**COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME**

**ICT Policy Support Programme (ICT PSP)**

****

**Project acronym: e-SENS**

**Project full title: Electronic Simple European Networked Services**

**ICT PSP call identifier: CIP-ICT-PSP-2012-6**

**ICT PSP main theme identifier: CIP-ICT-PSP-2012-6-4.1 Basic Cross Sector Services**

**Grant agreement n°: 325211**

Trust Models: White Paper

|  |  |  |
| --- | --- | --- |
|  |  | |
|  |  | |
|  |  |
| Status : | Draft 0.4 |
| Dissemination Level : | Project internal |
|  |  |
|  |  |
| Work Package : | WP6 |
| Organisation name of lead partner for this deliverable : | Governikus KG, Germany |
| Author(s): | Jörg Apitzsch |
| Partner(s) contributing : | Elif ÜSTÜNDAĞ SOYKAN**,** TÜBİTAK |

**Abstract:**

**Options for Trust Circle establishment:**

**- Overview on Trust Models to be established on central or piloting domain level**

**- Applicability estimation**

Contents

[History 3](#_Toc411578950)

[Disclaimer 3](#_Toc411578951)

[1. Aims and Scope 4](#_Toc411578952)

[2. Assumptions 6](#_Toc411578953)

[3. Evaluation Criteria for Trust Models and Services 7](#_Toc411578954)

[4. Brief Overview on Trust Models 8](#_Toc411578955)

[4.1. Direct Trust – Mutual Key Exchange 8](#_Toc411578956)

[4.2. Indirect Trust Models 9](#_Toc411578957)

[4.2.1. Community Trust 11](#_Toc411578958)

[4.2.2. Root-Stores 14](#_Toc411578959)

[4.3. Brokered Trust Models 14](#_Toc411578960)

[4.4. Trust Federation using Trust Lists 15](#_Toc411578961)

[5. Usage of SAML Token and Security Token Services for Trust-Brokerage 17](#_Toc411578962)

[6. “Big Picture” using Trust Brokers and Trust Lists 19](#_Toc411578963)

History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Changes made** | **Modified by** |
| 0.1 | 02.01.2015 | First draft | Jörg Apitzsch |
| 0.2 | 19.01.2015 | Draft completed for further reconcilement | Jörg Apitzsch |
| 0.3 | 11.02.2015 | Further detailing of model descriptions; draft evaluation criteria | Jörg Apitzsch |
| 0.4 | 12.02.2015 | Evaluation criteria per model, review | Jörg Apitzsch, Elif Üstündağ Soykan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Disclaimer

This paper adopts findings of other LSPs, namely to be mentioned: epSOS “D.3.7.2. Final Security Services Specification Definition”.

Further on, WP6.3 contributions to e-SENS “D6.2 Enterprise Interoperability Architecture n°1” as well as relevant WP6.3 internal workouts are incorporated, like “Reference models for cross-border signing and signature validation”, provided by Jon Ølnes in July 2014.

# Aims and Scope

eIDAS states: “Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services.” In line with the objectives of eIDAS, e-SENS WP6 aims to provide Building Blocks to interconnect IT-solutions used by public administration, their providers and customers in different domains and/or EUMS in an interoperable, secure and trustworthy manner.

Related HHB and ABBs descriptions provided with D6.2 identify different models and technical means to establish trust in and between IT-Systems involved in cross-border / cross-solution electronic transactions. These “Trust Services” (TS) are electronic services which enhance trust and confidence in electronic transactions, provided by “Trust Service Providers” (TSP)***.*** Consumers and Providers of the interconnected distributed solutions must be able to rely on and validate the authenticity and trustworthiness of each service / service-provider carrying out electronic transactions; this implies mutual trust between services/nodes involved.

This paper summarizes a selection of the most common models, most of them already assessed in D6.1 and further generalized in D6.2. This overview is intended to facilitate Trust Model preference decisions actually to be taken by WP5 piloting domains. It is assumed, that there is no “one solution fit for all”, but choices should be aligned with respective Trust Model preferences of EC/ISA for for CEF.

TSPs and their related service definitions have to be registered and supervised by means of a governance model and policy assessment process to be defined by WP4 and WP3; Governance models and policies may differ according to domain-specific requirements. Trust Circle Management systems must provide registration, maintenance and lookup services for TSPs covered by this Trust Circle. Consumers of e-SENS electronic services must be able to assess at any time the actual policy / service quality and trust status of TSPs services offered by them.

Services that must be trustworthy in the context of e-SENS are:

* Services for application and validation of e-Signatures and e-Seals
* Services attesting electronic identities
* e-Delivery/e-Interaction services
* Time-stamping services
* Directory-Services used to discover attributes, capabilities and constraints of services and end-entities in the network
* Services issuing different types of security tokens (e.g. Certification Authorities providing X509-Certificates, Security Token Services issuing SAML Token, Attribute Service Providers)
* Services providing sources of authenticated documents / long term archiving and signature preservation
* Services performing format/protocol transformations and semantic mapping.

Trust in distributed environments is established by using cryptographic mechanisms for

* authenticating entities involved in electronic transactions;
* authenticating claims presented by interacting entities, as may be required specific to underlying business scenario;
* authenticating requests to and outcomes of services, mostly by signing requests and responses/data delivered;
* securing data exchanged between entities (by means of signature and/or encryption).

**Note:**

1. The Trust Realms that are identified by bilateral agreements to fulfil the specific requirements of the domains are out of scope this document.
2. If domains have needs for different Trust Models /-mechanisms, this may have an impact on the possibility to share certain services in a cross-domain manner, like e.g. e-Delivery Gateways / Accesspoints / National Contact points. To deal with the different requirements for authentication/authorization, it may require to set up such service instances per domain, at least when generally restricting to X509v3 certificates as security tokens.

# Assumptions

We assume Trust Realms – aka “Trust Circles” - are established on domain- or Member state level for existing solutions and their service providers. e-SENS does not impose changes to domestic Trust Realms, anyhow Realms accepted to join the e-SENS Trust Circle must fulfil minimum policy and government model requirements, to be detailed by WP3 and WP4 with respect to existing MS or EU regulation. To establish trust when interconnecting these Trust Circles established on domain- or Member State (MS) level, a trust relationship must be build up between these realms, including eventually needed external services. If needed and feasible, domestic Trust Realm means for proving authenticity must be technically mapped to those of the e-SENS infrastructure.

Independent from the Trust Model used, e-SENS basically relies on X509v3 certificates as security tokens; their actual validity must be verified by the Relying Party by means of OCSP/CRL or other trusted certificate validation services.

This is seen in line with result of the ENISA-survey “Trusted e-ID Infrastructures and services in EU”[[1]](#footnote-1), depicting that 88% of TSPs already use electronic certificates to grant access to their services. Even if additional security tokens like e.g. SAML assertions are used, they are usually signed by the issuing Security Token Service[[2]](#footnote-2) (STS, which again must be a TSP) using his X509v3 certificate.

For Trust Models in discussion here, it is assumed that all of them, namely the PKI infrastructure used behind, are able to fulfil basic technical and operational security requirements as specified by related related ETSI and CEN specifications for TS / TSPs (namely EN 319 series, TS 119 312 on Cryptographic suites - about to be published in final versions in course of 2015). CEN and ETSI standards in turn are based on according international standards.

Related to PKI Security Services, LSP epSOS provided very precise requirements and profiles in its deliverable D3.7.2[[3]](#footnote-3), which as far as being not domain-specific should be adopted be e-SENS - probably to be aligned with mentioned ETSI ENs.

# Evaluation Criteria for Trust Models and Services

As mentioned above, applicability of different models with respect to security requirements is assumed and thus security-related rating is left out here. Models described in this paper are discussed regarding following criteria:

1. General applicability regarding establishing cross-realm trust
2. Support of Model by IT solutions available on the market
3. Degree of adoption of model by MS
4. Scalability
5. Degree of standardisation of service and its interfaces, implementation challenges
6. Efforts regarding operational setup / maintenance
7. Business model – how is operation of the service financed? Basically three models are possible:
   1. Commercial service based on fees for use of the service;
   2. Government funding;
   3. Funding by the actors covered by the service.
8. Liability issues

*Author: More to be considered, e.g. cross-domain applicability ?*

# Brief Overview on Trust Models

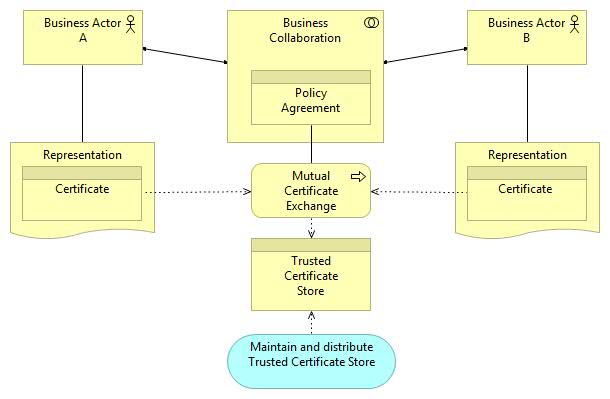
The different Trust Models described below may be applied as alternatives or even being used in a hybrid manner, depending on the e-SENS piloting domain needs. Definitions and guidelines on different Trust Models have already been given in “Liberty Trust Models Guidelines version 1.0” by the Liberty Alliance Project in 2003[[4]](#footnote-4), in 2004 adopted by the OASIS Security Services Technical Committee in “Trust Models Guidelines”[[5]](#footnote-5).

## Direct Trust – Mutual Key Exchange

WS-Trust[[6]](#footnote-6) defines: “Direct trust is when a relying party accepts as true all (or some subset of) the claims in the token sent by the requestor”, even more concrete defined Liberty Alliance: “Direct Trust is obtained when communicating entities hold each other’s keys within their Trust Anchor Lists (TALs), so that their validity is established without reliance on intermediaries.”

This describes the case where two entities establish mutual trust by exchanging their keys, which is commonly done out of band of established infrastructures. Most established solutions hold those keys in Trust Stores, which are used for transport-layer ([mutual] SSL/TLS) or message-level (SOAP Message Security) authentication.

Even being used broadly in many domains, this model obviously has disadvantages with regard to manageability, scalability and synchronisation among a large number of domain actors and services. Anyhow, for sake of better control, key exchange could be managed centrally or on domain-level, what would require an adequate governance model and some centralized infrastructure:



***Figure 1: Central Management of Key Exchange***

Evaluation against criteria (Section [3]):

1. For a larger community, pairwise key exchange is hard to handle and synchronize. May be applicable if only applied for mutual authentication between dedicated services establishing cross-border/-domain connectivity, which in turn use established mechanism in face to the domestic infrastructure they connect to. If free choice certificate issuing CA[[7]](#footnote-7), no or only very restricted means to derive policy/business domain/service type the certificate owner is bound to.
2. Well stablished mechanism, broadly used.
3. Same as (2), but not valid in general.
4. See (1) – restricted scalability.
5. Well standardized, provided by common infrastructure components (not valid for central Trust Store maintenance and – distribution. This would require (minor) implementation efforts.
6. Pairwise key exchange and Trust Store synchronisation has operational challenges, and mayor deficits regarding control of policy-adherence of entities included in the Trust Circle. Could be leveraged by (Domain-) central Trust Store maintenance and – distribution.
7. Comes in play when deciding for central Trust Store maintenance and – distribution. No commercial service known; probably would require funding by government or stakeholders.
8. Liability must be regulated by pairwise business agreements respective those to be set up with a central Trust Store maintainer.

## Indirect Trust Models

“Indirect Trust is obtained when communicating entities ascertain the validity of each other’s keys based on pre-existing trust established with an intermediary, as represented by a trust anchor.”4

For the PKI case, this trusted intermediary is the certificate issuing Certification Authority (CA).

Inside established business domains or even on MS level the number of CAs normally may be small enough and well-known known to the relying party. For cross-border use of certificates the situation is however that the relying party must handle a potentially large number of separate and unknown CAs; how big this number is depends on the relying party’s business needs. Considering only the subset “qualified CAs in the EU/EEA area”, the number is between 100 and 150 CAs. Expanding the scope outside of the EU and to non-qualified CAs inside or outside of the EU, the number of public CAs will be at least several hundred. Then, in some cases even company internal and other non-public CAs may need to be considered, increasing the number further.

To the relying party, the situation is as shown in the figure below. Managing information on such a large number of CAs quickly becomes difficult for the relying party, in particular because the relying party need to know not only the public keys of these CAs but also information related to validation constraints such as the quality and legal status of each CA.

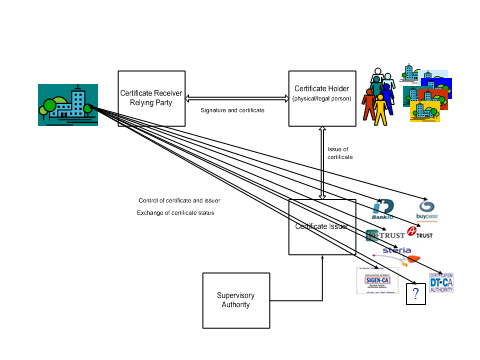


Figure 1: Relying party has to trust many CAs

In this figure, the supervisory authority has also been brought in to show that public CAs will often, and in particular in the EU, be subject to supervision.

Further complicating the picture, each relying party must manage the information individually leading to the situation shown in the figure below.

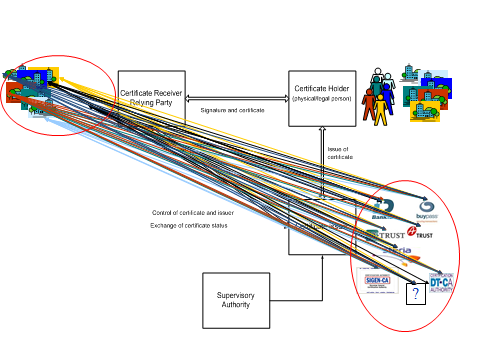


Figure 2: A large number of relying parties trusting a large number of CAs.

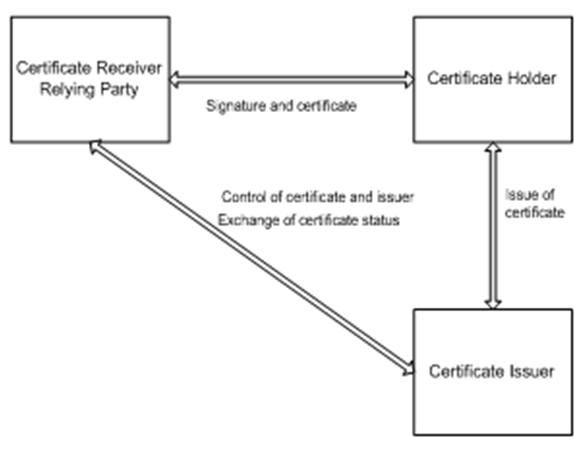
To facilitate trust in CAs, different solutions are used as described below.

### Community Trust

“Community Trust applies when the business trust between a pair of entities is derived from their enrolment in a common authentication infrastructure and acceptance of its practices, without reliance on other business agreement paths. As such, the entities' mutual trust in a business sense is based on their membership in a community constructed and linked for authentication purposes.” 4

#### Community Trust using a dedicated PKI

Communities may decide for a dedicated PKI to issue certificates for all participants and nodes in their network. In the dedicated PKI model there is a single Certification Authority (CA) that guarantees consistency among issued certificates, and a process of issuing certificates only to community members which agree on a specific domain policy and governance model. For the relying party, the latter can implicitly be derived from the certificate issuer. This is the classical PKI “Three-corner Model” as explicitly used today by closed PKI-systems.



***Figure 3: Original three-corner PKI model***

This agreements-based PKI is a system where all relying parties must have an agreement for use of certificates. The underlying governance model and policy the certificate owner is bound to can implicitly be derived from the certificate issuer. Corporate internal and other special purposes PKIs typically also use this model.

The Relying Party just must be able to verify the actual validity, authenticity and integrity of the certificate and interpret the certificate’s content. The actual validity of the certificate must be verified by the Relying Party by means of OCSP/CRL or other trusted certificate validation services[[8]](#footnote-8).

Evaluation against criteria (Section [3]):

1. One Central PKI for all actors in the network not applicable. May be applicable for central shared services and for mutual authentication between dedicated services establishing cross-border/-domain connectivity, which in turn use established mechanism in face to the domestic infrastructure they connect to. Applicability has to be checked for MS (may by specific domains, too) which impose the use of dedicated national or domain PKIs. Policy/business domain/service type all certificate owners are bound to is the one agreed upon in this dedicated PKI, no differentiation possible.
2. No “off the shelf” mechanism broadly supported by standard solutions, but often established in closed business domains / company networks etc .
3. Some MS (e.g. Germany) provide a “Public Administration PKI”, but most of them being hierarchical ones.
4. See (1) – restricted scalability.
5. Well standardized, provided by some common infrastructure components (see Root-Stores below, which may be a one restricting to this single PKI). Would anyhow require some implementation efforts for e-SENS SBBs to restrict to defined certificate issuer(s).
6. PKI services are well established and on the market, or even provided by Public Administration. Setup/provisions of central EC PKI so far seems not to be an option.
7. Business model is usually fees from the CAs; additional government funding is possible.
8. Liability is an issue between the relying party and CA.

#### Community Trust using a hierarchical PKI

In extension of the dedicated single PKI model, a community may choose set up hierarchical PKI model. In this model, the community root CA issues certificates to different sub-CAs, which in turn issue certificates to end entities acting in different, well defined roles in this community network.

At a broader level, a hierarchical PKI for qualified signature certificates is in use today in several EU countries, e.g. on governmental level in Germany and Poland, and in countries outside the EU. The root-CA policy poses requirements to CAs that can obtain certificates, e.g. a government root-CAs may only accept qualified and supervised CAs, or the government may run different root-CAs for different types of CAs. Government root-CA certificates are today (at least usually) not distributed in root-stores but may be included in Trusted Lists.

A number of commercial root-CA operators operate in a global market, e.g. CAcert, DigiCert, GlobalSign and Verisign. These services are strongly linked to use of root-stores. All CA-certificates placed under one of these root-CA operators will be trusted by default by all users of the root-stores where the root-CA is present. Some software and service suppliers, like Adobe, run their own root-CA services.

A number of issuers of (qualified and other) certificates in Europe have their CAs placed under commercial root-CA schemes. The root-CA operators usually provide several root-CAs covering different certificate types and possibly quality levels. Requirements for obtaining a certificate must be compatible with requirements for inclusion in the root-stores. Thus, a relying party can draw some conclusions from the root-CA certificate on CA quality. However, “qualified”, commercial root-CAs do not exist.

One concrete example of this model is the OpenPEPPOL Trust Network (PTN), the hierarchy consists of an OpenPEPPOL root CA with three sub-CAs. The OpenPEPPOL root CA issues certificates for following sub-CAs only:

1. OpenPEPPOL Access Point Sub-CA
2. OpenPEPPOL Security Token Service Sub-CA
3. OpenPEPPOL Service Metadata Publisher CA.

Sub-CA (2) issues certificates for end entities interacting in this community. Thus, depending on the certificate issuing sub-CA, certificate owners role can directly be derived from the issuer, which implies a policy the certificate owning end entity and issuing sub-CA agree upon.

Evaluation against criteria (Section [3]):

Principally the same applies as for one single dedicated PKI, with one advantage: Policy/business domain/service type a certificate owners is bound to can be differentiated according policy agreement with issuing sub-CA.

#### Bridge-CA

A bridge-CA is a central hub, with which CAs cross-certify. The bridge-CA should be run by a neutral actor, and it shall itself only issue cross-certificates. The usual situation is cross-certification between the bridge-CA and root-CAs although individual CAs may also obtain cross-certificates. A relying party may obtain a certificate path to a given CA by starting at its own root-CA, and then proceed to a certificate issued by its root to the bridge-CA. This is shown in the figure below.

Compli­cated certificate paths with related challenges in path discovery and path validation may occur when using a bridge-CA.

Cross-certification between a CA and a bridge-CA is considerably simpler than peer-CA cross-certifi­cation, as the bridge-CA has no (competing) role in issuing of certificates to end entities.

Bridge-CAs are used at national level in some countries, notably the Federal Bridge CA (FBCA) in the USA. Commercial bridge-CAs exist usually targeted at specific business areas such as the SAFE Bridge-CA in the pharmaceutical area and the bridge-CA for the defence and aerospace area, both operating at global level.

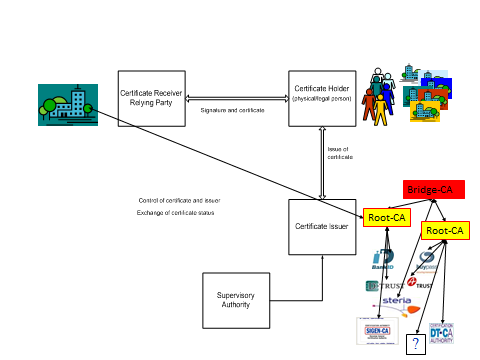


Figure 4: Bridge-CA solution

Evaluation against criteria (Section [3]):

This model is given for completeness, but actually it has no noteworthy advantages to the models depicted above, rather it’s more complicated to build up the trust path, as the relying party initially has to . A European bridge-CA cross-certifying with all CAs across Europe could be a solution to EU-wide PKI interoperability but there is no initiative in this direction at present. Thus, an “EU bridge-CA” is not a solution model or building block that shall be promoted by e-SENS. Detailed evaluation against criteria is omitted here.

### Root-Stores

Many operating system (e.g. Microsoft and Apple), software and service suppliers have their own root-store services, thereby distributing lists of acknowledged CA-certificates, mainly root-CA certificates, to their users. Normally, certificates from a root-store are “installed” locally on the user’s (the relying party) equipment, and certificates in the root-store are trusted by default. The local copy of the root-store may be managed by removing certificates that are not to be trusted and by adding further root-CA or other certificates.

To be added in a root-store, a CA typically has to prove conformance to certain requirements, most often a “Web Trust for CA” certification is required. Some actors, e.g. Microsoft, accepta certificate of compliance with ETSI TS 101 456 (policy requirements for qualified certificates) as replacement for the Web Trust certificate.

The root-stores themselves do not normally distinguish between different types of root-CA certificates. All certificates in the root-store are trusted at the same level and the relying party must perform further checks on the certificates, e.g. if verification against particular certificate quality requirements is necessary.

Evaluation against criteria (Section [3]):

*tdb*

## Brokered Trust Models

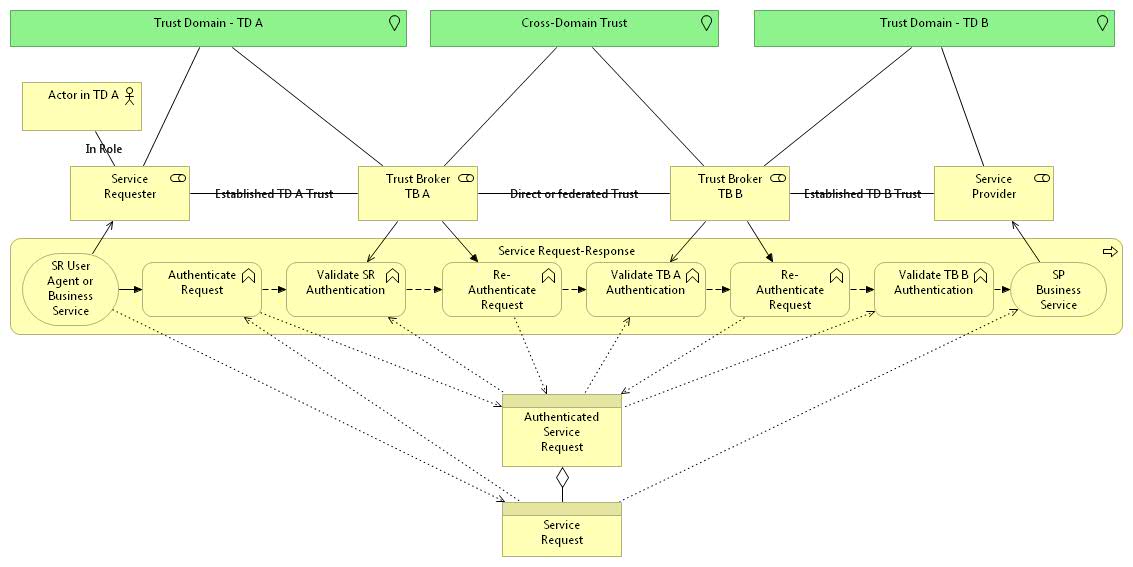
In the Brokered Trust Models, there is no direct trust established between interacting parties of different Trust Domains. There must be a broker - trusted intermediary – available, able to validate security tokens of foreign Trust Domains. “… Brokered Trust is when one party trusts a second party who, in turn, trusts or vouches for, a third party”2; this includes vouching for claims of entities carried out in third party security tokens. This model fits best when establishing trust between different Trust Domains, which even may use different local mechanisms for trust establishment. The challenge for e-SENS is to establish trust to those second parties vouching for trust of the entities inside the particular Trust Domains. Different from the Indirect (PKI based) Trust Models described above a relying party also needs to assess the risk related to the acceptance of the second party certificate and the trustworthiness of the issuing CA as well as the second party TSP itself.

In the Direct Brokered Trust Model, it is assumed that there is a business agreement in place between the relying party and the broker, which explicitly identifies trust relationships to foreign security token issuers and thus allows for direct trust in those tokens by the relying party.

Different from the Direct Brokered Trust Model, the Indirect Brokered Trust Model places broader trust in the broker, “allowing it to act as an agent for the service provider and to establish paths to other parties without requiring that those parties be identified in advance in the business agreement between the local service provider and the intermediary. This subcase can allow business trust to be established more dynamically and to a broader range of peers.” [[9]](#footnote-9)

**Note:** From the technical viewpoint, there is no difference between these two Brokered Trust Models.

Following figure depicts the cross Trust Domain flow and authentication of a service request:



***Figure 6: Brokered Trust Use Case***

Evaluation against criteria (Section [3]):

*tdb – in conjunction with section 5*

## Trust Federation using Trust Lists

Among others, to enable Trust Federation at least for CAs issuing qualified signature certificates (which is just one type of TS), the EUMS already implemented the concept of “Trust Service Status List”, which should be adopted by e-SENS and extended to other types of TS.

“Trusted lists … enable in practice any interested party to determine whether a trust service is or was operating in compliance with relevant requirements, currently or at some time in the past (e.g. at the time the service was provided, or at the time at which a transaction reliant on that service took place). In order to fulfil this requirement, trusted lists necessarily contain information from which it can be established whether the TSP’s service is, or was, known by the Trusted List Scheme Operator (TLSO) and, if so, the status of the service. Trusted lists therefore contain not only the service's current status, but also the history of its status.” (ETSI TS 119 612 “Trusted Lists”[[10]](#footnote-10), page 8).

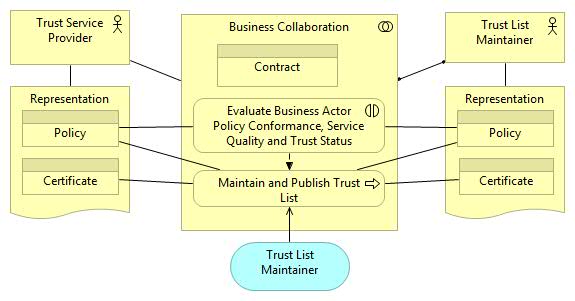
Actually the eIDAS regulation gives a legislative base to expand Trust List (TL) usage to cover the mutual recognition and acceptance at EU level of notified electronic identification schemes and other essential related electronic Trust Services. Independent from the aims of the eIDAS regulation to extend the “official national TLs” to cover more types of Trusted Services, TLs can be set up at a community level – which could be an e-SENS wide TL or even different instances on domain level, which then may have different TL Scheme Operator policies in effect, if needed.[[11]](#footnote-11)

A TL entry includes a “digital identity” of the TS used to authenticate it (this usually is an X509v3-Certificate used for signing tokens and service results provided by the respective TS). The digital identity token and signature of the service output can be used by TS consumers as Relying Party to validate its authenticity and integrity; they may use the TL to discover the actual (as well as historical) TS status. Anyhow, the underlying concept of “Trust Service Status List” does not replace the need of verifying the actual validity of the digital identity token; this again must be done using the means of the token issuing authority.

The Community- as well as Brokered Trust models may be combined with the Trust List. If a certificate is presented from a PKI not trusted by default, the TL should be checked if the certificate is the one listed “digital identity” of the service in question.

The e-SENS Trusted Service Lists may include TSPs and their TSs of EU and Non-EU member states participating in e-SENS. Different TLs may be set up according to domain needs, operating under domain-specific policy schemes.

TL(s) could be managed centrally or on domain-level, what would require an adequate governance model and some centralized infrastructure:



***Figure 7: Trust Establishment using a Trust List***

Perquisite is a common agreement of the TSP and the Trust List Maintainer on a contractual base, liability agreements and operational policy. An exposure of a TSP in the Trust List (which may be Domain specific instances) must be preceded by an accurate policy conformance evaluation and rating of Trust Status and TSP Service Quality. Continuous or periodic supervision of conformance of TSP status and operation is a matter of the operational policy of the TL Provider. This policy should be based on contractual agreements between the TL Provider and TSPs covered by this TL instance or even may be regulated by law (as e.g. for CA’s issuing certificates for qualified Signature / Seals). TSP attributes exposed in the actual Trust List must reflect the actual TSP status. Historical records must be kept in the TL to allow retrospective lookup of TSP attributes.

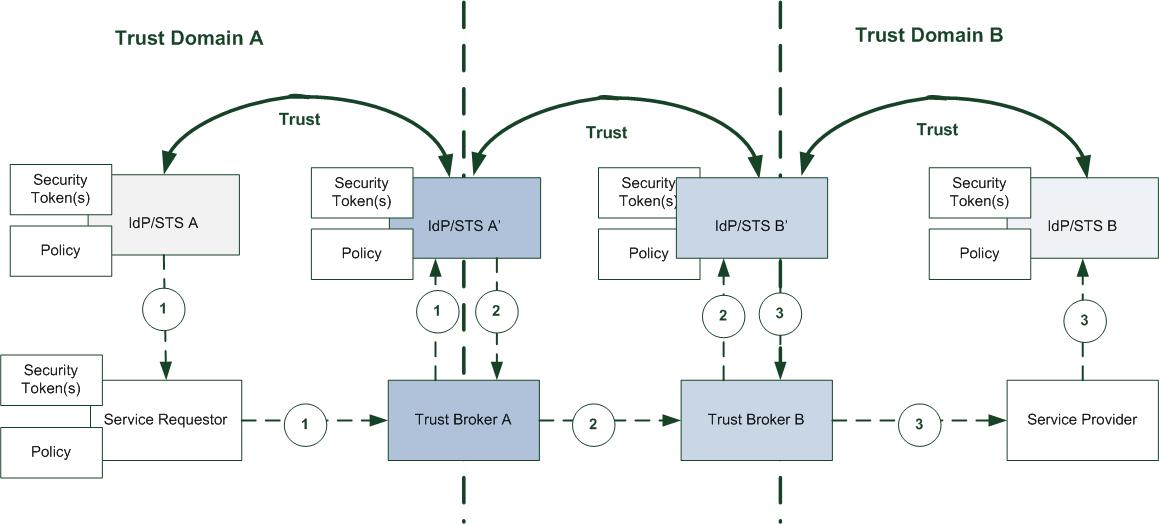
Evaluation against criteria (Section [3]):

*tdb*

# Usage of SAML Token and Security Token Services for Trust-Brokerage

For purposes of authentication, X509v3-Certificates have very limited means. If additional claims, attributes, token validity time spans, intended audience / targeted business scenarios etc. are needed, SAML token are the means of choice. This in addition is state of the art for federated Trust Model solutions.

Building on WS-Trust, WS-Federation[[12]](#footnote-12) identifies a couple of alternate Trust Federation models; aligned with the Trust Use Case depicted in [***Figure 6***], federation would look like:



***Figure 8: Trust Brokerage/Federation***

Note that WS-Trust/WS-Federation, like WS-Security, allow for a wide range of security token types. All Tokens (x) above could just be X509v3-Certificates, too.

Description of flow – Service Requestor (SR) has to authenticate at Service Provider (SP):

1. IdP/STS A in Trust Domain A issues Token (1) to SR (Note: IdP/STS A could be a CA)
2. Token (1) is presented at Trust Broker A, using IdP/STS A’ to validate Token (1), resulting in Token (2). IdP/STS A’ trusts tokens issued by IdP/STS A, or both are just the same instance – depending on setup of domestic Trust Domain A.
3. Token (2) is presented at Trust Broker B, using IdP/STS B’ to validate Token (3), resulting in Token (3). IdP/STS A’ and IdP/STS B’ are in Trust relationship.
4. Token (3) is presented at Service Provider, which may either directly trust tokens issued by IdP/STS B’ or involve IdP/STS B to validate Token (3) - depending on setup of domestic Trust Domain A. Like for Trust Domain A, IdP/STS B’ and IdP/STS B may be just one instance.

*This section still has to be completed: SAML usage as the better fitting token, and option to expose of IdP/STS above in a Trust List.*

Evaluation against criteria (Section [3]):

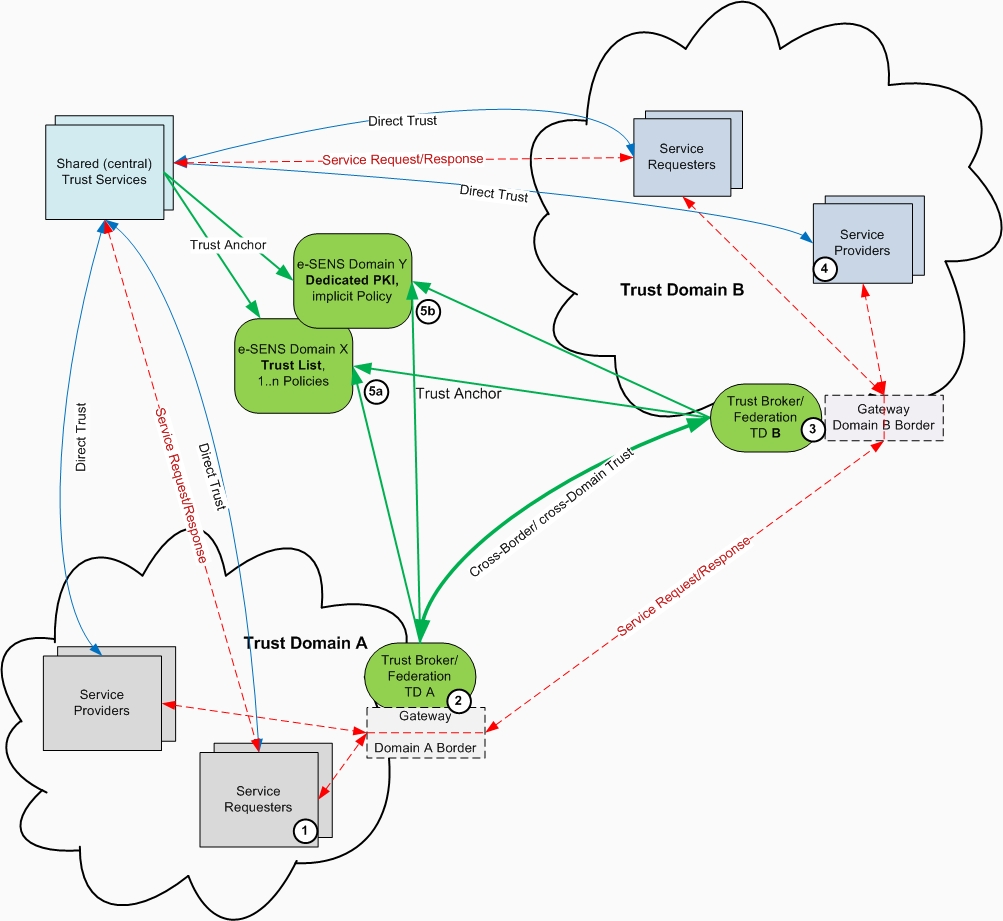
*tdb*

# “Big Picture” using Trust Brokers and Trust Lists

An overview of Trust Circle relationship of involved entities is given below. The “Trust Broker” instances depicted conceptual entities, whose functionality may be realized by different means, fitting to the needs of concrete distributed electronic transaction types. A Trust Broker covers “Trust Validator” functionality, able to check the existence of a presented digital identity in the underlying trust anchor (Trust List or affiliation to dedicated PKI) and its actual validity.

Depending on the topology established for a concrete scenario, Trust Broker functionality can

1. directly be allocated to the respective applications used by interacting Service-Requesters (SR) and Service Providers (SP);
2. or being allocated to active intermediary nodes used at respective SR/SP domain boundaries for realizing connectivity and interoperability between different technical infrastructures used in these domains. Such nodes e.g. are e-Delivery / e-Interaction Gateways (from former LSPs also known as Access Points (PEPPOL AP) or National Contact Points (epSOS NCP).

When enabling existing, so far “closed” domains for cross-border/-domain connectivity, typically (2) is the choice, to disburden applications itself by using centralized services/providers of such.

***Figure 7: Cross-Domain/-Border Trust Circle***

**Note:** Instead of having different Trust Brokers instances per Trust Domain, Domains could agree on one commonly used instance. In this case, the Trust Broker is able to trust and validate all Certificates used for Authentication in all affiliated Domains[[13]](#footnote-13), and all SR’s/SP’s just trust this Trust Broker instance. Authentication validation and re-authentication depicted in [***Figure 6***] collapse to one single pair of steps.

1. See Section 3.1.5 “Authentication mechanisms” in <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid/at_download/fullReport> [↑](#footnote-ref-1)
2. See <http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html> for more details [↑](#footnote-ref-2)
3. See section 8 in <http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_SECTION_II_epSOS_Security_Services_01.pdf> [↑](#footnote-ref-3)
4. <http://www.projectliberty.org/liberty/content/download/1232/8000/file/liberty-trust-models-guidelines-v1.0.pdf> [↑](#footnote-ref-4)
5. <https://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf> [↑](#footnote-ref-5)
6. <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html> [↑](#footnote-ref-6)
7. For public administration services, some MS impose the use of dedicated national PKIs [↑](#footnote-ref-7)
8. As e.g. XKMS/XKISS-Responders provided by PEPPOL [↑](#footnote-ref-8)
9. Liberty Alliance Project “Liberty Trust Models Guidelines Version 1.0”, Section 2 “Definitions, Taxonomy, and Conceptual Processing Procedure”; <http://www.projectliberty.org/liberty/content/download/1232/8000/file/liberty-trust-models-guidelines-v1.0.pdf> [↑](#footnote-ref-9)
10. ETSI TS 119 612 V1.1.1, (2013-06), <http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/01.01.01_60/ts_119612v010101p.pdf> [↑](#footnote-ref-10)
11. Such TLs already where established and used by other LSPs, e.g. PEPPOL, SPOCS, epSOS [↑](#footnote-ref-11)
12. OASIS 2009, Web Services Federation Language (WS-Federation) Version 1.2 <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf> [↑](#footnote-ref-12)
13. This could e.g. achieved by a Bridge-CA or Trust List model [↑](#footnote-ref-13)