Specifications of a Common Template for the "Trusted List of Supervised/Accredited Certification Service Providers" versus ETSI TS 102 231

SEALED

Trust Services Architects

Focus shift from Technology to Trust issues

Regarding eSignatures:

- Legal framework is in place (eSignature Directive)
- Technology framework is in place (e.g., PKI, WPKI)
- Standardisation landscape is in place (ETSI/CEN from EESSI)

But there are still issues:

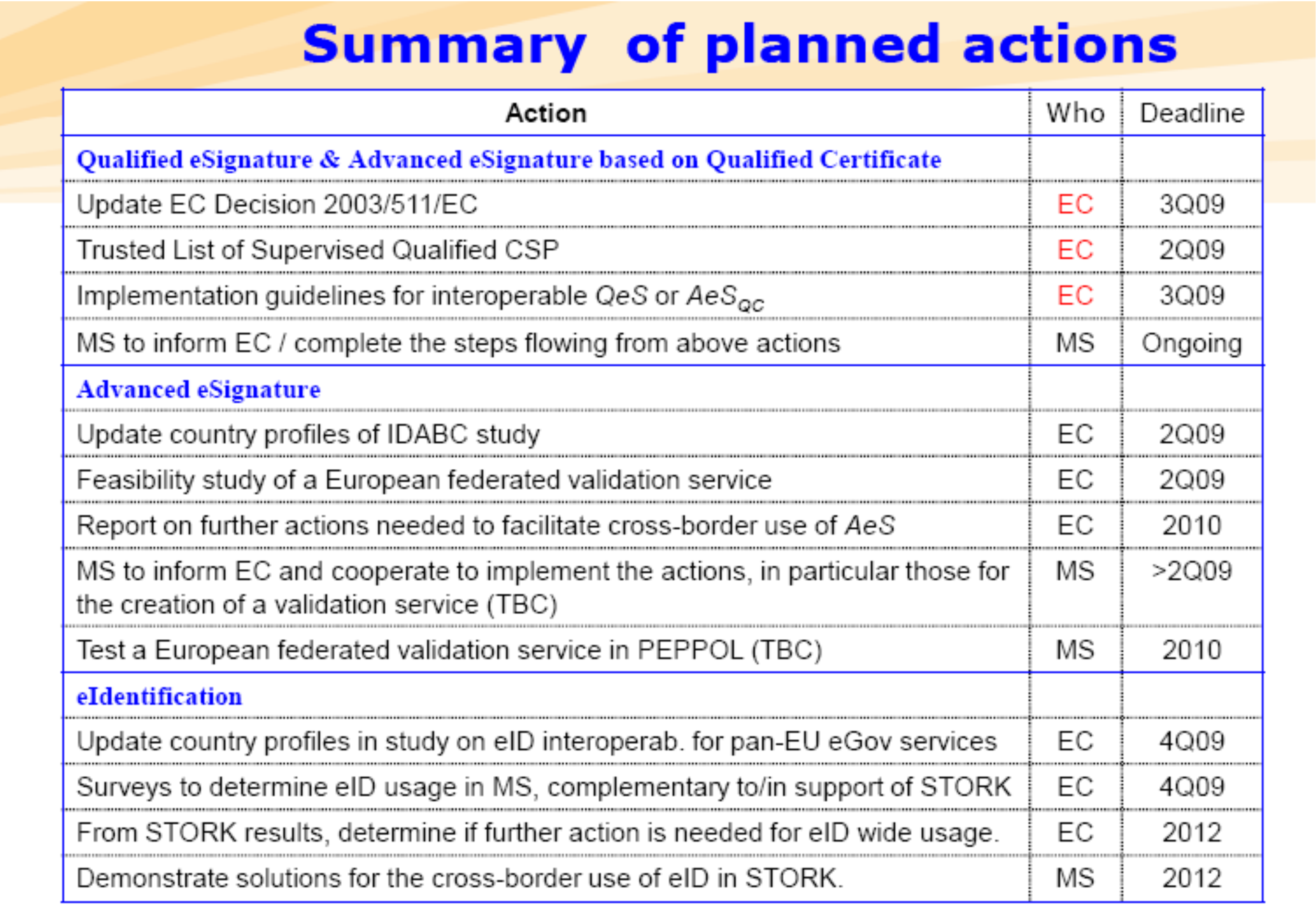
- Standardisation landscape is inappropriate (despite some successes)
  ➡ Global reshaping and restructuring required
- Insufficient mapping between eSig DIR requirements & standardisation deliverables (even if successful for what has been referenced)
  ➡ No review of the eSignature Directive but Decision update
- Those have resulted in a lack of truly interoperable eSignature applications even if usage is growing (e.g., 1. eGov, 2. eDoc, 3. eTrade (financial services, eInv, eProc))
- Not enough Trust in those existing frameworks ➡ **eSignature Action Plan + CROBIES**

eSignature Action Plan – COM(2008)798

Actions to enhance interoperability of

Part I: eSignatures

Part II: electronic identity



Summary of planned actions

Action	Who	Deadline
Qualified eSignature & Advanced eSignature based on Qualified Certificate		
Update EC Decision 2003/511/EC	EC	3Q09
Trusted List of Supervised Qualified CSP	EC	2Q09
Implementation guidelines for interoperable *QeS* or AeS_{QC}	EC	3Q09
MS to inform EC / complete the steps flowing from above actions	MS	Ongoing
Advanced eSignature		
Update country profiles of IDABC study	EC	2Q09
Feasibility study of a European federated validation service	EC	2Q09
Report on further actions needed to facilitate cross-border use of *AeS*	EC	2010
MS to inform EC and cooperate to implement the actions, in particular those for the creation of a validation service (TBC)	MS	>2Q09
Test a European federated validation service in PEPPOL (TBC)	MS	2010
eIdentification		
Update country profiles in study on eID interoperab. for pan-EU eGov services	EC	4Q09
Surveys to determine eID usage in MS, complementary to/in support of STORK	EC	4Q09
From STORK results, determine if further action is needed for eID wide usage.	EC	2012
Demonstrate solutions for the cross-border use of eID in STORK.	MS	2012

CROBIES – Cross-Border Interoperability of eSignatures

eSig Standard° aspects Study (ESSS):

- Quick-wins on QES & QCSP recognition
- Global reshaping of eSig standardisation
- Decision update
- Marketing

CROBIES:

- specific focus on
  - Trust(ed) Lists of QCSPs
  - Common Supervision Model of QCSP's Practices
  - Interoperable QC Profile
  - Interoperable AdES (QES) formats
  - Interoperable SSCD Profile
- Providing input to:
  - ▪ Quick-wins in IOP for use of QES and AdES+QEC
  - ▪ Collaboration with ESOs for eSig. standardisation reshaping
  - ▪ Better mapping between eSig Directive & Std° deliverables
  - ▪ eSig Action Plan – PART 1, 2.1 (active) & 2.2 (input)

eSig Action Plan - (2.1 eSignatures)

- §7: CROBIES as supporting study
- **Q3 2009**: Update of Decision 2003/511/EC (as a result of "standardisation reshaping" initiated from CROBIES & ESSS)
- **Q2 2009**: Compiled "Trusted List" at EU level
- **Q3 2009**: Guidelines and Guidance on common rqmts to implement QES & AdES +QC

General principles – fine-tuned scope

- Trusted List for supervised/accredited CSPs:
    - "Supervision/Accreditation Status List of those services from Certification Service Providers that are supervised/accredited by a Member State for compliance with the relevant provisions laid down in the eSignature Directive 1999/93/EC".
    - *Defines the (approval) "Scheme" as per ETSI TS 102 231*
    - *Covers "CSPs" as defined in eSignature Directive, i.e., covering*
        - *CSP issuing QC*
        - *CSP not issuing QC*
    - *Supervision/Accreditation status provided at "service" level and not at CSP level*
    - *One single list of supervision/accreditation of services*
    - *Status determination approach: "appropriate"*

General principles – fine-tuned scope

- **Scope of the List**:
  - "Qualified CSP" not defined as such by Directive but well "CSP":

    where "certification-service-provider means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" – Art 2.11 eSig. Dir. 1999/93/EC

    - CSP issuing QC
    - CSPs not issuing QC (providing other certification services)
  - Some MS have national laws, and supervision/accreditation schemes for CSP issuing TST, CSP issuing non-QC, etc.
  - Importance to not discriminate between two sets of CSPs being covered by the Directive
    - CSP issuing QC: Sup./Accr. Frameworks and criteria defined in DIR
      - Established "appropriately" at MS level
      - Trust framework established
    - Other CSPs: Accr. Framework defined in DIR for but no additional criteria
      - May be established / extended in accordance at MS level
      - Trust framework not established
  - *TL should allow facilitating trust in all supervised/accredited CSP*
  - *According to a common agreed template (which is possible from simple fine-tuning of current Technical Specifications)*

General principles

- Certification Service Providers (in the sense of 1999/93/EC):

  ("means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" – Art 2.11 eSig. Dir.)

  - **CAs issuing QC** (Qualified Certificates)
    - Must be supervised and may be accredited as being compliant with the relevant provisions laid down in the eSig. Dir.
    - Mandatory part of the TL
    - For which there would be no "need" to have details about underlying supervision/accreditation systems since the trust framework is set up by the Directive
  - **Other CSPs** (not issuing QC)
    - Optional part of the TL, on MS voluntary basis, with regards to supervision/ accreditation scheme(s) defined at MS level, implementing or extending (supervision of-model for) compliance with the provisions laid down in 1999/93/EC
    - **provided** they are supervised/accredited as being compliant with the relevant provisions laid down in the eSig. Dir.
      - As based on National schemes
    - For which the provision of information about the supervision/accreditation systems is "essential" since the trust framework is not set up by the Directive

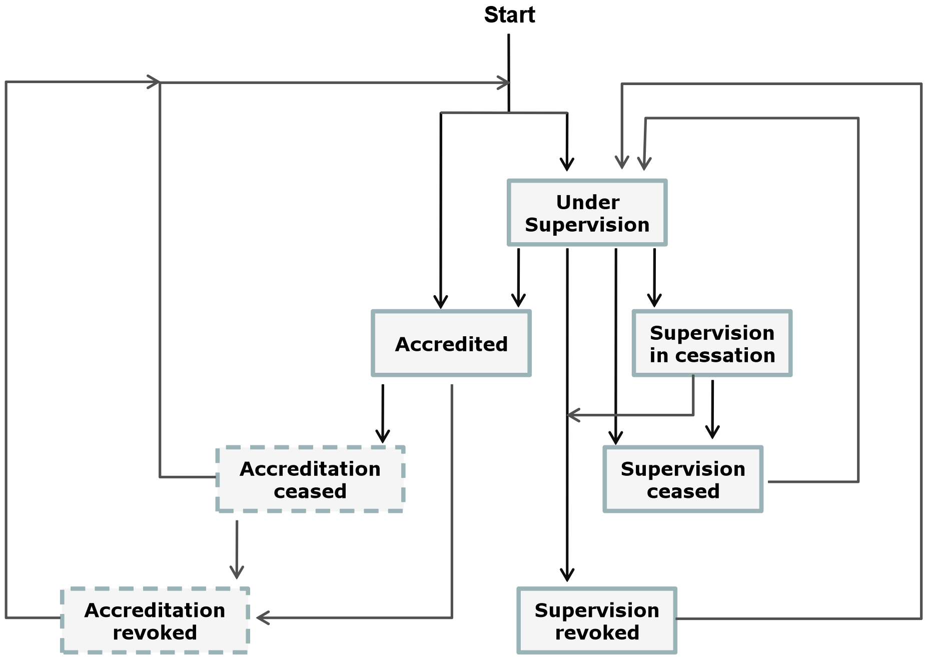
General principles – fine-tuned scope

- Trusted List for supervised/accredited CSPs:
  - "Supervision/Accreditation Status List of those services from Certification Service Providers, established in a Member State and that are supervised/accredited as being compliant with the relevant provisions laid down in the eSignature Directive 1999/93/EC".
  - *Defines the (approval) "Scheme" as per ETSI TS 102 231*
  - *Supervision/Accreditation status at "service" level and not at CSP level*
    - *A single "entity, legal or natural person" can provide several types of services, being supervised / accredited accordingly and independently (differently) from one service to another*
    - *E.g., a single organisation can:*
      - *Provide certification services being issuance of QC that must be supervised and may be accredited; and*
      - *Provide certification services being issuance of nonQ certificates being supervised (or not, or even accredited or not) according to another scheme*
      - *Provide certification services being issuance of TST that may be accredited as QTST according to National Law in an national "extended" implementation framework of the 1999/93/EC eSig Directive*

General principles

- Supervision & Accreditation
  - One single list for listing supervised/accredited services
  - One single "framework" for supervision/accreditation status flow to be used by MS to indicate current/previous status of any listed service

Expected supervision/accreditation status flow for a single CSP service



Start

Under Supervision

Accredited

Supervision in cessation

Accreditation ceased

Supervision ceased

Accreditation revoked

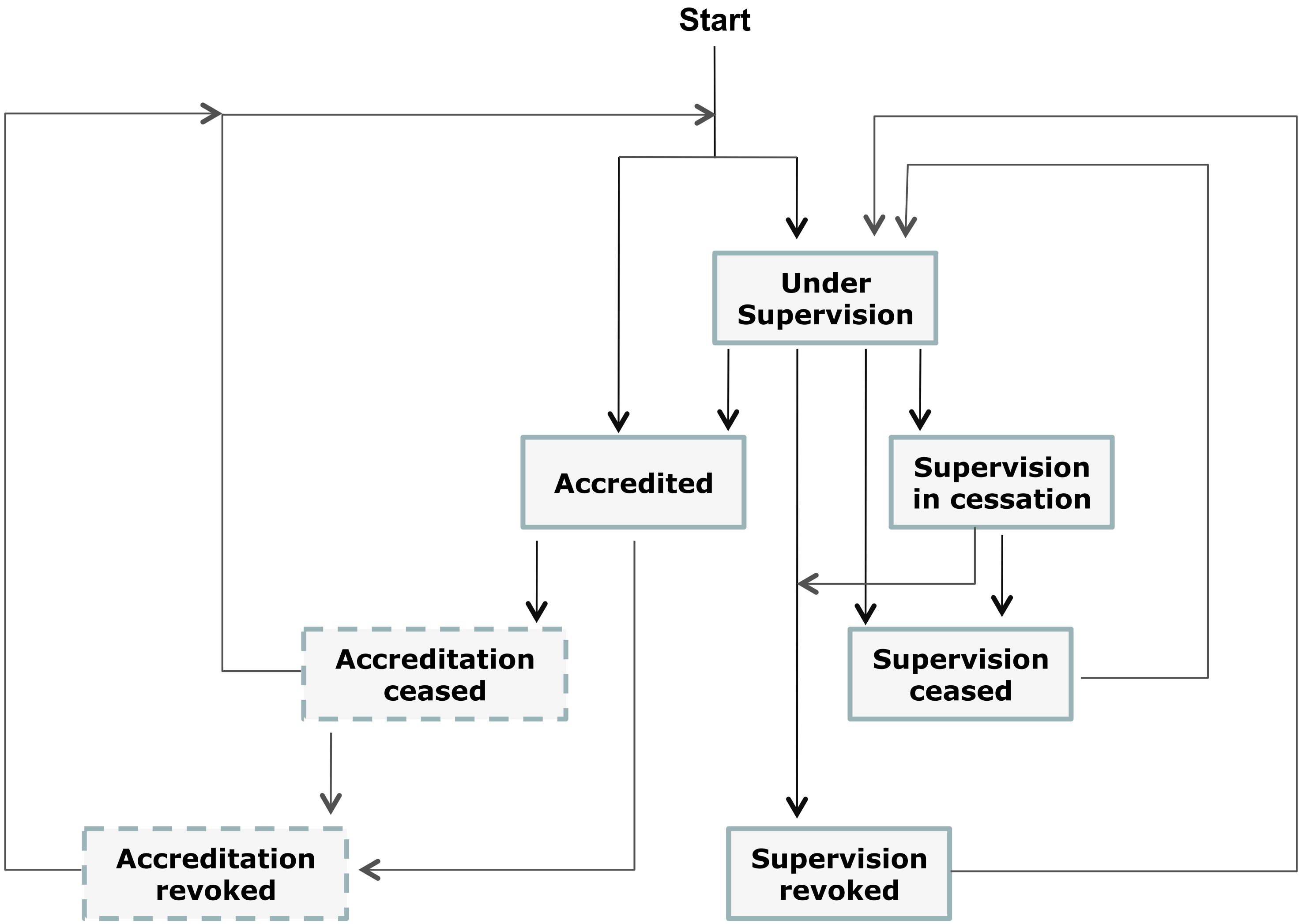
Supervision revoked

Legend:

▭ Transit Status when there is an associated supervision model (e.g., as it must be the case for CSP issuing QC), Possible Current Status for when there is no associated supervision model (only for CSP not issuing QC)

▭ Possible Current Status

Expected supervision/accreditation status flow for a single CSP service



Start

Under Supervision

Accredited

Supervision in cessation

Accreditation ceased

Supervision ceased

Accreditation revoked

Supervision revoked

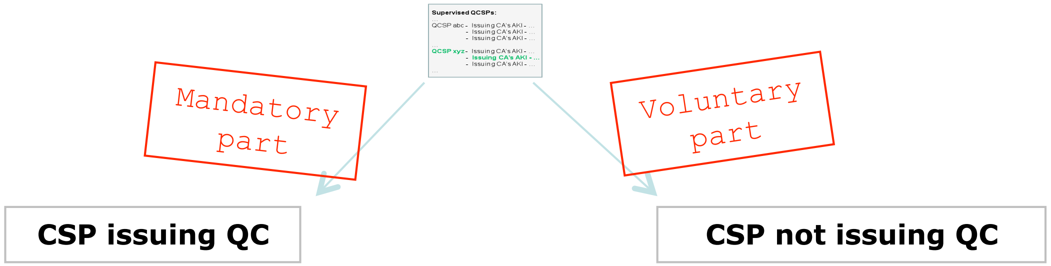
Legend:

⬚ Transit Status when there is an associated supervision model (e.g., as it must be the case for CSP issuing QC), Possible Current Status for when there is no associated supervision model (only for CSP not issuing QC)

▭ Possible Current Status

General principles

MS Trusted List of supervised/accredited CSPs



Supervised QCSPs:

...

QCSP abc - Issuing CA's AKI - ...
- Issuing CA's AKI - ...
- Issuing CA's AKI - ...

...

QCSP xyz - Issuing CA's AKI - ...
- **Issuing CA's AKI - ...**
- Issuing CA's AKI - ...

...

CSP issuing QC

- CSP compliant with Annex II and issuing QC compliant with Annex I

- that are supervised/accredited according to the provisions laid down in the eSig. Directive:

○ "supervision" (eSig. Dir.):
  - Art.3.3, Art. 8.1, Art. 11.
  - recital (13)

○ "voluntary accreditation" (eSig. Dir.):
  - Art. 2.13
  - Art. 3.2, 7.1(a), 8.1, 11
  - recitals (4, 11-13)

- with those "supervision"/"voluntary accreditation" systems being "defined" and associated to a trust framework established under the eSig. Dir.

CSP not issuing QC

- CSP issuing nonQ certificates

- CSP issuing Time-Stamp Tokens
  - may be labelled as "Qualified" but according to National Laws

- CSP providing Archiving services

- Other CSPs ...

that are supervised/accredited according to the provisions laid down in the eSig. Directive and extended as per National Laws

○ "supervision" (eSig. Dir.):
  - same spirit as per eSig. Dir.

○ "voluntary accreditation" (eSig. Dir.):
  - recitals (4, 11-13)
  - Art. 2.13
  - Art. 3.2, 8.1, 11

Note: Must include revocation services when info not present in AIA field of end certificates, and when not signed by CA being part of listed CAs (hierarchy)

Principles

- List organised per CSP and then per service;
- Clear distinction between service types:
  - CA/QC or RootCA/QC
  - CA/PKC
  - TSA/TST (additional qualifications defined at national level)
  - OCSP, OCSP/QC
  - CRL, CRL/QC
  - Etc.
- Sup°/Accred° status is given service per service
  - according to one set of values with defined flows between values
  - For which the meaning is defined per service type and through the respective ...
- Definition of National Sup/Acc. Schemes:
  - CSP_{QC} supervision scheme
  - CSP_{QC} Accred° scheme if any
  - Other CSP supervision and/or accreditation scheme(s)

  provided through "Scheme information URIs"

  and potential sub-levels on a per service level

General principles – Editing rules – listed services per CSP

The general editing guidelines would be as such (services from CSP issuing QC):

1.If it is ensured (guarantee provided by CSP and supervised/accredited by Supervisory Body (SB) / Accreditation Body (AB)) that, "under a listed service identified by a "Sdi", any QC supported by an SSCD does contain QcC statement, and does contain QcSSCD statement and/or QCP+ oid, then the use of an appropriate "Sdi" is sufficient and the "Sie" field can be used in option, and the status information will not need to contain SSCD support information.

2.If it is ensured (guarantee provided by CSP and supervised/accredited by SB/AB) that, "under a listed service identified by a "Sdi", any QC not supported by an SSCD does contain either QcC statement and/or QCP oid, and it is such that it is meant to not contain QcSSCD statement or QCP+ oid, then the use of an appropriate "Sdi" is sufficient and the "Sie" field can be used in option and will not need to contain SSCD support information (meaning it is not supported by an SSCD)

3.If it is ensured (guarantee provided by CSP and supervised/accredited by SB/AB) that, "under a listed service identified by a "Sdi", QC does contain QcC statement, AND SOME OF THESE QC ARE MEANT TO BE SUPPORTED BY SSCDs AND SOME NOT (e.g. this may be differentiated by different QCSP specific Certificate Policy oids or through other QCSP specific information in the QC, directly or indirectly, machine processable or not), BUT IT CONTAIN NEITHER the QcSSCD statement NOR the ETSI QCP(+) oid , then the use of an appropriate "Sdi" may not be sufficient AND the "Sie field shall be used to indicate explicit SSCD support information together with potential information extension to precise the covered set of certificates. This is likely to require a sequence of several tuples of "Sie" values including different “SSCD support information values“ for a same “Sdi”.

4.If it is ensured (guarantee provided by CSP and supervised/accredited by SB/AB) that "under a listed service identified by a "Sdi", QC does not contain QcC statement, the QCP oid, the QcSSCD statement, and the QCP+ oid but it is ensured that some of these end-entity certificates issued under this "Sdi" are meant to be QC and/or supported by SSCDs and some not (e.g. this may be differentiated by different CSP specific Certificate Policy oids or through other CSP specific information in the QC, directly or indirectly, machine processable or not), then the use of an appropriate "Sdi" will not be sufficient AND the "Sie" field must be used including explicit SSCD support information. This is likely to require a sequence of several tuples of "Sie" values including different “SSCD support information values“ for a same “Sdi”.

CSP$_{QC}$ principles – Editing /usage rules – per listed services

A “CA/QC” (respectively “RootCA/CA/QC”) “Sti” entry

- indicates that from the “Sdi” identified CA (respectively within the CAs hierarchy starting from the “Sdi” identified RootCA),

  all issued end-entity certificates **are QC provided that** it is claimed as such in the certificate through the use of appropriate QcStatements (i.e., QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs

  (and this is ensured by Supervisory/Accreditation Body)

- and **IF** an “Sie” information is present,

  then in addition to this default edition/usage interpretation rule,

  those certificates that are further identified through the use of “Sie” constructed on the principle of a sequence of “filters to the result of which are associated some additional information regarding “SSCD support” and/or “Legal person as subject” ”

  (e.g., those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension) are to be considered according to “qualifiers” completing the lack of information in the QC, i.e.,:

  SSCD support:

  Value: “QC supported by an SSCD”
  Value: “QC not supported by an SSCD”
  Value : “QC SSCD support as indicated in certificate”

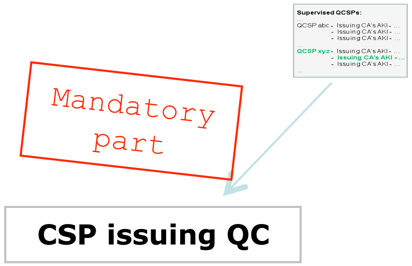
  AND/OR

  Legal Person:

  Value: “Certificate issued to a Legal Person”

CSP_{QC} principles

MS Trusted List of supervised/accredited CSPs



Supervised QCSPs:

...

QCSP abc - Issuing CA's AKI - ...
- Issuing CA's AKI - ...
- Issuing CA's AKI - ...

...

QCSP xyz - Issuing CA's AKI - ...
- **Issuing CA's AKI - ...**
- Issuing CA's AKI - ...

...

CSP issuing QC

- CSP compliant with Annex II and issuing QC compliant with Annex I

- that are supervised/accredited according to the provisions laid down in the eSig. Directive:

○ "supervision" (eSig. Dir.):
- Art.3.3, Art. 8.1, Art. 11.
- recital (13)

○ "voluntary accreditation" (eSig. Dir.):
- Art. 2.13
- Art. 3.2, 8.1, 11
- recitals (4, 11-13)

- with those "supervision"/"voluntary accreditation" systems being "defined" and associated to a trust framework established under the eSig. Dir.

Specific principles for CSP services issuing QC

- Clear distinction of the service type "issuing QC": CA/QC or RootCA/QC
- Sup°/Accred° status is given service per service
  - according to one set of values with defined flows between values
  - For which the meaning is defined per service type
    - CSP_{QC} supervision scheme, or
    - CSP_{QC} Accred° scheme
- Editing / usage rules

A ("RootCA/CA/QC") "CA/QC" "Sti" entry indicates that (within the CAs hierarchy starting) from the "Sdi" identified (Root)CA, all end-entity issued certificates **are QC provided that** it is claimed as such in the certificate through the use of appropriate QcStatements (i.e., QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs (and this is ensured by Supervisory/Accreditation Body, see section 2.2 in "Technical specifications"),

and **IF** an "Sie" information is present, then in addition to this default edition/usage interpretation rule, those certificates that are further identified through the use of "Sie" constructed on the principle of a sequence of "filters to the result of which are associated some additional information" (e.g., those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through a specific "name constraint", and/or filtered through the use of a specific value to appear in one specific certificate field or extension) are to be considered according to "complementary characteristic information", i.e.,:

SSCD support:
Value: "QC supported by an SSCD"
Value: "QC not supported by an SSCD"

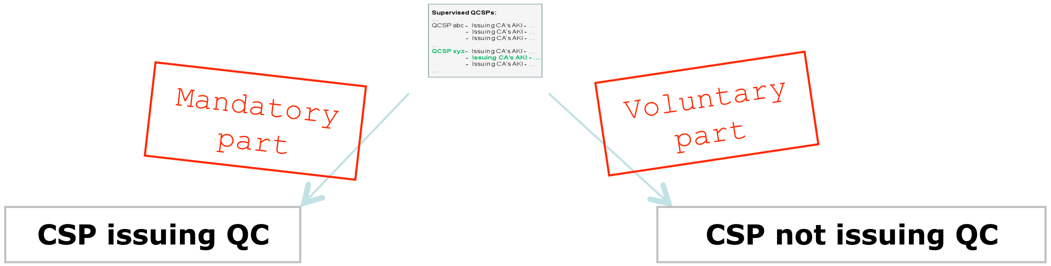
AND/OR

Legal Person:
Value: "Certificate issued to a Legal Person"

Note:
- Possible to explicitly use each one of these values (e.g., it must be possible to say that "this is not supported by an SSCD"), one per set of course when applying such values to the result of a filter.
- Possible to have both characteristics applied, e.g., (No)SSCD+LegalPerson

General principles

MS Trusted List of supervised/accredited CSPs



Supervised QCSPs:

…
QCSP abc - Issuing CA's AKI - …
- Issuing CA's AKI - …
- Issuing CA's AKI - …
…
QCSP xyz - Issuing CA's AKI - …
- **Issuing CA's AKI - …**
- Issuing CA's AKI - …
…

CSP issuing QC

CSP not issuing QC

- CSP compliant with Annex II and issuing QC compliant with Annex I

- **that must be supervised and may be accredited** according to the provisions laid down in the eSig. Directive:

○ "supervision" (eSig. Dir.):
  - recital (13)
  - Art.3.3, Art. 8.1, Art. 11.

○ "voluntary accreditation" (eSig. Dir.):
  - recitals(4, 11-13)
  - Art. 2.13
  - Art. 3.2, 8.1, 11

- CSP issuing nonQ certificates

- CSP issuing Time-Stamp Tokens
  - may be labelled as "Qualified" but according to National Laws

- CSP providing Archiving services

- Other CSPs ...

provided they are supervised / accredited according to the provisions laid down in the eSig. Directive and extended as per National Laws

○ "supervision" (eSig. Dir.):
  - same spirit as per eSig. Dir.

○ "voluntary accreditation" (eSig. Dir.):
  - recitals(4, 11-13)
  - Art. 2.13
  - Art. 3.2, 8.1, 11

Note: Must include revocation services when info not present in AIA field of end certificates, and when not signed by CA being part of listed CAs (hierarchy)

Examples

- FR – RGS/GSD (Référentiel Général de Sécurité/General Security Directory) :
  - Service type: CA/PKC
  - Scheme info available from TL (URIs)
  - Granularity: 3 defined levels (*/**/***) can be indicated using clause 5.5.6
- MT – Government regulated CSP issuing nonQC:
  - Service type: CA/PKC
  - Scheme info available from TL (URIs)

Examples

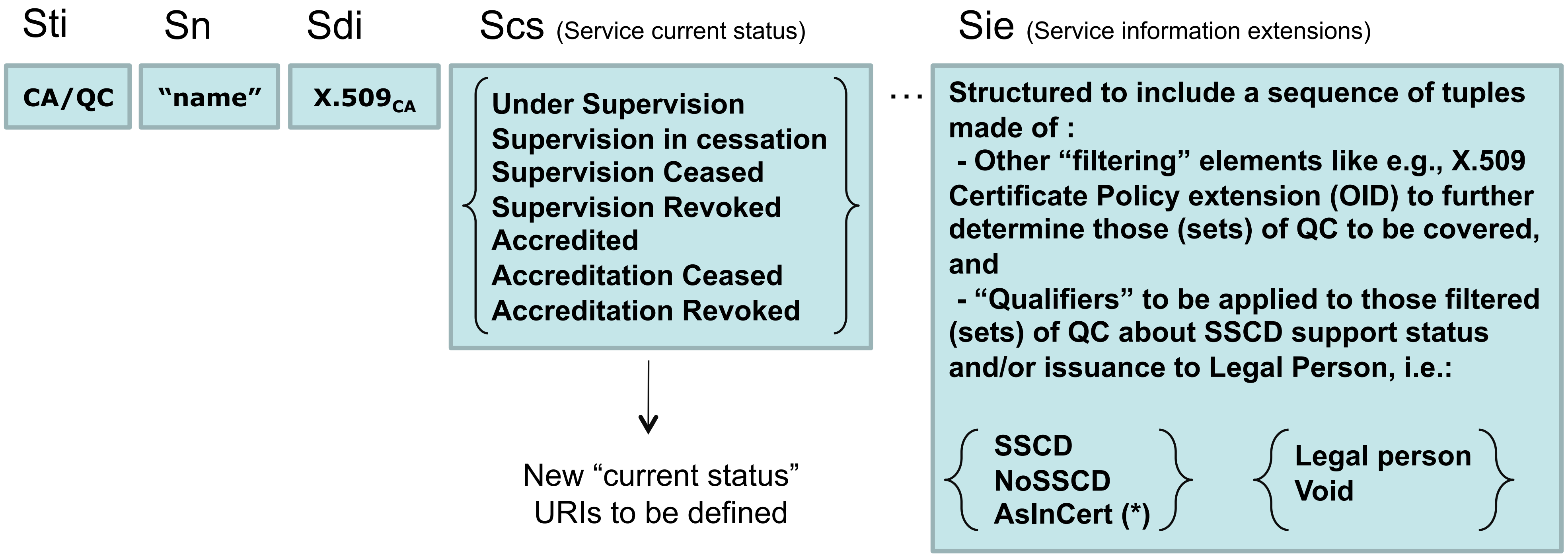
- HU – supervision of TSA for which a TST qualified level has been defined in HU law :
  - Service type: TSA/TST
  - Clause 5.5.6 for national qualification
  - Scheme info available from TL (URIs)
  - Supervision status
- DE – accreditation of TSA for which a TST qualified level has been defined in DE law
  - Service type: TSA/TST + clause 5.5.6 for national Q
  - Scheme info available from TL (URIs)
  - Accreditation status

General principles – Supervision/Accreditation Body(ies) / TSL Op^{tor}

- With regards to the TL, MS may have separate:
  - Supervisory Body
  - Accreditation Body
  - Operational Body (incl. for TSL related operations)
  - Etc.
- MS to designate one body as TSL “Scheme operator”
- Each MS Body associated to the T(S)L will have its own responsibility and liability according to national laws
- Any situation in which several bodies are responsible for supervision, accreditation or operational aspects SHALL be consistently reflected and identified as such in the Scheme information as part of the TSL, including in the scheme-specific information indicated by the "Scheme information URI" (clause 5.3.7).
- The named Scheme Operator (clause 5.3.4) is expected to sign the TSL.

General principles – Editing rules – CSP$_{QC}$ entries (listed services)

Service entry for a listed CSP$_{QC}$:



Sti

CA/QC

Sn

“name”

Sdi

X.509$_{CA}$

Scs (Service current status)

- Under Supervision
- Supervision in cessation
- Supervision Ceased
- Supervision Revoked
- Accredited
- Accreditation Ceased
- Accreditation Revoked

New “current status” URIs to be defined

. . .

Sie (Service information extensions)

Structured to include a sequence of tuples made of :

- Other “filtering” elements like e.g., X.509 Certificate Policy extension (OID) to further determine those (sets) of QC to be covered, and
- “Qualifiers” to be applied to those filtered (sets) of QC about SSCD support status and/or issuance to Legal Person, i.e.:

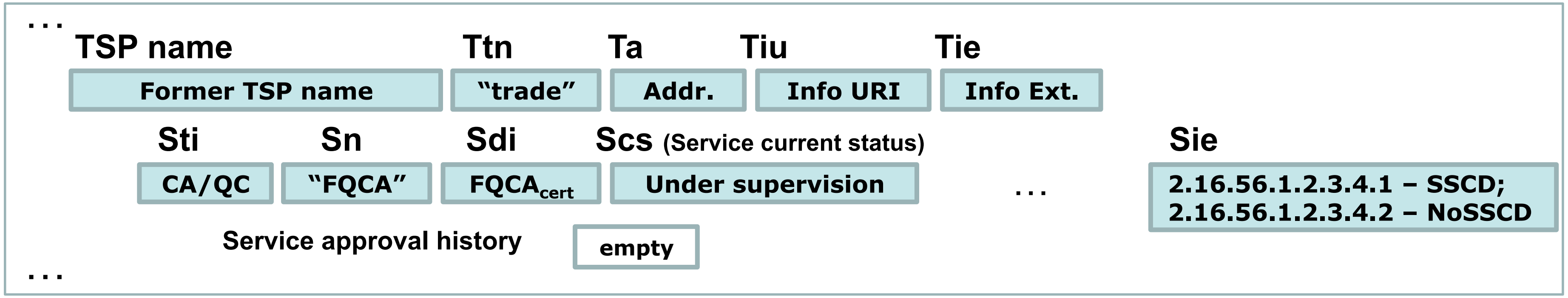
SSCD
NoSSCD
AsInCert (*)

Legal person
Void

(*) meaning that such information is ensured to be contained in any QC under Sdi-[Sie] defined QCA (if nothing in QC, then meaning is NoSSCD)

CSP QC issuing services cessation from "Under Supervision" status

Former entry into TL regarding the TSP in cessation, i.e.,



…

TSP name | Ttn | Ta | Tiu | Tie

Former TSP name | "trade" | Addr. | Info URI | Info Ext.

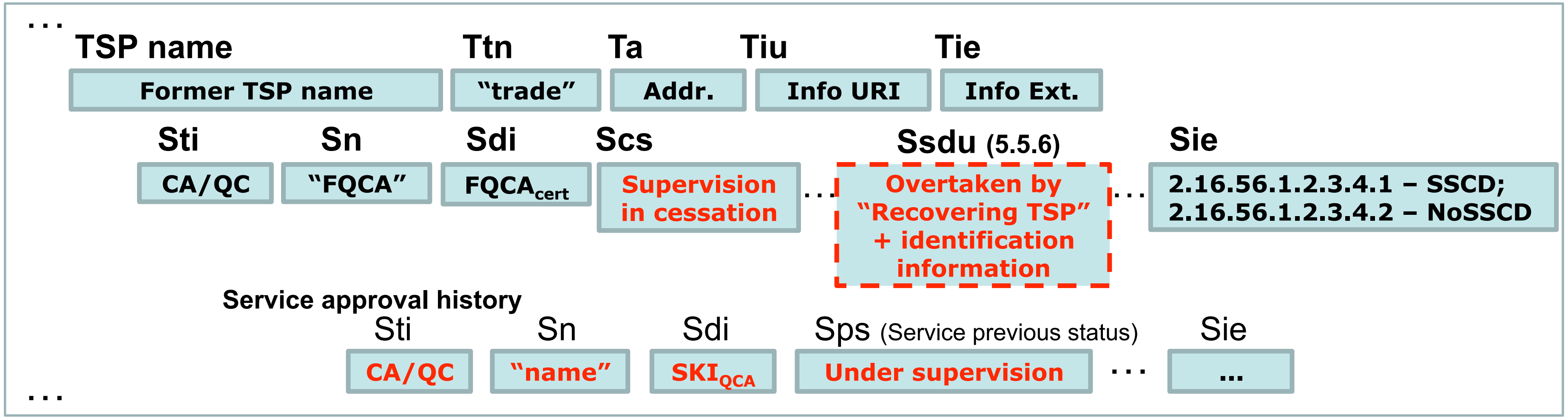
Sti | Sn | Sdi | Scs (Service current status) | Sie

CA/QC | "FQCA" | FQCA$_{cert}$ | Under supervision | … | 2.16.56.1.2.3.4.1 – SSCD; 2.16.56.1.2.3.4.2 – NoSSCD

Service approval history | empty

…

becomes, once it is acted by the Supervision Body to be in cessation,



…

TSP name | Ttn | Ta | Tiu | Tie

Former TSP name | "trade" | Addr. | Info URI | Info Ext.

Sti | Sn | Sdi | Scs | Ssdu (5.5.6) | Sie

CA/QC | "FQCA" | FQCA$_{cert}$ | Supervision in cessation | … | Overtaken by "Recovering TSP" + identification information | … | 2.16.56.1.2.3.4.1 – SSCD; 2.16.56.1.2.3.4.2 – NoSSCD

Service approval history

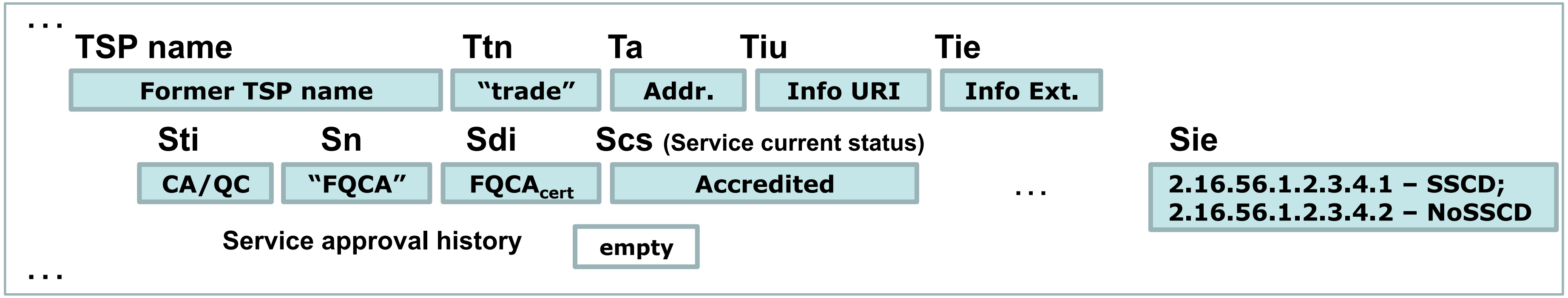
Sti | Sn | Sdi | Sps (Service previous status) | Sie

CA/QC | "name" | SKI$_{QCA}$ | Under supervision | … | ...

…

CSP issuing QC service cessation from “Accredited” status

Former entry into TL regarding the TSP in cessation, i.e.,



…

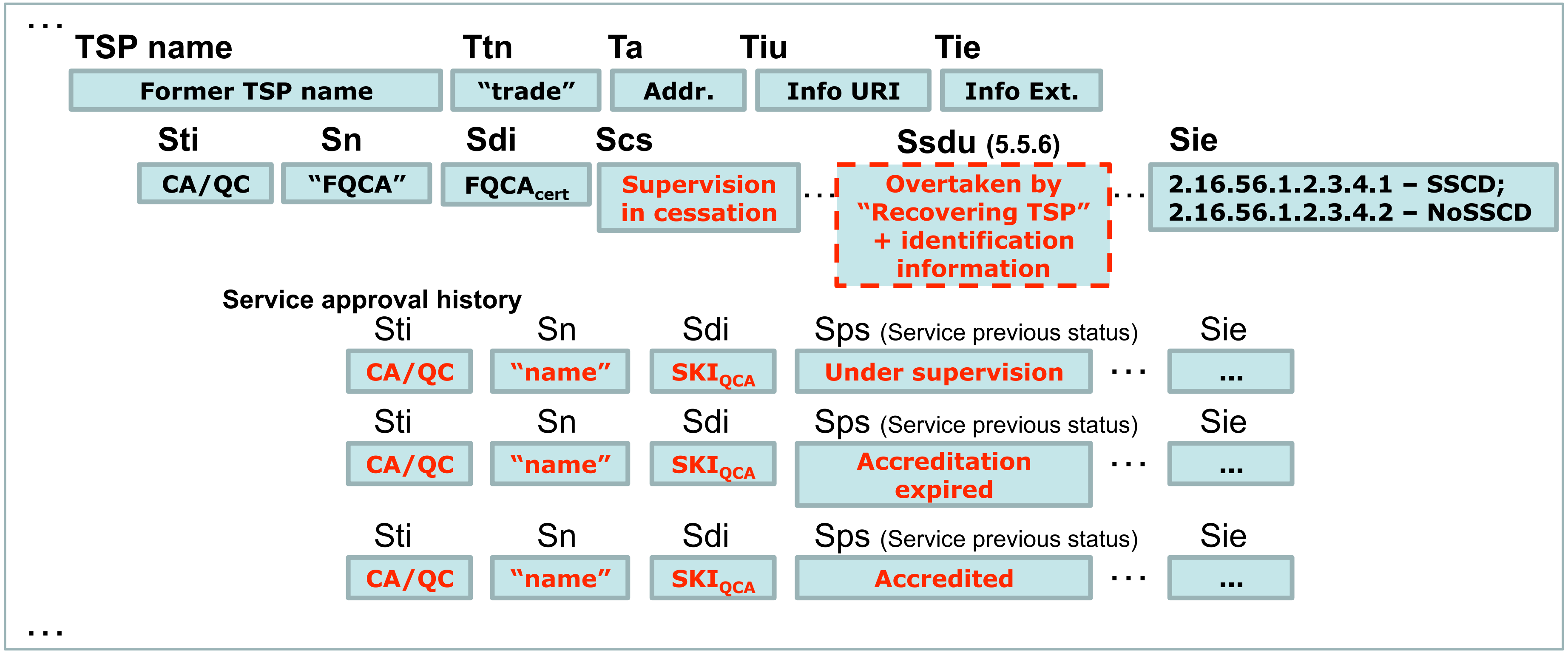
TSP name	Ttn	Ta	Tiu	Tie
Former TSP name	“trade”	Addr.	Info URI	Info Ext.

Sti	Sn	Sdi	Scs (Service current status)		Sie
CA/QC	“FQCA”	FQCA$_{cert}$	Accredited	…	2.16.56.1.2.3.4.1 – SSCD; 2.16.56.1.2.3.4.2 – NoSSCD

Service approval history: empty

…

becomes, once it is acted by the Supervision Body to be in cessation,



…

TSP name	Ttn	Ta	Tiu	Tie
Former TSP name	“trade”	Addr.	Info URI	Info Ext.

Sti	Sn	Sdi	Scs		Ssdu (5.5.6)		Sie
CA/QC	“FQCA”	FQCA$_{cert}$	Supervision in cessation	…	Overtaken by “Recovering TSP” + identification information	…	2.16.56.1.2.3.4.1 – SSCD; 2.16.56.1.2.3.4.2 – NoSSCD

Service approval history

Sti	Sn	Sdi	Sps (Service previous status)		Sie
CA/QC	“name”	SKI$_{QCA}$	Under supervision	…	…
CA/QC	“name”	SKI$_{QCA}$	Accreditation expired	…	…
CA/QC	“name”	SKI$_{QCA}$	Accredited	…	…

…

Abbreviations

- QC = Qualified Certificate
- nonQ = non Qualified
- CSP = Certification Service Provider
- CSP$_{QC}$ = Certification Service Provider issuing Qualified Certificate
- TL = Trusted List
- TSL = Trust Service List (defined by ETSI Technical Specifications 102 231 - standard)
- TST = Time Stamp Token
- “Sti” = “Service type identifier”
- “Sn” = “Service name”
- “Sdi” = “Service digital identity”
- “Scs” = “Service current status”
- “Sie” = “Service information extensions”
- CA/QC = Certification Authority issuing QC
- CA/PKC = Certification Authority issuing Public Key Certificate (nonQ certificate)
- TSA/QTST = Time Stamping Authority issuing Qualified Time Stamp Token
- OCSP = Online Certificate Status Provider
- CRL = Certificate Revocation List
- SSCD = Secure Signature Creation Device
- QCP = Qualified Certificate Policy
- QCP+ = Qualified Certificate Policy extended (plus)
- OID = Object IDentifier