Welcome to the World of Standards

ETSI

World Class Standards

TRUST SERVICES AND CROSS RECOGNITION:

Certification Policies for eIDAS Trust Services and Electronic Delivery Services.

Arno Fiedler, Nimbus Technologieberatung GmbH, Berlin, Member of ETSI ESI

Welcome to the World of Standards

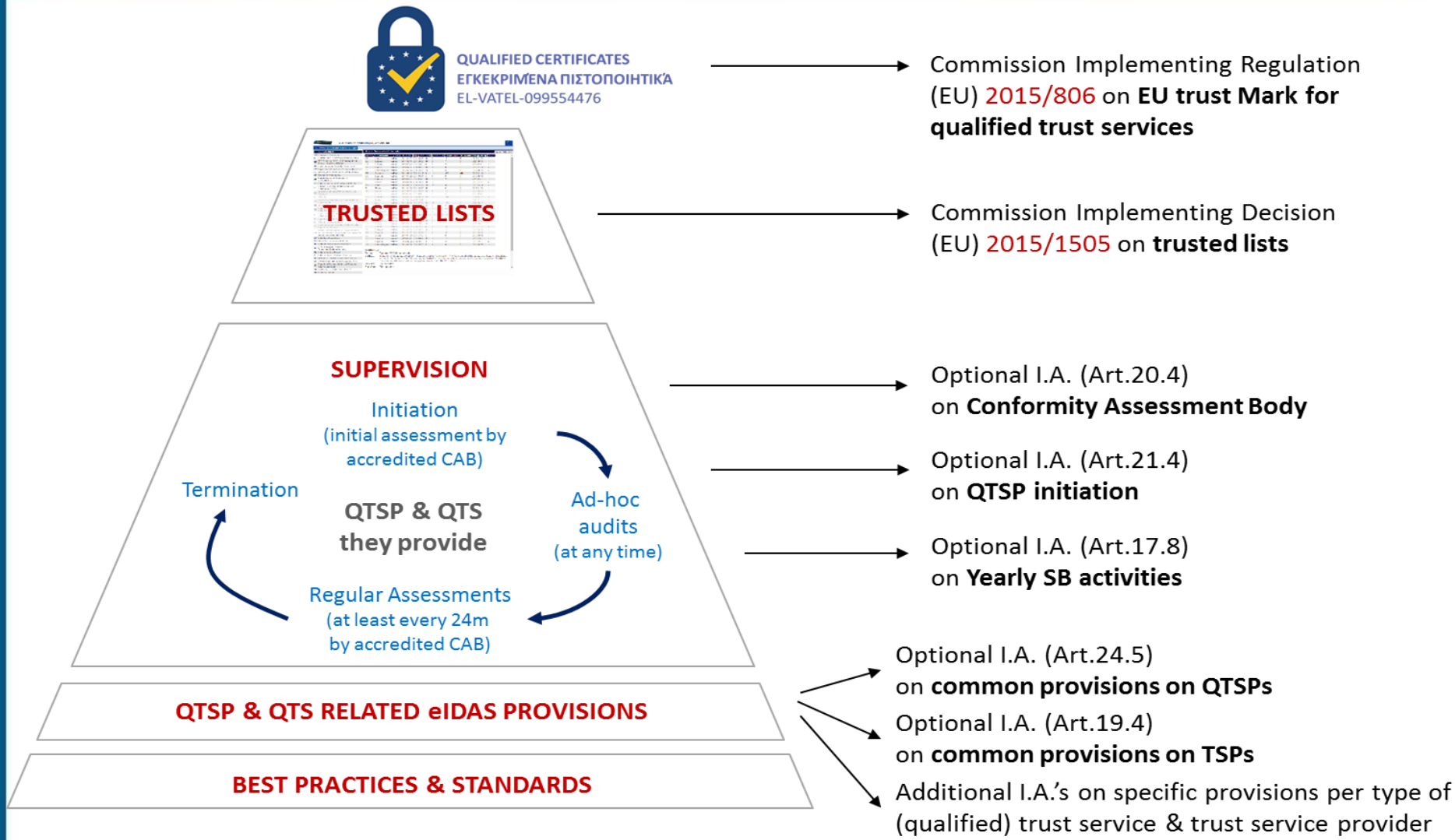
ETSI

World Class Standards

トラストサービスと相互承認：
eIDASトラストサービスとeデリバリサービスの認証ポリシー

Arno Fiedler, Nimbus Technologieberatung GmbH, Berlin, Member of ETSI ESI

eIDAS Assessment and Standards Framework

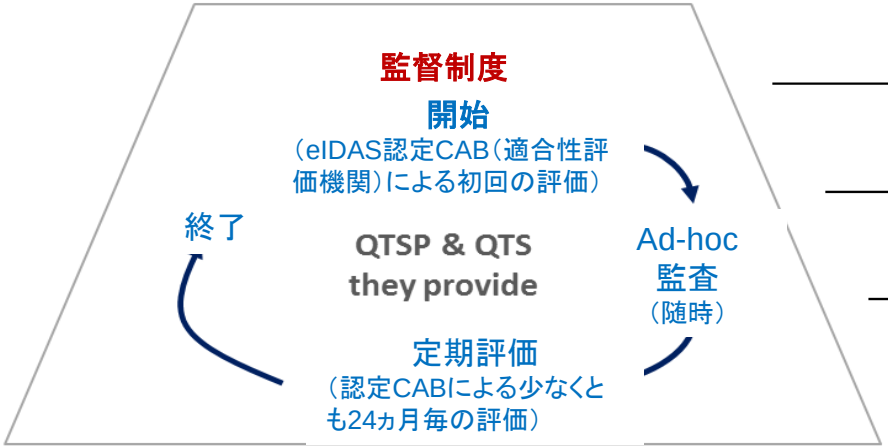


eIDAS評価および規格フレームワーク

適格証明書
ΕΓΚΕΚΡΙΜΈΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΆ
EL-VATEL-099554476

→ **適格トラストサービスのEUトラストマーク**に関する委員会実施規則（EU）2015/806

→ **トラストリスト**に関する委員会実施決定（EU）2015/1505



→ **適合性評価機関**に関する任意の実施法（第20.4条）

→ **適格トラストサービスプロバイダの開始**に関する任意の実施法（第21.4条）

→ **年次SB活動**に関する任意の実施法（第17.8条）

QTSPおよびQTSに関係するeIDAS規程

ベストプラクティスおよび規格

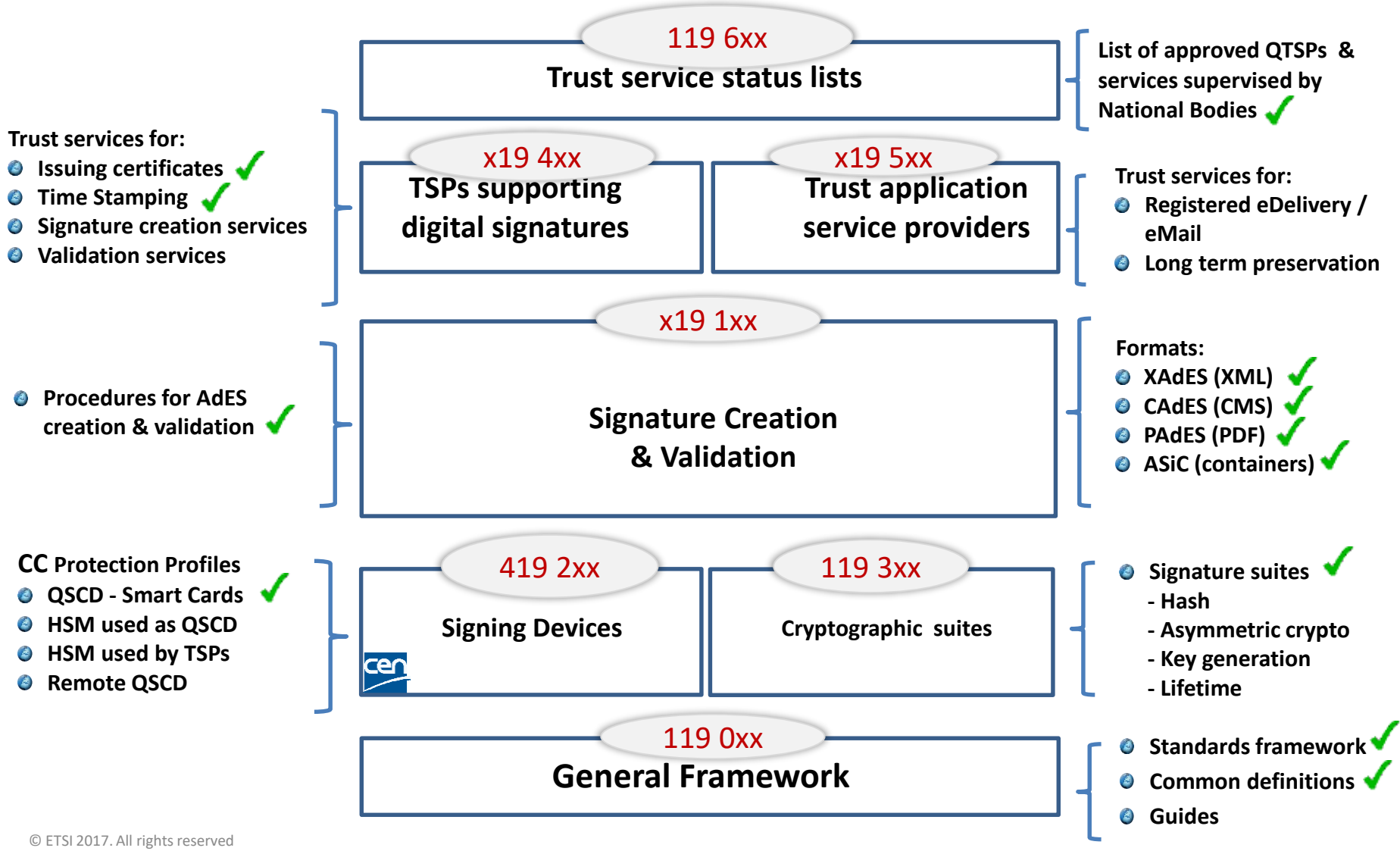
→ **QTSPの共通規定**に関する任意の実施法（第24.5条）

→ **TSPの共通規定**に関する任意の実施法（第19.4条）

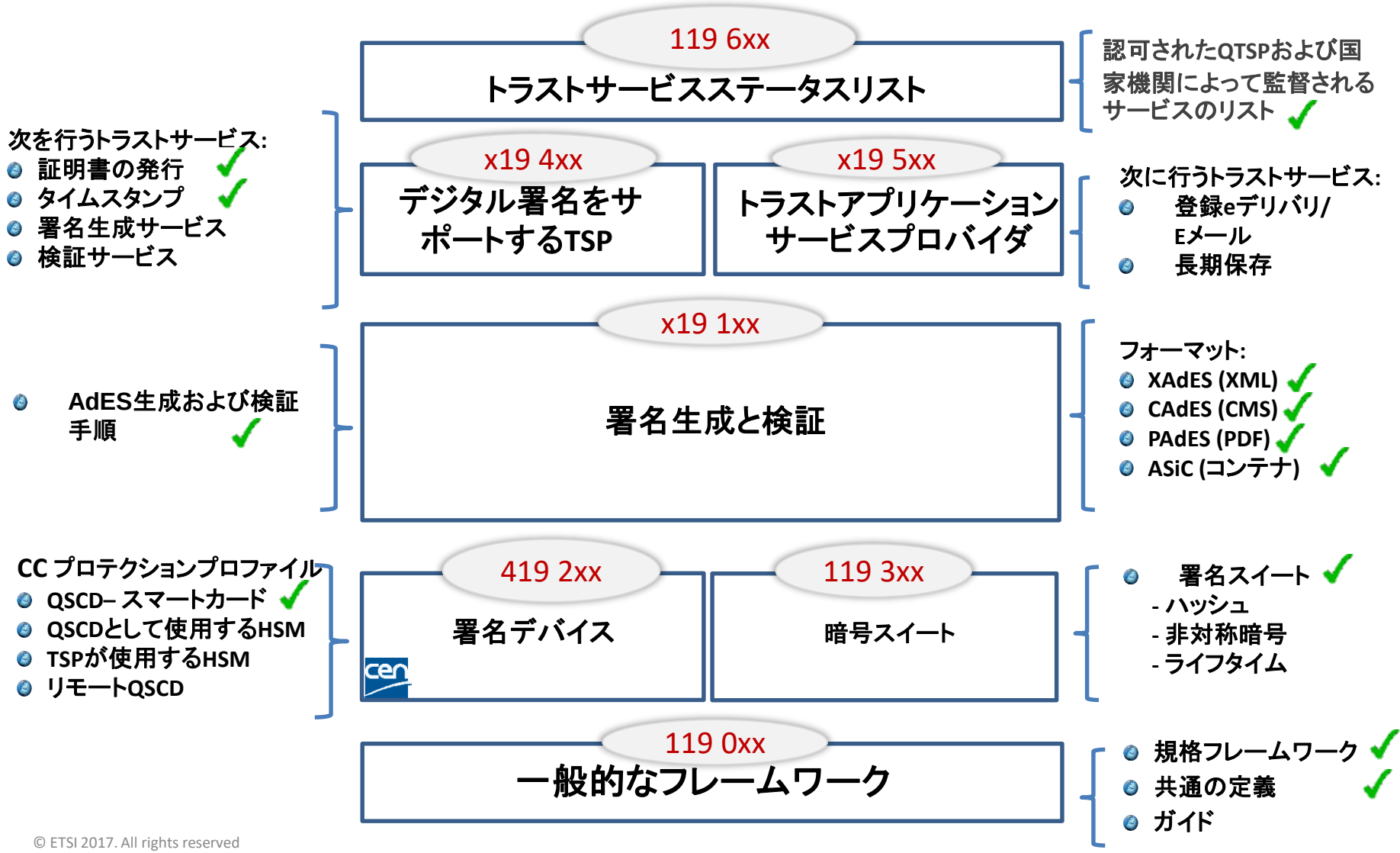
→ （適格）トラストサービス＆トラストサービスプロバイダのタイプ別特定規定に関する追加の実施法

QTS： 適格トラストサービス
QTSP：適格トラストサービスプロバイダ

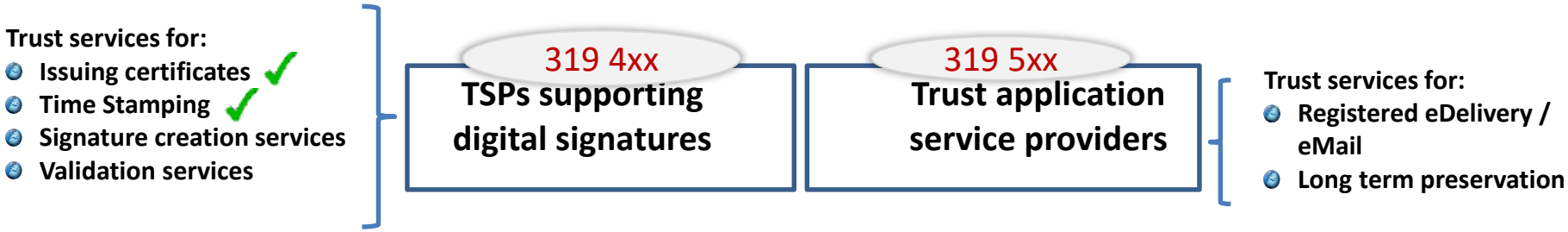
eIDAS Standards Framework:



eIDAS規格フレームワーク:



eIDAS Standards Framework: Certification Policies



eIDAS規格のフレームワーク: 認証ポリシー

次に行うトラストサービス:
- 証明書発行 ✓
- タイムスタンプ ✓
- 署名生成サービス
- 検証サービス

319 4xx
デジタル署名をサポートするTSP

319 5xx
トラストアプリケーションサービスプロバイダ

次に行うトラストサービス:
- 登録eデリバリ/Eメール
- 長期保存

Definitions and Policy purposes:

IETF RFC 3647 :

Certificate policy (CP) – A named set of rules that indicates ***the applicability of a certificate*** to a particular community and/or class of application with common security requirements.

ETSI EN 319 401 V2.2.1 (2017-06) :

Trust service policy: set of rules that indicates ***the applicability of a trust service*** to a particular community and/or class of application with common security requirements.

Trust service practice statement: statement of the practices that a TSP employs in providing a trust service

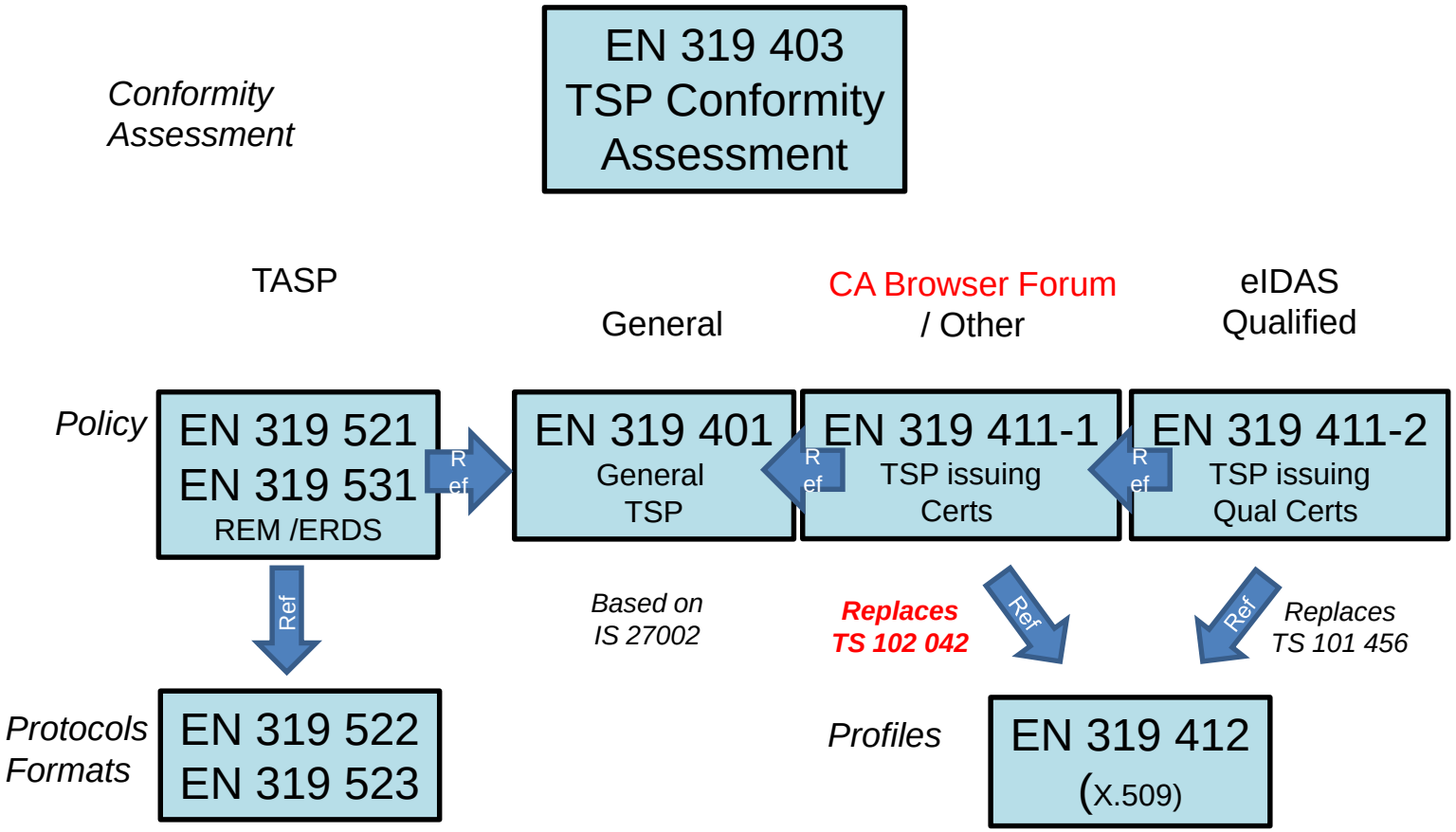
定義およびポリシーの目的:

IETF RFC 3647 :
証明書ポリシー(CP) – 共通のセキュリティ要件をもつ特定のコミュニティおよび/またはアプリケーションのクラスに対する***証明書の適用性***を示す、名付けられた規則集。

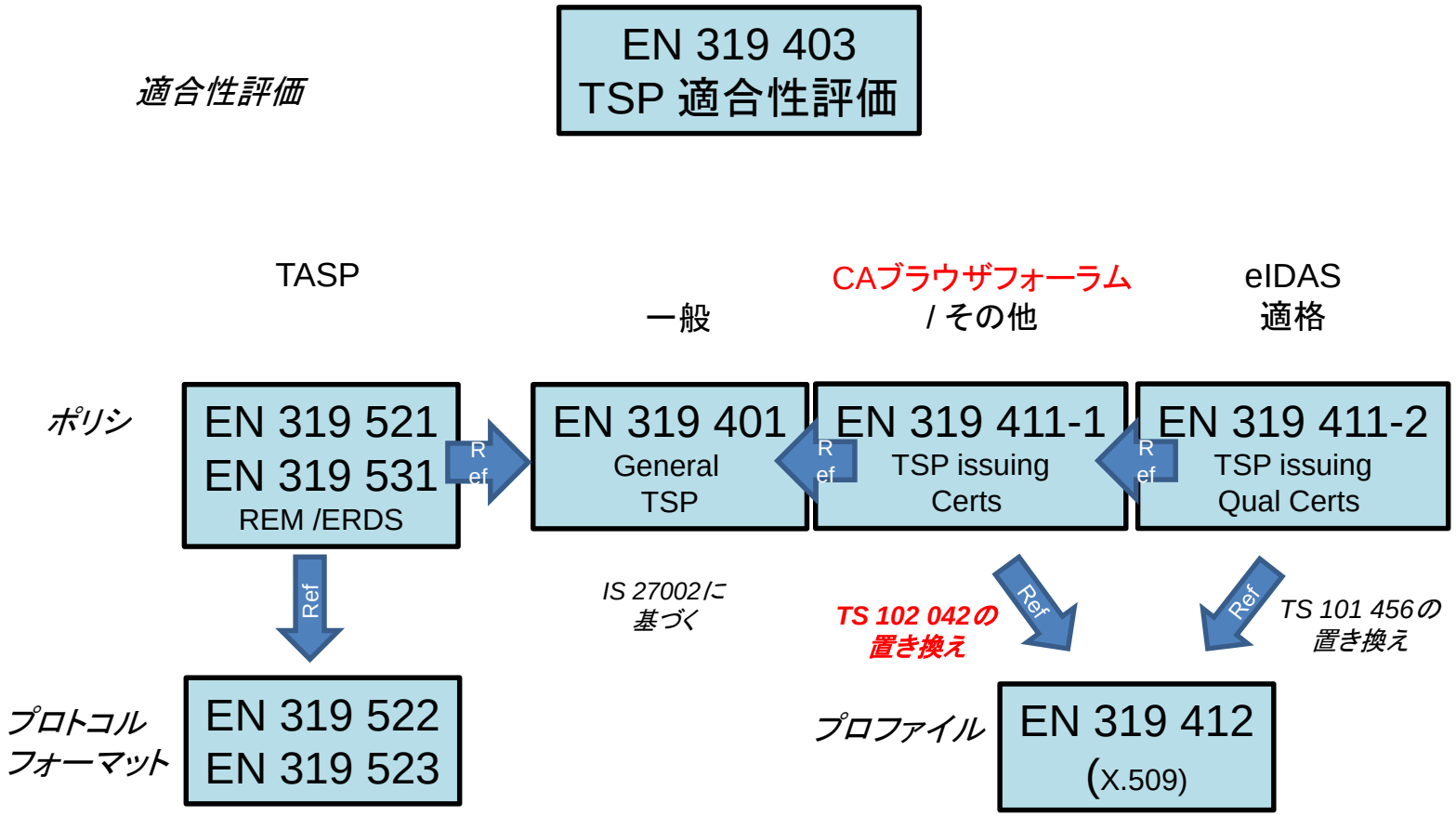
ETSI EN 319 401 V2.2.1 (2017-06) :
トラストサービスポリシー: 共通のセキュリティ要件をもつ特定のコミュニティおよび/またはアプリケーションのクラスに対する***トラストサービスの適用性***を示す規則集。

トラストサービス運用規程: TSPがトラストサービスの提供において採用する運用の規定

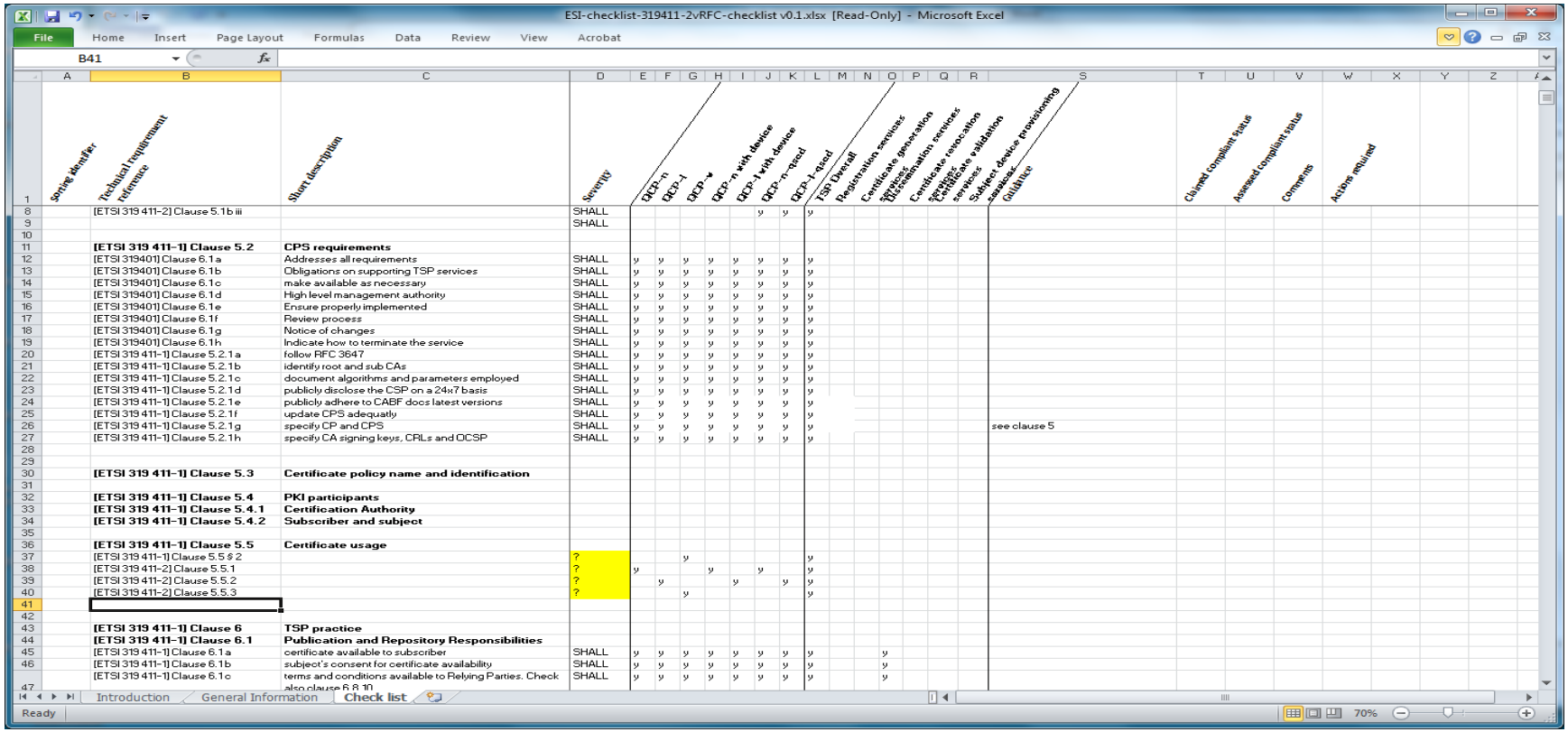
TSP Standards Overview (ETSI)



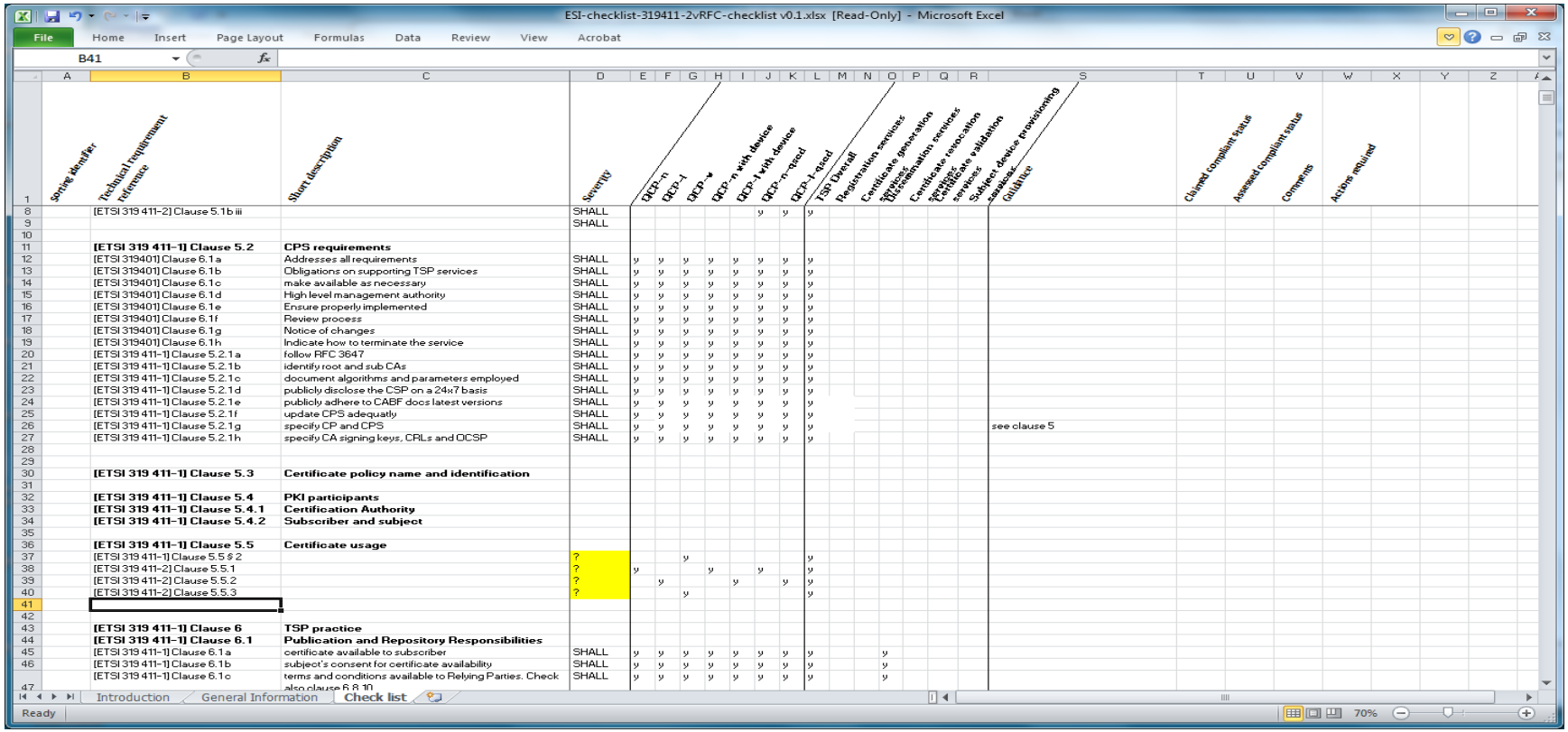
TSP規格概要（ETSI）



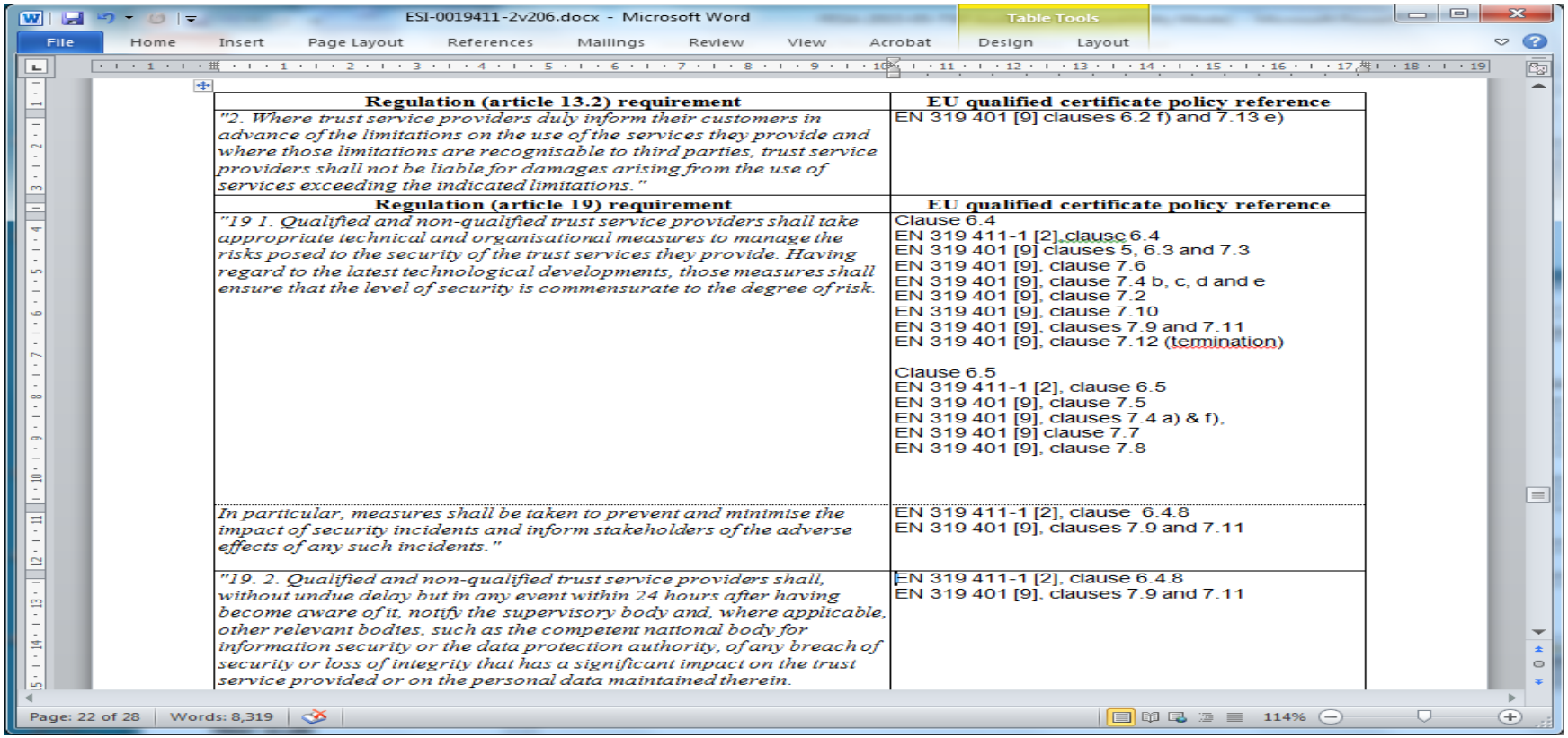
ETSI EN 319 411-2 Check List



ETSI EN 319 411-2 チェックリスト



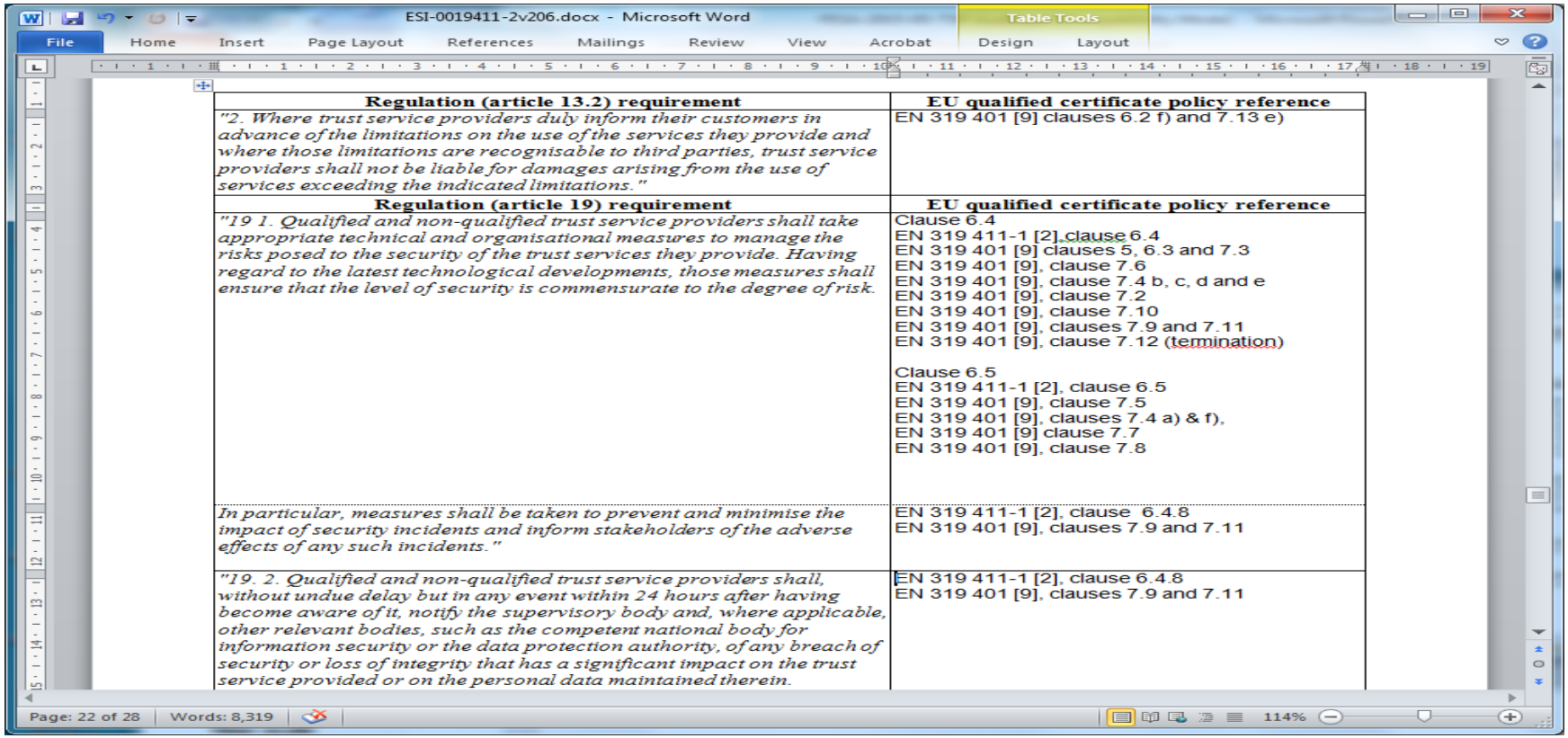
ETSI EN 319 411-2 Regulation Mapping



ESI-0019411-2v206.docx - Microsoft Word

Regulation (article 13.2) requirement	EU qualified certificate policy reference
"2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."	EN 319 401 [9] clauses 6.2 f) and 7.13 e)
Regulation (article 19) requirement	**EU qualified certificate policy reference**
"19 1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.	Clause 6.4 EN 319 411-1 [2] clause 6.4 EN 319 401 [9] clauses 5, 6.3 and 7.3 EN 319 401 [9], clause 7.6 EN 319 401 [9], clause 7.4 b, c, d and e EN 319 401 [9], clause 7.2 EN 319 401 [9], clause 7.10 EN 319 401 [9], clauses 7.9 and 7.11 EN 319 401 [9], clause 7.12 (termination) Clause 6.5 EN 319 411-1 [2], clause 6.5 EN 319 401 [9], clause 7.5 EN 319 401 [9], clauses 7.4 a) & f), EN 319 401 [9] clause 7.7 EN 319 401 [9], clause 7.8
In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."	EN 319 411-1 [2], clause 6.4.8 EN 319 401 [9], clauses 7.9 and 7.11
"19. 2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.	EN 319 411-1 [2], clause 6.4.8 EN 319 401 [9], clauses 7.9 and 7.11

ETSI EN 319 411-2 規則マッピング



Regulation (article 13.2) requirement	EU qualified certificate policy reference
"2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."	EN 319 401 [9] clauses 6.2 f) and 7.13 e)
Regulation (article 19) requirement	**EU qualified certificate policy reference**
"19 1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.	Clause 6.4 EN 319 411-1 [2] clause 6.4 EN 319 401 [9] clauses 5, 6.3 and 7.3 EN 319 401 [9], clause 7.6 EN 319 401 [9], clause 7.4 b, c, d and e EN 319 401 [9], clause 7.2 EN 319 401 [9], clause 7.10 EN 319 401 [9], clauses 7.9 and 7.11 EN 319 401 [9], clause 7.12 (termination) Clause 6.5 EN 319 411-1 [2], clause 6.5 EN 319 401 [9], clause 7.5 EN 319 401 [9], clauses 7.4 a) & f), EN 319 401 [9] clause 7.7 EN 319 401 [9], clause 7.8
In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."	EN 319 411-1 [2], clause 6.4.8 EN 319 401 [9], clauses 7.9 and 7.11
"19. 2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.	EN 319 411-1 [2], clause 6.4.8 EN 319 401 [9], clauses 7.9 and 7.11

ETSI Policies and CA/Browser-Forum Baseline Requirements:

8.4. TOPICS COVERED BY ASSESSMENT

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;

2. A national scheme that audits conformance to ETSI TS 102 042/ ETSI EN 319 411-1;

Or

3. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
(a) encompasses all requirements of one of the above schemes or
(b) consists of comparable criteria that are available for public review.

See: https://cabforum.org/baseline-requirements-documents/

ETSIポリシおよび CA/ブラウザフォーラム基本要件:

8.4評価対象事項
CAは次のスキームのいずれかに従って監査を行うこと[SHALL]。

1. WebTrust for Certification Authorities v2.0;

2. ETSI TS 102 042/ETSI EN 319 411-1の適合性を監査する国家スキーム;

もしくは
3. 証明書ポリシーによって、政府のCAが別の内部監査スキームを使用することが義務付けられている場合、以下の監査のいずれかに該当することを条件として、このようなスキームを使用することができる[MAY]。
(a) 上記スキームのうちいずれかの全要件を含む
(b) 国民審査を使用出来るのと同等の基準で構成されている

https://cabforum.org/baseline-requirements-documents/ 参照

ETSI Policies and Mozilla Policy:

3.1.2.2 ETSI

•For the SSL trust bit, a CA and all subordinate CAs technically capable of issuing server certificates must have one of the following audits:

- ETSI TS 102 042 (DVCP, OVCP, or PTC-BR)
- ETSI EN 319 411-1 (LCP and (DVCP or OVCP)) and/or (NCP and EVCP)
- ETSI EN 319 411-2 (QCP-w)

- For the email trust bit:
  - TSI TS 101 456
  - ETSI TS 102 042 (LCP, NCP, or NCP+)
  - ETSI EN 319 411-1 (LCP, NCP, or NCP+)
  - ETSI EN 319 411-2 (QCP-l, QCP-l-qscd, QCP-n, or QCP-n-qscd)

ETSI TS 102 042 and TS 101 456 audits are only acceptable for audit periods ending in July 2017 or earlier.

See: https://github.com/mozilla/pkipolicy/blob/master/rootstore/policy.md

ETSIポリシとMozillaポリシ:

3.1.2.2 ETSI

•SSLトラストビットについて、サーバ証明書の発行が技術的に可能であるCAおよびすべての下位CAは、次のうちいずれかによる監査を受けなければならない。

- ETSI TS 102 042 (DVCP、OVCP、またはPTC-BR)
- ETSI EN 319 411-1 (LCP および (DVCP または OVCP)) および/または(NCP および EVCP)
- ETSI EN 319 411-2 (QCP-w)

•Eメールトラストビットについては、次のうちのいずれかによる監査を受けなければならない。

- TSI TS 101 456
- ETSI TS 102 042 (LCP、NCP、またはNCP+)
- ETSI EN 319 411-1 (LCP、NCP、またはNCP+)
- ETSI EN 319 411-2 (QCP-l、QCP-l-qscd、QCP-n、またはQCP-n-qscd)

ETSI TS 102 042 およびTS 101 456 監査は、2017年7月末までに終了する場合についてのみ認められる。

https://github.com/mozilla/pkipolicy/blob/master/rootstore/policy.md 参照

Electronic Registered Delivery and Registered Electronic Mail

- Existing standards:
  - TS 102 640 (parts 1 to 6) Registered Electronic Mail
- Standards being developed
  - EN 319 522: Electronic Registered Delivery Services
  - EN 319 532: Registered Electronic Mail (REM) Services
  - **EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers**
  - **EN 319 531: Policy and security requirements for Registered Electronic Mail Service Providers**
  - TS 119 524: Testing Conformance and Interoperability of Electronic Registered Delivery Services
  - TS 119 534: Testing Conformance and Interoperability of Registered Electronic Mail Services
- Timescale
  - Stable draft of ENs for review: End Oct 2017
  - EN approval starts: End April 2018
  - ENs published : Feb 2019

電子登録デリバリおよび登録電子メール

- 現行の規格:
  - TS 102 640 (パート1から6)登録電子メール
- 策定中の規格
  - EN 319 522: 電子登録デリバリサービス
  - EN 319 532:登録電子メール(REM)サービス
  - **EN 319 521:電子登録デリバリサービスプロバイダのポリシーおよびセキュリティ要件**
  - **EN 319 531: 登録電子メールサービスプロバイダのポリシーおよびセキュリティ要件**
  - TS 119 524: 電子登録デリバリサービスの適合性および相互運用性試験
  - TS 119 534: 登録電子メールサービスの適合性および相互運用性試験
- タイムスケール
  - レビューのための基礎の定まった草案: 2017年10月末
  - EN認定開始: 2018年4月末
  - EN発行 : 2019年2月

Conclusions

- Information on available standards and current activities:
  https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

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

多くの感謝

Ōku no kansha

終わりに

- 利用可能な規格および現在の動向に関する情報：
  https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

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

多くの感謝

Ōku no kansha