ABB - Trust Network – Mutual Recognized Certificates - 1.1

Objective

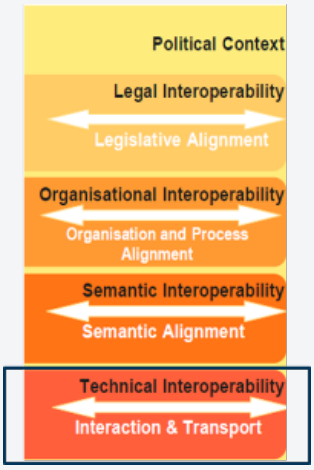
Mutual exchange of certificates is a widely used simple mechanism of the Direct Trust Model. Due to its restricted scalability, it may be a first choice for interacting communities with a manageable number of participants having knowledge from each other.

Certificates are used for digital signatures on service-request and –response messages for purposes of authentication and integrity, for client authentication (e.g. SSL / TLS) and may optionally also be used for encryption of messages. The certificates are exchanged between all members of a Trust Domain (TD) and kept in a trusted Key Store by all TD nodes which mutually must authenticate each other.

Every affiliation of new TD members as well as replacement or revocation of certificates of TD members imposes an update/renewal of the trusted Key Store by all TD members.

Version:	1.1
Status:	N/A
Sustainability Assessment:	N/A

Interoperability Level:



Requirements

Requirement ID	Requirement description
R-TruNet-MRC-T1	e-Signature validation services must be trustable *(Special case of requirement below. Note that every TD member which is validating signatures must have the Certificates of Validation Services in its trust Store, and conversely Validation Services must include the Certificates of all the other TD Members, if these services require client authentication and use the same Direct Trust Model.)*
R-TruNet-MRC-T2	Shared central services and nodes used to interconnect national/application domain trust circles must be recognizable as trustworthy; their underlying trust and service quality status, operational policy, governance model must be verifiable by all actors involved at any time. *(Note: For this Direct Trust Model is based on Mutual Certificate Exchange. TD Members' policy conformance is implied, as policy conformance validation has to take place before Certificates are exchanged. If shared central services used in the TD require client authentication, the client (TD member) certificates must be held in the Key Stores of these services)*

Related ABBs

For Certificate Validation, see ABB e-Signature Verification Service.

Authentication on base of mutual recognized certificates can be used need mutual authentication is required.

Provided Services

Provided Service	Purpose
Maintain and distribute Trusted Certificate Store	Maintain Trust Store and synchronize with local Trust Store instance
Certificate and Policy Validation	

Exchange of Certificates inside Trust Domain

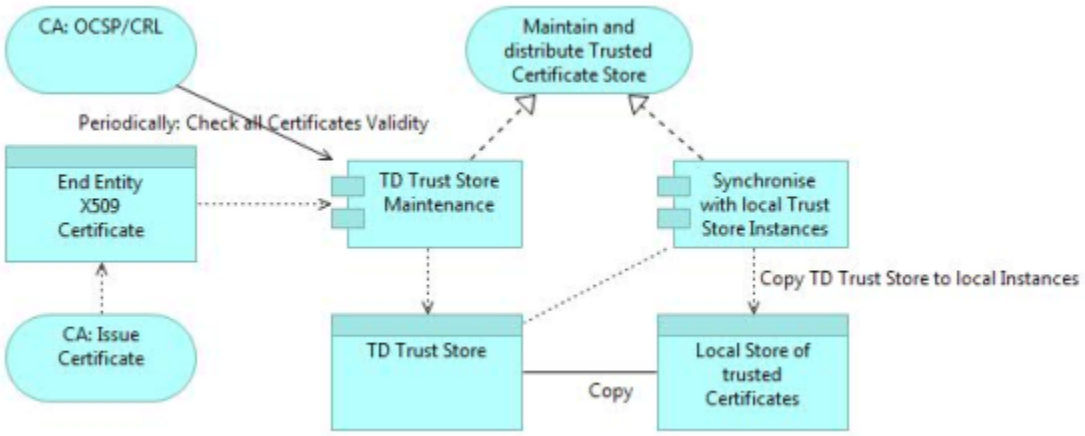


Figure 1: Mutual Certificate Exchange using TD Trusted Key Store

Note that the validity of End Entity Certificates held in the TD Trust Store should be checked on a periodical basis according to the underlying Trust Domain Policy. Revoked End Entity Certificates should be removed from the TD Trust Store, any changes maintained centrally must be replicated to local copies immediately in a secure and authorized manner.

When using TLS for authentication, the usage of OCSP stapling Formally known as the TLS Certificate Status Request extension should be considered. If activated, the timeliness of the TD Trust Store replication at least is not critical to publish Certificate revocation events.

More sophisticated implementations also support LDAP directory servers as a trusted certificate repository. In this case, the TD Trust Store may be accessed directly; no replicated local instance is needed.

Trusted Certificate Validation

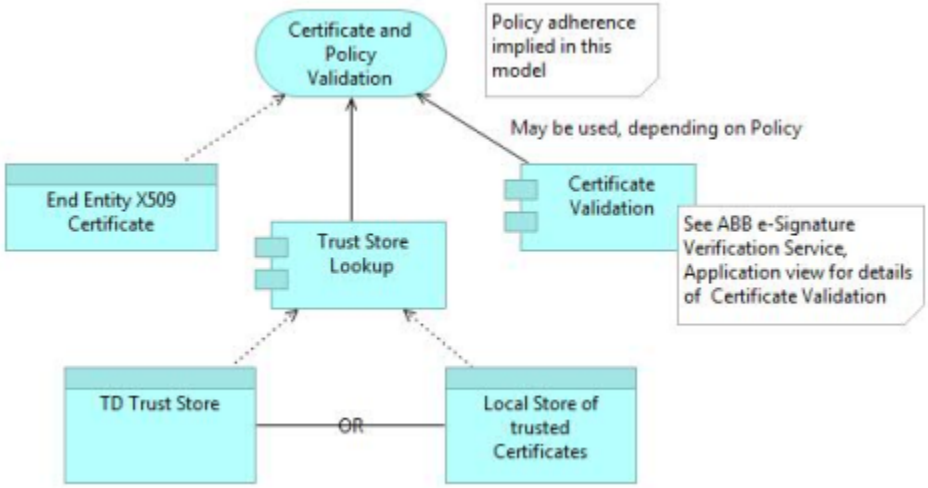


Figure 2: Trusted Certificate Validation

As described above, depending on the implementation, the local Trust Store or the central TD one is used for lookup. Depending on the TD Policy, the actual Certificate validity may be checked by using the issuing CA's OCSP/CRL service.

No additional Policy adherence is checked, as Certificate owners' Policy is implicitly bound to his Certificate.

Information view

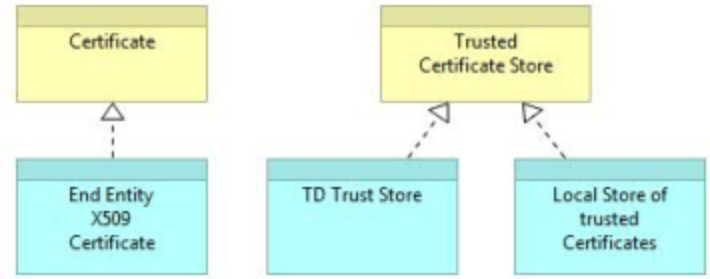


Figure 3: Involved Data Objects

As mentioned above, implementations may use a central TD Trust Store directly or a local copy of it.

ABB Capability Realization

Author Note

We restrain here from listing all the PKIX-specifications (most of them referenced in ETSI ESI Rationalized Framework)

ETSI ESI Standards for Trust Service Providers Supporting Electronic Signatures:

EN 319 401General Policy Requirements for Trust Service Providers
EN 319 411Policy & Security Requirements for TSPs Issuing Certificates
In particular:
Part 1: Policy requirements for TSPs issuing Web Site Certificates
Part 2: Policy requirements for TSPs issuing Public Key Certificates
EN 319 412 Certificate Profiles
In particular:
Part 1: Overview and common data structures
Part 4: Certificate profile for Web Site Certificates issued to organisations
TS 119 312Cryptographic Suites
EN 319 102Procedures for Signature Creation an Validation
EN 319 403Trust Service Provider Conformity Assessment – requirements for conformity assessment bodies assessing Trust Service Providers
Other related international standards, as far as not already referenced / profiled by the ETSI Standards:
RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2
RFC 6066 Transport Layer Security (TLS) Extensions: Extension Definitions
RFC 4510 Lightweight Directory Access Protocol (LDAP)

Implementation Guidelines

This ABB functionality mostly is given by infrastructure components implementing SSL/TLS and/or SOAP Message Security (according to the OASIS specification WS-Security 1.1).

Contributors

Name	Surname	Organization	Country
Jörg	Apitzsch	Governikus KG	Germany
Elif	Üstünda Soykan	TUBITAK	Turkey
Cagatay	Karabat	TUBITAK	Turkey

History

Version	Date	Changes made	Modified by
0.2	17.03.2014	Template	Klaus Vilstrup Pedersen
0.3	08.08.2014	Draft	Jörg Apitzsch
0.4	25.08.2014	First version completed	Jörg Apitzsch
0.5	04.09.2014	Proofreading	Damien Magoni
1.0	30.09.2014	Final Review	Jörg Apitzsch
1.1	11.06.2015	Editorial Updates	Cagatay Karabat