

FESA meeting, 29<sup>th</sup> October 2015

## Trusted Lists

-

Implementing CID 2015/1505/EU  
and TS 119 612 v2.1.1 specifications

Olivier Delos

Managing Partner



- Current CD 2013/662/EU amending CD 2009/767/EC is referring to TS 119 612 v1.1.1
- CID 2015/1505/EU
  - Adopted 8<sup>th</sup> of Sep. 2015
  - Not for implementation before 1<sup>st</sup> of July 2016
  - But for implementation **exactly on the 1<sup>st</sup> of July 2016 !**
  - Refers to TS 119 612 v2.1.1
- TLManager and ETSI Conformance Checker to be updated accordingly and to increase the number of checks.

## Trusted lists

- have a constitutive value
- shall include information on QTSPs/QTSSs supervised by EU MS
- may include information on nonQ TSPs and nonQ TSs while indicating they are not qualified
- shall be available as a signed or sealed machine processable form compliant with annex I of CID relying on ETSI TS 119 612 v2.1.1
- If available as a human readable form,
  - shall contain same data as machine processable one and
  - shall be signed or sealed
- Notification of Reg. Art. 22(3) using template in Annex II of CID, including 2 or more TLSO certificates
- EC to provide LOTL in signed or sealed machine readable form and may provide LOTL under signed or sealed human readable form

Annex I of CID 2015/1505/EU relies on ETSI TS 119 612 v2.1.1 with some changes compared to CD 2009/767/EC as amended

What does not change however are

- Inclusion of both current and all historical information, dating from the inclusion of a TSP in the TL, about the status of listed TS's
- Logical model of the TL is unchanged
- Same XSD has the previous one (already correcting several inconsistencies in Annex B of TS 119 612 v1.1.1)

- **Clause 5.2.1: TSL Tag**

- No change (<http://uri.etsi.org/19612/TSLTag>)

- **Clause 5.3: Scheme information**

- **TSL version identifier** (clause 5.3.1)

- Version identifier value updated from 4 to **5**
- **No impact on “sequence number” which will not be recycled to “1”**

- **TSL sequence number** (clause 5.3.2)

- No change in specifications

- **TSL type** (clause 5.3.3)

- No change (<http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric>)

- **Clause 5.3: Scheme information**
  - **Scheme operator name** (clause 5.3.4)
    - No change in specifications
    - **Reminder:**
      - **Notify name(s) to EC in as many languages as in TL (case sensitive)**
      - **At least one name value must match “O=” attribute value in TLSO certificates**
  - **Scheme operator postal address** (clause 5.3.5.1)
    - No change in specifications

## • Clause 5.3: Scheme information

- **Scheme Operator electronic address** (clauses 5.3.5.2) – No change
  - Both email address and website to be provided as part of the electronic address for Scheme Operator and for all listed TSPs.
  - Sequence of multilingual character strings - 'en' as minimum
  - Examples:

### 2 web addresses and 1 email

```
<tsl:ElectronicAddress>
  <tsl:URI xml:lang="en">http://www.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="en">mailto:rrt@rrt.lt</tsl:URI>
  <tsl:URI xml:lang="lt">http://www.rrt.lt/lt/</tsl:URI>
</tsl:ElectronicAddress>
```



### 4 web addresses (http(s)) and 2 emails

```
<tsl:ElectronicAddress>
  <tsl:URI xml:lang="lt">http://www.rrt.lt/lt/</tsl:URI>
  <tsl:URI xml:lang="en">http://www.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="lt">https://www.rrt.lt/lt/</tsl:URI>
  <tsl:URI xml:lang="en">https://www.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="lt">mailto:rrt@rrt.lt</tsl:URI>
  <tsl:URI xml:lang="en">mailto:rrt@rrt.lt</tsl:URI>
</tsl:ElectronicAddress>
```



### Multiple http addresses

```
<tsl:ElectronicAddress>
  <tsl:URI xml:lang="lt">http://www.rrt.lt/lt/</tsl:URI>
  <tsl:URI xml:lang="en">http://www.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="lt">http://www2.rrt.lt/lt/</tsl:URI>
  <tsl:URI xml:lang="en">http://www2.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="lt">mailto:rrt@rrt.lt</tsl:URI>
  <tsl:URI xml:lang="en">mailto:rrt@rrt.lt</tsl:URI>
</tsl:ElectronicAddress>
```



```
<tsl:ElectronicAddress>
  <tsl:URI xml:lang="en">http://www.rrt.lt/</tsl:URI>
</tsl:ElectronicAddress>
```



```
<tsl:ElectronicAddress>
  <tsl:URI xml:lang="en">http://www.rrt.lt/</tsl:URI>
  <tsl:URI xml:lang="lt">mailto:rrt@rrt.lt</tsl:URI>
</tsl:ElectronicAddress>
```



- **Clause 5.3.6: Scheme name**
    - **New 'EN\_name\_value' as per CID 2015/1505/EU Annex I**
  
  - **Clause 5.3.7: Scheme information URI**
    - Common text to be used as introductory information common to all EU MS **has changed as per CID 2015/1505/EU Annex I (→ change on URI webpage)**
    - Specific information
      - Info on the national supervision scheme applicable to QTSPs/QTS and TSPs/TSs under eIDAS Regulation
      - Info, where applicable, on national voluntary accreditation scheme for CSP issuing QCs under Directive 1999/93/EC
- with for each, at least:
1. General description
  2. Info on process followed for supervision system, and where applicable (w.a.) for the approval under a national approval scheme
  3. Info about criteria against which TSPs are supervised, or w.a., approved
  4. Info about criteria and rules used to select supervisors/auditors and how they assess TSPs/TSs
  5. Where applicable, other contact and general information




- **Clause 5.3.8: Status determination approach**
  - **URI changed**  
<http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate>
- **Clause 5.3.9: Scheme type/community/rules**
  - **It shall only include UK English URIs**
  - otherwise unchanged specifications

- **Clause 5.3: Scheme information**

- **Scheme type/community/rules (clause 5.3.9)**

- Example:




```
<tsl:SchemeTypeCommunityRules>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</tsl:URI>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/LT</tsl:URI>
</tsl:SchemeTypeCommunityRules>
```

- Additional languages / URIs:

- About languages **the only option** is to populate the webpage referenced by the second URI (**/CC**) with a text provided both in English and in national language(s) on the same page. One may also provide a structured text on this page with additional links to external pages.

- Additional URIs as part of the « /CC » hierarchy:



```
<tsl:SchemeTypeCommunityRules>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</tsl:URI>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/LT</tsl:URI>
  <tsl:URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/LT/sub</tsl:URI>
</tsl:SchemeTypeCommunityRules>
```

where « /sub » can be replaced by any appropriate character string.

- **Clause 5.3: Scheme information**
  - **Clause 5.3.10: Scheme territory**
    - No change in specifications.
  - **Clause 5.3.11: TSL policy/legal notice**
    - **Character string values changed as per CID 2015/1505/EU**
  - **Historical information period (clause 5.3.12) and handling historical information**
    - No change in specifications.

- **Clause 5.3: Scheme information**
  - **Pointers to other TSLs** (clause 5.3.13)
    - No change in specifications.
  - **Distribution points** (clause 5.3.16)
    - No change in specifications.
  - **Scheme extensions** (clause 5.3.17)
    - No change in specifications. Not used.

- **Clause 5.3: Scheme information**

- **List issue date and time (clause 5.3.14)**

- No change in specifications.
- But TLSO to ensure the consistency of the (re)-issuance of a trusted list and the actual date when a service status has been updated (clause 5.5.5).

- **Next update (clause 5.3.15)**

- Coordinated Universal Time (UTC) by which, at the latest, an update of the TL shall be issued.
- TLSO shall issue and publish an update of the TL before that Next Update date and time whenever the underlying approval scheme will require so, in particular when changes occur to TSP or service related information (e.g. its status).
- In the event of no interim status changes to any TSP or service covered by the scheme, the TL shall be re-issued by the time of expiration of the last TL issued

- **Clause 5.4: TSP information**

- **TSP name** (clause 5.4.1): no change in specifications.
- **TSP trade name** (clause 5.4.2)
  - Formalization of “VATCC-xxx” and “NTRCC-yyy” formats for legal persons
  - “VATCC-xxx” to be used when both exist
  - Formalization of “PASCC-aaa”, “IDCCC-bbb”, “PNOCC-ccc” and “TINCC-ddd” for natural persons
  - May additionally include any operational name
  - Must include any “O=” attribute value of Sdi certificate conveying the associated public key (in clause 5.5.3) that are ≠ from TSPName and in this case, TLSO shall provide a formal statement in ‘Ssdu’ confirming such a mapping.

*Example:*

```
<tsl:TSPTradeName>  
  <tsl:Name xml:lang="en">Trust Services Architects</tsl:Name>  
  <tsl:Name xml:lang="en">VATBE-0876866142</tsl:Name>  
</tsl:TSPTradeName>
```



- **Clause 5.4: TSP information**
  - **TSP address** (clause 5.4.3)
    - No change in specifications.
  - **TSP information URI** (clause 5.4.4)
    - No change in specifications.
  - **TSP information extensions** (clause 5.4.5)
    - No change in specifications.

- **Clause 5.5: Service information**

- **Clause 5.5.1: Service type identifier**

The quoted URI shall be:

- (a) one of the URIs specified in clause 5.5.1.1 corresponding to the type of listed trust service for QTS's specified in eIDAS Regulation; or
- (b) one of the URIs specified in clause 5.5.1.2 corresponding to the type of listed trust service for non-qualified trust services specified in eIDAS; or
- (c) one of the URIs specified in clause 5.5.1.3 corresponding to the type of listed trust service for trust services that are not specified in eIDAS but specified on a EU MS national basis, a non-EU country basis or on the basis of an international organization specifications; or
- (d) any other URI value registered and described by the scheme operator or another entity.



- **Clause 5.5.1: Service type identifier**

The quoted URI shall be:

(a) one of the URIs specified in clause 5.5.1.1 corresponding to the type of listed trust service for QTS's specified in eIDAS Regulation

- QTSP issuing QCs (CA/QC)
  - + two component services
    - Certstatus/OCSP/QC
    - Certstatus/CRL/QC
  - QTSP issuing qualified time stamps (TSA/QTST)
  - QTSP providing qualified electronic registered delivery services (EDS/Q)
    - + a specific type of qualified EDS
      - QTSP providing qualified electronic registered mail delivery services (EDS/REM/Q)
    - QTSP providing qualified preservation services for QESig/QESeal (PSES/Q)
    - QTSP providing qualified validation services for QESig/QESeal (QESValidation/Q)

- **Clause 5.5.1: Service type identifier**

The quoted URI shall be:

(a) one of the URIs specified in clause 5.5.1.1 corresponding to the type of listed trust service for QTS's specified in eIDAS Regulation

- In line with eIDAS Regulation, no “qualified” status possible for QTSP providing qualified generation/creation services for QESig/QESeal
- Annex II.3 cases can be identified through specific case of CA/QC provisioning

- **Clause 5.5.1: Service type identifier**

- <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>:
  - when applicable, **shall** be further identified by using the <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC> identifier (described in clause D.4) which is included in the additionalServiceInformation extension (clause 5.5.9.4) within a Service information extension (clause 5.5.9).
  - when applicable, shall be further specified by using an additionalServiceInformation extension (clause 5.5.9.4) within a Service information extension (clause 5.5.9) by using the appropriate identifiers indicating the nature of the qualified certificates for which the qualified status has been granted: "ForeSignatures", "ForeSeals", "ForWebSiteAuthentication".
  - When, in accordance with Annex II of eIDAS, CA/QC service includes the management of the electronic signature/seal creation data on behalf of the signatory for QESig/QESeal as part of the provision of QSCD, then the QCs for which the private key resides in such a device shall be further identified and specified through the use of a Qualifications extension (clause 5.5.9.2) "QCQSCDManagedOnBehalf" within a Service information extension (clause 5.5.9) by using the appropriate criteria and qualifiers (clause 5.5.9.2.3).

- **Clause 5.5.1: Service type identifier**

The quoted URI shall be:

- b) one of the URIs specified in clause 5.5.1.2 corresponding to the type of listed trust service for **non-qualified** trust services specified in eIDAS;
  - TSP issuing not qualified certificates (CA/PKC)
    - + two component services Certstatus/OCSP & Certstatus/CRL
  - TSP issuing not qualified time stamps (TSA; TSA/TSS-QC; TSA/TSS-AdESQCandQES)
  - TSP providing not qualified electronic registered delivery services (EDS)
    - + a specific type of not qualified EDS
      - TSP providing not qualified electronic registered mail delivery services (EDS/REM)
  - TSP providing not qualified preservation services for ESig/ESeal (PSES)
  - TSP providing not qualified validation services for ESig/ESeal (AdESValidation)
  - TSP providing not qualified generation services for ESig/ESeal (AdESGeneration)

- **Clause 5.5.1: Service type identifier**

The quoted URI shall be:

- c) one of the URIs specified in clause 5.5.1.3 corresponding to the type of listed trust service for trust services that are not specified in eIDAS but specified on a EU MS national basis, a non-EU country basis or on the basis of an international organization specifications;
  - RA – RA/nothavingPKIid
  - ACA
  - SignaturePolicyAuthority
  - Archiv – Archiv//nothavingPKIid
  - IdV – IdV//nothavingPKIid
  - KEscrow – Kescrow/nothavingPKIid
  - PPwd – PPwd/nothavingPKIid
  - TlIssuer
  - NationalRootCA-QC
  - unspecified

- **Clause 5.5: Service information**
  - **Service name** (clause 5.5.2)
    - No change in specifications.

- **Sdi - One service - One public key – n certificates** (clause 5.5.3)

## When using PKI public-key technology:

- A service **shall** be identified by exactly one public key (= Sdi)
- A public key identifying a service **shall** be represented by
  - One or more certificate being the container of the public key identifying the service.
    - It **should** be represented by exactly one certificate
    - When the same public key is represented by more than one certificate, all those certificates:
      - **must** relate to the same public key and
      - **must** have identical subject names.
    - When candidate certificates for the same public key do not have subject names identical to subject names of certificates already representing the same key, they are not eligible and **shall not** be added.
  - X.509SubjectName **should be used** (optional)
  - ds:KeyValue optional
  - SKI optional
- The same public key must only be used to represent one service (and hence appear only once) in a MS TL for a specific service type (while it can appear in another MS TL for the same service type, or in the same TL for another service type).

- **Sdi - One service - One public key – n certificates** (clause 5.5.3)

## When using PKI public-key technology:

- A service **shall** be identified by exactly **one public key** (= Sdi)
  - not “identified” by any one of the certificates provided, which are only provided as representations of the public key and identical sources of DN
- When used as Trust Anchor for X.509 certificate path validation, when TL are used as source for TA, the Sdi is **the public key and is the TA input together with the “subject name”** (extracted from any listed certificate)
  - such use as TA confirmed by CID 2015/1505/EU
- Sdi’s certificates as Trust Anchors are not to be validated as part of the RFC 5280 certificate path validation.



- **Service digital identifier** (clause 5.5.3)

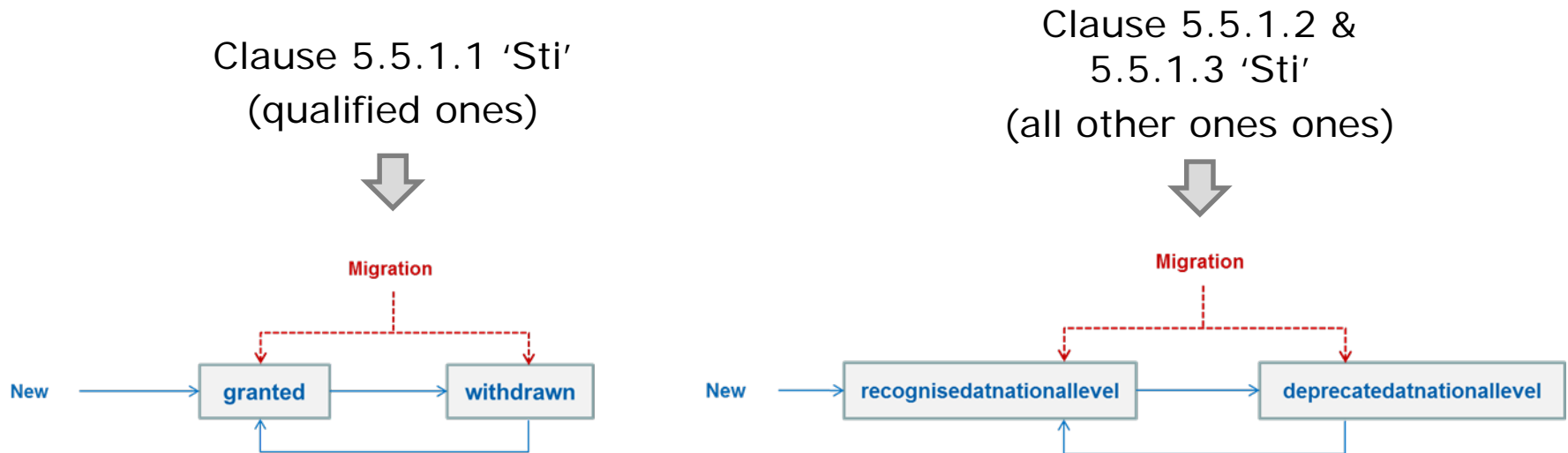
**When not using PKI public-key technology:**

(e.g. for a service with a service type identifier

"http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid"),

- an indicator expressed as a URI
- This indicator shall be defined by the TLSO in a scheme specific context in such a way that it identifies uniquely and unambiguously the listed service.

- **Service current status** (clause 5.5.4)



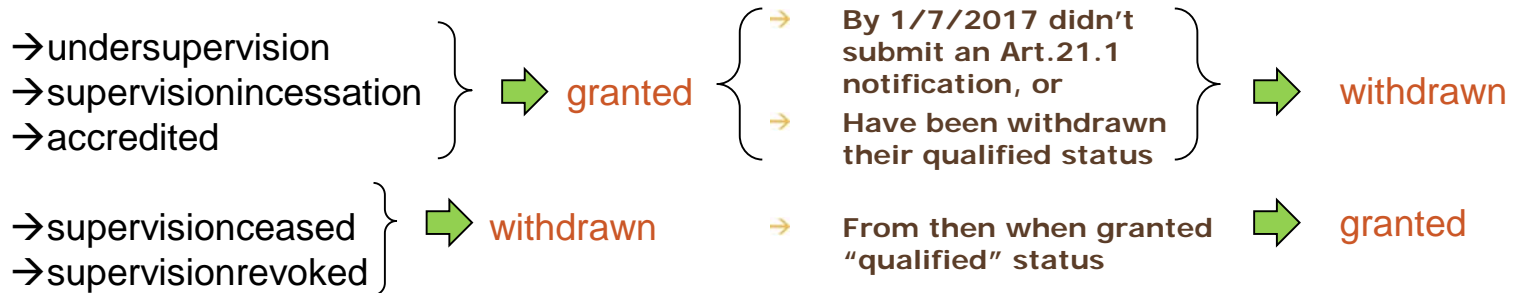
- The migration of the 'Service current status' value of services listed in EUMS trusted list as of the day before the date eIDAS Regulation applies (i.e. 30 June 2016) shall be executed on the day the Regulation applies (i.e. 01 July 2016) as specified in annex J.
- As from the day eIDAS Regulation applies (i.e. 01 July 2016), when a trust service is first approved for being listed in the trusted list, the initial status shall be respectively "granted" or "recognisedatnationallevel"

- **Service current status** (clause 5.5.4) – Migration

**'Scs' value of listed services at 30 June 2016 shall be executed on 01 July 2016) as follows:**

For each service of type **"CA/QC"** ... by using a service history instance & new 'Scs'

- When @ 30 June 2016



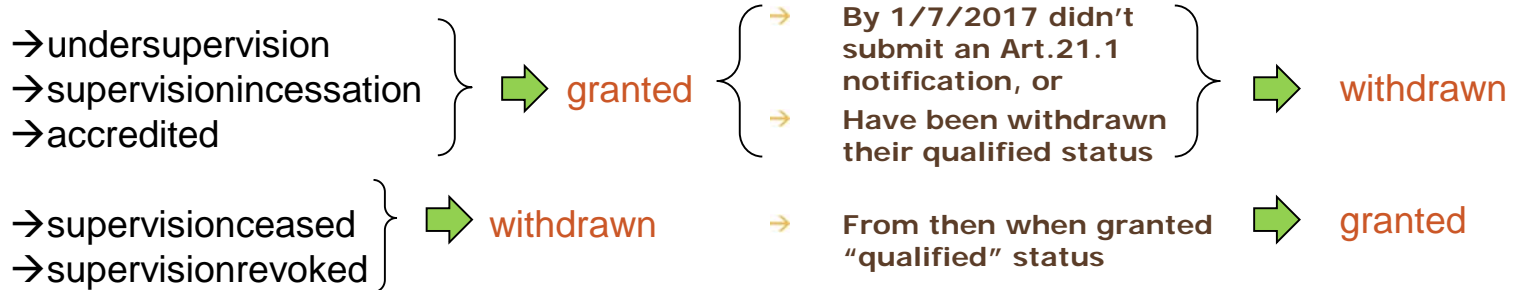
- Add '**Sie:aSI:ForeSignature**' for further specifying type of QC issuance
- Any existing Sie:aSI "RootCA-QC" extension is kept
- Existing Sie:Q extensions are kept but migrated as follows
  - QCWithSSCD → **QCWithQSCD**
  - QCNoSSCD → **QCNoQSCD**
  - QCSSCDStatusAsInCert → **QCQSCDStatusAsInCert**
  - QCStatement → **QCForESig**
  - QCForLegalPerson → **NotQualified**

- **Service current status** (clause 5.5.4) – Migration

'Scs' value of listed services at 30 June 2016 shall be executed on 01 July 2016) as follows:

For each service of type “OCSP/QC” & “CRL/QC”... by using a service history instance

- When @ 30 June 2016



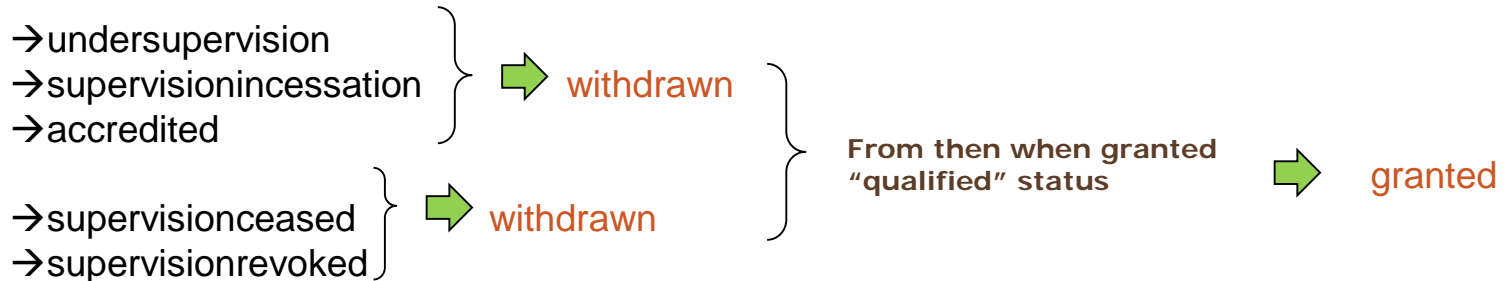
- Add '**Sie:aSI:ForeSignature**' for further specifying type of QC issuance

- **Service current status** (clause 5.5.4) – Migration

'Scs' value of listed services at 30 June 2016 shall be executed on 01 July 2016) as follows:

For each service of type **“TSA/QTST”**, **“EDS/Q”**, **“EDS/REM/Q”**, **“QESValidation/Q”**, & **“PSES/Q”** ... by using a service history instance

- When @ 30 June 2016



- When 'Scs' moved to "granted" for **“QESValidation/Q”** or **“PSES/Q”** add **‘Sie:aSI:ForeSignature’** and/or **‘Sie:aSI:ForeSeal’** as applicable for further specifying type of service

- **Service current status** (clause 5.5.4) – Migration

'Scs' value of listed services at 30 June 2016 shall be executed on 01 July 2016) as follows:

For each service of type **defined in clause 5.5.1.2** ... by using a service history instance

- When @ 30 June 2016



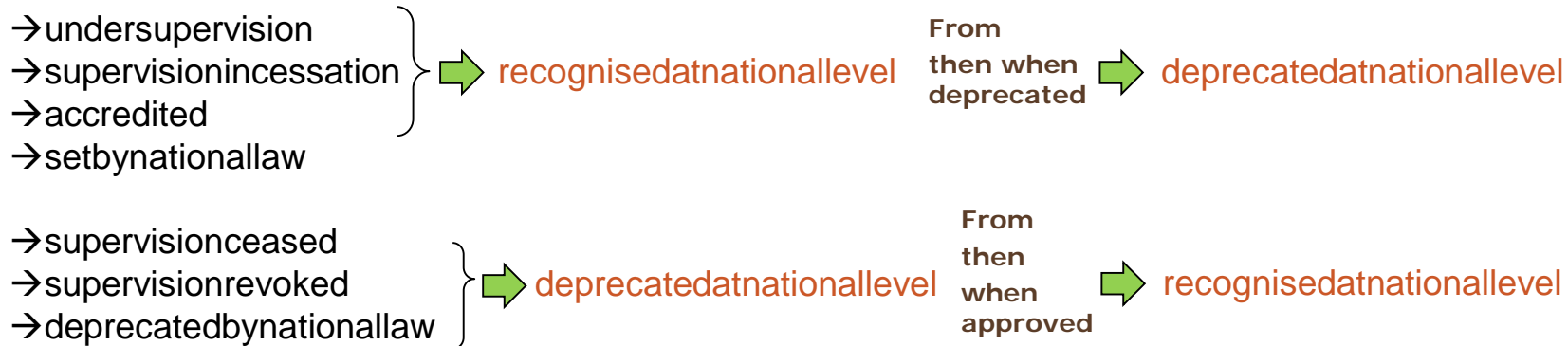
- Where applicable, may add 'Sie:aSI:ForeSignature', 'Sie:aSI:ForeSeal' and/or 'Sie:aSI:ForWebSiteAuthentication', as appropriate for further specifying type of service

- **Service current status** (clause 5.5.4) – Migration

'Scs' value of listed services at 30 June 2016 shall be executed on 01 July 2016) as follows:

For each service of type **defined in clause 5.5.1.3** ... by using a service history instance

- When @ 30 June 2016



- **Current status starting date and time** (clause 5.5.5)
  - TLSO shall ensure the consistency of the (re)-issuance of a trusted list and the actual date when a service status has been updated (e.g. granted or withdrawn), i.e. the 'List issue date and time' (clause 5.3.14), the time of signing the trusted list and the time of change.
  - The date and time associated to the new current status of a listed service shall not be set before the date of (re)issuance of the trusted list as retroactive status change can have undesired effects to previous validations of listed services and of their outputs.
- **Scheme service definition URI** (clause 5.5.6)
  - No change in specifications
- **Service supply points** (clause 5.5.7)
  - No change in specifications
- **TSP service definition URI** (clause 5.5.8)
  - No change in specifications



- **Service information extension** (clause 5.5.9)

- **New Qualifiers in Sie:Q extension**

- QCWithSSCD
    - QCNoSSCD
    - QCSSCDStatusAsInCert
    - QCWithQSCD
    - QCNoQSCD
    - QCQSCDStatusAsInCert
    - QCQSCDManagedOnBehalf
    - QCForLegalPerson
    - QCForESig
    - QCForESeal
    - QCForWSA
    - NotQualified
    - QCStatement

- **Sie:TOB** (clause 5.5.9.3)
  - No change in specifications
- **Sie:aSI** (clause 5.5.9.4)

## New URIs

- "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures": in order to further specify the "Service type identifier" identified service as being provided for electronic signatures;
- "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals": in order to further specify the "Service type identifier" identified service as being provided for electronic seals;
- "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication": in order to further specify the "Service type identifier" identified service as being provided for web site authentication.

- Clause 5.6: Service approval history information
  - Changes applicable to service fields apply
- Clause 5.7: Signature
  - Reference to TS 102 176-1 changed into reference to **TS 119 312**
  - The TLSO certificate, to be used to validate its digital signature on the TL, shall be protected with the digital signature **by incorporating the TLSO certificate within the ds:KeyInfo element** that shall not contain any other certificate forming any kind of associated certificate chain.

- Clause 6: Operations
  - Clause 6.1 – TL publication
    - The HTTP URI pointing to the TL shall be without any special character, shall contain a fully qualified domain name in the host section, and an absolute path, without a query section. It shall be as stable and permanent URI as possible, without implying any redirection, without requiring acceptance of cookies or explicit action for downloading, and it shall lead directly to the .xml /.xslt file that shall be downloadable by an application. The absolute path shall end with the string ".xml" or ".xslt". There shall not be any extraneous header or trailer information in the file.
    - When publishing their TLs, TLSOs should make sure that the cache control is set to a reasonable period, i.e. avoiding that an old version of the TL is allowed to linger in network caches long after it was replaced by a new one by the TLSO. The use of this cache-control should be limited to a maximum value not exceeding 4 hours.



Olivier DELOS (CISSP, CISA)

Mobile: +32 477 78 79 74

Email: [olivier.delos@sealed.be](mailto:olivier.delos@sealed.be)

Web: [www.sealed.be](http://www.sealed.be)



UNIVERSITAT POLITÈCNICA  
DE CATALUNYA  
BARCELONATECH