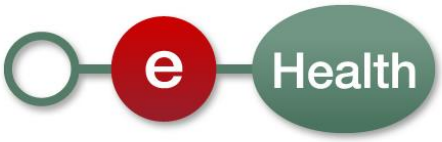


Technical specifications
Trusted Certificates List
Version 1.0

eHealth platform

Willebroekkaai 38

38, Quai de Willebroek

1000 BRUSSELS

Table of contents

To the attention of: “IT expert” willing to integrate this web service.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	19/02/2016	eHealth	Initial version

2. Introduction

2.1 Context

Software packages for healthcare actors use truststores which contain all the certificates that may be trusted in the eHealth domain.

As the list of trusted certificates changes over time, these truststores need to be updated from time to time. To reduce security risks and maintenance cost, this process should be automated and it should be possible to quickly add or remove a certificate.

Therefore, the list of trusted certificates should be made available online in a secure manner.

2.2 Goal of the document

This document describes a solution where the list of certificates is distributed following the technical specification ETSI TS 119 612[1]: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

2.3 External document references

ID	Title	Version	Last modification date	Author
1	RTS/ESI-0019612v121[2]	1.2.1	04/2014	ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)

[1] http://uri.etsi.org/19612/v1.2.1/

[2] http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/01.02.01_60/ts_119612v010201p.pdf

3. Support

3.1 Support in general

For issues in production only

eHealth ContactCenter:

- Phone: 02/788 51 55
- Mail: ***support@ehealth.fgov.be***
- *Contact Form :*

https://www.ehealth.fgov.be/nl/neem-contact-met-de-openbare-instelling-eHealth-platform (Dutch)

https://www.ehealth.fgov.be/fr/contactez-institution-publique-plate-forme-eHealth (French)

FOR PARTNERS AND SOFTWARE DEVELOPERS ONLY

- For business issues please contact: ***info@ehealth.fgov.be***
- For technical issues in production please contact: ***support@ehealth.fgov.be or call 02/788 51 55***
- For technical issues in acceptance please contact: ***Integration-support@ehealth.fgov.be***

4. Specification

There exists a trusted list of certification service providers issuing qualified certificates to the public who are established in Belgium.

The list is the 'Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by Belgium for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The list is distributed by a scheme operator (TLSO: Trusted List Scheme Operator).

For Belgium it is available at http://tsl.belgium.be/tsl-be.xml.

Other European countries have a similar list.

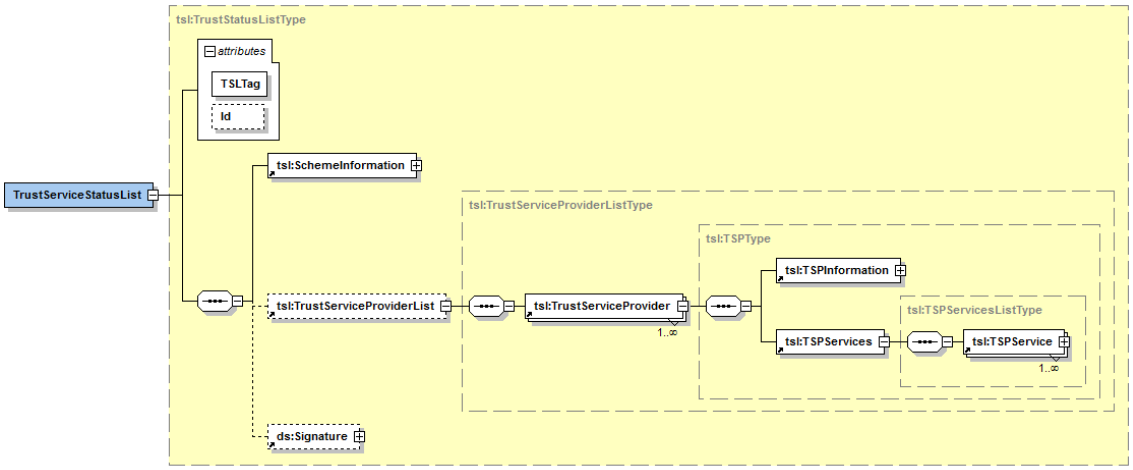
eHealth uses this specification (ETSI TS 119 612) to distribute its own list of trusted certificates and plays the role of scheme operator with its own set of rules that trusted service providers must follow.

4.1 Trust list format and contents

The specification defines an XML structure.

Only keypoints of the structure will be explained here. For a description of each element, see the ETSI specification.

4.1.1 TrustServiceStatusList

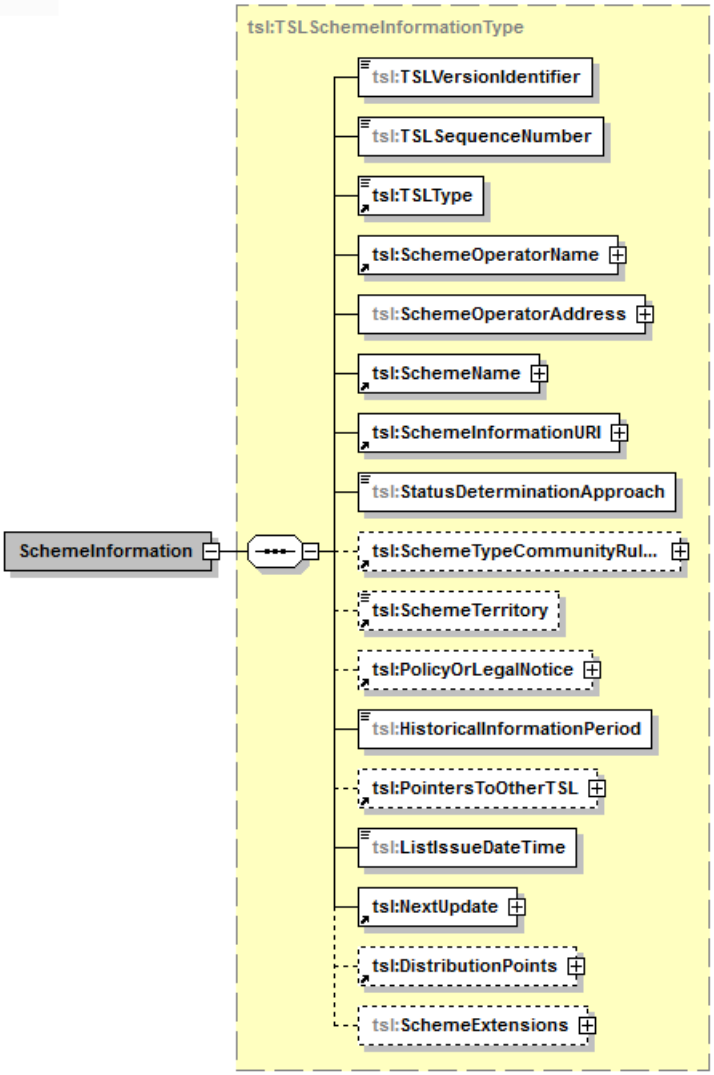


Some important elements:

- **TSLTag**: http://uri.etsi.org/19612/TSLTag (A data structure which conforms to the TSL specification published in TS 119 612).

- **SchemeInformation**: administrative information on which standard is used, who published the document, where things can be found, …
- **TrustServiceProviderList**: 1 or more providers that offer services for which a certificate is used.
- **Signature**: Xades signature to let subscribers validate if this document can be trusted.

4.1.2 SchemeInformation

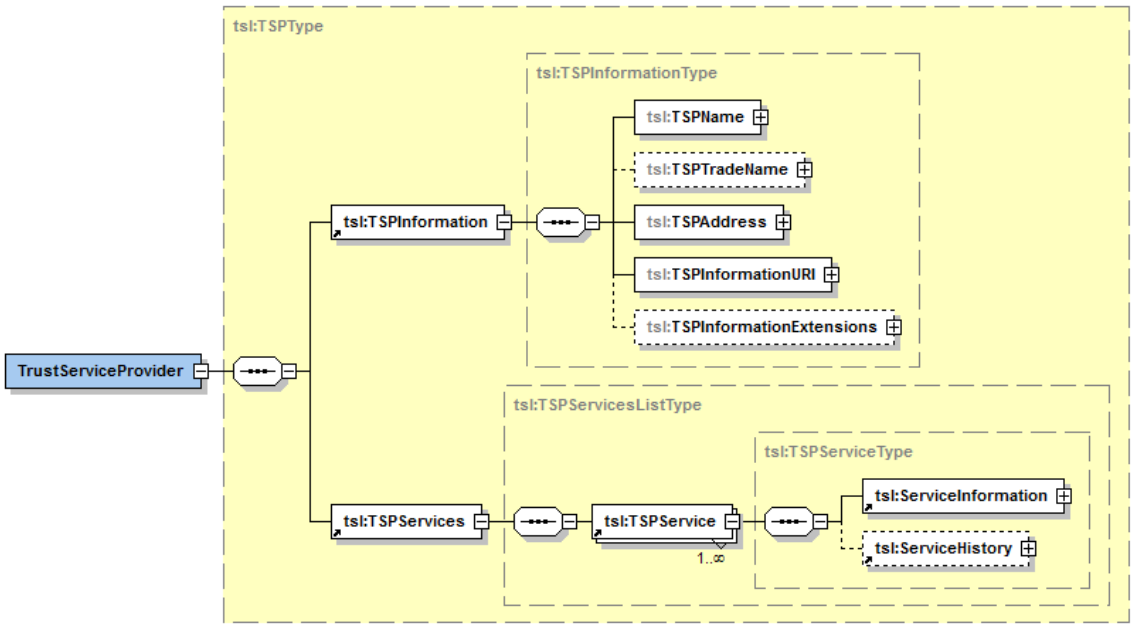


Some important elements:

- **TSLVersionIdentifier**: "4", according to the specification
- **TSLSequenceNumber**: Starts with "1" (and is incremented when a new version is published)
- **TSLType**: http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EHPBElist (**EH**ealth **P**latform **BE**lgium **list**: Indicates a trusted list providing assessment scheme based approval status information about trust services from trust service providers which are approved by the competent trusted list scheme operator).
- **SchemeOperatorName**: "eHealth Platform Belgium TLSO"
- **SchemeName**: unique name for each scheme, published by the operation. See Section 5. eHealth community.

- **InformationURI**: https://tsl.ehealth.fgov.be (Link to eHealth platform page where the lists are published).
- **StatusDeterminationApproach**: http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EHPBEdetermination (**EH**ealth **P**latform **BE**lgium **determination**: Services listed have their status determined after assessment by or on behalf of the scheme operator against the scheme's criteria (active approval/recognition) and as further described in the 'Scheme information URI' pointed-to information.).

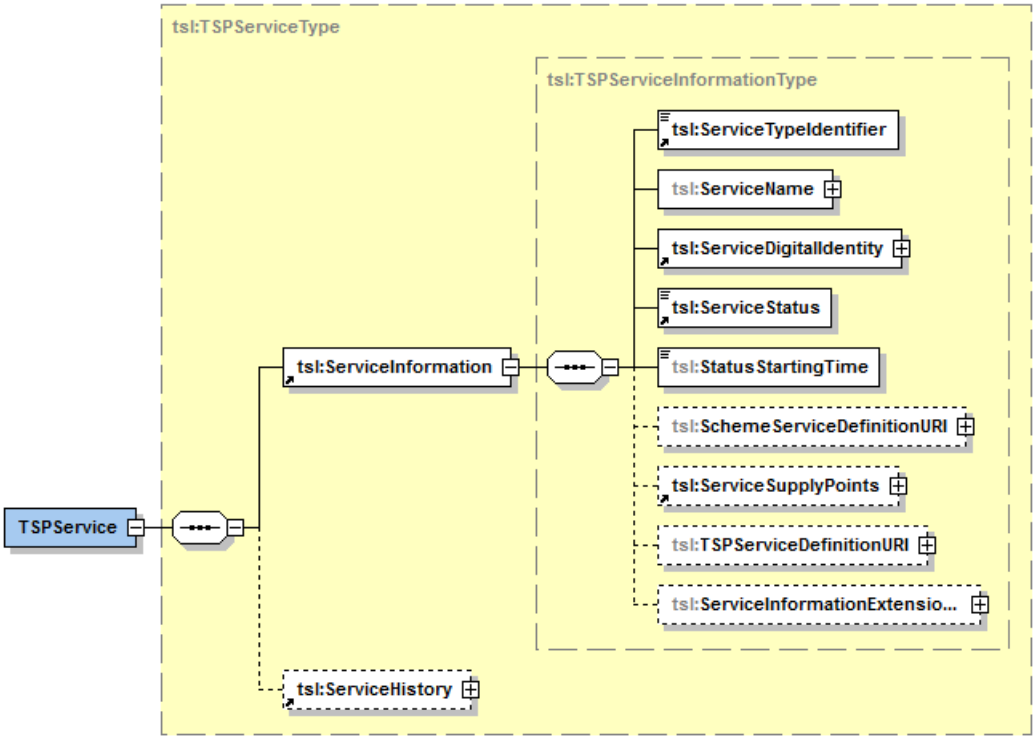
4.1.3 TrustServiceProvider



The TrustServiceProvider contains following info:

- **TSPInformation**: name, address and site info
- **TSPServices**: Info on all offered services

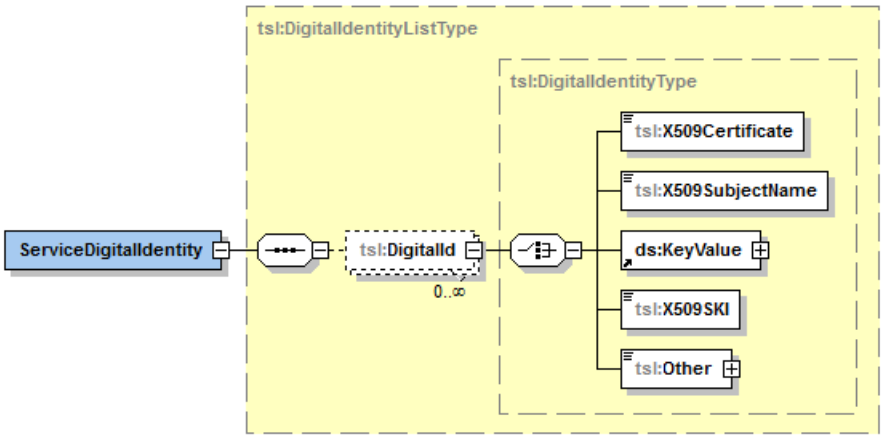
4.1.4 TSPService



Important elements in the ServiceInformation:

- **ServiceTypeIdentifier**: Some predefined service types.
  - http://uri.etsi.org/TrstSvc/Svctype/CA/PKC (A Certification authority issuing public key certificates).
  - http://uri.etsi.org/TrstSvc/Svctype/CA/QC (A Certification authority issuing Qualified Certificates).
  - http://uri.etsi.org/TrstSvc/Svctype/TSA (A Time stamping authority).
  - http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP (A Certificate status provider operating an OCSP-server).
  - http://uri.etsi.org/TrstSvc/Svctype/RA (A Registration authority).
  - http://uri.etsi.org/TrstSvc/Svctype/IdV (An Identity verification service).
  - http://uri.etsi.org/TrstSvc/Svctype/KEscrow (A Key escrow service).
  - http://uri.etsi.org/TrstSvd/Svctype/TLIssuer (A service issuing trusted lists).
- **ServiceDigitalIdentity**: info on the certificate used by the service
- **ServiceStatus**: http://uri.etsi.org/TrstSvc/Svcstatus/inaccord (The subject service is in accordance with the scheme's specific status determination criteria).

4.1.5 ServiceDigitalIdentity



For distribution of trusted certificates, at least the X509Certificate with the base64 encoded value of the full certificate will be available. Also the X509SKI and X509SubjectName will be available.

Example

```
<tsl:ServiceDigitalIdentity>
    <tsl:DigitalId>
        <tsl:X509Certificate>MIIDlDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBgk
    </tsl:DigitalId>
    <tsl:DigitalId>
        <tsl:X509SubjectName>CN=Belgium Root CA,C=BE</tsl:X509SubjectName>
    </tsl:DigitalId>
    <tsl:DigitalId>
        <tsl:X509SKI>EPAMVpth6lc6tjWXbZ/duRSO2+Y=</tsl:X509SKI>
    </tsl:DigitalId>
</tsl:ServiceDigitalIdentity>
```

4.1.6 Signature

The XML file includes a Xades signature and the signer's certificate will be bound into that signature.

The signature is placed with a TLSO (Trusted List Scheme Operator) certificate, following the rules as defined in the specification (section 5.7.1).

Example

```
<ds:Signature Id="xmldsig-759b4ce7-f1a8-43ec-a6ba-c2f8bbb8071b">
    <ds:SignedInfo>
    <ds:SignatureValue>
    <ds:KeyInfo>
    <ds:Object>
        <xades:QualifyingProperties Target="#xmldsig-759b4ce7-f1a8-43ec-a6ba-c2f8bbb8071b">
            <xades:SignedProperties Id="xmldsig-759b4ce7-f1a8-43ec-a6ba-c2f8bbb8071b-xades">
                <xades:SignedSignatureProperties>
                    <xades:SigningTime>2015-10-28T20:38:33.663+01:00</xades:SigningTime>
                    <xades:SigningCertificate>
                        <xades:Cert>
                            <xades:CertDigest>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                <ds:DigestValue>8od4FWF71bBK9g/nRgOzL8BfZlPVpEMbaTae2jQwHS0=</ds:DigestValue>
                            </xades:CertDigest>
                            <xades:IssuerSerial>
                                <ds:X509IssuerName>C=BE, O=eHealth-platform, CN=Trusted List Scheme Operator</ds:X509IssuerName>
                                <ds:X509SerialNumber>99873241478510099l5</ds:X509SerialNumber>
                            </xades:IssuerSerial>
                        </xades:Cert>
                    </xades:SigningCertificate>
                </xades:SignedSignatureProperties>
            </xades:SignedProperties>
        </xades:QualifyingProperties>
    </ds:Object>
</ds:Signature>
```

4.2 Publication

As defined in the specification (section 6), the list is made available through HTTP (transport: TLS, media-type: “application/vnd.etsi.tsl+xml”) with a fully qualified domain, an absolute path ending with “.xml” or “.xtsl” and no query section.

At the same URL but ending with “.sha2”, the SHA-256 hash value of the binary representation is published. This hash is to let clients verify if a new version is available, not for authentication! Clients should NOT wait until the time contained in the NextUpdate field.

Clients should follow the algorithm as described in section 6.1 of the specification.

4.3 Authentication

The trusted list is signed with a Xades signature.

To trust the certificate, referenced in that signature, one can not rely on the contents of the trusted list as the scheme issuing the TLSO (operator) is effectively positioned ‘above’ the TSPs (providers) approved by that scheme.

Before a client can start trusting the list, the TLSO certificate must be installed on the client’s system (it is embedded in the distribution of the eHealth connector and available on eHealth Platform Site). To ensure continuity in trusted list authentication, the trusted list contains itself the TLSO certificate that is actually used for signing AND it’s successor that will be used in the future (long enough before the active TLSO certificate expires). They are added as TSPService with ServiceIdentifierType “http://uri.etsi.org/TrstSvd/Svctype/TLIssuer”.

Clients should register digital identities from those TSPServices in the trustStore they use to verify the signature certchain of the published trusted list. This will ensure key roll-over and eliminates the need for interventions on the client’s system when the TLSO certificate is replaced with a new one.

5. eHealth community

Certificates are used for multiple purposes in the eHealth community:

1. server authentication (TLS)
2. (legal) person authentication
3. Partner/Application authentication

The scope of trust is different for each purpose:

1. Global web trust (+ optional: non global web trust CA)
2. eID + eHealth Certificates
3. Specific certificates (e.g. eHealth TSA)

eHealth publishes the list of digital identities that can be trusted for each purpose.

Clients can build up trust for each purpose by filtering the published list(s).

5.1 eHealth Platform Belgium Trusted List Scheme Operator

5.1.1 TSL-EHPBE-Transport

A list which contains all the certificates that can be trusted to setup a connection with an authenticated server (TLS).

5.1.1.1 SchemeName

Status List of certification services from Certification Service Providers, which are accredited by eHealth Platform Belgium for Transport Layer Security.

5.1.1.2 DistributionPoints

Production	https://tsl.ehealth.fgov.be/tsl-ehpbe-transport.xml
Acceptation	https://tsl-acpt.ehealth.fgov.be/tsl-ehpbe-transport.xml
Integration	https://tsl-int.ehealth.fgov.be/tsl-ehpbe-transport.xml

5.1.1.3 TrustServiceProviders

All providers of Root CAs with Global Web Trust (by default available in web browsers, Sun cacerts keystore, windows certificate store).

5.1.1.4 ServiceTypeIdentifiers

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

5.1.2 TSL-EHPBE-Person

A list which contains all the certificates that can be trusted to authenticate persons and organizations.

5.1.2.1 SchemeName

Status List of certification services from Certification Service Providers, which are accredited by eHealth Platform Belgium for Legal Person Authentication.

5.1.2.2 DistributionPoints

Production	https://tsl.ehealth.fgov.be/tsl-ehpbe-person.xml
Acceptation	https://tsl-acpt.ehealth.fgov.be/tsl-ehpbe-person.xml
Integration	https://tsl-int.ehealth.fgov.be/tsl-ehpbe-person.xml

5.1.2.3 TrustServiceProviders

Belgium Root CAs, Government CAs.

5.1.2.4 ServiceTypeIdentifiers

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

5.1.3 TSL-EHPBE-Application

A list which contains all the certificates that can be trusted to verify a message received from an application.

5.1.3.1 SchemeName

Status List of certification services from Certification Service Providers, which are accredited by eHealth Platform Belgium for Application Authentication.

5.1.3.2 DistributionPoint

Production	https://tsl.ehealth.fgov.be/tsl-ehpbe-application.xml
Acceptation	https://tsl-acpt.ehealth.fgov.be/tsl-ehpbe-application.xml
Integration	https://tsl-int.ehealth.fgov.be/tsl-ehpbe-application.xml

5.1.3.3 TrustServiceProviders

TSA certificates.

5.1.3.4 ServiceTypeIdentifiers

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

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

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

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

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

http://uri.etsi.org/TrstSvd/Svctype/TLIssuer

5.2 Recommendations

5.2.1 TLSO

5.2.1.1 Publication

As recommended by the specification, the TLSO:

- will republish its list(s) from time to time, even if nothing has changed, to make sure a fresh list is available (at least before the NextUpdate field expires).
- A sha-256 digest will be available so clients can verify for updates.

5.2.1.2 Authentication

The security department of eHealth Platform has issued a certificate as TLSO certificate, following section 5.7 in the specification.

To ensure continuity in trusted list authentication, the trusted list (TSL-EHPBE-Application) contains the TLSO certificate itself AND it's successor will be added long enough before the successor is actually used and the active TLSO certificate expires. They are added as TSPService with ServiceIdentifierType "http://uri.etsi.org/TrstSvd/Svctype/TLIssuer".

5.2.2 Client implementations

Clients can cache the published certificates for local trust purposes. Below are some recommendations.

5.2.2.1 Truststore

As the lists contain certificates of services for different purposes, clients should build up different truststores by filtering the lists.

Recommendation:

1. A trustStore to setup connections to authenticated servers (similar to a browser's truststore), based on the digital identities published in TLS-EHPBE-Transport).
2. A trustStore to authenticate persons and organizations, based on the digital identities published in TLS-EHPBE-Person).
3. A trustStore to validate timestamps, based on the digital identities published in TLS-EHPBE-Application, with a filter on serviceTypeIdentifiers that start with http://uri.etsi.org/TrstSvc/Svctype/TSA.
4. A trustStore to validate trusted list issuers, based on the digital identities published in TLS-EHPBE-Application, with a filter on serviceTypeIdentifiers that start with http://uri.etsi.org/TrstSvc/Svctype/TLissuer.

5.2.2.2 Refresh

It is important that clients refresh their local cache frequently to make sure they don't trust certificates which shouldn't be trusted and start trusting new certificates which should be trusted.

The published lists contain a field ‘NextUpdate’ which states when a new version will be made available. However, eHealth will only publish from time to time. Clients should check for updates daily.

The specification proposes an algorithm for this, which we publish here as recommendation:

For example, the TLSOx's TL published at the location http://www.TLSOx.xyz/TrustedList/TL.xml is accompanied by its sha2 digest file i.e. on location http://www.TLSOx.xyz/TrustedList/TL.sha2. Downloaders may adopt the following strategy for downloading file TL.xml:

- check whether TL.sha2 is available for download.
    - if TL.sha2 has been successfully downloaded, verify the digest against the cached TL.xml file.
        - If different, download and process TL.xml.
    - if TL.sha2 has not been successfully downloaded, download and process TL.xml directly.

TL.xml should be downloaded/processed anyway if the nextUpdate (in the cached file) has been reached.