European Commission

Reaching relying parties after a change of LOTL Administrative Anchors

eIDAS technical subgroup webinar
11/05/2017

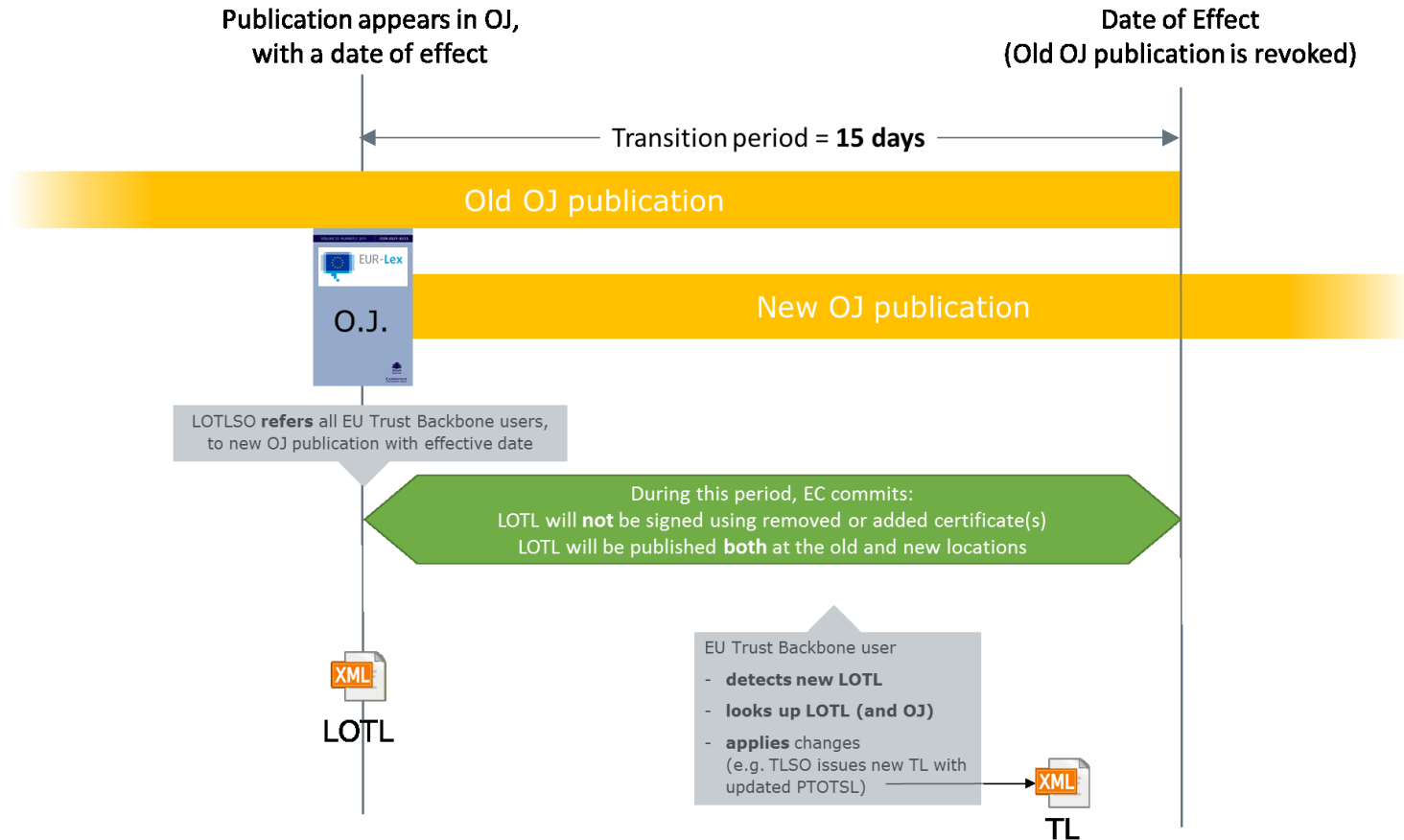# Service continuity for relying parties when LOTL's Administrative Anchors change

- **Timely update** of the LOTL administrative anchor set is critical
  - For TLSOs in their Member State Trusted Lists.
  - for configuration of end-using services or applications (private eSignature validation platforms, document management solutions enabling eSignature validation, etc.).

- Transition period of **15 days**, yet to be **detected.**

- Measures to **timely inform** all relying parties of all data needed
  - In a machine-processable way.
  - In addition of Official Journal publication, as a root of trust.

Machine-processable announcement in the LOTL

- As presented in Official Journal publication 2016/C 233/01

  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

- Since June 2016, the LOTL now contains:
  - An **EU PTOTSL**, announcing the LOTL signing certificates, and the XML location
    - An `<OtherTSLPointer>` with `<SchemeTerritory>` = EU.
  - **URI** pointing to the last issued Official Journal publication
    - added in the `<SchemeInformationURI>`, before the legal notice URIs.

- Comparing the **URI** to its previous value, relying parties can detect the new Official Journal publication
- Comparing the **EU PTOTSL** to its previous value, relying parties can detect a change in the LOTL Administrative Anchors, and extract the new ones
- Both in a machine-processable way

Machine-processable announcement in the LOTL

Publication appears in OJ,
with a date of effect

Date of Effect
(Old OJ publication is revoked)

Transition period = **15 days**

Old OJ publication

EUR-Lex

O.J.

New OJ publication

LOTLSO **refers** all EU Trust Backbone users,
to new OJ publication with effective date

During this period, EC commits:
LOTL will **not** be signed using removed or added certificate(s)
LOTL will be published **both** at the old and new locations

EU Trust Backbone user

- **detects new LOTL**

- **looks up LOTL (and OJ)**

- **applies** changes
  (e.g. TLSO issues new TL with
  updated PTOTSL)

XML

LOTL

XML

TL

European Commission

Pivot LOTL

- Official Journal Publication 2016/C 233/01 plans for a further improvement:
  - Change of LOTL Administrative Anchors **without** a new Official Journal Publication
- Objective: **Minimize** the number of Official Journal Publications
  - Improve reactivity
  - Minimize risk of disruption

- **EU PTOTSL** may announce a change of administrative anchors
  - Without a new Official Journal Publication
  - This change is **machine-processable**

Pivot LOTL: Example: Change of signing certificate

O.J.

cert_1
cert_2

LOTL Sn1
Signed with cert_2

cert_2
cert_3

LOTL Sn2
Signed with cert_3

cert_2
cert_3

- **LOTL Sn1** announces new Administrative Anchor, and can be trusted as it is signed with cert_2, and **cert_2 is in the Official Journal**.

- Relying parties detect the change and have 15 days to update their configuration

- After these 15 days, European Commission may use cert_3 in a **LOTL sn2**

- LOTL Sn1 is a "**Pivot LOTL**"

- **Trust chain** may continue with other changes of Administrative Anchors in additional **Pivot LOTLs**, or may be reset with a new **Official Journal publication**

Pivot LOTL: Initialization (or missing a step)

- The Trust Chain works if one **follows** every change of Administrative Anchors

- What if a relying party needs to configure a **new** system from scratch ?

- What if a relying party has not implemented a automated detection, **misses** the transition period, and the European Commission publishes a new LOTL using the new Administrative Anchors ?

Pivot LOTL: Initialization (or missing a step)

- `<SchemeInformationURI>` will contain
  - **URI** pointing to the last issued **Official Journal publication**
  - **URIs** pointing to all **Pivot LOTLs**, archived at European Commission
- So that one can **reconstruct** the Trust Chain

O.J.

cert_1
cert_2

...

Pivot LOTL Sn1
Signed with cert_2

cert_2
cert_3

...

LOTL Sn2
Signed with cert_3

cert_2
cert_3

...

Pivot LOTL Sn3
Signed with cert_3

cert_3
cert_4

...

LOTL Sn4
Signed with cert_4

cert_3
cert_4
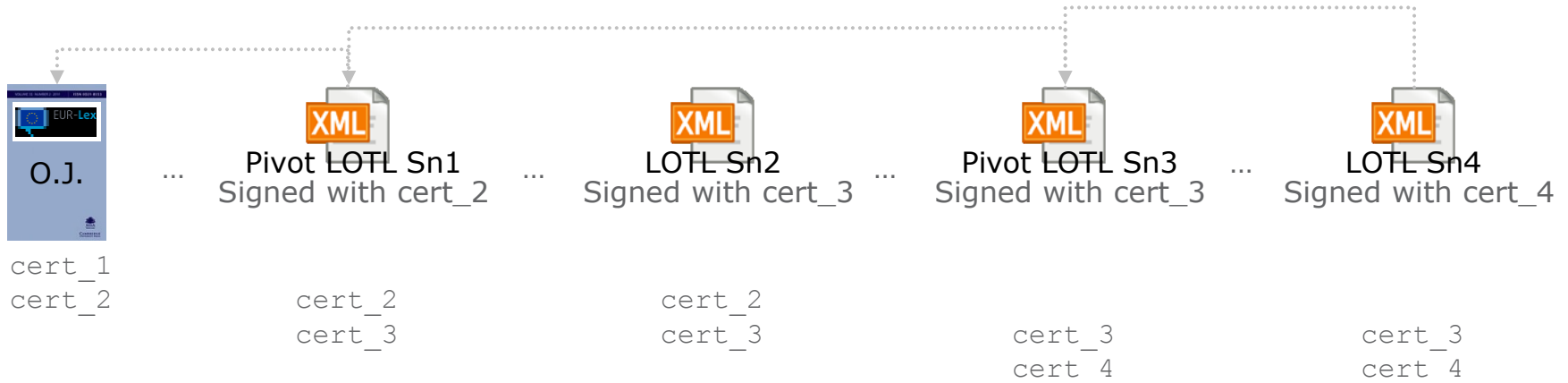
Pivot LOTL: Practical case with 2 new signing certificates

- The Trust Chain is:

URI2 = http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

URI1 = https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-pivot-171-mp.xml

URI1 = http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

O.J.   LOTL Sn170   Pivot LOTL Sn171   LOTL Sn172
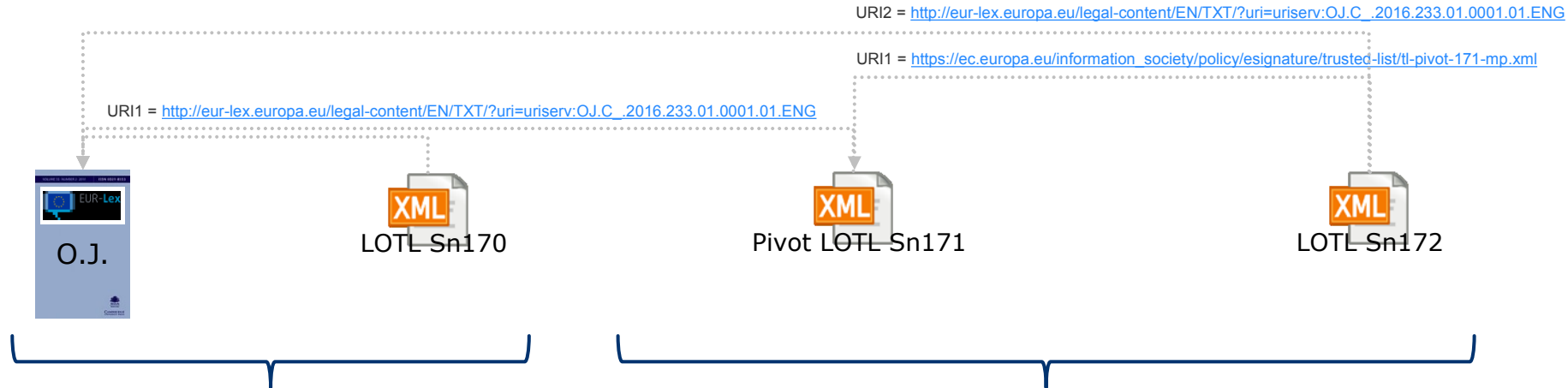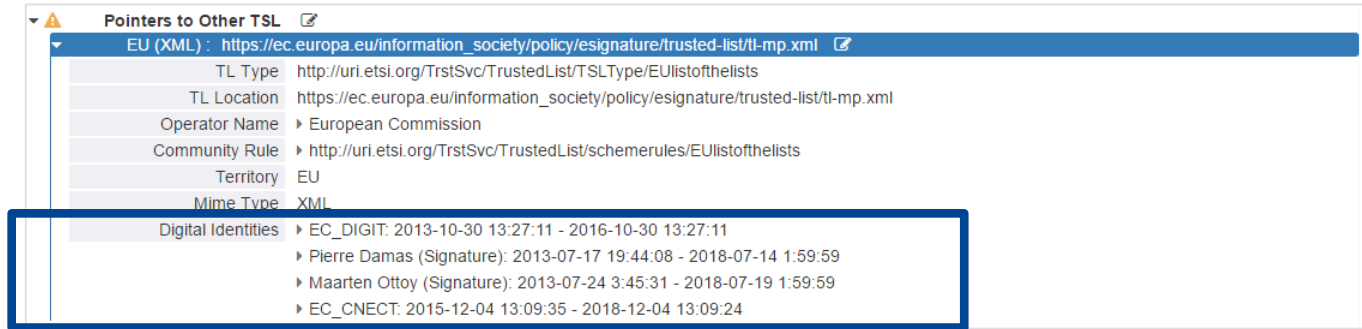
Signing certificates
Pierre_Damas (Signature)
Maarten_Ottoy(Signature)
EC_DIGIT
EC_CNECT

Signing certificates
Pierre_Damas (Signature)
Maarten_Ottoy(Signature)
Maarten_Joris_Ottoy
Jean-Marc Verbergt (Signature)

Pivot LOTL: Practical case, regarding the new signing certificates

Current (Sn170)

New (Sn171)
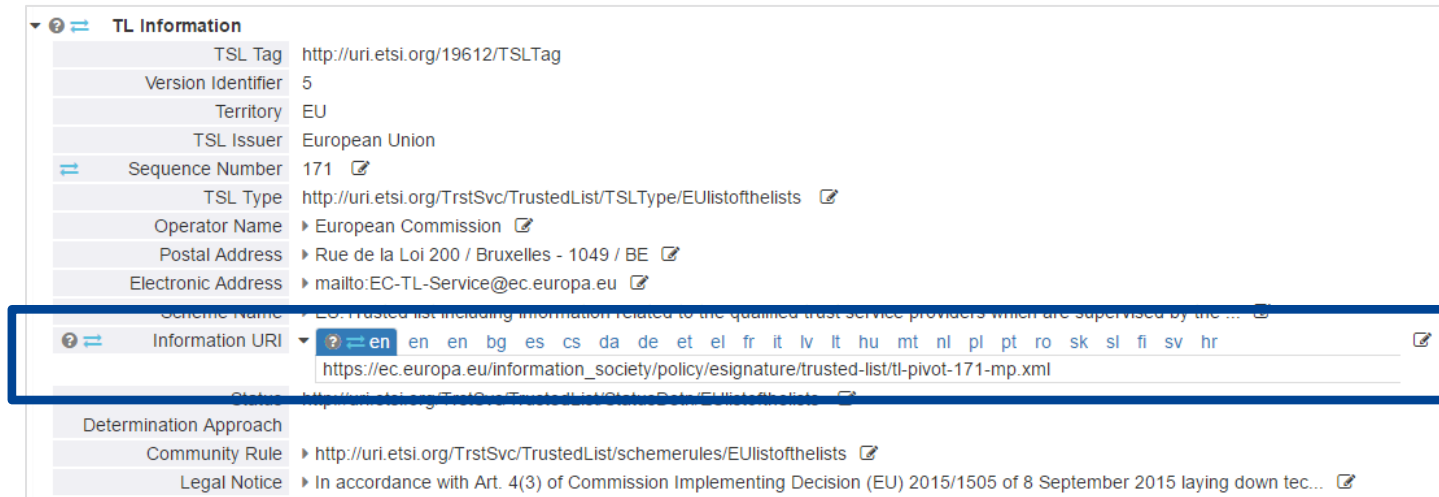
Pivot LOTL: Practical case, regarding the Scheme Information URIs

No change in LOTL **Sn171** regarding Scheme Information URI:

Pivot LOTL: Practical case, regarding the Scheme Information URIs

- New Scheme Information URI added in LOTL **Sn172**
- LOTL **Sn171** is renamed and kept as a **pivot**

Pivot LOTL: Relying party being unaware ?

- European Commission will sign with a certificate **not known** to the relying party
- Relying party **unable to validate** the signature of the LOTL
- Relying party has to **check the Official Journal** for publication 2016/C 233/01, which explains the behavior

- Same situation as when **no announcement** was present in the LOTL: the information is in the Official Journal.

Pivot LOTL: TL Manager 5.0+

- TL Manager is implementing this LOTL monitoring to update its configuration

- This configuration is used in
  - The checks that are performed on a draft/published TL
  - The prefill of the EU PTOTSL in a draft TL

Thank you!

Contact us

✉ Michael.DE-BOER@ec.europa.eu