation 910/2014
Assuring Trust Services

- All trust services (including those supporting “advance”)
  - Liable unless appropriate security measures taken.
  - Must report any security breach
- TSP supporting “qualified”
  - Must meet specific requirements of eIDAS regulation
  - 2 yearly audit (if also CAB Forum 1 yearly)
  - If legally accepted as qualified placed in Trusted List

EU eIDAS規則910/2014
トラストサービスの保証

- すべてのトラストサービス(「先進」をサポートするものも含む)
  - 適切なセキュリティ措置が取られていない場合、法的責任を負う。
  - すべてのセキュリティ違反について報告しなければならない

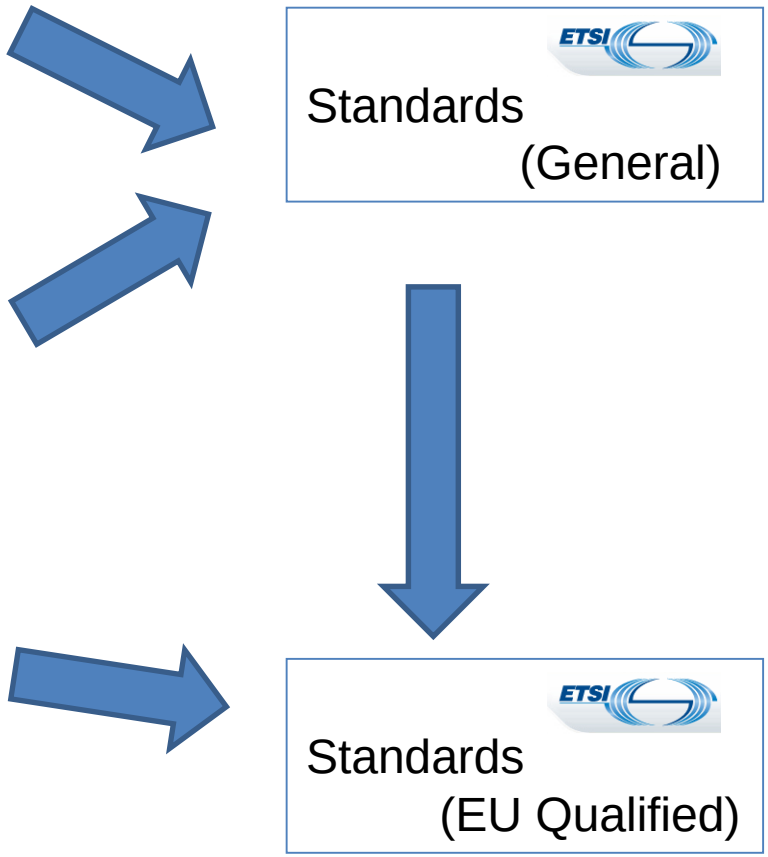
- 「適格」をサポートするTSP
  - eIDAS規則の特定要件を満たさなければならない
  - 2年毎の監査(CABフォーラムにも該当する場合は1年毎)
  - 適格として法的に認められると、トラストリストに掲載される

ETSI meeting eIDAS requirements and Industry accepted best practice

Recognised standards:
- ISO, IETF, OASIS, CAB Forum …

TSP best practices

eIDAS Qualified TSP requirements

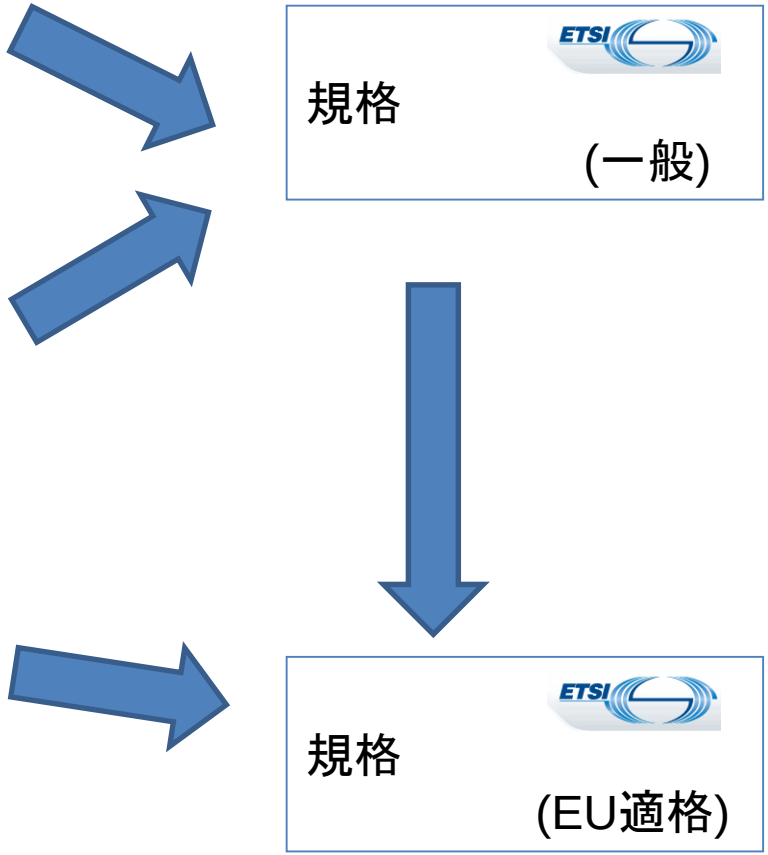


eIDAS要件および業界で受け入れられているベストプラクティスを満たすETSI

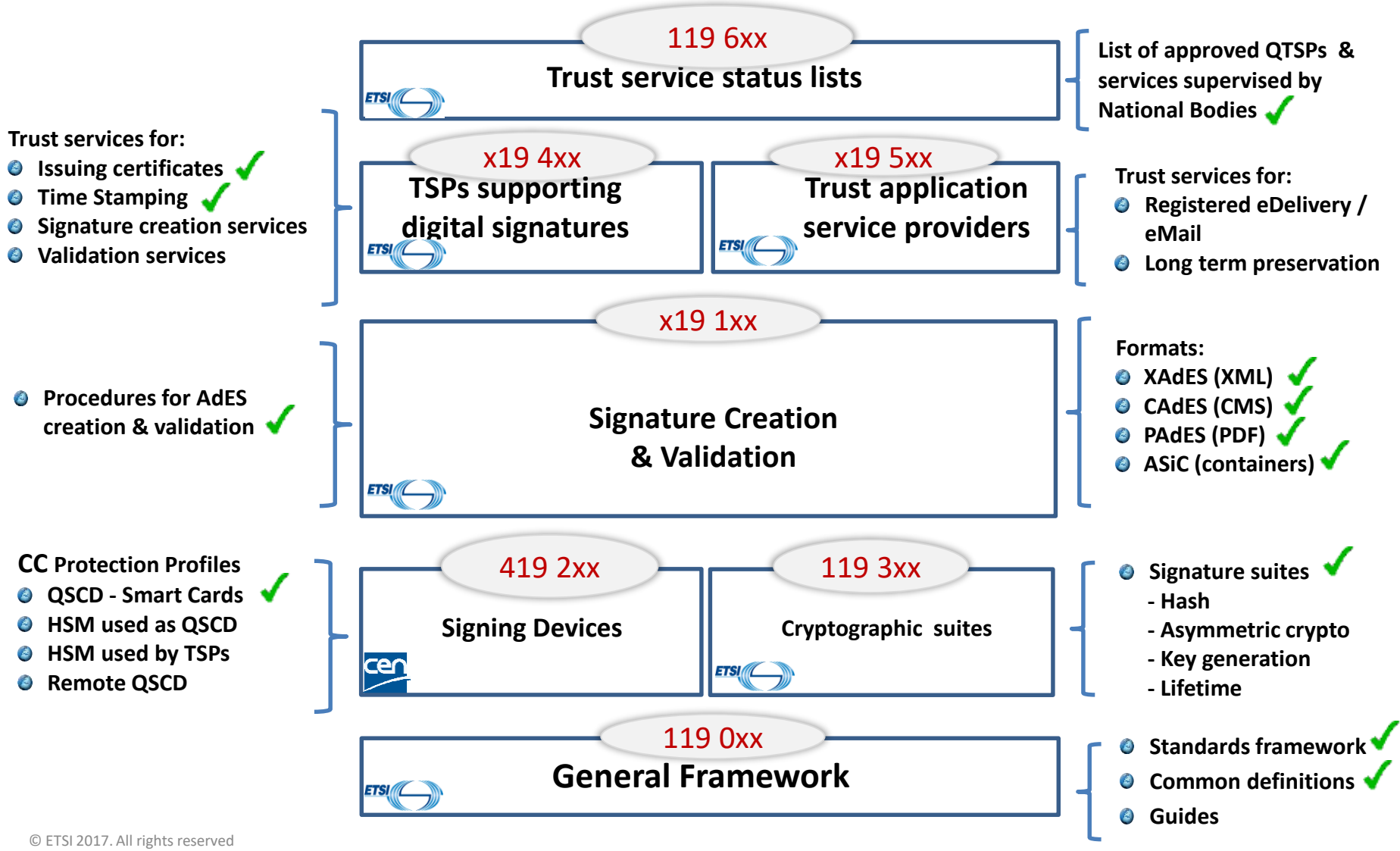
認められている規格:
○ISO, IETF, OASIS, CABフォーラム…

TSPベストプラクティス

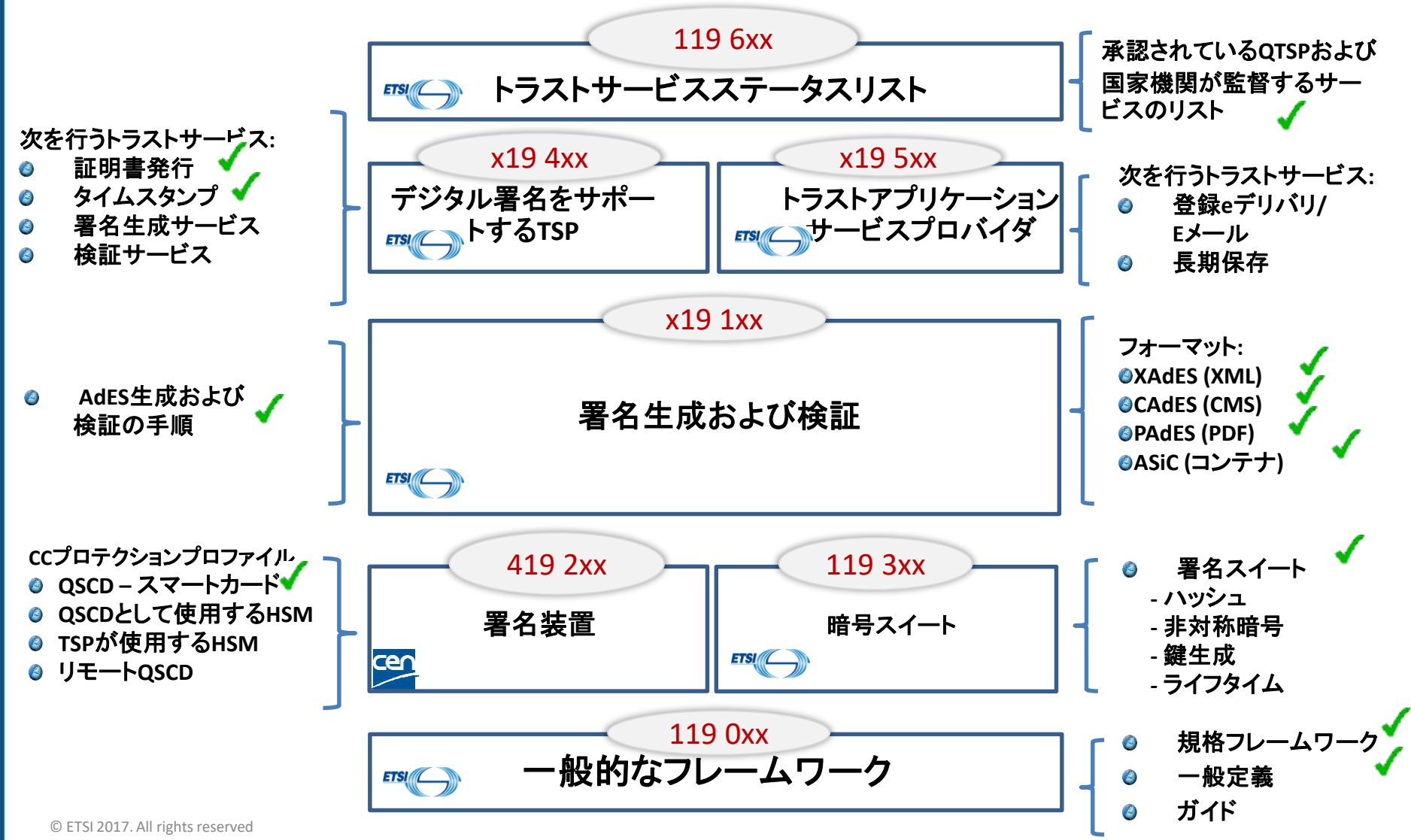
eIDAS適格TSP要件



eIDAS Standards Framework: Published Standards



eIDAS規格フレームワーク: 公開されている規格



Elements of Framework for Trust Services

	Europe
Trust Management	EU Trusted List TS 119 612
Trust Audit	EU TSP Audit EN 319 403 based on ISO 17065 (ISO 17065 Accreditation globally recognised through IAF)
Trust Criteria	Policy Requirements for TSP Issuing Certificates: EN 319 411-1: general EN 319 411-2: qualified

トラストサービスフレームワークの要素

	欧州
トラスト管理	EUトラストリスト TS 119 612
トラスト監査	EU TSP監査 ISO 17065 に基づくEN 319 403 (IAFにより世界的に承認されているISO 17065認定)
トラスト基準	証明書を発行するTSPのポリシー要件: EN 319 411-1: 一般 EN 319 411-2: 適格

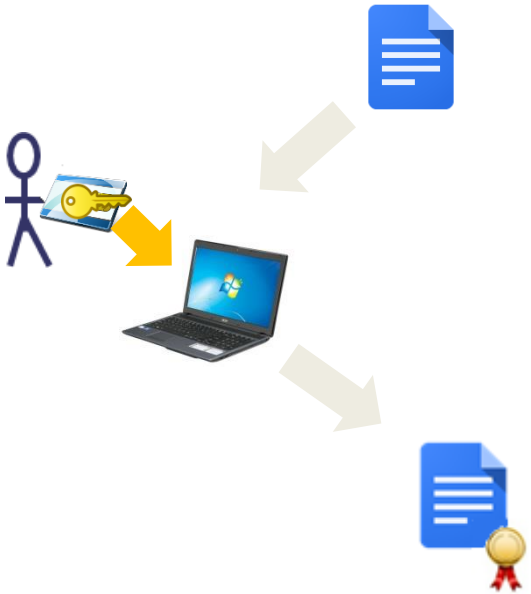
Cross recognition

- Advanced level: Relying party needs to know that TSP is trustworthy
  - Case by case analysis of Certificate Policy and Audit
  - Trust status indicated by trusted party
    - Bridge CA
    - Application platform provider (Microsoft, Google, Apple …) root CA store
    - Trust status list from recognised authority
- Qualified level:
  - Legal agreement between nations
  - Trusted list managed by recognised authority

相互承認

- 先進レベル: 依拠当事者はTSPが信頼できるものであることを知る必要がある
  - 証明書ポリシーおよび監査の個別分析
  - 信頼できる機関によって示されるトラストステータス
    - ブリッジ CA
    - アプリケーションプラットフォームプロバイダ (Microsoft, Google, Apple …) ルートCAストア
    - 承認されている機関が発行するトラストステータスリスト
- 適格レベル:
  - 国家間の法的取り決め
  - 承認されている機関が管理するトラストリスト

Why remote signing ?
Conventional Smart card like QSCD



Features:

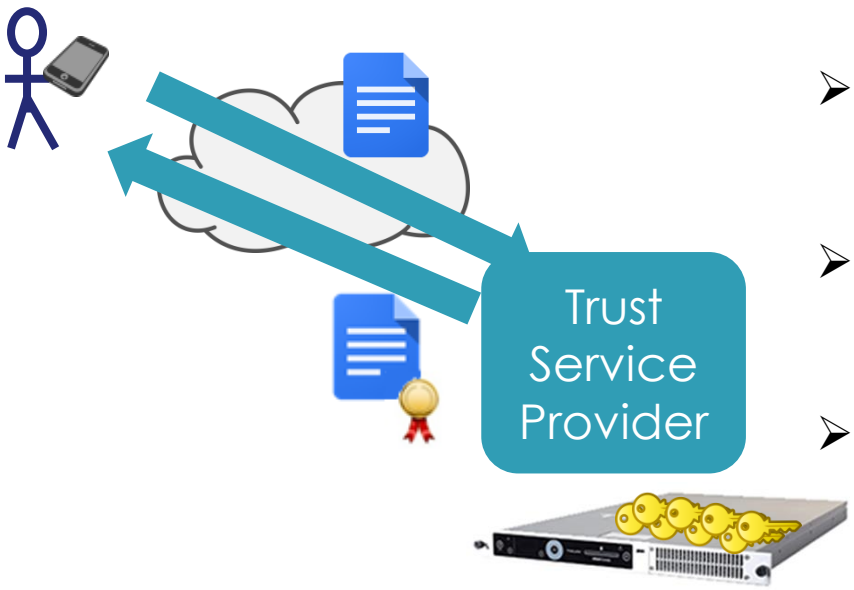
- User's signing key in user held device such as smart cards
- Document to be signed on user's PC
- Need special interface / reader on PC
- Not suited to modern use of mobile devices such as smart phone's
- If card is compromised:
  - user must report loss
  - TSP must verify report
  - TSP must updated revocation list OCSP database

なぜリモート証明？
QCSDのような従来のスマートカード

特徴:

- ユーザの署名鍵はユーザが所有するスマートカードなどのデバイス内で保有
- 署名する文書はPC内で保有
- PCに特別なインターフェース/リーダーが必要
- スマートフォンなどのようなモバイル端末の使用には適していない
- カードが危殆化した場合には:
  - ユーザはそれを報告しなければならない
  - TSPは報告を検証しなければならない
  - TSPは失効リストOCSPデータベースを更新しなければならない

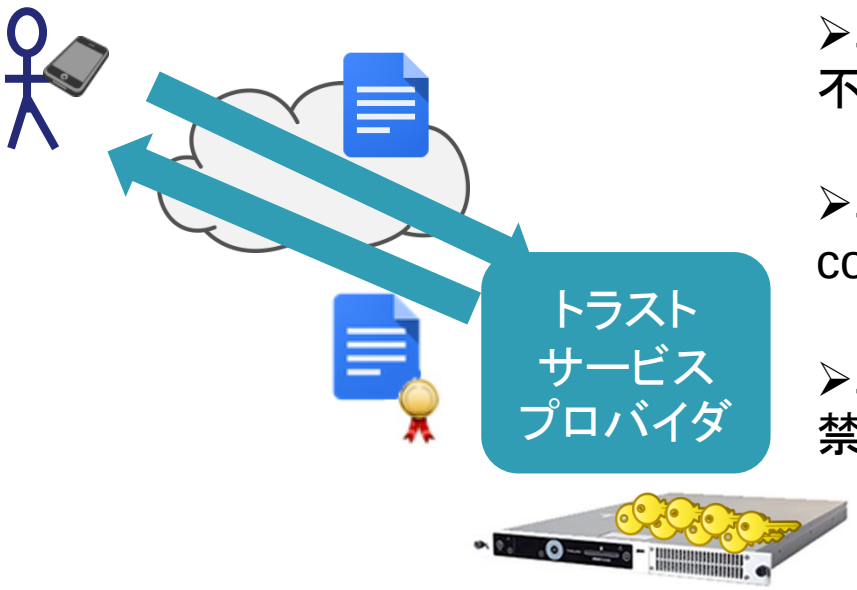
Using Cloud based “Remote Signing”



Features:

- User’s signing key held on secure device managed by a Trust Service Provider
- Document to be signed can be processed “in the cloud”
- No need for hardware interface to user device
- User must have “sole control” over the signing key
- In case of user compromise
  use of key instantly prohibited

クラウドベース「リモート署名」の利用

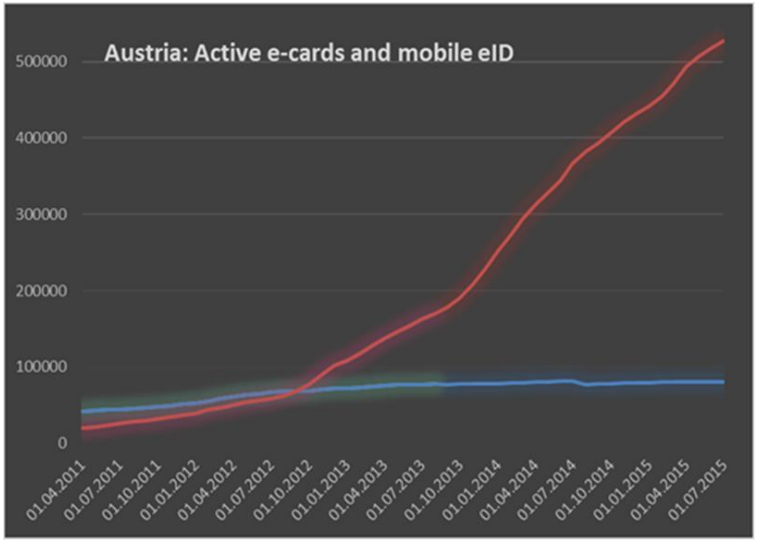


特徴:

- ユーザの署名鍵はトラストサービスプロバイダが管理するセキュアデバイス内で保有
- 署名する文書は「クラウド」で処理できる
- ユーザ機器にハードウェアインターフェースは不要
- ユーザは署名鍵について「単独管理（sole control）」しなければならない
- ユーザ危殆化の場合は、鍵の使用は即時に禁止される

The move to Mobile Based Signatures

- Many EU countries are moving from card based to mobile signatures

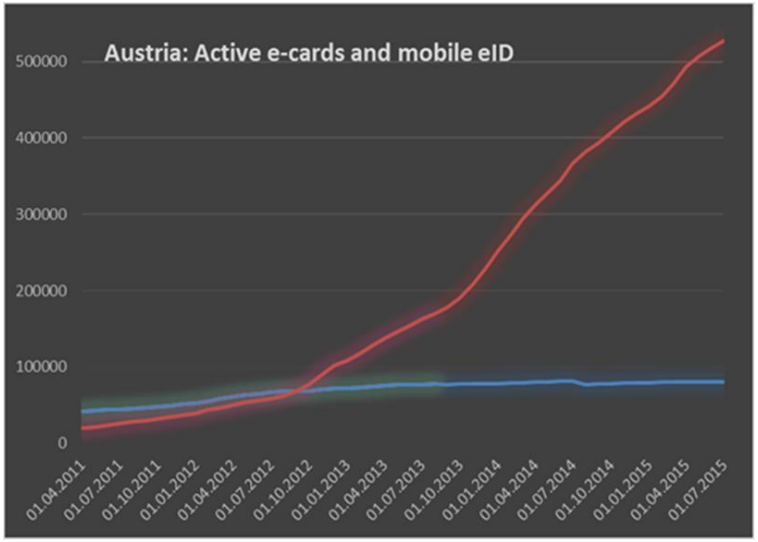


- Advantages
  - Easy deployment
    - Everyone has a mobile
  - No special hardware
    - No special card interface
  - Flexibility in authentication
    - Any two factors
  - Use of key can be prohibited in case of user compromise

モバイルベース署名への移行

- 多くのEU諸国は、カードベースからモバイル署名へ移行している

- メリット
  - 展開が容易である
    - 誰でもモバイル端末を所有している
  - 特別なハードウェアが不要である
    - 特別なカードインターフェース不要
  - 認証における柔軟性
    - 二要素認証であればどの組み合わせでも可
  - ユーザ危殆化の場合は鍵の使用を禁止することができる



Remote Signing
Relevant eIDAS Requirements

- Requirement on Advanced Electronic Signatures (Article 26)

  ……

  c) it [the advanced electronic signature] is created using electronic signature creation data [key] that the signatory can, with a high level of confidence, use under his sole control;

- Requirement on QSCD (Annex II)

  ….

  3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

リモート署名
関連するeIDAS規則

- 先進電子署名に関する要件（第26条 ）

  ……

  c) （先進電子署名は）署名者が、高い信頼性をもって、自らによる単独の管理（sole control）の下で使用することができる電子署名生成データ（鍵）を使って生成する ;

- QSCDに関する要件（付属書II）

  ….

  3.署名者の代わりに電子署名生成データを生成または管理することができるのは適格トラストサービスプロバイダのみである。

Standards for Remote Signing

Recognised standards:
- Cloud Signature Consortium
- OASIS DSS & DSS-X

TS 119 432: Protocols for remote digital signature creation

TSP best practices

TS 119 431 : Policy and security requirements for TSP service components
1) operating QSCD / SCD
2) AdES creation

eIDAS QSCD requirements

prEN 419241
1) General System Security Requirements
2) QSCD Protection Profile

リモート署名に関する規格

認められている規格:
○クラウド署名コンソーシアム
○OASIS DSS & DSS-X

TS 119 432: リモートデジタル署名生成のプロトコル

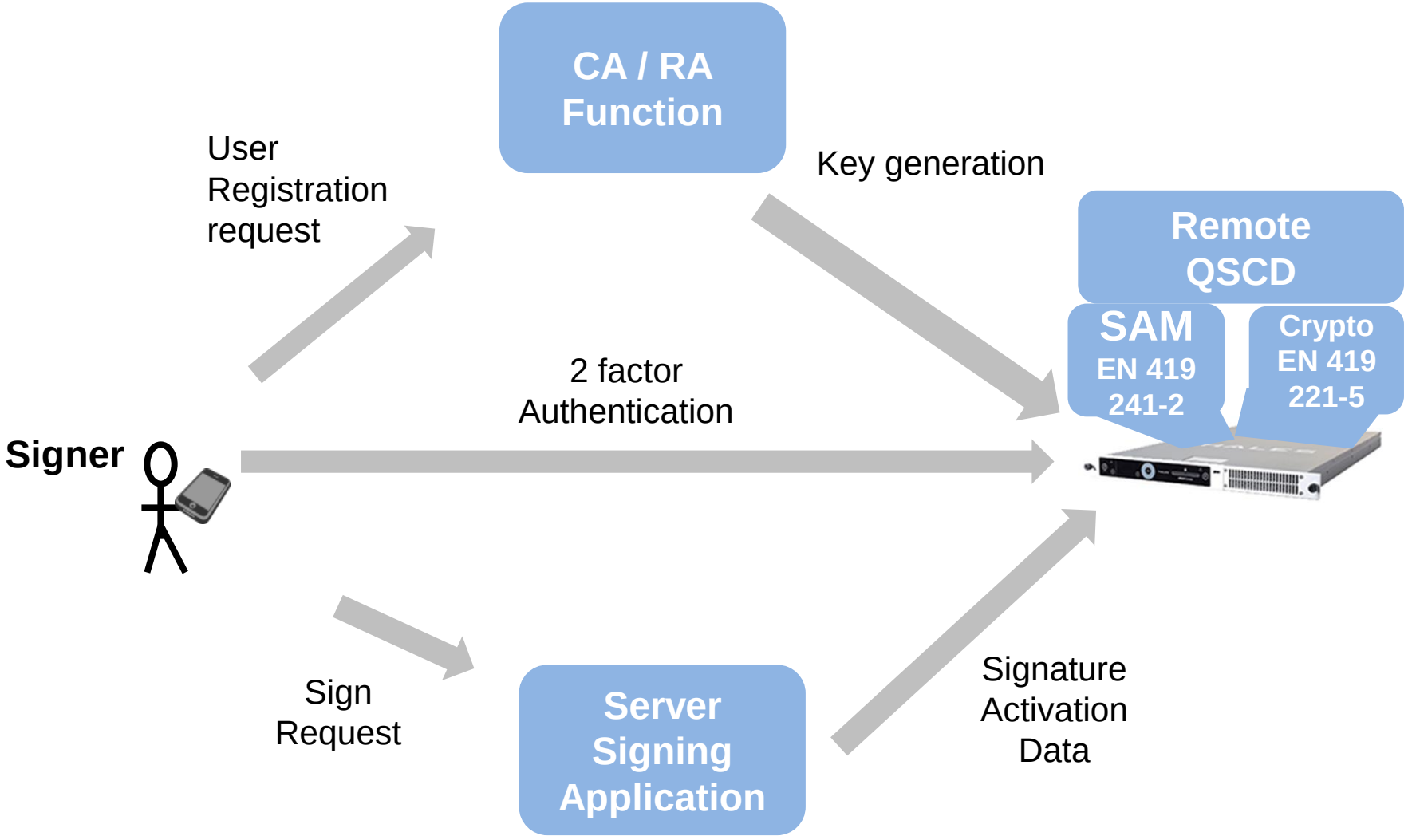
TSP ベストプラクティス

TS 119 431 : TSPのサービス内容のポリシーおよびセキュリティ要件
1) QSCD / SCD運用
2) AdES生成

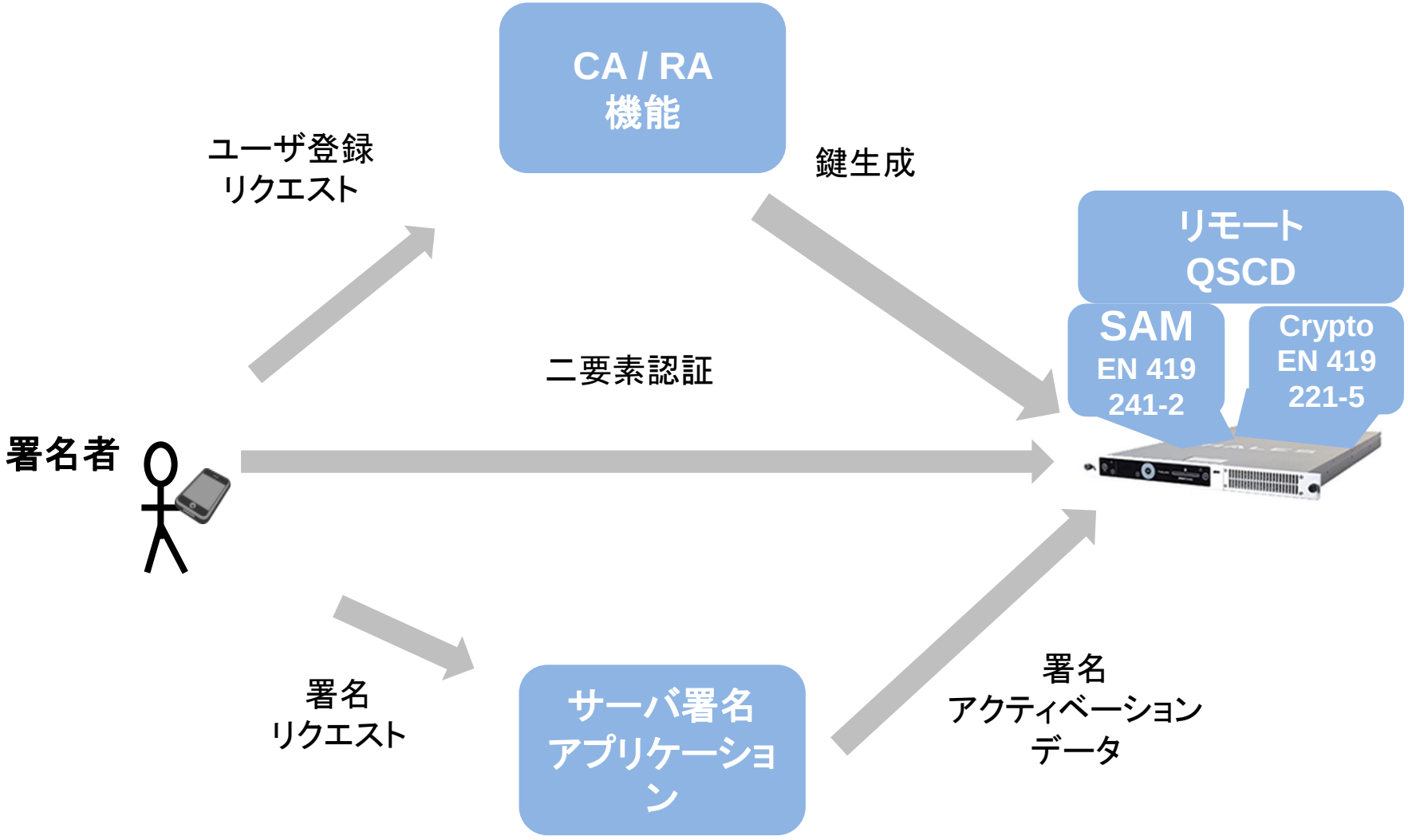
eIDAS QSCD 要件

prEN 419241
1) 一般的なシステムセキュリティ要件
2) QSCDプロテクションプロファイル

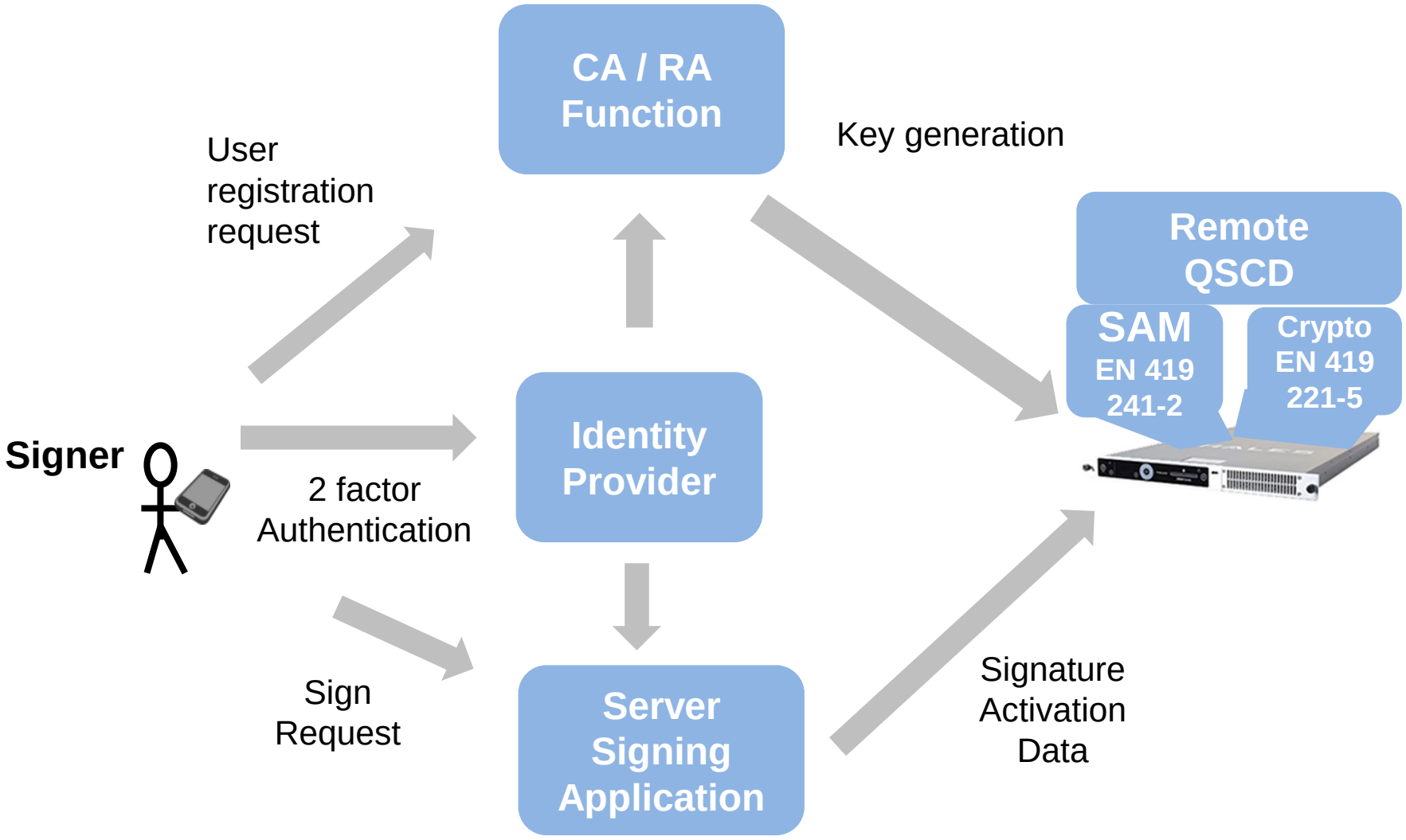
Remote Signing
Example without delegation



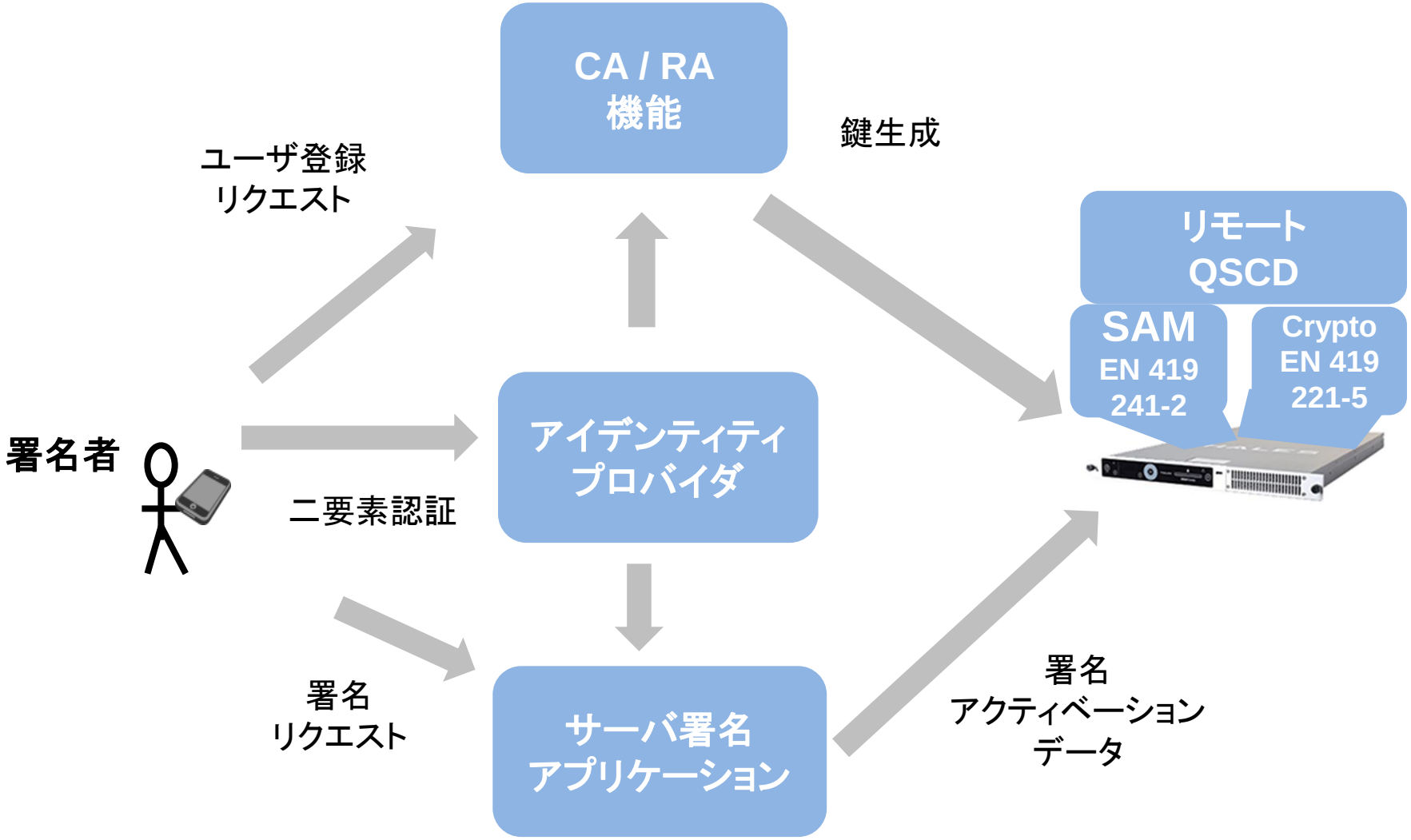
リモート署名
委任しない場合の例



Remote Signing
Example with delegation



リモート署名
委任する場合の例



Further Information

ETSI standards available for free download
http://www.etsi.org/standards-search

Overview of Electronic Signature and Infrastructure standards:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

E-mail: nick.pope@thales-esecurity.com

詳細情報

無料ダウンロードできるETSI規格
http://www.etsi.org/standards-search

電子署名および基盤規格の概要:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

E-mail: nick.pope@thales-esecurity.com