委員会決定 2009/767/EC

[参考訳]

2018 年 12 月 16 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (2009/767/EC)（OJ L 274, 20.10.2009, p.36-37）のテキスト（英語版）に基づき、和訳を試みた。そのテキストは、下記の Eur-lex の Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0767&from=EN
[2018 年 12 月 4 日確認]

委員会決定 2009/767/EC は、サービス指令 2006/123/EC（OJ L 376, 27.12.2006, p.36-68）の細則の 1 つである。委員会決定 2009/767/EC は、主として、サービス指令 2006/123/EC に基づく行政手続の簡素化に伴う手続及び方式の整合化の一部としての電子認証事業者の信頼リストの統一に関する事項を定めている。これらの事項は、同委員会決定の別紙（ANNEX）の中で定められているが、委員会決定 2009/767/EC の最初に公示された版には別紙が欠けていたため、EU 官報（OJ L 299, 14.11.2009, p.18-54）により、同委員会決定の別紙を付加する訂正が行われている[1]。

委員会決定 2009/767/EC は、委員会決定 2010/425/EU（OJ L 199, 31.7.2010, p.30-35）、委員会実装決定 2013/662/EU（OJ L 306, 16.11.2013, p.21-39）及び委員会規則(EU) No 519/2013（OJ L 158, 10.6.2013, p.74-171）により、一部改正が行われている。

委員会決定 2009/767/EC は、前文、本文及び別紙の 3 つの部分で構成されている。この参考訳においては、前記 EU 官報による訂正後のテキストに基づき、委員会決定 2009/767/EC の前文、本文及び別紙の全文を訳した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

この参考訳は、あくまでも委員会決定 2009/767/EC の私的な和訳であり、関連分野の研究者のため

[1] 通常の法令データベース検索の結果では、EU 官報による訂正前のテキスト、すなわち、別紙が欠落した版のテキストのみが示される。これは、別紙の内容が電子証明の技術仕様を示すものであり、別紙それ自体が一般的なレベルの法律家にとっては読解不可能な内容であることに加え、別紙に記載された技術仕様の中にはやや機微の要素も含まれていることに鑑み、意図的に行われたものである可能性を否定できない。

の参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があるときは、随時、法と情報雑誌上においてその正誤を公表する。

この参考訳に訳注はない。脚注は、全て原注である。

委員会決定 2009/767/EC の第 I 章に定める信頼リスト（TL）のための共通テンプレートの詳細仕様は、ETSI TS 102 231 v3.1.1 に準拠している。

ETSI TS 102 231 v3.1.2 に準拠する信頼リストのための共通テンプレートの詳細仕様（別紙の第 I 章及び第 IV 章に関しては、差分のみ）は、委員会決定 2010/425/EU（SL L 199, 31.7.2010., p.30-35）によって定められている。

ETSI TS 119 612 v1.1.1 に準拠する信頼リストのための共通テンプレートの詳細仕様は、委員会実装決定 2013/662/EU（SL L 306, 16.11.2013., p.21-39）によって定められている。

ETSI TS 119 612 v2.1.1 に準拠する信頼リストのための共通テンプレートの詳細仕様は、委員会実装決定(EU) 2015/1505（OJ L 235, 9.9.2015, p.26-36）によって定められている。

W3C XML Signature specifications に準拠する信頼リストのための XML、CMS または PDF の高度電子署名の関連技術仕様は、委員会決定 2011/130/EU（SL L 53, 26.2.2011., p.66-72）によって定められている。同決定は、委員会実装決定 2014/148/EU（OJ L 80, 19.3.2014, p.7-9）によって一部改正されている。ETSI TS 119 612 v2.1.1 に準拠する信頼リストのための XML、CMS または PDF の高度電子署名の関連技術仕様は、委員会実装決定 (EU) 2015/1506（OJ L 235, 9.9.2015, p.37-41）によって定められている。

電子署名指令 1999/93/EC（OJ L 13, 19.1.2000, p.12-20）は、電子識別規則(EU) No 910/2014（OJ L 257, 28.8.2014, p.73-114）の第 50 条により、2016 年 6 月 30 日をもって廃止された。電子署名指令 1999/93/EC への参照は、電子識別規則(EU) No 910/2014 への参照として読み替えられる。

（この参考訳を作成するに際し考慮した事項）

委員会決定 2009/767/EC の別紙第 I 章の冒頭にある「要求される（REQUIRED）」は、RFC 2119 に準拠するものであるが、意味的には、「不可欠的ある」または「必須である」というニュアンスを含むものである。しかし、日本語の特性上、「REQUIRED」を同一の語で統一的に訳出することは、困難である。

そこで、この参考訳においては、文脈に応じて、「REQUIRED」を、「要求される」、「必須である」等と訳し分けることにした。

委員会決定 2009/767/EC の別紙第 I 章の冒頭にある「すべきである（SHOULD）」は、RFC 2119 に準拠するものであり、「しなければならない（MUST）」、「要求される（REQUIRED）」及び「する（SHALL）」とは異なるニュアンスをもつものとして使用されている。ところが、EU のほぼ全ての法令の前文（recital）の中では、「must」及び「shall」と同じ意味をもつものとして、ただし、単なる未来形ではなく命令的または義務的な要素を含む語であることを明示する趣旨で「should」が用いられている。これは、条文の

「shall」が単なる「will」ではなく、「ある法律要件が満たされるときは、ある法律効果が必ず発生する」という規範的な因果関係を包含するために生ずることである。しかし、法学の素養のない一般人が条文だけを読んだ場合、「shall」を単なる「will」と同義と誤解する危険性があるため、前文の中では、同じ条文を記述する場合であっても（意図的に）「shall」ではなく「should」が使用される。この場合の「should」の用法は、必ずしも、厳密な意味での RFC 2119 に準拠しているわけではない場合が含まれる（ただし、同一の法令の前文の中で「MUST」、「SHOULD」及び「REQUIRED」が明示で意識的に使い分けられているときは、細心の注意を払って読み解く必要性がある）。

以上を考慮に入れた上で、この参考訳においては、別紙第 I 章に限り、「SHOULD」を「すべきである」と訳すことにした。

なお、以上のような EU の法令における語法上の問題が明らかに存在することから、一般に、EU の法令を読むときは、必ず当該法令の前文も精読し、かつ、当該法令の本体と一体となっている別紙（ANNEX）、別添の独立の法律文書（附属書等）及び別添の独立の附属文書（別冊等）、当該法令の附属法令（細則等）及び関連法令、並びに、（法令によっては）当該法令の関連技術標準（EU の技術標準及び関連構成国の技術標準、並びに、これらと対応する国際的な技術標準または関連国際機関の勧告等）も精読した上で、総合的に検討することが求められる。

「legal entity」は、電子識別規則(EU) No 910/2014（OJ L 257, 28.8.2014, p.73-114）における「legal entity」の用例と同様、自然人（natural person）及び法人（legal person）の両者を含むものであり、要するに、法律上の権利及び義務の主体となる者のことを意味する。

この参考訳においては、「legal entity」を「法主体」と訳すことにした。

電子署名指令 1999/93/EC の法的枠組みの下においては、「scheme」は、電子署名の仕様や関連制度の監督または認定のための行政制度のことを指す。電子署名指令 1999/93/EC の改正法令である電子識別規則 (EU) No 910/2014 においては、行政上の枠組みだけではなく技術的な枠組みを含めて「scheme」が用いられているので、「scheme」が異なる意味で用いられていることになる。

そこで、電子識別規則 (EU) No 910/2014 及び関連法令の参考訳においては「scheme」を「スキーム」とカタカナ表記することにしたけれども、委員会決定 2009/767/EC の参考訳（この参考訳）を含め、電子署名指令 1999/93/EC 及びその関連法令の参考訳においては、「scheme」を「制度」と訳すことにした。

「Secure Signature Creation Device」は、電子署名指令 1999/93/EC の別紙 III において定められている「device」のことを指すが、これは、公開鍵暗号システムで使用される 1 対の公開鍵及び秘密鍵を（乱数発生アルゴリズム等を用いて）生成するためのシステムのことを指し、物体としての機器であることを要しない。すなわち、現実の存在形態としては、電子署名のための認証局に設置されたコンピュータシステム内で稼働する鍵生成モジュールであるソフトウェア及び生成した鍵のデータを保存するデータベースの形態をとることが予定されている。この場合の「device」の用法は、欧州評議会のサイバー犯罪条約（ETS No.185）における「違法な機器（illegal device）」が、その定義からも明確であるように、物体としての機械装置だけではなく、ソフトウェア及びデータを含むということと同じである。

以上を踏まえた上で、この参考訳においては、「Secure Signature Creation Device」を「安全な署名生成機器」と訳すことにした。

「qualifiers」は、一般用語としては、「限定子」等と訳されている。この参考訳においては、「qualifiers」を「適格子」と訳すことにした。

委員会決定 2009/767/EC の中には、上述の EU 官報により修正された部分以外にも誤記の一種と推定される箇所が散見されるが、その大部分は、委員会決定 2010/425/EU の別紙（ANNEX）によって修正されているので、この参考訳においては、委員会決定 2010/425/EU による修正前の原文のままの直訳とすることにした。

以上のほかは、後掲サービス指令 2006/123/EC、後掲電子識別規則(EU) No 910/2014 の参考訳及び後掲 IMI 規則(EU) No 1024/2012 の参考訳の各冒頭部分において述べたとおりである。

（訳出済みの関連法令等及び参考文献）

サービス指令 2006/123/EC の参考訳は、法と情報雑誌 3 巻 12 号 1～56 頁にある。委員会決定 2009/739/EC の参考訳は、法と情報雑誌 3 巻 12 号 57～62 頁にある。委員会決定 2010/425/EU の参考訳は、法と情報雑誌 3 巻 12 号 116～125 頁にある。委員会実装決定 2013/662/EU の参考訳は、法と情報雑誌 3 巻 12 号 126～152 頁にある。電子識別規則(EU) No 910/2014 の参考訳は、法と情報雑誌 2 巻 10 号 147～196 頁にある。委員会実装決定(EU) 2015/1505 の参考訳・改訂版は、法と情報雑誌 3 巻 12 号 151～224 頁にある。委員会実装決定(EU) 2015/1506 の参考訳・改訂版は、法と情報雑誌 3 巻 12 号 187～194 頁にある

IMI 規則(EU) No 1024/2012 の参考訳は、法と情報雑誌 2 巻 9 号 93～114 頁にある。IMI 委員会決定 2008/49/EC の参考訳は、法と情報雑誌 2 巻 9 号 93～114 頁にある。

規則 (EU) 2016/679（一般データ保護規則）の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。個人データ保護指令 95/46/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 332～365 頁にある。指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 頁にある。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記の各文献等のほか、経済産業省「平成 27 年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））調査報告書」（平成 28 年 3 月 25 日）、社団法人日本ネットワークインフォメーションセンター（JPNIC）「電子認証フレームワークのあり方に関する調査報告書」（2006 年 3 月）、株式会社 NTT データ経営研究所「平成 26 年度内外一体の経済成長戦略構築のための国際経済事業：先進的電子商取引章規律のための調査」（2015 年 2 月）、西原啓輔・宮川寧夫訳「MD5 メッセージダイジェストアルゴリズム (The MD5 Message-Digest Algorithm)」（1992 年 4 月）、宮川寧夫訳「インターネット X.509 PKI - 証明書と CRL のプロファイル（Internet X.509 Public Key Infrastructure Certificate and CRL Profile）」（1999 年 1 月）、日本情報処理開発協会（JIPDEC）電子署名・認証センター「電子署名・認証関連 用語・技術標準集 Ver.1.3」（2007 年 3 月）、橋本英彦訳「Uniform Resource Identifier (URI): 一般的構文」（2005 年 1 月）を参考にした。

＊＊＊

域内市場のサービスに関する欧州議会及び理事会の指令 2006/123/EC に基づく「連絡部局」を介する電子的な手段による手続の利用を容易にする措置を定める 2009 年 10 月 16 日の委員会決定 2009/767/EC
（文書 C(2009)7806 の下で通知された）

欧州共同体の委員会は、
欧州共同体設立条約に鑑み、
域内市場のサービスに関する欧州議会及び理事会の 2006 年 12 月 12 日の指令 2006/123/EC[1]、とりわけ、その第 8 条第 3 項に鑑み、

以下のとおりであるので、この決定を採択する:

(1) 指令 2006/123/EC の第 2 章において、とりわけ、その第 5 条及び第 8 条において、構成国に対して課せられる行政上の簡素化の義務は、サービス活動へのアクセス及びその実施に適用される手続及び方式の簡素化の義務、並びに、それらの手続及び方式が、隔地者間において、電子的な手段により、「連絡部局」を介して、サービスプロバイダによって容易に完了され得ることを確保する義務を含む。
(2) 「連絡部局」を介する手続及び方式を完了することは、指令 2006/123/EC の第 8 条に定めるように、構成国間の国境を越えて可能なものでなければならない。
(3) 手続及び方式を簡素化する義務を遵守するため、及び、「連絡部局」の国境を越える利用を容易なものとするため、電子的な手段による手続は、電子署名の利用に関するものを含め、単純なソリューションに準拠するものでなければならない。具体的な手続及び方式の適切なリスク評価の後、高いレベルの安全性、または、手書きの署名と均等な安全性が必要であると判断される場合、一定の手続及び方式に関し、サービスプロバイダから、安全な署名生成機器による適格証明書またはその機器なしの適格証明書を基礎とする高度電子署名が要求され得る。
(4) 電子署名に関する欧州共同体の枠組みは、電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 12 月 13 日の指令 1999/93/EC[2]の中で構築された。適格証明書を基礎とする高度電子署名の効果的な国境を越える利用を容易にするため、これらの電子署名への信頼は、署名サービスプロバイダまたはその適格証明書を発行する認証サービスプロバイダが設けられている構成国がどこであるかに拘らず、拡大されなければならない。これは、電子署名を検証するために必要な情報を、とりわけ、構成国内において監督／認定される認証サービスプロバイダに関する情報及びそれらのプロバイダが提供するサービスに関する情報を、信頼性のある方式により、より容易に利用可能にすることによって、達成され得る。
(5) 構成国が、その利用を容易にするため、共通のテンプレートを通じてその情報を公衆が利用可能にすることを確保し、また、受け手側が電子署名を検証できるようにする適正なレベルの詳細さを確保する必要がある。

[1] OJ L 376, 27.12.2006, p.36.
[2] OJ L 13, 19.1.2000, p.12.

第 1 条　電子署名の利用及び承認

1. 含まれるリスクの適切な評価を基礎として、かつ、指令 2006/123/EC の第 5 条第 1 項及び第 3 項に従って正当化されるときは、構成国は、指令 2006/123/EC の第 8 条に基づく連絡部局を介する一定の手続及び方式の完了のために、サービスプロバイダによる、指令 1999/93/EC によって定義され、定められているとおり、安全な署名生成機器による適格証明書またはその機器なしの適格証明書に基礎とする高度電子署名の利用を要求できる。
2. 構成国は、それが第 1 項に示すリスク評価に従うものである場合、適格証明書を基礎とし、かつ、安全な署名生成機器によって生成される高度電子署名に対するこの承認を構成国が制限し得ることを妨げることなく、第 1 項に示す手続及び方式の完了のために、安全な署名生成機器による適格証明書またはその機器なしの適格証明書を基礎とする高度電子署名を承認する。
3. 構成国は、安全な署名生成機器による適格証明書またはその機器なしの適格証明書を基礎とする高度電子署名の承認を、連絡部局を介する一定の手続及び方式のサービスプロバイダによる利用を妨げる障碍をつくり出す要件に服させてはならない。
4. 第 2 項は、構成国が、安全な署名生成機器による適格証明書またはその機器なしの適格証明書を基礎とする高度電子署名以外の電子署名を承認することを妨げない。

第 2 条　信頼リストの作成、維持管理及び公表

1. 各構成国は、別紙に定める技術仕様に従い、公衆に対して適格証明書を発行し、その構成国によって監督／認定される認証サービスプロバイダと関連するミニマムの情報を含める「信頼リスト」を作成し、維持管理し、かつ、公表する。
2. 構成国は、別紙に定める仕様に従い、ミニマムのものとして、人間が読取可能な方式の信頼リストを作成し、かつ、公表する。
3. 構成国は、欧州委員会に対し、信頼リストの作成、維持管理及び公表について職責を負う組織、その信頼リストが公表される場所、並びに、それらの変更を通知する。

第 3 条　適用

この決定は、2009 年 12 月 28 日から適用する。

第 4 条　発出

この決定は、構成国に対して発出される。

2009 年 10 月 16 日にブリュッセルにおいて行われた。

欧州委員会として
委員会委員　Charlie McCreevy

別 紙

「監督／認定される認証サービスプロバイダの信頼リスト」のための共通テンプレートに関する技術仕様

序 文

1. 総 説

構成国の「監督／認定される認証サービスプロバイダの信頼リスト」のための共通テンプレートの目的は、指令 1999/93/EC の関連条項を遵守するために、その構成国によって監督／認定される認証サービスプロバイダ [1]（CSP）による認証サービスの監督／認定ステータスに関して、各構成国から提供される情報の共通の方法を確立することにある。これは、監督／認定される認証サービスの監督／認定ステータスに関する履歴情報の提供を含む。

信頼リスト（TL）中の必須情報は、指令 1999/93/EC に定める条項（第 3 条第 3 項、第 3 条第 2 項及び第 7 条第 1 項(a)）に従い、電子署名を支える QC 上の情報を含め、かつ、その署名が安全な署名生成機器（SSCD）[2]によって生成されるものであるか否かを問わず、適格証明書（QC）[3]を発行する監督／認定される CSP に関するミニマムの情報を含める。

QC を発行するわけではないが、電子署名と関連するサービスを提供する上記以外の監督／認定される CSP（例：タイムスタンプサービスを提供する CSP 及びタイムスタンプトークンを発行する CSP、非適格証明書を発行する CSP 等）に関する追加情報は、任意に、国内レベルで、信頼リストの中に含められ得る。

この情報提供は、基本的に、適格電子署名（QES）及び適格証明書によって支えられた高度電子署名（AdES）[4]を支援することを狙いとしている [5][6]。

共通テンプレート案は、そのような種類のリストの作成、発行、所在、アクセス、真正性及び信頼性に対処するために使用される ETSI TS 102 231[7]の仕様を基礎とする実装と互換性がある。

---

[1] 指令 1999/93/EC の第 2 条(11)に定義するとおり。
[2] 指令 1999/93/EC の第 2 条(6)に定義するとおり。
[3] 指令 1999/93/EC の第 2 条(10)に定義するとおり。
[4] 指令 1999/93/EC の第 2 条(2)に定義するとおり。
[5] QC によって支えられた AdES に関し、現行の文書全体を通じて、「$AsES_{QC}$」との略語が用いられる。
[6] 支援する認証サービス（例：非適格証明書の発行）が、その構成国の任意情報部分中の構成国によってカバーされる監督／認定されるサービスの一部であることを条件として、その国境を越える利用が促進され得る単純な AdES を基礎とする多数の電子サービスが存在することに留意すべきである。
[7] ETSI TS 102 231 - 電子署名及びインフラ（ESI）：整合化された信頼サービスステータス情報の提供。

2. TL 内のエントリの編集に関する運用指針

2.1. *監督／認定される認証サービスに的を絞った TL*

単一リスト中の関連認証サービス及び認証サービスプロバイダ

構成国の信頼リストは、「指令 1999/93/EC の関連条項を遵守するために、被参照構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスのリスト」として定義される。

そのようなリストは、以下のものを含めなければならない：

- 指令 1999/93/EC の第 2 条(11)に定義する全ての認証サービスプロバイダ、すなわち、「証明書を発行し、または、それ以外の電子署名と関連するサービスを提供する組織または法人もしくは自然人」；
- 指令 1999/93/EC に定める関連条項の遵守に関し監督／認定されるサービスプロバイダ。

とりわけ、関連 CSP 及びその構成国の監督／任意の認定制度に関し、指令 1999/93/EC に定める定義及び条項を検討する際、2 セットの CSP が区別され得る。すなわち、公衆に対して QC を発行する CSP（CSP_{QC}）、及び、公衆に対して QC を発行しないが、「電子署名と関連するその他の（付随的な）サービス」を提供する CSP である：

- **QC 発行 CSP**：
  - それらの CSP は、別紙 I の要件（QC に関する要件）及び別紙 II の要件（QC 発行 CSP の要件）を含め、指令 1999/93/EC に定める条項の遵守に関し、（それらの CSP が構成国内に設けられているときは）それらの CSP が設けられている構成国によって監督されなければならず、また、認定を受けることもできる。構成国において認定を受けている QC 発行 CSP は、その CSP が当該構成国内に設けられていない場合を除き、当該構成国の適切な監督制度の下にあるものとしなければならない。
  - 適用される「監督」制度（それぞれ該当する場合、「任意の認定」制度）は、定義され、かつ、指令 1999/93/EC の関連する要件、とりわけ、第 3 条第 3 項、第 8 条第 1 項、第 11 条、前文(13)（それぞれ該当するときは、第 2 条(13)、第 3 条第 2 項、第 7 条第 1 項(a)、第 8 条第 1 項、第 11 条、前文(4)～(11～13)）に定める要件に適合しなければならない。
- **QC 非発行 CSP**：
  - それらの CSP は、（指令 1999/93/EC の中に定義され、かつ、それを遵守する）「任意の認定」制度の下にあるものとすることができ、及びまたは、その指令に定める条項及び（指令 1999/93/EC の第 2 条(11)の意味における）認証サービスの提供と関連する可能的な国内条項の遵守の監督のために、国内的に実装され、国内的に定義された「承認された認定制度」の下にあるものとすることができる。
  - 認証サービスの結果として生成または発行される幾つかの物理オブジェクトまたはバイナリ（論理）オブジェクトは、国内レベルで定められる条項及び要件をそれらが遵守することを基礎として、個別の「適格」を受けることができるが、そのような意味における「適格」は、国内レベルのみに限定され得る。

構成国の信頼リストは、指令 1999/93/EC に定める条項（第 3 条第 3 項、第 3 条第 2 項及び第 7 条第

1 項(a)）に従い、公衆に対して適格証明書を発行する監督／認定される CSP に関するミニマムの情報、その電子署名を支える QC に関する情報、及び、その署名が安全な署名生成機器によって生成されるものであるか否かの情報を提供しなければならない。

公衆に対して QC 非発行 CSP（例：タイムスタンプサービス及びタイムスタンプトークンを提供する CSP、非適格証明書を発行する CSP 等）による上記以外の監督／認定されるサービスに関する追加情報は、任意に、国内レベルで、信頼リストの中に含めることができる。

信頼リストは、以下を狙いとする：

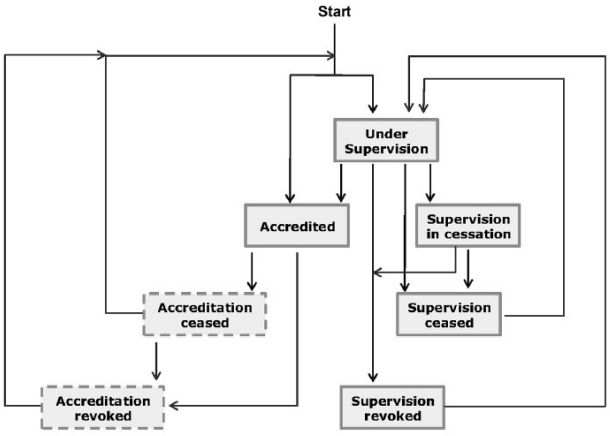
- 指令 1999/93/EC に定める関連条項の遵守に関するリストを作成及び維持管理することに職責を負う構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスに関する信頼できる情報のリスト及び提供；
- リストされた CSP によるリストされた監督／認定される認証サービスにより支えられた電子署名の検証を容易にすること。

単一のセットの監督／認定ステータスの値

構成国毎に、その構成国によって監督／認定される CSP による認証サービスの監督ステータス及びまたは認定ステータスを示す 1 個の単一 TL が作成され、維持管理されなければならない。

サービスが現に監督または認定されているという事実は、その現在のステータスの一部である。それに加え、監督ステータスまたは認定ステータスは、「継続（ongoing）」、「停止（in cessation）」、「終了（ceased）」または「取消（revoked）」とすることができる。そのライフタイムを通じて、同じ認証サービスは、監督ステータスから認定ステータスへ、及び、その逆へと遷移可能である[1]。

以下の図 1 は単一の認証サービスの可能的な監督／認定ステータスの間の予想される流れを示す。



[1] 構成国内に設けられ、当初は構成国（監督機関）により監督される認証サービスを提供する認証サービスプロバイダは、一定期間経過後、現行の監督される認証サービスに関して任意の認定を受けることを決定できる。その反対に、別の構成国内の認証サービスプロバイダは、認定される認証サービスを停止しないが、例えば、事業遂行上の理由及びまたは経済的な理由により、認定ステータスから監督ステータスに遷移することを決定できる。

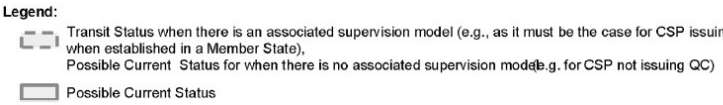


図 1：単一の CSP サービスの予想される監督／認定ステータスの流れ

QC を発行する認証サービスは、（構成国内に設けられているときは）監督を受けなければならず、また、任意の認定を受けることができる。信頼リストの中にリストされる際のそのようなサービスのステータスの値は、「current status value」として上記に示したステータス値のいずれかをもち得る。ただし、「認定終了（Accreditation ceased）」及び「認定取消（Accreditation revoked）」の両者は、そのようなサービスが（認定されていない場合、または、認定されなくなった場合においても）デフォルトで監督を受けなければならないことから、構成国内に設けられている CSPQC の場合に限り、「遷移ステータス」の値ももつものとしなければならない、という点に留意すべきである。

QC 非発行 CSP によるサービスによる指令 1999/93/EC に定める条項の遵守及び（指令の第 2 条(11)の意味における）認証サービスの提供と関連する可能的な国内条項の遵守の監督のために国内的に実装され、国内的に定義された「承認された認定制度」を設けている構成国またはそれを設けた構成国は、そのような認定制度を、以下の 2 つの類型に基づき分類することを要する：

- 指令 1999/93/EC（第 2 条(13)、第 3 条第 2 項、第 7 条第 1 項(a)、第 8 条第 1 項、第 11 条、前文(4)～((11)～(13))）の中で定義され、規制される「任意の認定」；
- 指令 1999/93/EC の中で要求され、かつ、国内条項及び国内法による要件によって実装される「監督」。

従って、QC を発行しない認証サービスは、監督され、または、任意の認定を受け得ることになる。信頼リストの中にリストされる際のそのようなサービスのステータスの値は、「current status value」として上記に示したステータス値のいずれかをもち得る（図 1 参照）。

信頼リストは、基礎となっている監督／認定制度に関する情報、とりわけ、以下の情報を含めるものとしなければならない：

- CSP_{QC} に適用される監督制度に関する情報；
- 該当するときは、CSP_{QC} に適用される国内「任意の認定」制度に関する情報；
- 該当するときは、QC 非発行 CSP に適用される監督制度に関する情報；
- 該当するときは、QC 非発行 CSP に適用される国内「任意の認定」制度に関する情報。

最後の 2 つのセットの情報は、QC 非発行 CSP に対して国内レベルで適用される監督／認定制度の品質及び安全性のレベルを評価するために依拠者にとって、特に重要な情報である。QC 非発行 CSP によるサービスに関し、TL の中で監督／認定ステータスの情報が提供される場合、上述の 2 つのセットの情報は、「Scheme information URI」（5.3.7 節－構成国から提供される情報）、「Scheme type/community/rules」（5.3.9 節－全ての構成国に共通のテキストの利用を通じて、及び、構成国から提供される選択的な個別情報）、並びに、「TSL policy/legal notice」（5.3.11 節－指令 1999/93/EC に示す全ての構成国に共通のテキスト。各構成国は、構成国固有のテキスト／参照を付加できる。）において提供される。QC 非発行 CSP のための国内監督／認定制度のレベルで定義される付加的な「適格性」情報は、（例えば、複数の品質／安全性レベルを区別するために）それに該当し、かつ、それが要求されるときは、「Service information extension」（5.5.9 節）の一部として、「additionalServiceInformation」エク

ステンション（5.8.2 節）の使用を通じて、そのサービスのレベルで提供され得る。対応する技術仕様に関する別の情報は、第 I 章の詳細仕様の中で提供される。

構成国の別の組織が当該構成国内の認証サービスの監督及び認定に従事し得ることがあるとしても、1 個の単独認証サービスに対しては、（ETSI TS 102 231[1]によるそのサービスの「Service digital identity」によって識別される）1 個のエントリのみが使用されること、及び、その監督／認定ステータスがしかるべくアップデートされることが望ましい。上記に示したステータスの意味は、第 I 章の詳細技術仕様の 5.5.4 節との関係において示される。

2.2. *QES 及び $AdES_{QC}$ の検証を容易にすることを狙いとする TL エントリ*

個々のそのような QC を発行する認証サービスの確実な発行状況を正確に反映するため、及び、（このエントリの中にリストされる認証サービスを基礎として CSP から発行されるエンドエンティティ QC の内容と組み合わされる場合）個々のエントリの中で提供される情報が、QES 及び $AdES_{QC}$ の検証を容易にするために十分なものであることを確保するため、TL をつくる上での最も重要な部分は、TL の必須の部分、すなわち、QC 発行 CSP 毎の「サービスのリスト」の作成である。

QC のための真に相互運用可能で国境を越えるプロファイルが存在しない限り、要求される情報は、単一（Root）CA の「Service digital identity」以外の情報、とりわけ、発行された証明書の QC の状態を識別する情報、及び、サポート署名が SSCD によって作成されたか否かの情報を含め得る。それゆえ、TL を作成、編集及び維持管理するために指定される構成国内の機関（すなわち、ETSI TS 102 231 による制度運営者）は、その TL に含まれる CSP_{QC} 毎に、発行された個々の QC 内にある現在のプロファイル及び証明内容を考慮に入れなければならない。

観念的には、発行された個々の QC は、それが QC であると宣言する場合、ETSI が定義する QcCompliance[2]文を含めなければならず、また、それが電子署名を生成するための SSCD により支えられていることを宣言する場合、及びまたは、ETSI TS 101 456[3]に定義する QCP/QCP + certificate policy Object Identifiers (OIDs)のいずれかを発行された個々の QC が含めていることを宣言する場合、ETSI が定義する QcSSCD 文を含めなければならない。QC 発行 CSP によって、参照として異なる基準が使用されていること、それらの基準の解釈に幅があること、並びに、幾つかの規範的な技術仕様または技術標準の存在及び優先順位の認識が欠落していることは、現在発行されている QC の実際の内容に相違（例：ETSI によって定義された QcStatements の使用または不使用）をもたらしてきたし、また、その結果として、電子署名を支える証明書が QC であると宣言されているか否かと拘りなく、かつ、その電子署名が生成された SSCD と関係するか否かと拘りなく、少なくとも機械読取可能な態様で、その受領者が、署名者の証明書（及び関係する連鎖／パス）に単純に準拠することを妨げている。

「Service type identifier」（Sti）フィールド、「Service name」（Sn）フィールド及び「Service digital identity」（Sdi）フィールドを「Service information extension」（Sie）フィールド内で提供される情報で埋めることは、TL 共通テンプレート案が、リストされた QC 発行 CSP 認証サービスから発行された特定のタイプの適

[1] ETSI TS 102 231－電子署名及びインフラ（ESI）：整合化された信頼サービスステータス情報の提供

[2] ETSI TS 101 862－電子署名及びインフラ（ESI）：適格認証プロファイル参照。

[3] ETSI TS 101 456－電子署名及びインフラ（ESI）：適格証明書を発行する認証局に関するポリシーの要求事項

格証明書を完全に決定できるようにし、また、（そのような情報が発行された QC の中から失われた場合において）それが SSCD によって支えられているか否かに関する情報を提供できるようにする。個々の「Service current status」（Scs）の情報は、無論、このエントリと関係している。このことは、後掲の図 2 の中で示される。

（Root）CA の「Sdi」を正確に提供することによりサービスをリストすることは、それが QC であるか否か、及び、それが SSCD によって支えられているか否かを評価するための ETSI が定義した機械処理可能な十分な情報を、この（Root）CA（階層構造）に基づいて発行されたエンドエンティティ証明書が含んでいることが（QC 発行 CSP によっても、その CSP を監督／認定を遂行する監督／認定機関によっても）確保されているということを意味し得る。例えば、後者の確認が真ではない場合（例：その QC の中に、SSCD によって支えられているか否かに関する ETSI 標準の機械処理可能な表示が存在しない場合）、当該（Root）CA の「Sdi」をリストすることだけでは、その（Root）CA 階層構造の下で発行された QC が SSCD によって支えられていないということが推定され得るのみである。その QC が SSCD によって支えられていると判断するためには、そのことを表示するために「Sie」が使用されなければならない（これは、それが QC 発行 CSP によって保証されていること、及び、それぞれ該当する監督機関または認定機関によって監督／認定されていることも表示する）。

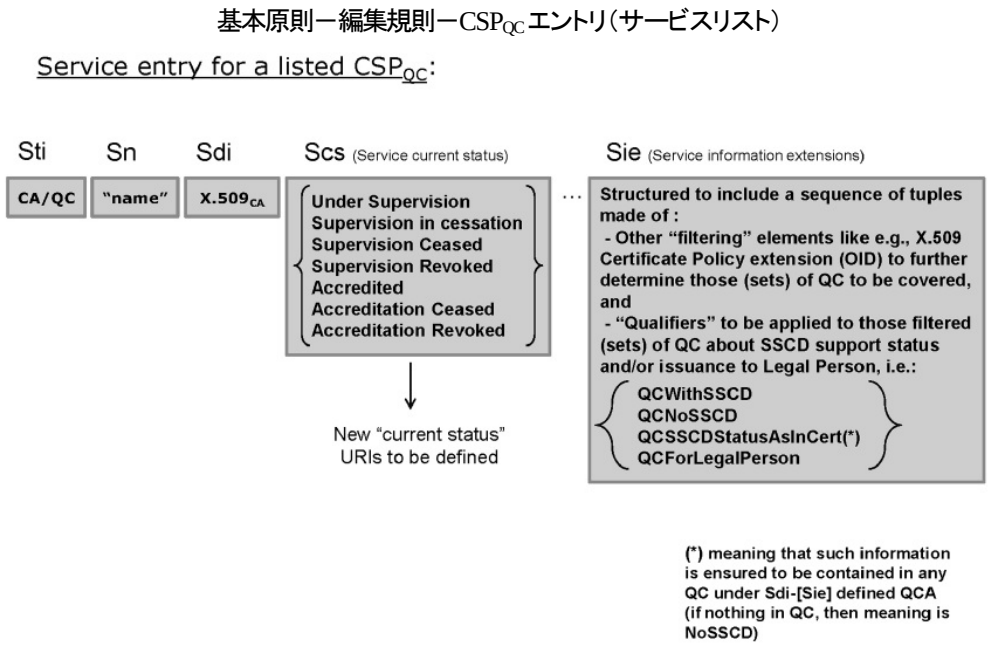


図 2：TSL フォーマットの中に実装されるリストされる QC 発行 CSP の TL へのサービスエントリ

現行の TL 共通テンプレート技術仕様は、サービスエントリ内の情報の 5 つの主要な部分の組み合わせを使用できるようにする：

－ 「Service type identifier」（Sti）、例：QC 発行 CA（CA/QC）の識別、

－ 「Service name」（Sn）、

- リストされるサービスを識別する「Service digital identity」（Sdi）情報、例:（ミニマムのものとして）QC 発行 CA の X.509v3 証明書、
- CA/QC サービスに関し、個々のタプルが以下の情報を提供する 1 または複数のタプルの列を含めることを許容する選択的な「Service information extension」（Sie）情報:
  - 「Sdi」によって識別される認証サービスを基礎として、当該サービスの詳細（すなわち、適格証明書のセット）を更に識別（フィルタ）するために使用され、そのために、SSCD サポートの表示と関連する追加情報が要求／提供される基準; 並びに、
  - この更に識別されるサービス（適格証明書のセット）が SSCD によって支えられているか否かに関する関連情報（適格子）、または、この関連情報が、標準化された機械処理可能な方式の下で QC の一部となっているか否か、及びまたは、そのような QC が法人宛に発行されていることに関する情報（デフォルトとして、それらの QC は、自然人に対してのみ発行されているものと判断される。）;
- 以下に関する情報提供するこのサービスのエントリに関する「current status」情報:
  - それが監督または認定されるサービスであるか否か、及び、
  - 監督／認定ステータスそれ自体。

2.3. *CSP_{QC} サービスエントリのための編集及び利用の運用指針*

一般的な編集運用指針は、以下のとおりである:

1. 「Sdi」によって識別されるリストされたサービスに関し、SSCD によって支えられた QC が ETSI 定義の QcCompliance 文を含めていること、及び、QcSSCD 文及びまたは QCP+ Object Identifier（OID）を含めていることが確保されているときは（CSP_{QC} から提供され、監督機関（SB）／認定機関（AB）によって監督／認定される保証）、適切な「Sdi」の使用が満たされており、「Sie」フィールドをオプションとして使用でき、かつ、SSCD サポート情報を含める必要がない。
2. 「Sdi」によって識別されるリストされたサービスに関し、SSCD によって支えられていない QC が QcCompliance 文及びまたは QCP OID のいずれかを含めていること、及び、そのことが、QcSSCD 文及びまたは QCP+OID を含めていることを意味しないことが確保されているときは（CSP_{QC} から提供され、SB/AB によって監督／認定される保証）、適切な「Sdi」の使用が満たされており、「Sie」フィールドをオプションとして使用でき、かつ、SSCD サポート情報を含める必要がない（SSCD により支えられていることを意味しない）。
3. 「Sdi」によって識別されるリストされたサービスに関し、QC が QcCompliance 文を含めていること、及び、それらの QC の幾つかが SSD によるサポートを意味するけれども、他の QC はそうではなく（このことは、例えば、異なる CSP specific Certificate Policy OID により、または、それ以外の QC 内にある CSP 個別情報により、直接または間接に、機械処理可能または不能により区別され得る。）、いかなる QcSSCD 文も ETSI QCP(+)OID も含んでいないことが確保されているときは（CSP_{QC} から提供され、SB/AB によって監督／認定される保証）、適切な「Sdi」の使用が満たされているとは言えず、かつ、その「Sie」フィールドは、含まれる証明書のセットを識別する可能的な情報エクステンションと共に、明示の SSCD サポート情報を表示して使用されなければならない。

これは、「Sie」フィールドを使用する際、同じ「Sie」に異なる「SSCD support information values」を含めることを要求するためである。

4. 「Sdi」によって識別されるリストされたサービスに関し、QC が QcCompliance 文、QCP OID、QcSSCD 文及びまたは QCP+OID のいずれをも含めていないことが確保されているが（CSP_{QC}から提供され、SB/AB によって監督／認定される保証）、この「Sdi」を基礎として発行されたエンドエンティティ証明書の幾つかが、QC であること、及びまたは、SSCD サポートを意味するけれども、幾つかの証明書はそうではないこと（このことは、例えば、異なる CSPQC specific Certificate Policy OID により、または、それ以外の QC 内にある CSPQC 個別情報により、直接または間接に、機械処理可能または不能により区別され得る。）が確保されているときは、適切な「Sdi」の使用が満たされているとは言えず、かつ、その「Sie」フィールドは、明示の SSCD サポート情報を表示して使用されなければならない。これは、「Sie」フィールドを使用する際、同じ「Sie」に異なる「SSCD サポート情報の値」を含めることを要求するためである。

デフォルトの一般原則として、信頼リスト中のリストされた CSP に関し、CA/QC タイプ認証サービス、すなわち、QC を（直接に）発行する認証局に関し、単独 X.509v3 証明書毎に 1 つのサービスエントリが存在しなければならない。注意深く想定された状況及び注意深く管理された条件の下において、構成国の監督機関／認定機関は、RootCA または上位 CA（すなわち、エンドエンティティ QC を直接に発行しないが、QC 発行 CA からエンドエンティティに至る CA の階層構造を証明する認証局）の X.509v3 証明書を、リストされた CSP によるサービスのリスト中で単独エントリの Sdi として使用することを決定できる。そのような X.509v3RootCA または上位 CA を TL サービスエントリの Sdi 値として使用することによる結果（利益及び不利益）は、構成国により、注意深く検討され、かつ、是認されなければならない。更に、デフォルトの基本原則のこの是認された例外処理を使用する場合、構成国は、パス構築の証明及び検証を容易にするために必要な文書を提供しなければならない。

一般的な編集運用指針を表現するため、以下の例が与えられる：すなわち、それに基づいて複数の CA が適格証明書及び非適格証明書を発行するが、それに関する QC が QcCompliance 文のみを含んでおり、それが SSCD により支えられているか否かを何ら表示していない 1 つの RootCA を使用する CSP_{QC} という文脈において、RootCA を「Sdi」にリストすることは、上記に説明したルールに基づき、この RootCA の階層構造を基礎として発行された全ての QC が SSCD によって支えられていないということのみを意味し得る。それらの QC が実際に SSCD によって支えられているときは、将来発行される QC の中で QcSSCD 文を使用することが強く推奨される。その間（この情報を含めていない最後の QC が失効するまでの間）、その TSL は、例えば、（幾つかのものは SSCD により支えられているが、幾つかのものはそうではない）異なるタイプの QC を区別するために CSP_{QC} によって使用される可能性のある特定の CSP_{QC} が定義する OID により証明書をフィルタし、「適格子」の使用によりフィルタされた証明書に関する明示の「SSCD support information」を含めるような、Sie フィールド及び関係適格性エクステンションを使用すべきである。

現行の技術仕様による信頼リストの TSL 実装に準拠する電子署名のアプリケーション、サービスまたは製品に関する**一般的な利用運用指針**は、以下のとおりである：

「CA/QC」「Sti」エントリ（同様に、「Sie」additionalServiceInformation extension の使用により RootCA/QC

であるとして更に適格化される CA/QC エントリ）は、

- 適切な QcStatements 文（すなわち、QcC、QcSSCD）及びまたは、ETSI 定義の QCP(+) OID の使用により、その証明書の中でそのように宣言されていること（及び、このことが監督／認定機関によって確保されること、上述の「一般的な編集運用指針」参照）を**条件として**、「Sdi」で識別される CA から（同様に、「Sdi」で識別される RootCA から始まる CA の階層構造内において）発行された全てのエンドエンティティ証明書が QC であることを表示し、
  注記:「Sie」「Qualification information」が全く存在しない場合、または、QC であると宣言するエンドエンティティ証明書が、関連「Sie」エントリによって「更に識別され」ない場合、QC の中でみつけられる「機械読取可能な」情報は、正確なものであるべきことが監督／認定されることとなる。このことは、適切な QcStatements（すなわち、QcC、QcSSCD）及びまたは ETSI 定義の QCP(+) OID の使用（または不使用）が、CSP_{QC} によって宣言されるところに従って確保されることを意味する。
- **かつ**、「Sie」「Qualification」情報が存在する場合、上述のデフォルトの利用方法解釈ルールに加え、証明書のセットを更に識別する「フィルタ」の列の基本原則に基づいて構築され、「SSCD サポート」及びまたは「主体としての法人」と関連する幾つかの追加情報を提供する「Sie」「Qualification」エントリの使用により識別される証明書（例：Certificate Policy extension 中の特定の OID を含む証明書、及びまたは、特定の「鍵利用方法」パターンをもつ証明書、及びまたは、特定のフィールドもしくはエクステンションの中で表示される特定の値の使用によってフィルタされる証明書等）は、対応する QC の内容中に情報が欠けている場合を埋める以下のセットの「適格子」に従って判断されなければならない。すなわち：
- SSCD サポートを表示するため：
  - 「QCWithSSCD」適格子の値は、「QC が SSCD により支えられていること」を意味し、または、
  - 「QCNoSSCD」適格子の値は、「QC が SSCD により支えられていないこと」を意味し、または、
  - 「QCSSCDStatusAsInCert」適格子の値は、この CA/QC エントリの中で「Sdi」-「Sie」が提供した情報を基礎として、QC の中に SSCD サポート情報が含められることが確保されていることを意味し；

  及びまたは、
- 法人宛の発行であることを表示するため：
  - 「QCForLegalPerson」適格子の値は、「法人宛の発行であること」を意味する。

2.4. *「CA/QC」「Sdi」の一部ではない「CA/QC」をサポートするサービス*

CRL 及び OCSP 応答が QC 発行 CA（「CA/QC」）の鍵以外の鍵によって署名されている場合も含められなければならない。この場合は、TL の TSL 実装の中において、それらのサービスをそのようにリストすることによって（すなわち、QC の提供の一部であるものとして OCSP または CRL を反映する「additionalServiceInformation」エクステンションによって更に適格化される「Service type identifier」を用いて、例えば、「OCSP/QC」または「CRL/QC」のサービスタイプを用いて）含められ得る。それは、それらのサービスが、QC 認証サービスの提供と関連する監督／認定された「適格」サービスの一部であると考えられることによるものである。無論、リストされた CA/QC サービスの階層構造を基礎とする CA によってそれらの証明書が署名されている OCSP レスポンダまたは CRL 発行者は、「有効」と判断されな

ければならず、リストされた CA/QC サービスのステータスの値に従わなければならない。

デフォルトの ETSI TS 102 231 OCSP 及び CRL のサービスタイプを用いる（「CA/PKC」サービスタイプの）非適格証明書を発行する認証サービスに対しても、同様の条項が適用され得る。

TL の TSL 実装は、関連情報がエンド証明書の AIA フィールドの中に存在しない場合、または、リストされた CA のいずれかの CA によって署名されていない場合、失効サービスを含めるものとしなければならないという点に留意すべきである。

2.5. *相互運用性のある QC プロファイルへの移行*

原則として、可能な限り、サービスのエントリ（異なる「Sdi」）の数を単純化（削減）することを試みなければならない。ただし、このことは、QC の発行と関連するサービスの正確な識別、及び、発行された QC の中からその情報が失われている場合、それらの QC が SSCD によって支えられているか否かに関する信頼性のある情報の提供と均衡するものでなければならない。

宣言された適格ステータス及び宣言された SSCD サポートの有無に関する十分な情報を QC が含めなければならないので、観念的には、「Sie」フィールド及び「適格性」エクステンションの使用は、その方法で解決されるべき個々のケースに（厳格に）限定されなければならない。

構成国は、可能な限り、相互運用可能な QC プロファイルの採択及び使用を執行しなければならない。

3. 信頼リストのための共通テンプレートの構成

構成国の信頼リストのための共通テンプレート案は、以下の類型の情報により構成される：

1. 信頼リスト及びその発行制度に関する情報；
2. その制度を基礎とする全ての監督／認定される CSP に関する紛れのない識別情報をもつフィールドの列（この列は、選択的なものである。すなわち、それが使用されない場合、そのリストは、その信頼リストの適用範囲内において、いかなる CSP も関係構成国内で監督または認定されていないという無内容のものとみなされる。）；
3. 個々のリストされた CSP に関し、その CSP から提供される監督／認定された認証サービスの紛れのない識別子をもつフィールドの列（この列は、少なくとも 1 つのエントリをもたなければならない。）
4. 個々のリストされた認証／認定された認証サービスに関し、そのサービスの現在のステータスの識別子及びそのステータスの履歴。

QC 発行 CSP の文脈において、リストされるべき監督／認定された認証サービスの紛れのない識別子は、その証明書の「適格」ステータス、その証明書の SSCD サポートの可否に関し、その適格証明書の中に利用可能な十分な情報が存在しない状況を考慮に入れなければならず、また、特に（商用）CSP の大半が、適格及び非適格の両者の複数のタイプのエンドエンティティ証明書を発行するために 1 つの単独適格発行 CA を利用しているという付加的な事実に対処するためでなければならない。

例えば、RootCA から発行 CA に至る CA の商用階層構造の中におけるように、1 または複数の上位 CA サービスが存在する場合、承認された CSP 毎のリスト内のエントリの数は、削減され得る。ただし、それらの場合においても、CSP_{QC} 認証サービスと、QC として識別されるべきことを意味する証明書のセットとの間の紛れのない関連性を確保するという基本原則は、堅持され、かつ、確保されなければならない。

1. *信頼リスト及びその発行制度に関する情報*

以下の情報は、この類型の一部である：

- 電子的な検索の間に信頼リストの識別を容易にし、かつ、人間が読取可能な方式による場合においてもその目的を確保するための信頼リストのタグ、
- 信頼リストのフォーマット及びフォーマットの版の識別子、
- 信頼リストの通し番号（またはリリース番号）、
- （例えば、その信頼リストが、指令 1999/93/EC に定める条項を遵守するために、被参照構成国によって監督／認定される CSP による認証サービスの監督／認定ステータスに関する情報を提供していることを識別するための）信頼リストの**タイプ情報**、
- 信頼リストの保有者情報（例：その信頼リストを作成し、安全に発行し、かつ、維持管理する業務を遂行する構成国の機関の名称、住所、連絡先情報等）、
- その信頼リストが関係し、その基盤となっている監督／認定制度に関する情報。これは、以下のものを含めるが、それに限定されない：
  - その信頼リストが適用される国、
  - その制度に関する情報（例：制度モデル、法令、基準、適用されるコミュニティ、タイプ等）をみつけることのできる場所に関する情報、または、その場所の指示、
  - （履歴）情報の保持期間、
- 信頼リストのポリシー及びまたは法律上の告知、法的責任、職責、
- 信頼リストの発行日時及び次のアップデート予定、

2. *制度によって承認された全ての CSP に関する紛れのない識別情報*

- 正規の法律上の登録において使用されている CSP の機関名称（これは、構成国の実務に従う CSP 機関 UID を含めることができる。）、
- CSP の住所及び連絡先情報、
- 直接的なもの、及び、そのような情報をダウンロードし得る場所の指示による場合を含め、CSP に関する追加情報、

3. *個々のリストされた CSP に関し、その CSP から提供され、指令 1999/93/EC の文脈において監督／認定された認証サービスの紛れのない識別子をもつフィールドの列*

この情報のセットは、少なくとも、リストされた CSP による個々の認証に関する以下の情報を含める：

- 認証サービスのタイプの識別子（例：CSP による監督／認定された認証サービスが QC 発行認証局であることを示す識別子）、
- その認証サービスの（商業上の）名称、
- その認証サービスの紛れのないユニーク識別子、
- その認証サービスに関する追加情報（例：直接的に含められ、または、そのような情報をダウンロ

ードし得る場所の指示によって含められる、そのサービスと関連するアクセス情報)、

- CA/QC サービスに関し、個々のタプルが以下の情報を提供する選択的な情報タプルの列、
  (i) 「Sdi」により識別される認証サービスを基礎として、当該サービスの詳細(すなわち、適格証明書のセット)を更に識別(フィルタ)するために使用され、そのために、SSCD サポート(及びまたは、法人宛の発行)の表示に関する追加情報が要求/提供される基準;並びに、
  (ii) 更に識別された適格証明書のサービスのセットが SSCD により支えられているか否かに関する情報、及びまたは、そのような QC が法人宛に発行されるものであるか否かに関する情報(デフォルトでは、自然人宛に QC が発行されるものと判断される。)を提供する関連「適格子」。

4. *個々のリストされた認証サービスに関し、そのサービスの現在のステータスの識別子及びそのステータスの履歴*

この情報のセットは、少なくとも、以下の情報を含める:

- 現在のステータスの識別子;
- 現在のステータスの開始日時;
- そのステータスの履歴情報。

4. 定義及び略語

現行の文書の目的のために、以下の定義及び略語が適用される:

用 語	略 語	定 義
認証サービスプロバイダ	CSP	指令 1999/93/EC の第 2 条(11)に定義するとおり。
認証局	CA	CA は CSP の 1 つであり、エンドエンティティ証明書を発行するために、それぞれが関係証明書をもつ複数の技術 CA の非公開署名鍵を使用できる。証明書を作成し、付すために、1 または複数の利用者から信任される機関である。選択的に、認証局は、利用者の鍵を作成できる[ETSI TS 102 042]。CA は、その CA の非公開署名鍵と関係付けられており、かつ、その CA によるエンティティ証明書発行のために実効的に使用されている(証明用の)公開鍵と関係する CA 証明書の発行者フィールド内に表示される識別情報によって識別されるものとみなされる。CA は、複数の署名鍵をもつことができる。全ての CA 署名鍵は、その CA の証明書の機関鍵識別子フィールドの一部であるユニーク識別子によってユニークに識別される。
適格証明書発行認証局	CA/QC	指令 1999/93/EC の別紙 II に定める要件に適合し、かつ、指令 1999/93/EC の別紙 I の要件に適合する適格証明書を発行する CA。
証明書	Certificate	指令 1999/93/EC の第 2 条(9)に定義するとおり。
適格証明書	QC	指令 1999/93/EC の第 2 条(10)に定義するとおり。
署名	Signatory	指令 1999/93/EC の第 2 条(3)に定義するとおり。

監督	Supervision	監督は、指令 1999/93/EC（第 3 条第 3 項）の意味において用いられる。指令は、構成国に対し、その構成国の領土内に設けられており、かつ、公衆に対して適格証明書を発行する CSP の監督が可能であり、指令に定める条項の遵守を確保する適切な制度を設けることを要求している。
任意の認定	Accreditation	指令 1999/93/EC の第 2 条(13)に定義するとおり。
信頼リスト	TL	指令 1999/93/EC に定める条項の遵守に関し、被参照構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスを示すリストのことを指す。
信頼サービスステータスリスト	TSL	ETSI TS 102 231 に定める仕様による信頼サービスステータス情報の表示の基礎として使用される署名されたリストのフォーム。
信頼サービス		電子取引における信頼及び信頼性を拡大するサービス（典型的には、暗号技術を利用し、または、機密性保護材を含めるが、それらは、必須のものではない）（ETSI TS 102 231）。
信頼サービスプロバイダ	TSP	1 または複数の（電子的な）信頼サービスを運営する組織（この用語は、CSP よりも広範な適用範囲で使用される）。
信頼サービストークン	TrST	信頼サービスの利用の結果として生成または発行される物理オブジェクトまたはバイナリ（論理）オブジェクト。バイナリ TrST の例は、証明書、CRL、タイムスタンプトークン及び OCSP 応答である。
適格電子署名	QES	QC によって支えられ、かつ、指令 1999/93/EC の第 2 条に定義する SSCD によって作成される AdES。
高度電子署名	AdES	指令 1999/93/EC の第 2 条(2)に定義するとおり。
適格証明書によって支えられる高度電子署名	$AdES_{QC}$	AdES の要件に適合し、かつ、指令 1999/93/EC の第 2 条に定義する QC によって支えられる電子署名を意味する。
安全な署名生成機器	SSCD	指令 1999/93/EC の第 2 条(6)に定義するとおり。

第 I 章

「監督／認定される認証サービスプロバイダ」の「信頼リスト」の共通テンプレートのための詳細仕様

この文書の以下の部分では、「しなければならない（MUST）」、「してはならない（MUST NOT）」、「要求される（REQUIRED）」、「する（SHAL）」、「してはならない（SHALL NOT）」、「すべきである（SHOULD）」、「すべきではない（SHOULD NOT）」、「推奨される（RECOMMENDED）」、「できる（MAY）」及び「選択的（OPTIONAL）」のキーワードは、RFC 2119 に示すとおりに解釈されなければならない。

現行の仕様は、ETSI TS 102 231 v3.1.1（2009-06）の中で示される仕様及び要求事項に準拠している。現行の仕様の中に個別の要求事項が存在しない場合、ETSI TS 102 231 の要求事項がそのまま適用される。現行の仕様の中に個別の要求事項が示される場合、その要求事項は、ETSI TS 102 231 に定めるフォーマット仕様によって補完されるが、ETSI TS 102 231 の対応する要求事項よりも優先する。現行の仕様と ETSI TS 102 231 の仕様との間に矛盾が存在する場合、現行の仕様が基準となる。

言語の支援は、少なくとも、英語で実装及び提供され、かつ、追加的に、別の国内言語で実装及び提供され得る。

指示される日時は、ETSI TS 102 231 の 5.1.4 節を遵守する。

URL の使用は、ETSI TS 102 231 の 5.1.5 節を遵守する。

信頼リスト発行制度に関する情報

タグ

TSL Tag（5.2.1 節）

このフィールドは、ETSI TS 102 231 の 5.2.1 節を遵守することが要求され、かつ、そのようにする。

XML 実装の過程において、xsd ファイルは、ETSI によって利用可能とされたものであり、かつ、別紙 I の中で定められているものである。

制度の情報

TSL version identifier（5.3.1 節）

このフィールドは、「3」（整数）と設定することが要求され、かつ、そのようにする。

TSL sequence number（5.3.2 節）

このフィールドは、必須である。このフィールドは、TSL の通し番号を示す。最初の版の TSL におい

て「1」から開始し、この整数値は、TSL のその後の改訂の際に 1 ずつ増加する。このフィールドは、上述の「TSL version identifier」を増やす場合、「1」を再利用してはならない。

TSL type（5.3.3 節）

このフィールドは、TSL のタイプを示すことが要求される。このフィールドは、http://uri.etsi.org/TrstSvc/ eSigDir-1999-93-EC-TrustedList/TSLtype/generic (Generic)において示される。

注記: ETSI TS 102 231 の 5.3.3 節を遵守するため、及び、構成国の信頼リスト[1]の TSL 実装の作成を規律する現行の仕様が存在することを指示し、（構成国の信頼リストである場合）表示される TSL のタイプによってこれらのフィールドが個別の（または代替的な）意味をもつ場合、それに続く予定のフィールド[2]を決定するためのパーサを許容する個別のタイプの TSL を指示するため、上述の個別の URI が登録され、かつ、以下のように記述される：

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic

記述文：（任意的であるか法定のものであるかを問わず）直接の監督のプロセスを通じて、指令 1999/93/ EC に定める関連条項の遵守のための TSL 実装の責任を負う被参照構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスのリストの TSL 実装。

Scheme operator name（5.3.4 節）

このフィールドは、必須である。このフィールドは、国内信頼リストの作成、公表及び維持管理を遂行する構成国の機関の名称を指示する。このフィールドは、関係する法人または（例えば、政府の行政機関のために）その機関の運営に関して委任を受けた組織の正式名称を示す。このフィールドは、正式の法律上の登録または認定において使用される名称、または、正式の通信の宛名とすべき名称でなければならない。このフィールドは、多言語の文字列としなければならず、かつ、義務的な言語として英語（EN）によって、また、可能的に、1 または複数の国内言語によって実装しなければならない。

注記: 国は、監督機関と認定機関を分けてもつことができ、かつ、その活動と関連する何らかの業務遂行のための追加的な機関を設けることもできる。構成国の TL の TSL 実装の制度運営者を指定することは、各構成国に任されている。監督機関、認定機関及び（それらが別の機関として現れる場合）制度運営者のそれぞれが、それぞれの機関自身の職責及び法的責任をもつことが望ましい。

複数の機関が、監督、認定及び運営の各側面に関する職責を負う状況については、「Scheme information URI」（5.3.7 節）によって表示される制度固有情報の中にあるものを含め、TL の一部として、

[1] すなわち、指令 1999/93/ EC に定める関連条項の遵守のために参照される構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスのリスト（略称「信頼リスト」）

[2] ETSI TS 102 231：電子署名及びインフラ（ESI）：整合化された信頼サービスステータス情報の提供によって指示され、かつ、構成国の信頼リストの策定を指示するために現行の仕様によって「プロファイル」されるフィールドのことを意味する。

その制度情報の中で継続的にそのように反映され、表示される。
　指定された制度運営者（5.3.4 節）は、TSL を署名することが望ましい。

Scheme operator address（5.3.5 節）

　このフィールドは、必須である。このフィールドは、郵便による通信及び電子的な通信の両者に関し、「Scheme operator name」（5.3.4 節）の中で識別される法人または委任を受けた機関の住所を示す。このフィールドは、5.3.5.1 節を遵守する「PostalAddress」（すなわち、番地、地域、[国または区域]、[郵便番号]及び ISO3166-1 alpha-2 国コード）；並びに、5.3.5.2 節を遵守する「ElectronicAddress」（すなわち、電子メール及びまたは Web サイト URL）を含めるものとする。

Scheme name（5.3.6 節）

　このフィールドは、それに基づいて制度を運営する名称を示すことが要求される。このフィールドは、（義務的な言語として英語（EN）により、及び、可能的なものとして 1 または複数の国内言語により）以下に定める多言語の符号列であるものとする：

－　EN 版は、以下の符号列とする：
　CC: EN_name_value
　以下のとおり
　　－「CC」＝　「Scheme territory field」（5.3.10 節）の中で使用される ISO 3166-1 alpha-2 国コード；
　　－「:」＝　セパレータとして使用される；
　　－「EN_name_value」＝　指令 1999/93/EC に定める関連条項を遵守するために参照される制度運営者の構成国によって監督／認定される認証サービスプロバイダによる認証サービスの監督／認定ステータスのリスト。

－　構成国の国内言語版は、以下の符号列とする：
　CC: name_value
　以下のとおり
　　－「CC」＝　「Scheme territory field」（5.3.10 節）の中で使用される ISO 3166-1 alpha-2 国コード；
　　－「:」＝　セパレータとして使用される；
　　－「name_value」＝　上述の EN_name_value の公式翻訳国内言語。

　制度の名称は、名称の順に、Scheme information URI によって示される制度をユニークに識別することが要求され、かつ、制度運営者が複数の制度を運用する場合、それぞれについて異なる名称が与えられていることを確保することが要求される。
　構成国及び制度運営者は、構成国または制度運営者が複数の制度を運用する場合、それぞれについて異なる名称が与えられていることを確保する。

Scheme information URI (5.3.7 節)

このフィールドは、必須であり、かつ、利用者（依拠者）が（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）制度指示情報を入手できる URI を指示する。このフィールドは、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多言語のポインタ列とする。指示される URI は、「制度に関する適切な情報」を記述する情報へのパスを提供しなければならない。

ミニマムのものとして、制度に関する適切な情報は、以下のものを含めるものとする:

－ 信頼リストの適用範囲及び内容に関する全ての構成国に共通の一般的で序文的な情報、基礎をなす監督／認定制度。共通の文は、以下の文が用いられる:

「このリストは、電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 12 月 13 日の指令 1999/93/EC の関連条項を遵守するために、[関連構成国の名称]による監督／認定を受ける認証サービスプロバイダ（CSP）による認証サービスの監督／認定ステータスと関連する情報を提供する「監督／認定された認証サービスプロバイダの信頼リスト」の[関連構成国の名称]の TSL 実装である。

この信頼リストは、以下を狙いとしている:

－ 指令 1999/93/EC に定める関連条項の遵守のために[関連構成国の名称]による監督／認定を受ける認証サービスプロバイダによる認証サービスの監督／認定のステータスに関する信頼性のある情報をリストし、提供すること;

－ それらのリストされた CSP によるリストされた監督／認定を受けた認証サービスによって支えられる電子署名の検証を容易にすること。

構成国の信頼リストは、電子署名を支える QC に関する情報、及び、その署名が安全な署名生成機器によって生成されるか否かを含め、指令 1999/93/EC（第 3 条第 3 項、第 3 条第 2 項、第 7 条第 1 項(a)）に定める条項に従って適格証明書を発行する監督／認定を受けた CSP に関するミニマムの情報を提供する。

ここにリストされる適格証明書（QC）を発行する CSP は、別紙 I の要件（QC の要件）及び別紙 II の要件（QC 発行 CSP の要件）を含め、指令 1999/93/EC に定める条項の遵守に関し、[関連構成国の名称]による監督を受けなければならず、また、認定も受けることもできる。適用される「監督」制度（それぞれ該当するときは、「任意の認定」制度）は、定義され、かつ、指令 1999/93/EC の関連要件、とりわけ、第 3 条第 3 項、第 8 条第 1 項、第 11 条（それぞれ該当するときは、第 2 条(13)、第 3 条第 2 項、第 7 条第 1 項(a)、第 8 条第 1 項、第 11 条）に適合しなければならない。

それ以外の、QC を発行しないが電子署名と関連するサービスを提供する監督／認定を受ける CSP（例:タイムスタンプサービスを提供する CSP 及びタイムスタンプトークンを発行する CSP、非適格証明書を発行する CSP 等）に関する追加情報は、国内レベルで、任意に、信頼リスト及び現行の TSL 実装の中に収録される。」

－ 基礎をなす監督／認定制度に関する個別情報、とりわけ[1]:

[1] 後者の 2 つの情報セットは、そのような監督／認定制度の品質及び安全性のレベルを依拠者が評価するために特に重要なものである。これらの情報セットは、現行の「Scheme information URI」（5.3.7 節－構成国か

- CSP_{QC} に適用される監督制度に関する情報;
- 該当するときは、CSP_{QC} に適用される任意の国内認定制度に関する情報;
- 該当するときは、QC 非発行 CSP に適用される監督制度に関する情報;
- 該当するときは、QC 非発行 CSP に適用される任意の国内認定制度に関する情報;

- この個別情報は、上記に列挙する基礎をなす制度それぞれについて、少なくとも、以下の事項を含める:
  - 総則的な記述;
  - CSP を監督／認定するための監督／認定機関が服する手続及び監督／認定を受けるために CSP が服する手続に関する情報;
  - 監督／認定を受ける CSP に対して適用される基準に関する情報。
- 該当するときは、個別の適格に関する情報。そのような適格の意味並びに関係する国内条項及び国内要件を含め、認証サービスの提供の結果として生成または発行される幾つかの物理オブジェクトまたはバイナリ（論理）オブジェクトは、国内レベルで定められた条項及び要件を遵守することを基礎として、それを受けることができる。

  制度に関する構成国の個別の追加情報は、任意で、追加され得る。この情報は、以下のものを含める:
  - 監督者／承認者を選定する際に使用され、かつ、それらの者によって CSP がどのように監督（管理）／認定（監査）されるかを定める基準及び法令に関する情報;
  - その制度運営に適用される上記以外の連絡先情報及び一般的な情報。

Status determination approach（5.3.8 節）

このフィールドは、必須であり、かつ、ステータス決定アプローチの識別子を指示する。以下のように登録及び記述される以下の特別の URI が使用される:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

記述文:リストされるサービスは、その構成国の領土上において設けられており（または、「任意の認定」の場合、第三国において設けられており）、かつ、指令 1999/93/EC の第 3 条第 3 項（それぞれ該当するときは、第 3 条第 2 項または第 7 条第 1 項(a)）により、公衆に対して適格証明書を発行する認証サービスプロバイダを監督（または、該当するときは、「任意の認定」）が可能である被参照構成国において、並びに、該当するときは、QC 非発行 CSP によるサービスの、指令 1999/93/EC に定める条項及びそのような認証サービスの提供と関連する国内条項による可能的な拡張条項の遵守に関し、国内ベースで実装され、承認された「認定制度」を国内的に定義及び構築することにより、適格証明書を発行しない認証サービスプロバイダの「監督／任意の認定」が可能である被参照構成国の適切な制度の下にお

ら提供される情報）、「Scheme type/community/rules」（5.3.9 節－全ての構成国に共通の文の使用を介する）及び「TSL policy/legal notice」（5.3.11 節－全ての構成国に共通の指令 1999/93/EC を指示する文、各構成国は、構成国の固有の文または参照を付加できる）の使用を通じて、TL 上で提供される。QC 非発行 CSP の国内監督／認定制度に関する追加情報は、それに該当し、かつ、（例えば、複数の品質レベルまたは安全性レベルを区別するために）必要な場合、「Scheme service definition URI」（5.5.6 節）により、サービスレベルで、提供され得る。

いて、制度運営者またはそれに代わる者によって決定されるそれらのサービスのステータスをもつ。

Scheme type/community/rules (5.3.9 節)

このフィールドは、必須であり、かつ、少なくとも、以下の登録された URI を含める：

－ 全ての構成国の信頼リストに共通の、全ての信頼リストに適用される記述文を指示する URI は、以下のとおりである：

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

－ どの URI によって、諸制度（すなわち、TSL の方式による TL を公表及び維持管理する全ての構成国の TSL リスティングポインタ）の制度の中における（TSL タイプ（5.3.3 節）及び制度の名称（5.3.6 節）によって識別される）構成国の制度の URI が示され；

－ ユーザが、リストに収録されているサービスを評価し、かつ、TSL のタイプ（5.3.3 節）を決定し得るポリシー／法令をどこで入手できるかが示され；

－ ユーザが、信頼リストの TSL 実装をどのように使用し、その内容を解釈するかに関する記述をどこで入手できるかが示される。これらの使用のルールは、リストされるサービスのタイプに関する限り、及び、監督／認定制度である限り、全ての構成国の信頼リストに共通のものとする。

記述文：

「**制度への参加**

各構成国は、電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 12 月 13 日の指令 1999/93/EC に定める関連条項の遵守のための関連構成国による監督／認定を受ける認証サービスプロバイダ（CSP）による認証サービスの監督／認定ステータスに関する情報を提供する「監督／認定を受ける認証サービスプロバイダの信頼リスト」を作成しなければならない。

そのような信頼リストの現行の TSL 実装は、欧州共同体によって合綴される各構成国の信頼リストの TSL 実装へのリンク（ポインタ）のリストの中においても参照されなければならない。

リストされたサービスの評価のためのポリシー／法令

構成国の信頼リストは、電子署名を支える適格証明書（QC）に関する情報、及び、その電子署名が安全な署名生成機器によって生成されるか否かに関する情報を含め、指令 1999/93/EC（第 3 条第 3 項、第 3 条第 2 項、第 7 条第 1 項(a)）に定める条項に従って適格証明書を発行し、監督／認定を受ける CSP に関するミニマムの情報を提供しなければならない。

適格証明書（QC）を発行する CSP は、別紙 I の要件（QC の要件）及び別紙 II の要件（QC 発行 CSP の要件）を含め、指令 1999/93/EC に定める条項の遵守に関し、（その CSP が構成国内に設けられている場合）構成国による監督を受けなければならず、また、認定も受け得る。その CSP が当該構成国内に設けられていない場合を除き、構成国内で認定を受けた

QC 発行 CSP は、当該構成国の適切な監督制度の下にあるものとしなければならない。適用される「監督」制度（それぞれ該当するときは、「任意の認定」制度）は、定義され、かつ、指令 1999/93/EC の関連要件、とりわけ、第 3 条第 3 項、第 8 条第 1 項、第 11 条（それぞれ該当するときは、第 2 条(13)、第 3 条第 2 項、第 7 条第 1 項(a)、第 8 条第 1 項、第 11 条）に適合しなければならない。

それ以外の、QC を発行しないが電子署名と関連するサービスを提供する監督／認定を受ける CSP（例：タイムスタンプサービスを提供する CSP 及びタイムスタンプトークンを発行する CSP、非適格証明書を発行する CSP 等）に関する追加情報は、国内レベルで、任意に、信頼リスト及び現行の TSL 実装の中に収録され得る。

QC を発行しないが付随サービスを提供する CSP は、（指令 1999/93/EC の中で定義され、かつ、それを遵守する）「任意の認定」制度の下にあるものとすることができ、及びまたは、指令 1999/93/EC に定める条項及び（指令の第 2 条(11)の意味における）認証サービスの提供と関連する可能的な国内条項の遵守の監督のための国内的に実装され、国内的に定義された「承認された認定制度」の下にあるものとすることができる。認証サービスの提供の結果として生成または発行される物理オブジェクトまたはバイナリ（論理）オブジェクト中の幾つかは、国内レベルで定められた条項及び要件を遵守することを基礎として、個別の「適格」を受けることができるが、そのような「適格」の意味は、国内レベルのみに限定され得る。

信頼リストの TSL 実装の解釈

委員会決定 2009/767/EC の別紙による信頼リストの TSL 実装に準拠する電子署名のアプリケーション、サービスまたは製品に関する**一般的な利用者運用指針**は、以下のとおりである：

「CA/QC」「Service type identifier」（「Sti」）エントリ（同様に、「Service information extension」（「Sie」）additionalServiceInformation extension の使用により、「RootCA/QC」であるとして更に適格化される CA/QC）は、

- 適切な ETSI TS 101 862 定義の QcStatements 文（すなわち、QcC、QcSSCD）及びまたは、ETSI TS 101 456 定義の QCP(+) OID の使用により、その証明書の中でそのように宣言されていること（及び、このことが、発行 CSP 及び監督／認定機関によって確保されること）を**条件として**、対応する CSP（関係する TSP information フィールド参照）により、「Sdi」で識別される CA から（同様に、「Sdi」で識別される RootCA から始まる CA の階層構造内において）発行された全てのエンドエンティティ証明書が適格証明書（QC）であることを表示し、
  注記：「Sie」「Qualification」情報が全く存在しない場合、または、QC であると宣言するエンドエンティティ証明書が、関連「Sie」エントリによって「更に識別され」ない場合、QC の中でみつけられる「機械読取可能な」情報は、正確なものであるべきことが監督／認定されることとなる。このことは、適切な QcStatements（すなわち、QcC、QcSSCD）及びまたは ETSI 定義の QCP(+) OID の使用（または不使用）が、CSP_{QC} によって宣言されるところに従って確保されることを意味する。

- **かつ**、「Sie」「Qualification」情報が存在する場合、上述のデフォルトの利用方法解釈ルールに加え、証明書のセットを更に識別する「フィルタ」の列の基本原則に基づいて構築され、「SSCD サポート」及びまたは「主体としての法人」と関連する幾つかの追加情報を提供する「Sie」「Qualification」エントリの使用により識別される証明書（例：Certificate Policy extension 中の特定の OID を含む証明書、及びまたは、特定の「鍵利用方法」パターンをもつ証明書、及びまたは、特定のフィールドもしくはエクステンションの中で表示される特定の値の使用によってフィルタされる証明書等）は、対応する QC の内容中に情報が欠けている場合を埋める以下のセットの「適格子」に従って判断されなければならない。すなわち：
- SSCD サポートを表示するため：
  - 「QCWithSSCD」適格子の値は、「QC が SSCD により支えられていること」を意味し、または、
  - 「QCNoSSCD」適格子の値は、「QC が SSCD により支えられていないこと」を意味し、または、
  - 「QCSSCDStatusAsInCert」適格子の値は、この CA/QC エントリの中で「Sdi」-「Sie」が提供した情報を基礎として、QC の中に SSCD サポート情報が含められることが確保されていることを意味し；

  及びまたは、
- 法人宛の発行であることを表示するため：
  - 「QCForLegalPerson」適格子の値は、「法人宛の発行であること」を意味する。

それ以外の「Sti」タイプのエントリの解釈のための一般的な解釈ルールは、当該「Sti」識別されたサービスタイプについては、「Service name」フィールドの値に従って命名され、「Sdi」フィールドの値によってユニークに識別されるリストされたサービスが、「Current status starting date and time」の中に示される日付による「Scs」フィールドの値に従い、現在の監督／認定ステータスをもつことである。

リストされたサービスと関係する追加情報（例えば、「Service information extensions」フィールド）に関する個別の解釈ルールは、該当するときは、現行の「Scheme type/community/rules」フィールドの一部として、構成国の個別の URI の中で見出され得る。

構成国の「信頼リスト」の TSL 実装のためのフィールド、記述及び意味の詳細については、委員会決定 2009/767/EC の別紙の中にある「監督／認定される認証サービスプロバイダの信頼リスト」のための共通テンプレートの技術仕様を参照されたい」。

- その構成国の信頼リストに適用される記述文を指示する各構成国の信頼リストを指示する URI：CC=「Scheme territory」フィールド（5.3.10 節）の中で使用される ISO 3166-1 alpha-2 の国コードの場合

  http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC
  - 利用者が入手可能な場合、リストに収録された信頼サービスに適用される被参照構成国の個別のポリシー／法令は、構成国の適切な監督制度及び任意の認定制度に従って評価される。
  - 利用者が入手可能な場合、QC の発行と関係しない認証サービスに関し、信頼リストの TSL

実装をいかに使用し、その内容を解釈するかに関する被参照構成国の個別の記述。この記述は、QC を発行しない CSP と関連する国内監督／認定制度の中にある潜在的な細分化を示すために使用され、また、「Scheme service definition URI」（5.5.6 節）及び「Service information extension」フィールド（5.5.9 節）が、その目的のためにどのように使用されるかを示すために使用され得る。

構成国は、上述の構成国の個別の URI の追加 URI（すなわち、この階層的な個別の URI から定められる URI）を定めることができる。

Scheme territory（5.3.10 節）

現行の仕様の文脈において、このフィールドは、必須であり、かつ、その制度が設けられている国を指示する（ISO 3166-1 alpha-2 国コード）。

TSL policy/legal notice（5.3.11 節）

現行の仕様の文脈において、このフィールドは、必須であり、かつ、その制度のポリシーを指示し、または、その制度が定められている国に関し、制度の法的ステータスまたはその制度に適合する法律上の要件、及びまたは、それに基づいて TL が維持管理及び公表される制約及び条件に関する告知を提供する。

このフィールドは、2 つの部分で構成される多言語の文字列（プレーンテキスト）とする：

- 第 1 の義務的な部分は、適用される法的枠組みが指令 1999/93/EC、及び、「Scheme Territory」フィールド内で示される構成国の法律の中にある指令の対応実装であることを表示する（義務的な言語としての EN による、及び、可能的に、1 または複数の国内言語による）全構成国の TL に共通である。

  共通文の英語版は、以下のとおりである：

  「[関連構成国の名称]の監督／認定を受けた認証サービスプロバイダの信頼リストの現行の TSL 実装に適用される法的枠組みは、電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 12 月 13 日の指令 1999/93/EC、並びに、[関連構成国の名称]の法律の中にある指令の実装である」。

  構成国の国内言語による文：[上述の英語文の公式翻訳文]。
- 第 2 の選択的な部分は、（例えば、とりわけ、QC 非発行 CSP に関する監督／認定の国内制度と関連する場合）適用される個別の国内法上の枠組みへの参照を示す（義務的な言語としての EN による、及び、可能的に、1 または複数の国内言語による）個々の TL に固有である。

Historical information period（5.3.12 節）

このフィールドは、必須であり、かつ、TSL 内の履歴情報が提供される期間（整数）を示す。整数の値は、日数を提供しなければならず、現行の仕様の文脈においては、3653 以上とする（すなわち、構成国の TL の TSL 実装は、ミニマムで 10 年間の履歴情報を収録しなければならない）。それよりも大

きな値は、「Scheme Territory」（5.3.10 節）に表示される構成国のデータ保持に関する法律上の要件を適正に考慮に入れるものとすべきである。

Pointers to other TSLs（5.3.13 節）

現行の仕様の文脈においては、このフィールドは、必須であり、かつ、それが利用可能なときは、構成国の信頼リストの全ての TSL 実装を指すリンク（ポインタ）の EC 合綴リストの ETSI TS 102 231 準拠フォームへのポインタを含める。ETSI TS 102 231 の 5.3.13 節の仕様は、5.5.3 節の中で示されるようにフォーマットされ、指示される TSL の発行者を表示する選択的なデジタル識別子の使用が義務的なものとされている間、適用される。

注記: 構成国の信頼リストの全ての TSL 実装を指すリンクの EC 結合リストの ETSI TS 102 231 結合が完了するまでの間においては、このフィールドを使用してはならない。

List issue date and time（5.3.14 節）

このフィールドは、必須であり、かつ、ETSI TS 102 231 の 5.1.4 節に示す日時の値を使用し、TSL が発行された日時（Zulu のように表現された UTC）を示す。

Next update（5.3.15 節）

このフィールドは、必須であり、（ETSI TS 102 231 の 5.1.4 節に示す日時の値を使用して）次の TSL が発行される直近の日時（Zulu のように表現された UTC）を示し、終了した TSL を指示するために null とする。

その制度の提供を受ける TSP またはサービスへの中間的なステータス変動が全く存在しない場合、最後に発行された TSL の有効期限満了日までに、TSL が再発行されなければならない。

現行の仕様の文脈において、「Next update」の日時と「List issue date and time」との間の差分は、6 か月を超過してはならない。

Distribution points（5.3.16 節）

このフィールドは、選択的である。このフィールドが使用される場合、TL の現行の TSL 実装が発行される場所及び現行の TSL を見つけることのできる場所を示す。複数の提供場所が示されるときは、それらの全ては、現行の TSL またはそのアップデートされた版と同一のコピーを提供しなければならない。このフィールドが使用される場合、各文字列が RFC 3986[1]を遵守する空欄のない文字列としてフォーマットされる。

[1] IETF RFC 3986: 'Uniform Resource Identifiers (URI): Generic syntax'.

Scheme extensions（5.3.17 節）

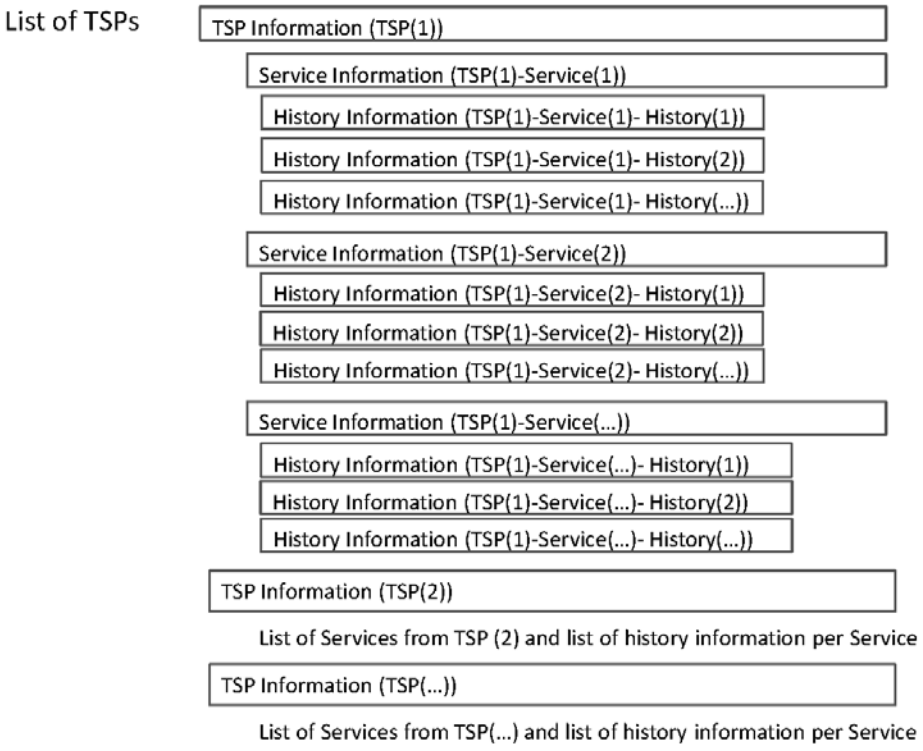
このフィールドは、選択的であり、かつ、現行の仕様の文脈においては使用されない。

信頼サービスプロバイダのリスト

このフィールドは、選択的である。

構成国の制度の過程において監督／認定されている CSP または監督／認定されていた CSP が存在しない場合、このフィールドは、存在しない。ただし、その制度によって監督または認定される CSP をその構成国がもたない場合においても、構成国が、このフィールドが存在しない TSL を実装することが合意されている。リストの中にいかなる CSP も存在しないということは、「Scheme Territory」の中で示される国において監督／認定される CSP が存在しないということを意味する。

1 または複数の CSP が制度によって監督／認定されており、または、監督／認定されていた場合、このフィールドは、監督／認定のステータス及び個々の CSP のサービスのステータス履歴に関する詳細と共に、それらの監督／認定されたサービス中の 1 または複数のものを提供する個々の CSP を識別する列を含めるものとする（TSP＝下記の図にある CSP）。



TSP のリストは、上記の図の中で描かれているように構成される。各 TSP に関し、その TSP に関する情報（TSP 情報）とそれに続くサービスのリストをもつフィールドの列がある。そのようにリストされた個々のサービスに関し、そのサービスに関する情報（サービス情報）をもつフィールドの列、及び、そのサービスの認定ステータス履歴（サービス認定履歴）に関するフィールドの列がある。

TSP 情報

TSP (1)

TSP name（5.4.1 節）

このフィールドは、必須であり、かつ、その制度の下で監督もしくは認定されている CSP または監督もしくは認定されていた CSP のサービスについて責任を負う**法主体**の名称を示す。このフィールドは、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多国語の文字列である。この名称は、正規の法律上の登録において使用され、かつ、正規の通信の宛名とされ得る名称でなければならない。

TSP trade name（5.4.2 節）

このフィールドは、選択的であり、かつ、それが表示される場合、その CSP の「TSP name」（5.4.1 節）エントリに基づき、その TSL の中でみつけられるその CSP のサービスの提供という個別の過程の中で、その CSP が自己を識別する代替的な名称を示す。

注記: 単一の CSP 法主体が、異なる商号の下で、または、異なる個別過程の下でサービスを提供する場合、そのような個別の過程と同数の CSP 主体が存在し得る（例: Name/Trade Name エントリ）。代替名称は、個別に、かつ、各 CSP（法主体）について 1 度だけリストされなければならず、個別の過程のサービス情報を提供するものでなければならない。CSP との間で最も適切なアプローチに関して意見交換及び合意するのは、構成国の制度運営者である。

TSP address（5.4.3 節）

このフィールドは、必須であり、かつ、郵便による通信及び電子的な通信の両者に関し、「TSP name」フィールド（5.4.1 節）の中で識別される法主体または委任を受けた組織の住所を示す。このフィールドは、5.3.5.1 節を遵守する「PostalAddress」（すなわち、番地、地域、[国または区域]、[郵便番号]及び ISO3166-1 alpha-2 国コード）；並びに、5.3.5.2 節を遵守する「ElectronicAddress」（すなわち、電子メール及びまたは Web サイト URL）を含めるものとする。

TSP information URI（5.4.4 節）

このフィールドは、必須であり、かつ、利用者（例: 依拠者）が CSP の個別情報を入手し得る場所の URI を示す。このフィールドは、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多国語のポインタ列である。指示される URI は、その CSP の一般的な規約及び条件を記述する情報、その実務、法的問題、その CSP の顧客対応ポリシー、並びに、上記以外の、その TSL 内のその CSP の CSP エントリにリストされたその CSP の全てのサービスに適用される一

般的な情報へのパスを提供するものでなければならない。

注記: 単一の CSP 法主体が、異なる商号の下で、または、異なる個別過程の下でサービスを提供する場合であり、かつ、そのような個別の過程と同数の TSP エントリの中で反映されている場合、そのフィールドは、特定の TSP/TradeName エントリの下でリストされた個別のセットのサービスと関連する情報を示すものとする。

TSP information extension（5.4.5 節）

このフィールドは、選択的あり、かつ、それが表示される場合、ETSI TS 102 231（5.4.5 節）を遵守し、個別の制度の規定に従って解釈される個別の情報を提供するために、制度運営者によって使用され得る。

サービスのリスト

このフィールドは、必須であり、かつ、個々の SCP の承認されたサービス、並びに、そのサービスの認定ステータス（及びそのステータスの履歴）を識別する列を含める。（保持される情報の全部が履歴情報である場合であっても）少なくとも 1 個のサービスがリストされなければならない。

現行の仕様の下においてはリストされたサービスに関する履歴情報を保持することが要求されるので、当該履歴情報は、そのサービスの現在のステータスが、通常は、リストされることを要求されないようなものである場合（例：そのサービスが廃止された場合）においても、保持されなければならない。そして、その CSP のリストされた唯一のサービスがそのようなステータスにある場合であっても、その履歴を保存するため、CSP が含められなければならない。

サービス情報

TSP (1) Service (1)

Service type identifier（5.5.1 節）

このフィールドは、必須であり、かつ、現行の TSL 仕様のタイプによるサービスタイプの識別子を示す（例：「/eSigDir-1999-93-EC-TrustedList/TSLtype/generic」）。

リストされるサービスが適格証明書の発行と関係するものである場合、その引用される URI は、http://uri.etsi.org/TrstSvc/Svctype/CA/QC（適格証明書を発行する認証局）とする。

リストされるサービスが QC ではない信頼サービストークンの発行と関連するものである場合、その URI は、ETSI 102 231 に定義され、その D.2 項に列挙される URI 中でこのフィールドと関係するものの中のいずれかとする。このことは、構成国の国内法による幾つかの個別の資格に適合していることについて監督／認定を受ける信頼サービストークン（例：いわゆる、DE または HU の適格タイムスタンプトークン）に対しても適用され、その引用される URI は、ETSI 102 231 に定義され、その D.2 項に列

挙される URI 中でこのフィールドと関係するものの中のいずれかとする（例：国内的に定義された適格タイムスタンプトークンのための TSA）。該当するときは、そのような信頼サービストークンの個別の国内適格性は、サービスエントリの中で提供され、また、その目的のために、5.5.9 節中の additionalServiceInformation（5.8.2 節）が使用される。

原則として、（例えば、CA/QC タイプ認証サービスのための）1 個の X.509v3 証明書について、その信頼リストの中にリストされた CSP によるリストされた認証サービス（例：（直接に）QC を発行する認証局）に基づく 1 個のエントリが存在するものとする。注意深く想定された状況及び注意深く管理及び承認された条件の下において、構成国の監督機関／認定機関は、RootCA または上位 CA（例えば、エンドエンティティ QC を直接に発行するわけではないが、QC 発行 CA からエンドエンティティに至る CA の階層構造を認証する認証局）の X.509v3 証明書を、リストされた CSP のサービスのリスト中で単独エントリの Sdi として使用することを決定できる。そのような X.509v3RootCA または上位 CA を TL サービスエントリの「Sdi」の値として使用することの結果（利益及び不利益）は、注意深く検討され、かつ、構成国による承認を受けなければならない [1]。加えて、デフォルトの基本原則のそのような是認された例外処理を使用する場合、構成国は、パス構築の証明及び検証を容易にするため、必要な文書を提供しなければならない。

注記：CSP_{QC} 認証サービスの一部であり、OCSP 応答をそれぞれ署名するための分離されたペア鍵の使用に服する OCSP レスポンダ及び CRL 発行者は、以下の URI の組み合わせを使用することにより、現行の TSL の中で同様にリストされ得る：

- 「Service type identifier」（5.5.1 節）の値：
  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP
  「Service information extension」（5.5.9 節）に続く additionalServiceInformation エクステンション（5.8.2 節）と結合される値：
  http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC
  記述文：適格証明書発行 CSP によるサービスの一部として OCSP サーバを運営する証明書ステータスプロバイダ、
- 「Service type identifier」（5.5.1 節）の値：
  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL
  「Service information extension」（5.5.9 節）に続く additionalServiceInformation エクステンション（5.8.2 節）と結合される値：
  http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC
  記述文：適格証明書発行 CSP によるサービスの一部として CRL を運営する証明書ステータスプロバイダ、
- 「Service type identifier」（5.5.1 節）の値：
  http://uri.etsi.org/TrstSvc/Svctype/CA/QC

[1] リストされたサービスの「Sdi」の値として RootCA の X.509v3 証明書を使用することは、制度運営者に対し、「supervision/accreditation status」に関し、全体としての RootCA に基づく全てのセットの認証サービスを検査することを強いることになる。例えば、リストされた Root 階層構造に基づく 1 個の単独 CA によって要求されるステータス変更は、当該ステータス変更を階層構造全体に付加することを強いることになる。

「Service information extension」（5.5.9 節）に続く additionalServiceInformation エクステンション（5.8.2 節）と結合される値:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

記述文：適格証明書発行認証局に至るまで構築され得る認証パスによる Root 認証局、

－ 「Service type identifier」（5.5.1 節）の値:

http://uri.etsi.org/TrstSvc/Svctype/TSA

「Service information extension」（5.5.9 節）に続く additionalServiceInformation エクステンション（5.8.2 節）と結合される値:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

記述文：QC が取消または失効となる場合において、適格署名検証プロセスの中で、その署名の有効性を確認及び延長するために使用され得る TST を発行する適格証明書を発行する認証サービスプロバイダによるサービスの一部としてのタイムスタンプサービス。

Service name（5.5.2 節）

このフィールドは、必須であり、かつ、「TSP name」（5.4.1 節）の中で識別される CSP が提供する「Service type identifier」（5.5.1 節）の中で識別されるサービスの名称を示す。このフィールドは、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多国語の文字列である。

Service digital identity（5.5.3 節）

このフィールドは、必須であり、かつ、そのタイプが「Service type identifier」（5.5.1 節）の中で識別され、それによって、そのサービスが紛れなく識別され得る、そのサービスに固有の、少なくとも 1 つのデジタル識別子の表示を示す。

現行の仕様において、このフィールドの中で使用されるデジタル識別子は、そのタイプが「Service type identifier」（5.5.1 節）によって指示されるサービスを提供するためにその CSP が使用する公開鍵（すなわち、RootCA/QC によって使用される鍵、証明書の署名 [1]、または、代替的なタイムスタンプトークンの発行、もしくは、CRL の署名、または、OCSP 応答の署名のために使用される鍵）の表現である関連 X.509v3 証明書であるものとする。この関連 X.509v3 証明書は、ミニマムで要求される（リストされたサービスを提供するために CSP が使用する公開鍵の表示である）デジタル識別子として使用される。以下のような追加的な識別子が使用され得るが、それら全ては、同一のアイデンティティ（すなわち、関連 X.509v3 証明書）を指すものでなければならない:

[1] これは、エンドエンティティ証明書（例：CA/PKC、CA/QC）を発行する CA の証明書、または、エンドエンティティ適格証明書まで至ることが確認され得るパスによる信頼性のある RootCA の証明書であり得る。この情報、及び、この信頼性のある Root を基礎として発行される全てのエンドエンティティ証明書の中で見出される情報が、適格証明書の関連特性を紛れなく決定するために使用され得るものであるか否かにより、その情報（Service digital identity）は、「Service information extension」（5.5.9 節参照）によって補完される必要のあるものであり得る。

(a) 「Service type identifier」（5.5.1 節）の中で指示される CSP の電子署名を検証するために使用され得る証明書の識別名（DN）；
(b) 関連する公開鍵の識別子（すなわち、X.509v3 の SubjectKeyIdentifier または SKI の値）；
(c) 関連する公開鍵。

デフォルトの一般原則として、デジタル識別子（すなわち、関連 X.509v3 証明書）は、信頼リスト中で複数回現れるものであってはならない。すなわち、その信頼リストの中にあるリストされた CSP によるリストされた認証サービスに基づく認証サービスに関し、1 個の X.509v3 証明書について 1 個のエントリが存在するのでなければならない。これとは反対に、1 個の単独 X.509v3 証明書は、単独のサービスエントリ内において、「Sdi」の値として使用される。

注記(1)：上述のデフォルトの一般原則が適用されない唯一の場合は、異なる監督／認定制度が適用されるものに関して異なるタイプの信頼サービスのトークンが発行される場合において 1 個の X.509v3 証明書が使用される場合、例えば、1 個の X.509v3 証明書が、一方では、ある適切な監督制度の下において QC を発行する際に、他方では、異なる監督／認定ステータスの下にある非適格証明書を発行する際に、CSP によって使用される場合である。この場合及び例において、異なる「Sti」の値（例：上記の例では、それぞれ CA/QC 及び CA/PKC）並びに同じ「Sdi」の値（関連 X.509v3 証明書）をもつ 2 つのエントリが使用され得る。

実装は、ASN.1 または XML によるものとし、ETSI TS 102 231 の仕様（ASN.1 に関しては、ETSI TS 102 231 の別紙 A 参照、及び、XML に関しては、ETSI TS 102 231 の別紙 B 参照）を遵守するものとする。

注記(2)：識別されたサービスエントリと関連して追加的な「適格性」情報が提供される必要がある場合、それが適切なときは、制度運営者は、そのような「適格性」情報を提供する目的により、「Service information extension」フィールド（5.5.9 節）の「additionalServiceInformation」エクステンション（5.8.2 節）の使用を検討する。

Service current status（5.5.4 節）

このフィールドは、必須であり、かつ、以下のいずれかの URI を介して、サービスのステータスの識別子を示す：

- **Under Supervision** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision)；
- **Supervision of Service in Cessation** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation)；
- **Supervision Ceased** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased)；
- **Supervision Revoked** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked)；

- **Accredited** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited)；
- **Accreditation Ceased** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditation ceased)；
- **Accreditation Revoked** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditation revoked)。

上記のステータスは、信頼リストの現行の仕様の文脈においては、以下のように解釈されるものとする：

- **Under Supervision**：「TSP name」（5.4.1 節）の中で識別される認証サービスプロバイダ（CSP）から提供され、「Service digital identity」（5.5.3 節）の中で識別されるサービスは、指令 1999/93/EC に定める条項を遵守するため、その CSP が設けられており、「Scheme territory」（5.3.10 節）の中で識別される構成国により、現在、監督の下にある。
- **Supervision of Service in Cessation**：「TSP name」（5.4.1 節）の中で識別される CSP から提供され、「Service digital identity」（5.5.3 節）の中で識別されるサービスは、現在、停止のフェーズにあるが、監督が終了または取消となるまでは、監督が継続する。「TSP name」の中で識別される法人とは異なる法人がこの停止のフェーズを確保する責任を承継した場合、この新たな法人または切替法人（fallback CSP）の識別子は、サービスエントリの 5.5.6 節の中で提供される。
- **Supervision Ceased**：「Service digital identity」（5.5.3 節）の中で識別されるサービスの再評価が行われることなく、監督上の評価の有効性が失われる。このサービスは、現在、そのサービスの業務遂行を終えたと理解されるので、現在のステータスの日以降は、監督の下にない。
- **Supervision Revoked**：その CSP が設けられており、「Scheme territory」の中で識別される構成国によって決定されるとおり、監督されてきたその CSP のサービス及び潜在的にはその CSP それ自体が、指令 1999/93/EC に定める条項を遵守し続けていない。従って、そのサービスは、その業務遂行の終了を要求されたものであり、かつ、上記の理由により終了したものと判断されなければならない。

注記(1)：「Supervision Revoked」のステータス値は、その CSP がその活動を完全に終了した場合においても、確定的なステータスとし得る；この場合、「Supervision of Service in Cessation」または「Supervision Ceased」のいずれに対しても、移行させることを要しない。実際には、「Supervision Revoked」ステータスを変更するための唯一の方法は、その TL をもつ構成国において有効である適切な監督制度に従い、指令 1999/93/EC に定める条項の不遵守から遵守への回復を行い、「Under Supervision」ステータスを再び獲得することである。「Supervision of Service in Cessation」ステータスまたは「Supervision Ceased」ステータスは、監督の下にあるその CSP の関連サービスを CSP が自ら終了する場合においてのみ生じ、監督が取消された場合には生じない。

- **Accredited**：「Scheme territory」（5.3.10 節）の中で識別される構成国の代わりに認定機関によって実施される認定評価、及び、「TSP name」（5.4.1 節）の中で識別される CSP[1]から提供され、「Service digital identity」（5.5.3 節）の中で識別されるサービスが、指令 1999/93/EC に定める条項を遵守するものと判断される。

[1] この認定された CSP が、TL の TSL 実装の「Scheme territory」の中で識別される構成国以外の構成国において、または、第三国（指令 1999/93/EC の第 7 条第 1 項(a)）において設けられ得るということに留意すべきである。

注記(2):「Scheme territory」（5.3.10 節）内に設けられている QC 発行 CSP の文脈において使用される場合、後述の「Accreditation Revoked」及び「Accreditation Ceased」という 2 つのステータスは、「遷移ステータス」として理解されなければならず、かつ、それらが使用される場合、「Service approval history information」または「Service current status」の中で直後に「Under supervision」で続けられ、可能的には、ここで上述のとおり定義し、図 1 に示すような別の監督ステータスで続けられなければならないものであるので、「Service current status」の値として使用してはならない。関連する監督制度のない関連する「任意の認定」制度のみが存在する場合において、または、「Scheme territory」（5.3.10 節）において CSP が設けられていない場所（すなわち、第三国）にある QC 発行 CSP の文脈において、QC 非発行 CSP の文脈において使用される場合、これらの「Accreditation Revoked」及び「Accreditation Ceased」ステータスは、「Service current status」の値として使用され得る:

- **Accreditation Ceased**:「Service digital identity」（5.5.3 節）の中で識別されるサービスが再評価されることなく、認定評価の有効性が失われた。
- **Accreditation Revoked**:「TSP name」（5.4.1 節）の中で識別される認証サービスプロバイダ（CSP）から提供され、「Service digital identity」（5.5.3 節）の中で識別され、制度基準を満たすものと判断されてきたサービス及び潜在的にはその CSP それ自体が、指令 1999/93/EC に定める条項を遵守し続けていない。

注記(3):QC 発行 CSP 及び QC 非発行 CSP（例:TST 発行タイムスタンプサービスプロバイダ、非適格証明書を発行する CSP 等）に関し、全く同じステータス値が使用されなければならない。「Service Type identifier」（5.5.1 節）は、適用される監督／認定制度の間を区別するために使用される。

注記(4):QC 非発行 CSP に関する国内監督／認定制度のレベルにおいて定義された追加的なステータスと関連する「適格性」情報は、それに該当し、かつ、（例えば、複数の品質／安全性レベルを区別するために）それが要求される場合、サービスレベルで提供され得る。制度運営者は、そのような追加的な「適格性」情報を適用する目的により、「Service information extension」フィールド（5.5.9 節）の「additionalServiceInformation」エクステンション（5.8.2 節）を使用する。加えて、制度運営者は、選択的に、5.5.6 節（Scheme service definition URI）を使用できる。

Current status stating data and time（5.5.5 節）

このフィールドは、必須であり、かつ、現在のステータスが有効となった日時を示す（ETSI TS 102 231 の 5.1.4 節に定義する日時の値）。

Scheme service definition URI（5.5.6 節）

このフィールドは、選択的であり、かつ、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多言語の文字列として制度運営者から提供されるサービス個別情報を依拠者が入手し得る場所の URI を示す。

それが使用される場合、指示される URI は、制度によって指示されるサービスを示す情報へのパスを提供するものでなければならない。とりわけ、このことは、以下が適用される場合を含めることができる:

(a) 切替 CSP が関与する停止（5.5.4 節の「Service current status」参照）におけるサービスの監督の場合において、切替 CSP の識別子を指示する URI；
(b) 5.8.2 節に定義する「additionalServiceInformation」エクステンションをもつ「Service information extension」フィールド（5.5.9 節）の使用との一貫性をもって、監督／認定された信頼サービストークン提供サービスに関する国内的に定められた幾つかの個別の資格の使用と関連する追加情報を提供する文書へと導く URI。

Service supply points（5.5.7 節）

このフィールドは、選択的であり、かつ、それが存在する場合、そのシンタクスが RFC 3986 を遵守する文字列を介して依拠者がアクセスし得る場所の URI を示す。

TSP service definition URI（5.5.8 節）

このフィールドは、選択的であり、それが存在する場合、（義務的な言語として英語（EN）による、及び、可能的なものとして 1 または複数の国内言語による）多国語の文字列として TSL から提供されるサービス特有の情報を依拠者が入手し得る場所の URI を示す。指示される URI は、その TSP によって指示されるサービスを示す情報へのパスを提供しなければならない。

Service information extension（5.5.9 節）

現行の仕様の文脈において、このフィールドは、選択的である。しかし、「Service digital identity」（5.5.3 節）の中で提供される情報が、そのサービスによって発行される適格証明書を紛れなく識別するために十分ではない場合、及びまたは、関連する適格証明書の中で示される情報が、その QC が SSCD によって支えられているか否かという事実の機械処理可能な識別を許容しないものである場合[1]、このフィールドが表示されるものとする。

現行の仕様の文脈において、例えば、CA/QC サービスに関し、その使用が必須である場合、選択的な「Service information extensions」（Sie）情報フィールドが使用され、ETSI TS 102 231 の別紙 L.3.1 の中で定義される「Qualifications」に従い、個々のタプルが以下の情報を提供する 1 または複数のタプルの列として構成される：

－ 「Sdi」により識別される認証サービスを基礎として、当該サービスの詳細（すなわち、適格証明書のセット）を更に識別（フィルタ）するために使用され、そのために、SSCD サポート（及びまたは法人向けの発行）の存在または不存在と関連する追加情報が要求／提供される基準；並びに、
－ この更に識別された適格証明書のサービスのセットが、SSCD によって支えられているか否か（その情報が「QCSSCDStatusAsInCert」の場合、その関連情報が ETSI 標準の機械処理可能なフォームに基づく QC の一部であることを意味する[2]。）に関する関連情報（適格子）、及びまたは、その

[1] この文書の 2.2 節参照。
[2] これは、ETSI が定める QcCompliance 文、QcSSCD 文 [ETSI TS 101 862] または QCP/QCP + ETSI が定める OID [ETSI TS 101 456]の組み合わせを示す。

QC が法人向けに発行されていることと関連する情報（デフォルトとして、それらの QC は、自然人に対してのみ発行されているものと判断される）。

- **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD)：
「Service digital identity」（5.5.3 節）の中で識別され、かつ、「Sdi」により識別される認証サービスを基礎として、当該詳細な適格証明書のセットを更に識別するために使用され、そのために、SSCD サポート（及びまたは法人向けの発行）の存在または不存在と関連する追加情報が要求／提供される上述の（フィルタの）情報によって更に識別されるサービス（QCA）を基礎として発行される QC が SSCD によって支えられていること（すなわち、その証明書中の公開鍵と関係する秘密鍵が、指令 1999/93/EC の別紙 III を満たす安全な署名生成機器の中に記録保存されていること）が、CSP によって確保され、かつ、構成国（それぞれ該当する監督機関または認定機関）によって管理されていること（監督モデル）、または、監査されていること（認定モデル）を意味し；
- **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD)：
「Service digital identity」（5.5.3 節）の中で識別され、かつ、「Sdi」により識別される認証サービスを基礎として、当該詳細な適格証明書のセットを更に識別するために使用され、そのために、SSCD サポート（及びまたは法人向けの発行）の存在または不存在と関連する追加情報が要求／提供される上述の（フィルタの）情報によって更に識別されるサービス（RootCA/QC または CA/QC）を基礎として発行される QC が SSCD によって支えられていないこと（すなわち、その証明書中の公開鍵と関係する秘密鍵が、指令 1999/93/EC の別紙 III を満たす安全な署名生成機器の中に記録保存されていないこと）が、CSP によって確保され、かつ、構成国（それぞれ該当する監督機関または認定機関）によって管理されていること（監督モデル）、または、監査されていること（認定モデル）を意味し；
- **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert)：
「Service digital identity」（5.5.3 節）の中で識別され、かつ、「Sdi」により識別される認証サービスを基礎として、当該詳細な適格証明書のセットを更に識別するために使用され、そのために、SSCD サポート（及びまたは法人向けの発行）の存在または不存在と関連する追加情報が要求／提供される上述の（フィルタの）情報によって更に識別されるサービス（CA/QC）を基礎として発行される QC が SSCD によって支えられているか否かを示す機械処理可能な情報を含むものであることが CSP によって確保され、かつ、構成国（それぞれ該当する監督機関または認定機関）によって管理されていること（監督モデル）、または、監査されていること（認定モデル）を意味し；
- **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson)：
「Service digital identity」（5.5.3 節）の中で識別され、かつ、「Sdi」により識別される認証サービスを基礎として、当該詳細な適格証明書のセットを更に識別するために使用され、そのために、法人向けの発行と関連する情報が要求される上述の（フィルタの）情報によって更に識別されるサービス（QCA）を基礎として発行される QC が、法人向けに発行されるものであることが CSP によって確保され、かつ、構成国（それぞれ該当する監督機関または認定機関）によって管理されていること（監督モデル）、または、監査されていること（認定モデル）を意味する。

そのサービスタイプが http://uri.etsi.org/TrstSvc/Svctype/CA/QC である場合、これらの適格子は、エク

ステンションとしてのみ使用されなければならない。

このフィールドは、実装（ASN.1 または XML）向けのものであり、かつ、ETSI TS 102 231 の別紙L.3.1 に定める仕様を遵守しなければならない。

XML 実装の過程において、追加情報のような個別のコンテントは、第 3 章に定める xsd ファイルを使用してコード化されなければならない。

サービス認定履歴

このフィールドは、選択的であるが、「Historical information period」（5.3.12 節）が非ゼロのときは、表示されなければならない。そして、現行の仕様の文脈において、制度は、履歴情報を保持しなければならない。履歴情報が保持される予定であるが、そのサービスが現在のステータス以前の履歴をもたない場合（すなわち、最初に記録されるステータスの場合、または、履歴情報が制度運営者によって保持されていない場合）、このフィールドは、空欄となる。それ以外の場合においては、ETSI TS 102 231 の 5.3.12 節の示履歴情報保存期間内に生じた TST サービスの現在のステータスにおける個々の変化がある度に、従前に承認されたステータスに関する情報は、ステータスの変動日時の降順で提供される（すなわち、後に承認されたステータスの日時が有効なものとなる）。

このフィールドは、以下に定義する履歴情報の列であるものとする：

TSP (1) Service (1) History (1)

Service type identifier（5.6.1 節）

このフィールドは、必須であり、かつ、「TSP Service Information — Service type identifier」（5.5.1 節）の中で使用されるフォーマット及び意味をもつサービスタイプの識別子を示す。

Service name（5.6.2 節）

このフィールドは、必須であり、かつ、「TSP Service Information —Service name」（5.5.2 節）の中で使用されるフォーマット及び意味をもつ「TSP Service Information — Service type identifier」（5.5.1 節）の中で識別されるサービスを CSP が提供する名称を示す。本項は、5.5.2 節の中で指示されるのと同じ名称を要求しない。名称の変更は、新たなステータスを要求する状況の 1 つとなり得る。

Service digital identity（5.6.3 節）

このフィールドは、必須であり、かつ、同じフォーマット及び意味をもつ「TSP Service Information — Service digital identity」（5.5.3 節）の中で指示されるサービスに固有の少なくとも 1 つのデジタルサービス識別子の表示を示す。

Service previous status（5.6.4 節）

このフィールドは、必須であり、かつ、「TSP Service Information — Service current status」（5.5.4 節）の中で使用されるフォーマット及び意味をもつサービスの従前のステータスの識別子を示す。

Previous status starting data and time（5.6.5 節）

このフィールドは、必須であり、かつ、「TSP Service Information — Service current status starting date and time」（5.5.5 節）の中で使用されるフォーマット及び意味をもつ当の従前のステータスが有効となった日時を示す。

Service information extension（5.6.6 節）

このフィールドは、選択的であり、かつ、「TSP Service Information — Service information extensions」（5.5.9 節）の中で使用されるフォーマット及び意味をもつ個別のサービス関連情報を提供するために制度運営者によって使用され得る。

TSP (1) Service (1) History (2)

…

TSP (1) Service (2)

…

TSP (2) information

…

署名された TSL

現行の仕様に基づいて作成される TSL は、真正性及び完全性を確保するため、「Scheme operator name」（5.3.4 節）によって署名される[1]。

署名のフォーマットが、ASN.1 実装に関しては CAdES BES/EPES であり、また、XML 実装に関しては ETSI TS 101 903 の仕様によって定義される XAdES BES/EPES であることが推奨される[2]。そのよう

[1] ETSI TS 102 231 を全て遵守し、かつ、電子的に署名された構成国の TL の実装は、QES 及び AdES QC の検証及び国境を越える利用を容易にするための真に相互運用性があり、オンラインかつ機械処理可能な枠組みを保証するため、全ての構成国にとっての理念上の目標として理解され得るが、構成国は、実務的な理由により、それらの中間的な方式が安全な経路を通じて伝達されることが確保されていることを条件として、現行の技術仕様に従い、その構成国の TL を中間的な方式で実装することが認められる。

[2] ETSI TS 101 733 または ETSI TS 101 903 によってそれぞれ指示された方法のいずれかによる署名により証明書に署名することを制度運営者が守ることは、義務的なことである。

な電子署名は、ETSI TS 102 231 の別紙 A 及び別紙 B にそれぞれ示される要求事項に適合するものとする。

署名に関する追加的な要求事項は、以下の各節の中で示される。

Scheme identification（5.7.2 節）

このフィールドは、必須であり、かつ、現行の仕様及び構築された TSL の中で示される制度をユニークに識別する制度運営者によって指定された参照を示すものとし、かつ、署名計算の中に含められなければならない。このフィールドは、文字列またはビット列であることが望ましい。

現行の仕様の文脈において、指定される参照は、「TSL type」（5.3.3 節）、「Scheme name」（5.3.6 節）及び TSL に電子的に署名するために制度運営者によって使用される証明書の SubjectKeyIdentifier エクステンションの値を連結したものとする。

Signature algorithm identifier（5.7.3 節）

このフィールドは、必須であり、かつ、署名を作成するために使用された暗号アルゴリズムを示す。使用されたアルゴリズムの相違により、このフィールドは、追加的なパラメータを必要とし得る。このフィールドは、署名計算の中に含められなければならない。

Signature value（5.7.4 節）

このフィールドは、必須であり、かつ、そのデジタル署名の実際の値を含める。（署名の値それ自体を除き）TSL の全てのフィールドは、署名計算の中に含められなければならない。

TSL extensions（5.8 節）

expiredCertsRevocationInfo Extension（5.8.1 節）

このフィールドは、選択的である。使用される場合、このフィールドは、ETSI TS 102 231 の 5.8.1 節の仕様を遵守しなければならない。

additionalServiceInformation Extension（5.8.2 節）

この選択的なエクステンションは、それが使用される場合、サービスレベルにおいてのみ、かつ、5.5.9 節に定義するフィールド（Service information extension）の中においてのみ使用されなければならない。このエクステンションは、サービスに関する追加情報を提供するために使用される。このエクステンションは、個々のタプルが以下の情報を与える 1 または複数のタプルの列とする:

(a) 追加情報を指示する URI、例えば:

— 監督／認定されたサービス提供の信頼サービストークンに関して国内的に定められた個別

の資格を指示する URL、例えば:

- ー QC 非発行 CSP に関する国内監督／認定制度と関連する個別の安全性保証／品質保証のレベル（例:フランス語では、RGS */**/***、ドイツ語では、個別の QC 発行 CSP に関する国内立法によって定められる個別の「監督」ステータス）、「Service current status」（5.5.4 節）の注記(4)参照;
- ー または、監督／認定された信頼サービストークン提供に関する個別の法的ステータス（例:ドイツ語またはハンガリー語では、国内的に定められた「適格 TST」）;
- ー または、「Sdi」フィールドの中に提供される X.509v3 認証の中で表示される個別のポリシー識別子の意味。

ー または、QC を発行する認証サービスプロバイダの内容であるサービスとなる「Sti」で識別されるサービスとの関係を別に定めるために、「Service type identifier」（5.5.1 節）の中で指定される登録された URI（例:OCSP-QC、CRL-QC 及び RootCA-QC）;

(b) その制度において定められる意味をもつ serviceInformation の値を含む選択的な文字列（例:*、**または***）;

(c) 制度固有のフォーマットの中で提供される選択的な追加情報。

URI の区別は、エクステンションを理解するために要する全ての詳細情報を含み、とりわけ、serviceInformation の可能的な値及び個々の値の意味を指示し、与えられた URI を説明する人間が読取可能な文書へ導くものとする。

Qualification Extension（L.3.1 節）

記述文: このフィールドは、選択的であるが、例えば、RootCA/QC または CA/QC に関してその使用が要求される場合、及び、以下の場合、表示される。

- ー 「Service digital identity」内で提供される情報が、そのサービスによって発行される適格証明書を紛れなく識別するためには十分ではなく、
- ー 関連適格証明書の中で表示される情報が、その QC が SSCD によって支えられているか否かに関する事実の機械処理可能な識別を可能とするものではない場合、

それが使用される場合、このサービスレベルエクステンションは、「Service information extension」（5.5.9 節）の中で定義されるフィールドの中においてのみ、使用される。

フォーマット: ETSI TS 102 231 の別紙 L.3 に定義する 1 または複数の Qualification-elements（L.3.1.2 項）の空欄ではない文字列。

第 II 章

ETSI TS 102 231 VERSION 3 に関する ETSI XSD ファイル

この情報は、現在の状態を提供するものである。この xsd ファイルの使用において問題が生ずる場合、その問題は、それを修正する作業のために、ETSI に対して報告されなければならない。

```
<?xml version='1,0' encoding='UTF-8'?>
<!-- edited with XML Spy v4,1 U (http://www.xmlspy.com) by Juan Carlos
Cruellas (UPC Dpt. Arquitectura de Computadors) -->
<!-- ****** NOTICE ******
This version of this document is NOT a formally-approved and issued ETSI
publication.
This document is a Â'work-in-progressÂ' being undertaken by the TC ESI STF
290 and has been revised
to correct identified errors and omissions in the current extant formal
ETSI publication and to
also resolve issues of interpretation raised during implementations based
upon that publication
which are considered to be neither contentious nor to change the
fundamental TSL structure defined
in the original TS 102 231 document and its XSD counterpart.
-->
<xsd:schema targetNamespace='http://uri.etsi.org/02231/v2#"
xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns:ds='http://www.w3.org/2000/09/xmldsig#"
xmlns:tsl='http://uri.etsi.org/02231/v2#" elementFormDefault='qualified'
attributeFormDefault='unqualified'>
        <!-- Imports -->
        <xsd:import namespace='http://www.w3.org/XML/1998/namespace'
schemaLocation='http://www.w3.org/2001/xml.xsd'/>
        <xsd:import namespace='http://www.w3.org/2000/09/xmldsig#"
schemaLocation='http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd'/>
        <!-- Begin auxiliary types -->
        <!--InternationalNamesType-->
        <xsd:complexType name='InternationalNamesType'>
        <xsd:sequence>
        <xsd:element name='Name' type='tsl:MultiLangNormStringType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name='MultiLangNormStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyNormalizedString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:complexType name='MultiLangStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:simpleType name='NonEmptyString'>
        <xsd:restriction base='xsd:string'>
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name='NonEmptyNormalizedString'>
        <xsd:restriction base='xsd:normalizedString'>
```

```
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- AddressType -->
        <xsd:complexType name='AddressType'>
        <xsd:sequence>
        <xsd:element ref='tsl:PostalAddresses'/>
        <xsd:element ref='tsl:ElectronicAddress'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--PostalAddressList Type-->
        <xsd:element name='PostalAddresses'
type='tsl:PostalAddressListType'/>
        <xsd:complexType name='PostalAddressListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:PostalAddress' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--PostalAddress Type-->
        <xsd:element name='PostalAddress' type='tsl:PostalAddressType'/>
        <xsd:complexType name='PostalAddressType'>
        <xsd:sequence>
        <xsd:element name='StreetAddress' type='tsl:NonEmptyString'/>
        <xsd:element name='Locality' type='tsl:NonEmptyString'/>
        <xsd:element name='StateOrProvince' type='tsl:NonEmptyString'
minOccurs='0'/>
        <xsd:element name='PostalCode' type='tsl:NonEmptyString'
minOccurs='0'/>
        <xsd:element name='CountryName' type='tsl:NonEmptyString'/>
        </xsd:sequence>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:complexType>
        <!--ElectronicAddressType-->
        <xsd:element name='ElectronicAddress'
type='tsl:ElectronicAddressType'/>
        <xsd:complexType name='ElectronicAddressType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- Types for extensions in TSL -->
        <xsd:complexType name='AnyType' mixed='true'>
        <xsd:sequence minOccurs='0' maxOccurs='unbounded'>
        <xsd:any processContents='lax'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='Extension' type='tsl:ExtensionType'/>
        <xsd:complexType name='ExtensionType'>
        <xsd:complexContent>
        <xsd:extension base='tsl:AnyType'>
        <xsd:attribute name='Critical' type='xsd:boolean' use='required'/>
        </xsd:extension>
        </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name='ExtensionsListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:Extension' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--NonEmptyURIType-->
        <xsd:simpleType name='NonEmptyURIType'>
        <xsd:restriction base='xsd:anyURI'>
```

```
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!--NonEmptyURIType with language indication-->
        <xsd:complexType name='NonEmptyMultiLangURIType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyURIType'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <!--List of NonEmptyURIType with language indication-->
        <xsd:complexType name='NonEmptyMultiLangURIListType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyMultiLangURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--List of NonEmptyURIType-->
        <xsd:complexType name='NonEmptyURIListType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- End auxiliary types -->
        <!-- ROOT Element -->
        <xsd:element name='TrustServiceStatusList'
type='tsl:TrustStatusListType'/>
        <!-- Trust Status List Type Definition -->
        <xsd:complexType name='TrustStatusListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:SchemeInformation'/>
        <xsd:element ref='tsl:TrustServiceProviderList' minOccurs='0'/>
        <xsd:element ref='ds:Signature'/>
        </xsd:sequence>
        <xsd:attribute name='TSLTag' type='tsl:TSLTagType' use='required'/>
        <xsd:attribute name='Id' type='xsd:ID' use='optional'/>
        </xsd:complexType>
        <!-- TSLTagType -->
        <xsd:simpleType name='TSLTagType'>
        <xsd:restriction base='xsd:anyURI'>
        <xsd:enumeration value='http://uri.etsi.org/02231/TSLTag'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- TrustServiceProviderListType-->
        <xsd:element name='TrustServiceProviderList'
type='tsl:TrustServiceProviderListType'/>
        <xsd:complexType name='TrustServiceProviderListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TrustServiceProvider' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSL Scheme Information -->
        <xsd:element name='SchemeInformation'
type='tsl:TSLSchemeInformationType'/>
        <xsd:complexType name='TSLSchemeInformationType'>
        <xsd:sequence>
        <xsd:element name='TSLVersionIdentifier' type='xsd:integer'
fixed='3'/>
        <xsd:element name='TSLSequenceNumber' type='xsd:positiveInteger'/>
        <xsd:element name='TSLType' type='tsl:NonEmptyURIType'/>
```

```
        <xsd:element name='SchemeOperatorName'
type='tsl:InternationalNamesType'/>
        <xsd:element name='SchemeOperatorAddress' type='tsl:AddressType'/>
        <xsd:element name='SchemeName' type='tsl:InternationalNamesType'/>
        <xsd:element name='SchemeInformationURI'
type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='StatusDeterminationApproach'
type='tsl:NonEmptyURIType'/>
        <xsd:element name='SchemeTypeCommunityRules'
type='tsl:NonEmptyURIListType' minOccurs='0'/>
        <xsd:element ref='tsl:SchemeTerritory' minOccurs='0'/>
        <xsd:element ref='tsl:PolicyOrLegalNotice' minOccurs='0'/>
        <xsd:element name='HistoricalInformationPeriod'
type='xsd:nonNegativeInteger'/>
        <xsd:element ref='tsl:PointersToOtherTSL' minOccurs='0'/>
        <xsd:element name='ListIssueDateTime' type='xsd:dateTime'/>
        <xsd:element ref='tsl:NextUpdate'/>
        <xsd:element ref='tsl:DistributionPoints' minOccurs='0'/>
        <xsd:element name='SchemeExtensions' type='tsl:ExtensionsListType'
minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- SchemeTerritory -->
        <xsd:element name='SchemeTerritory'
type='tsl:SchemeTerritoryType'/>
        <xsd:simpleType name='SchemeTerritoryType'>
        <xsd:restriction base='xsd:string'>
        <xsd:length value='2'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- Policy or Legal Notice -->
        <xsd:element name='PolicyOrLegalNotice'
type='tsl:PolicyOrLegalnoticeType'/>
        <xsd:complexType name='PolicyOrLegalnoticeType'>
        <xsd:choice>
        <xsd:element name='TSLPolicy' type='tsl:NonEmptyMultiLangURIType'
maxOccurs='unbounded'/>
        <xsd:element name='TSLLegalNotice' type='tsl:MultiLangStringType'
maxOccurs='unbounded'/>
        </xsd:choice>
        </xsd:complexType>
        <xsd:element name='NextUpdate' type='tsl:NextUpdateType'/>
        <xsd:complexType name='NextUpdateType'>
        <xsd:sequence>
        <xsd:element name='dateTime' type='xsd:dateTime' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--OtherTSLPointersType-->
        <xsd:element name='PointersToOtherTSL'
type='tsl:OtherTSLPointersType'/>
        <xsd:complexType name='OtherTSLPointersType'>
        <xsd:sequence>
        <xsd:element ref='tsl:OtherTSLPointer' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='OtherTSLPointer'
type='tsl:OtherTSLPointerType'/>
        <xsd:complexType name='OtherTSLPointerType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceDigitalIdentities' minOccurs='0'/>
        <xsd:element name='TSLLocation' type='tsl:NonEmptyURIType'/>
        <xsd:element ref='tsl:AdditionalInformation'/>
        </xsd:sequence>
```

```
        </xsd:complexType>
        <xsd:element name='ServiceDigitalIdentities'
type='tsl:ServiceDigitalIdentityListType'/>
        <xsd:complexType name='ServiceDigitalIdentityListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceDigitalIdentity'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='AdditionalInformation'
type='tsl:AdditionalInformationType'/>
        <xsd:complexType name='AdditionalInformationType'>
        <xsd:choice maxOccurs='unbounded'>
        <xsd:element name='TextualInformation'
type='tsl:MultiLangStringType'/>
        <xsd:element name='OtherInformation' type='tsl:AnyType'/>
        </xsd:choice>
        </xsd:complexType>
        <!--DistributionPoints element-->
        <xsd:element name='DistributionPoints'
type='tsl:ElectronicAddressType'/>
        <!-- TSPType -->
        <xsd:element name='TrustServiceProvider' type='tsl:TSPType'/>
        <xsd:complexType name='TSPType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TSPInformation'/>
        <xsd:element ref='tsl:TSPServices'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPInformationType -->
        <xsd:element name='TSPInformation' type='tsl:TSPInformationType'/>
        <xsd:complexType name='TSPInformationType'>
        <xsd:sequence>
        <xsd:element name='TSPName' type='tsl:InternationalNamesType'/>
        <xsd:element name='TSPTradeName' type='tsl:InternationalNamesType'
minOccurs='0'/>
        <xsd:element name='TSPAddress' type='tsl:AddressType'/>
        <xsd:element name='TSPInformationURI'
type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='TSPInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSP Services-->
        <xsd:element name='TSPServices' type='tsl:TSPServicesListType'/>
        <xsd:complexType name='TSPServicesListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TSPService' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='TSPService' type='tsl:TSPServiceType'/>
        <xsd:complexType name='TSPServiceType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceInformation'/>
        <xsd:element ref='tsl:ServiceHistory' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPServiceInformationType -->
        <xsd:element name='ServiceInformation'
type='tsl:TSPServiceInformationType'/>
        <xsd:complexType name='TSPServiceInformationType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceTypeIdentifier'/>
```

```
        <xsd:element name='ServiceName' type='tsl:InternationalNamesType'/>
        <xsd:element ref='tsl:ServiceDigitalIdentity'/>
        <xsd:element ref='tsl:ServiceStatus'/>
        <xsd:element name='StatusStartingTime' type='xsd:dateTime'/>
        <xsd:element name='SchemeServiceDefinitionURI'
type='tsl:NonEmptyMultiLangURIListType' minOccurs='0'/>
        <xsd:element ref='tsl:ServiceSupplyPoints' minOccurs='0'/>
        <xsd:element name='TSPServiceDefinitionURI'
type='tsl:NonEmptyMultiLangURIListType' minOccurs='0'/>
        <xsd:element name='ServiceInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- Service status -->
        <xsd:element name='ServiceStatus' type='tsl:NonEmptyURIType'/>
        <!-- Type for Service Supply Points -->
        <xsd:element name='ServiceSupplyPoints'
type='tsl:ServiceSupplyPointsType'/>
        <xsd:complexType name='ServiceSupplyPointsType'>
        <xsd:sequence maxOccurs='unbounded'>
        <xsd:element name='ServiceSupplyPoint' type='tsl:NonEmptyURIType'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPServiceIdentifier -->
        <xsd:element name='ServiceTypeIdentifier'
type='tsl:NonEmptyURIType'/>
        <!-- DigitalIdentityType -->
        <xsd:element name='ServiceDigitalIdentity'
type='tsl:DigitalIdentityListType'/>
        <xsd:complexType name='DigitalIdentityListType'>
        <xsd:sequence>
        <xsd:element name='DigitalId' type='tsl:DigitalIdentityType'
minOccurs='0' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name='DigitalIdentityType'>
        <xsd:choice>
        <xsd:element name='X509Certificate' type='xsd:base64Binary'/>
        <xsd:element name='X509SubjectName' type='xsd:string'/>
        <xsd:element ref='ds:KeyValue'/>
        <xsd:element name='X509SKI' type='xsd:base64Binary'/>
        <xsd:element name='Other' type='tsl:AnyType'/>
        </xsd:choice>
        </xsd:complexType>
        <!-- ServiceHistory element-->
        <xsd:element name='ServiceHistory' type='tsl:ServiceHistoryType'/>
        <xsd:complexType name='ServiceHistoryType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceHistoryInstance' minOccurs='0'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='ServiceHistoryInstance'
type='tsl:ServiceHistoryInstanceType'/>
        <xsd:complexType name='ServiceHistoryInstanceType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceTypeIdentifier'/>
        <xsd:element name='ServiceName' type='tsl:InternationalNamesType'/>
        <xsd:element ref='tsl:ServiceDigitalIdentity'/>
        <xsd:element ref='tsl:ServiceStatus'/>
        <xsd:element name='StatusStartingTime' type='xsd:dateTime'/>
        <xsd:element name='ServiceInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
```

```
        </xsd:sequence>
        </xsd:complexType>
        <!-- Elements and types for Extensions -->
        <!-- Extensions children of tsl:VaExtension-->
        <!-- Element ExpiredCertsRevocationInfo -->
        <xsd:element name='ExpiredCertsRevocationInfo'
type='xsd:dateTime'/>
        <!-- Element additionalServiceInformation -->
        <xsd:element name='AdditionalServiceInformation'
type='tsl:AdditionalServiceInformationType'/>
        <xsd:complexType name='AdditionalServiceInformationType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='InformationValue' type='xsd:string'
minOccurs='0'/>
        <xsd:element name='OtherInformation' type='tsl:AnyType'/>
        </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

第 III 章

「SIE」フィールドのコーディングに関する XSD ファイル

この情報は、現在の状態を提供するものである。

```
<?xml version='1,0' encoding='UTF-8'?>
<schema targetNamespace='http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-
1999-93-EC-TrustedList/#" xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns:xades='http://uri.etsi.org/01903/v1.3.2#"
xmlns:tsl='http://uri.etsi.org/02231/v2#"
xmlns:tns='http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-
TrustedList/#" xmlns='http://www.w3.org/2001/XMLSchema'
elementFormDefault='qualified' attributeFormDefault='unqualified'>
        <!--
        <xsd:import namespace='http://uri.etsi.org/02231/v2#"
schemaLocation='./draft_ts102231v030101xsd.xsd'>
</xsd:import>
-->
        <xsd:import namespace='http://uri.etsi.org/01903/v1.3.2#"
schemaLocation='http://uri.etsi.org/01903/v1.3.2/XAdES.xsd'></xsd:import>
        <element name='Qualifications' type='tns:QualificationsType'/>
        <complexType name='QualificationsType'>
        <sequence maxOccurs='unbounded'>
        <element name='QualificationElement'
type='tns:QualificationElementType'/>
        </sequence>
        </complexType>
        <complexType name='QualificationElementType'>
        <sequence>
        <element name='Qualifiers' type='tns:QualifiersType'/>
        <element name='CriteriaList' type='tns:CriteriaListType'/>
        </sequence>
        </complexType>
        <complexType name='CriteriaListType'>
        <sequence>
        <element name='KeyUsage' type='tns:KeyUsageType' minOccurs='0'
```

```
maxOccurs='unbounded'/>
        <element name='PolicySet' type='tns:PoliciesListType' minOccurs='0'
maxOccurs='unbounded'/>
        <element name='otherCriteriaList' type='tsl:AnyType'
minOccurs='0'/>
        </sequence>
        <attribute name='assert'>
        <simpleType>
        <restriction base='xsd:string'>
        <enumeration value='all'/>
        <enumeration value='atLeastOne'/>
        <enumeration value='none'/>
        </restriction>
        </simpleType>
        </attribute>
        </complexType>
        <complexType name='QualifiersType'>
        <sequence maxOccurs='unbounded'>
        <element name='Qualifier' type='tns:QualifierType'/>
        </sequence>
        </complexType>
        <complexType name='QualifierType'>
        <attribute name='uri' type='anyURI'/>
        </complexType>
        <complexType name='PoliciesListType'>
        <sequence maxOccurs='unbounded'>
        <element name='PolicyIdentifier'
type='xades:ObjectIdentifierType'/>
        </sequence>
        </complexType>
        <complexType name='KeyUsageType'>
        <sequence maxOccurs='9'>
        <element name='KeyUsageBit' type='tns:KeyUsageBitType'/>
        </sequence>
        </complexType>
        <complexType name='KeyUsageBitType'>
        <simpleContent>
        <extension base='xsd:boolean'>
        <attribute name='name'>
        <simpleType>
        <restriction base='xsd:string'>
        <enumeration value='digitalSignature'/>
        <enumeration value='nonRepudiation'/>
        <enumeration value='keyEncipherment'/>
        <enumeration value='dataEncipherment'/>
        <enumeration value='keyAgreement'/>
        <enumeration value='keyCertSign'/>
        <enumeration value='crlSign'/>
        <enumeration value='encipherOnly'/>
        <enumeration value='decipherOnly'/>
        </restriction>
        </simpleType>
        </attribute>
        </extension>
        </simpleContent>
        </complexType>
</schema>
```

第 IV 章

人間が読取可能な方式による信頼リストの TSL 実装の仕様

人間が読取可能（HR）な方式による信頼リストの TSL 実装は、公衆が利用可能なものとされ、かつ、電子的な手段でアクセス可能なものとされる。それは、PDF/A（ISO 19005）プロファイルに従ってフォーマットされなければならない ISO 32000 に従った Portable Document Format（PDF）文書の方式により、提供される。

PDF/A ベースの HR 方式による信頼リストの TSL 実装の内容は、以下の要求事項を遵守する：

- HR 方式の構成は、TS 102 231 の 5.1.2 節に示す論理モデルを反映するものとすること；
- 現行の全てのフィールドが表示され、かつ、以下の事項を提供すること：
  - フィールドの標題（例：「Service type identifier」）；
  - フィールドの値（例：「CA/QC」）；
  - 該当するときは、かつ、とりわけ、ETSI TS 102 231 の別紙 D の中で定められており、または、登録された URI に関する現行の仕様において定められているような、フィールドの値の意味（記述）（例：「公開鍵証明書を発行する認証局」）；
  - 該当するときは、その信頼リストの TSL 実装の中で定められる複数の自然言語の版。
- 以下のフィールド及び「Service digital identity」フィールドの中で表示されるデジタル証明書の対応する値は、ミニマムのものとして、HR 方式により表示される：
  - 版、
  - シリアル番号、
  - 署名アルゴリズム、
  - 発行者、
  - 有効期間の開始時、
  - 有効期間の終了時、
  - 主体、
  - 公開鍵、
  - 認証ポリシー、
  - 主体鍵識別子、
  - CRL 提供場所、
  - 認証局鍵識別子、
  - 鍵の用法、
  - 基本的な制限、
  - 拇印アルゴリズム、
  - 拇印、
- HR 方式は、容易に印刷可能なものとし、
- HR 方式は、電子的に署名され得る。署名される場合、その信頼リストの TSL 実装のためのものと同じ署名仕様に従い、制度運営者によって署名されなければならない。