SecNet-IE

A secure network for CNI Information Exchange

Fotios Basagiannis
SCNI, IPSC, JRC, European Commission
fotios.basagiannis@jrc.it

SCNI action

- Security of Critical Networked Infrastructures action
- Part of Joint Research Centre's (JRC) Institute for the Protection and Security of the Citizen (IPSC)
- JRC is an organic part of the European Commission
- The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.
- Action website: scni.jrc.it
- Action leader: Marcelo Masera
- About a dozen people

Problem Addressed by SecNet-IE

- System for the exchange of sensitive information among Critical Infrastructures (CI) stakeholders.
- Stakeholders from many different countries (EU) and from both the private and public sectors.
- Availability and sharing of data on the factors that determine CI security risks (vulnerabilities, threats, attacks, intrusion attempts) is crucial.
- Problem is finding a way to
  - Develop, manage and maintain trust among stakeholders
  - Remotely access distributed resources
  - Guarantee adherence to pre-agreed rules/procedures throughout
  - Do all of the above securely
- A system potentially encompassing a lot of technologies and perspectives but here focusing on just some.

Basic Requirements

Initial proposals, studies and prototyping suggest the Following basic high-level requirements:

- Decentralized data and control model
- Avoidance of singe points of failure
- Ability to fit in a wide variety of environments
- Multilingual operation and message translation
- Clear message semantics (metadata)
- Strong security characteristics

Furthermore, the Traffic Light Protocol (UK's Centre for the Protection of National Infrastructure) has been suggested for managing message dissemination among stakeholders and their organizations.

Project Status

- We have put together a special Software Development process to deal with our special needs
- We call it ROSF. A process for Research Oriented, Security Focused software development
- The process is the product of the synthesis of two proven models for software development but is more than the sum of
  - IID (Iterative & Incremental Development) and especially the Unified Process
  - Rapid Prototyping
- Rapid prototyping is used as a tool during the analysis phase.
- **The project is currently in the analysis phase** which requires feedback on high-level designs/architectures and prototype functionality.
- Participation to this workshop is part of this feedback seeking process.

Some seminal SecNet-IE MSFTs

- MDR (MetaData Registries) - ISO/IEC 11179
- FEA (Federal Enterprise Architecture)
- NIEM (National Information Exchange Model)
- ebXML
- Rains-Net (Secure Clients and Double-Gated Hubs)
- DHT P2P (Distributed Hash Table Peer-to-Peer)
- X.509 (PKI certs)
- X.500 (cert directories)
- E-mail related standards

A few assumptions

- A distributed system that is outside the control of a single authority would have trouble making a strong claim at being secure without making use of security hardware (like HSMs, TPMs, Smart Cards and biometric readers)
- Sustained and guaranteed control over the characteristics of a number of messaging nodes deployed in a large number of organizations (public and private) cannot really be achieved without the use of trusted agents (or a similar concept).
- Split knowledge (e.g. n/m custodians) and procedural/social controls where not impeding timely/efficient operation are crucial

Current Prototype Design Vectors

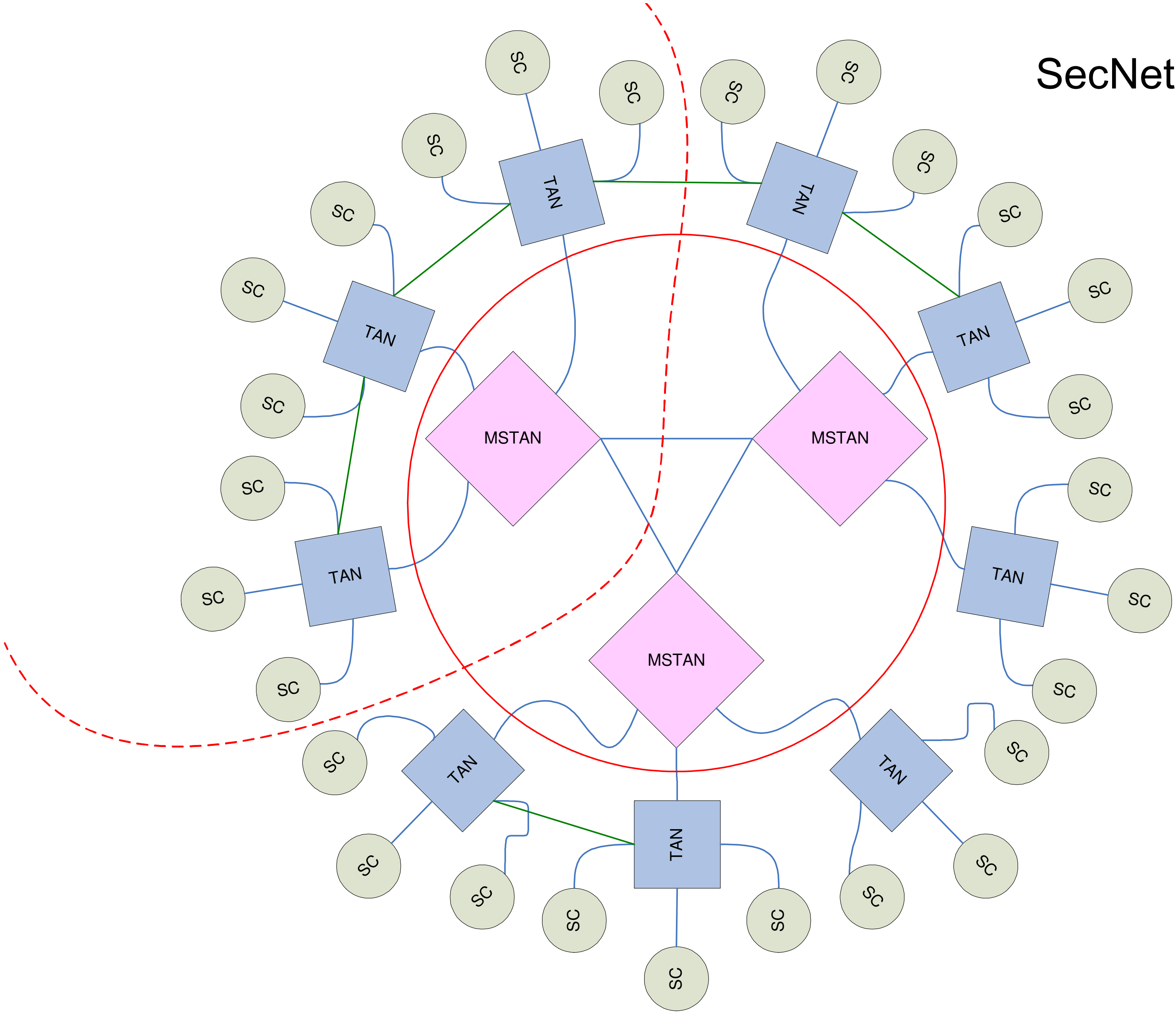
Our approach to designing and implementing such a proof of concept system is currently described by the following vectors:

- SecNet-IE is a DHT P2P network of secure nodes
- Secure nodes form a secure P2P messaging bus
- Secure clients connect to secure nodes
- Trusted agent implementation of nodes' and clients' core messaging functionality
- Proven communication paradigms and standards
- Mature open source technologies
- Hardware based security infrastructure (HSM & TPM)
- Local and distributed workflow support
- Use of TLP protocol for information dissemination

DHT in SecNet-IE

- In SecNet-IE DHT is used as efficient resource discovery mechanism, not for files or the body of messages but rather for the distributed dynamicly updated db of certs, CNI & CIP metadata and maybe as a person lookup mechanism
- The hows and whats of DHT’s place in SecNet-IE are still pretty fuzzy.

SecNet-IE network



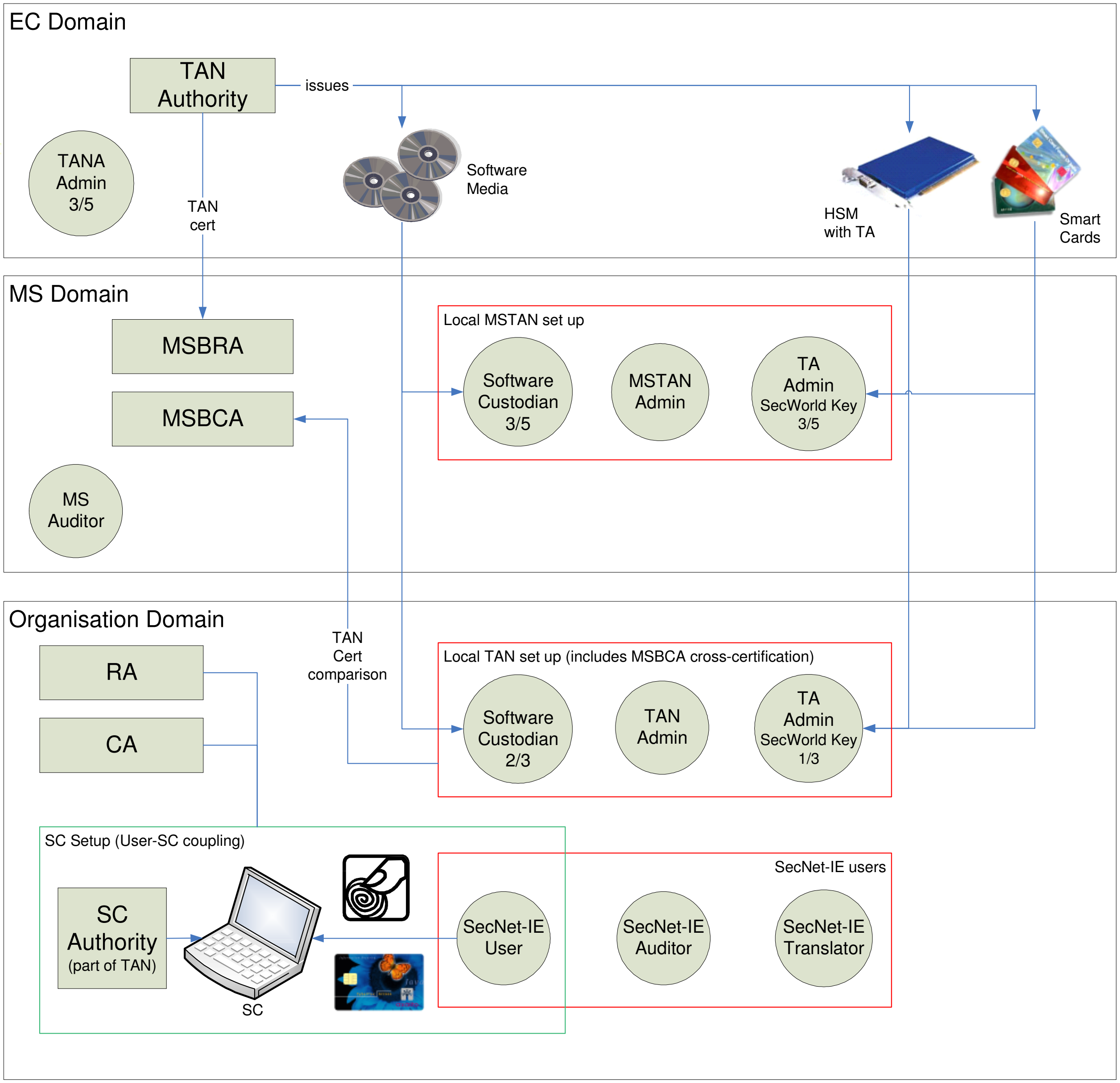
Notes

MSTAN graph is required to be complete to ensure trusted communication capability among all TANs
MSBCAs in MSTANs bridge MS mesh islands of trust and provide a default/initial introduction mechanism for new TANs
MSTANs exist in their own fully networked island of trust
Connections shown are network connections based on mutual trust (direct or implied)

━ connection
━ TAN-to-TAN connection
- - Island of trust

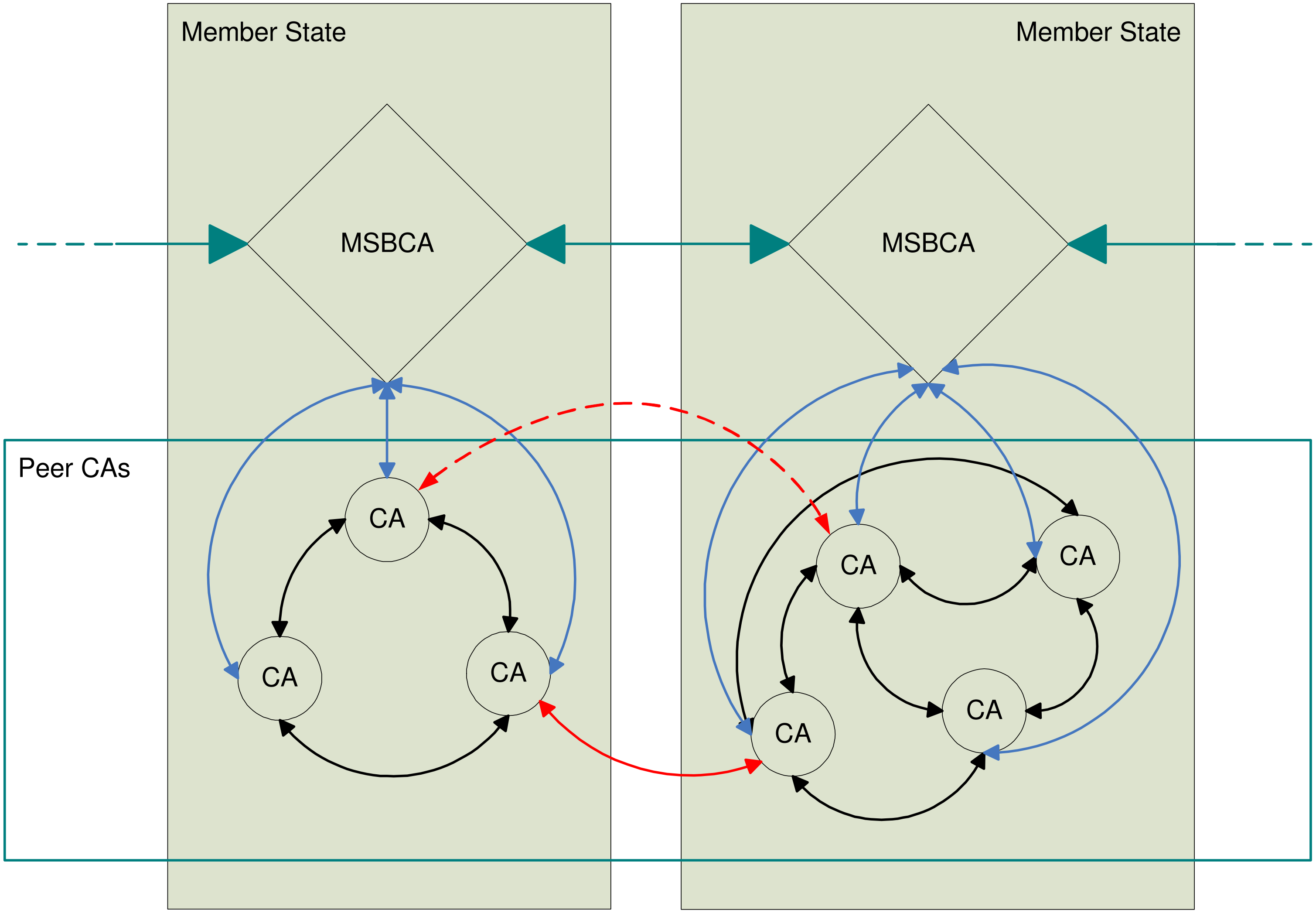
SecNet-IE Authorities, Domains and Users

TAN cert comparison: new TANs have to demonstrate a TANA generated cert (or other credential) that their respective BCA knows about in order to register with it. A protocol is needed that guides the process of TAN initiation and registration with an MSTAN BCA. Just relying on verifying the signature would introduce a weakness in case of TANA key compromise.



- Security World Key is used to unlock/activate the already embedded TA
- n/m custodians (split knowedge)
- TANA = TAN Authority
- TAN = Trusted Agent Node
- MSBRA = Member State Bridge Registration Authority
- MSBCA = Member State Bridge Certification Authority

Note: HSM is FIPS-140-2 Level 3 certified



↔ peerCA-MSBCA cross-certification

↔ peerCA-peerCA cross-certification

↔ cross-MS peerCA-peerCA cross-certification

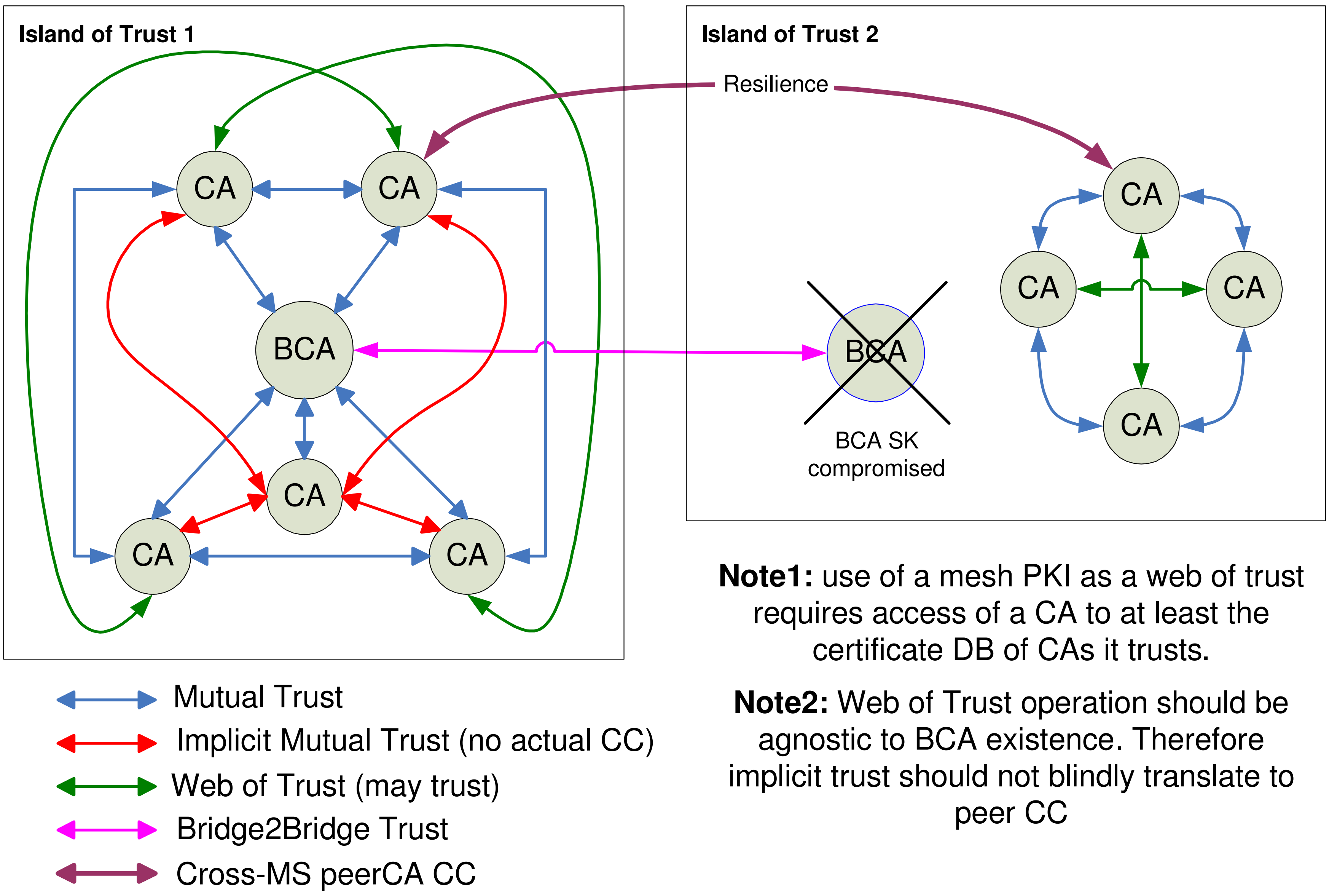
↔ MSBCA-MSBCA cross-certification

⇠ ⇢ Bridge facilitated trust chain

MSBCA = Member State Bridge CA

Note: peer CA graphs above need not be complete but each peer CA should normally cross-certify with its MSBCA. Peer and cross-MS peer cross-certification provide for reliability and availability in case of MSBCA compromise

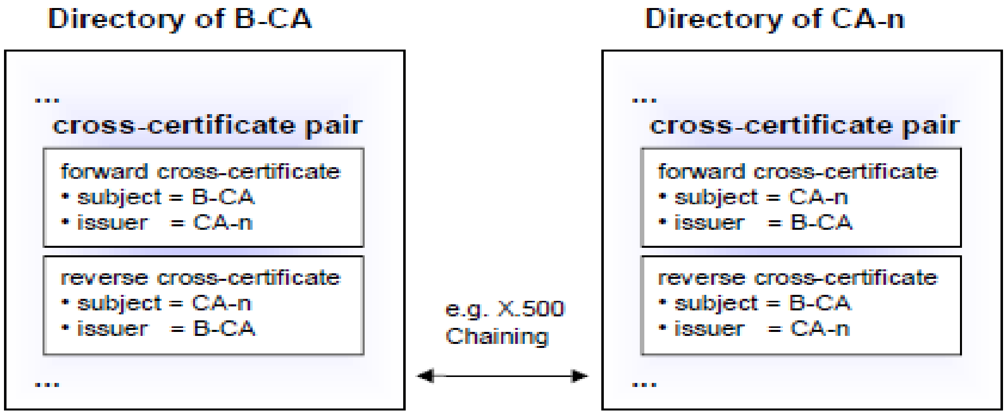
Bridged Mesh of Trust



Note1: use of a mesh PKI as a web of trust requires access of a CA to at least the certificate DB of CAs it trusts.

Note2: Web of Trust operation should be agnostic to BCA existence. Therefore implicit trust should not blindly translate to peer CC

SecNet-IE
Cert Directories and lookups



Directory of B-CA

...
cross-certificate pair

forward cross-certificate
- subject = B-CA
- issuer = CA-n

reverse cross-certificate
- subject = CA-n
- issuer = B-CA

...

e.g. X.500
Chaining

Directory of CA-n

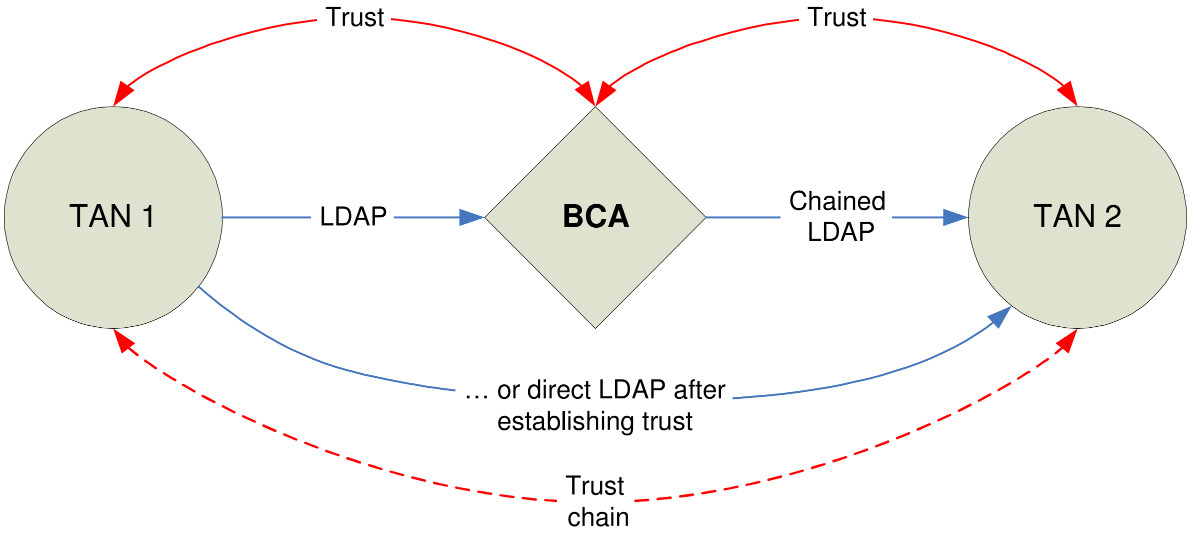
...
cross-certificate pair

forward cross-certificate
- subject = CA-n
- issuer = B-CA

reverse cross-certificate
- subject = B-CA
- issuer = CA-n

...

X.500 = Bridging Directory
X.509 = PKI certificates



Trust

Trust

TAN 1

LDAP

BCA

Chained
LDAP

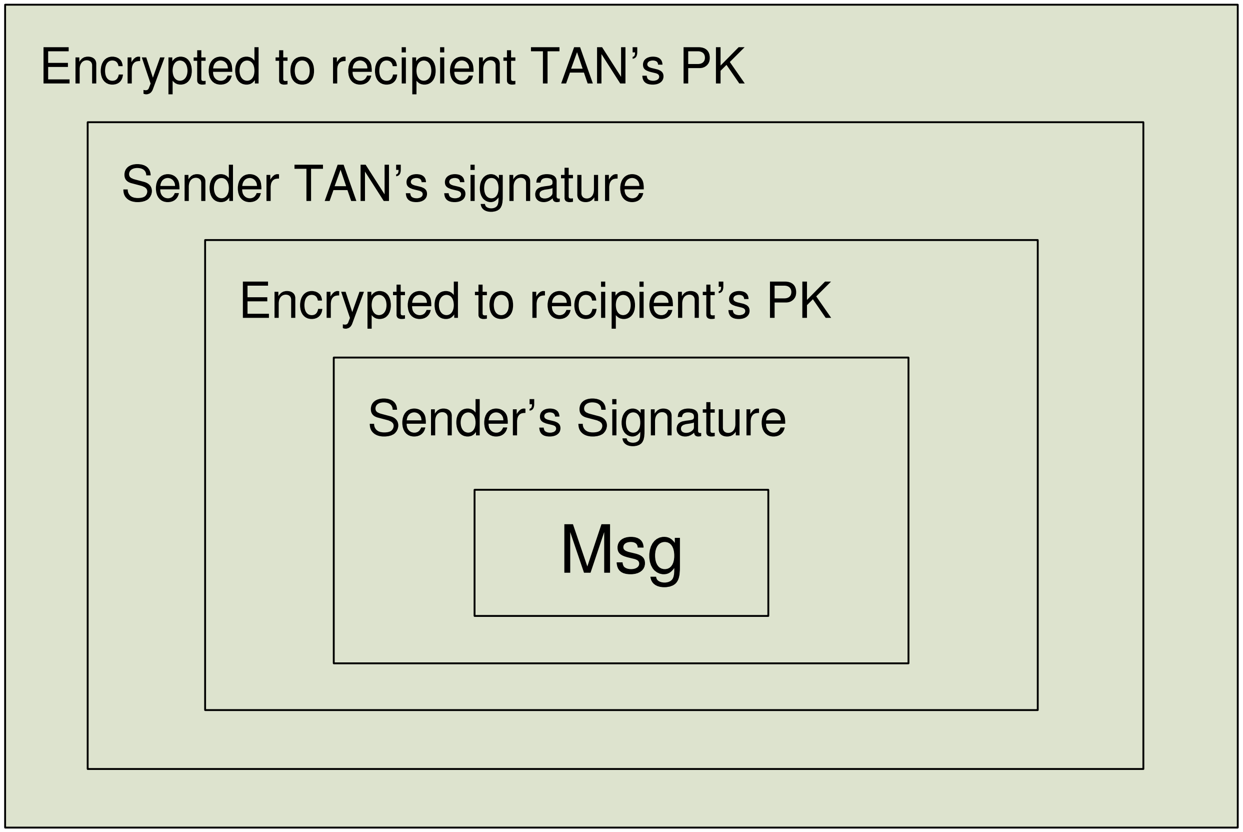
TAN 2

… or direct LDAP after
establishing trust

Trust
chain

Note: It is possible that in SecNet-IE Trust chaining will be used not for individual lookups but in order to initiate P2P cert db mirroring sessions – that is as long as the two peerCAs have not yet cross-certified.

Message Package upon reception at recipient TAN



Encrypted to recipient TAN's PK

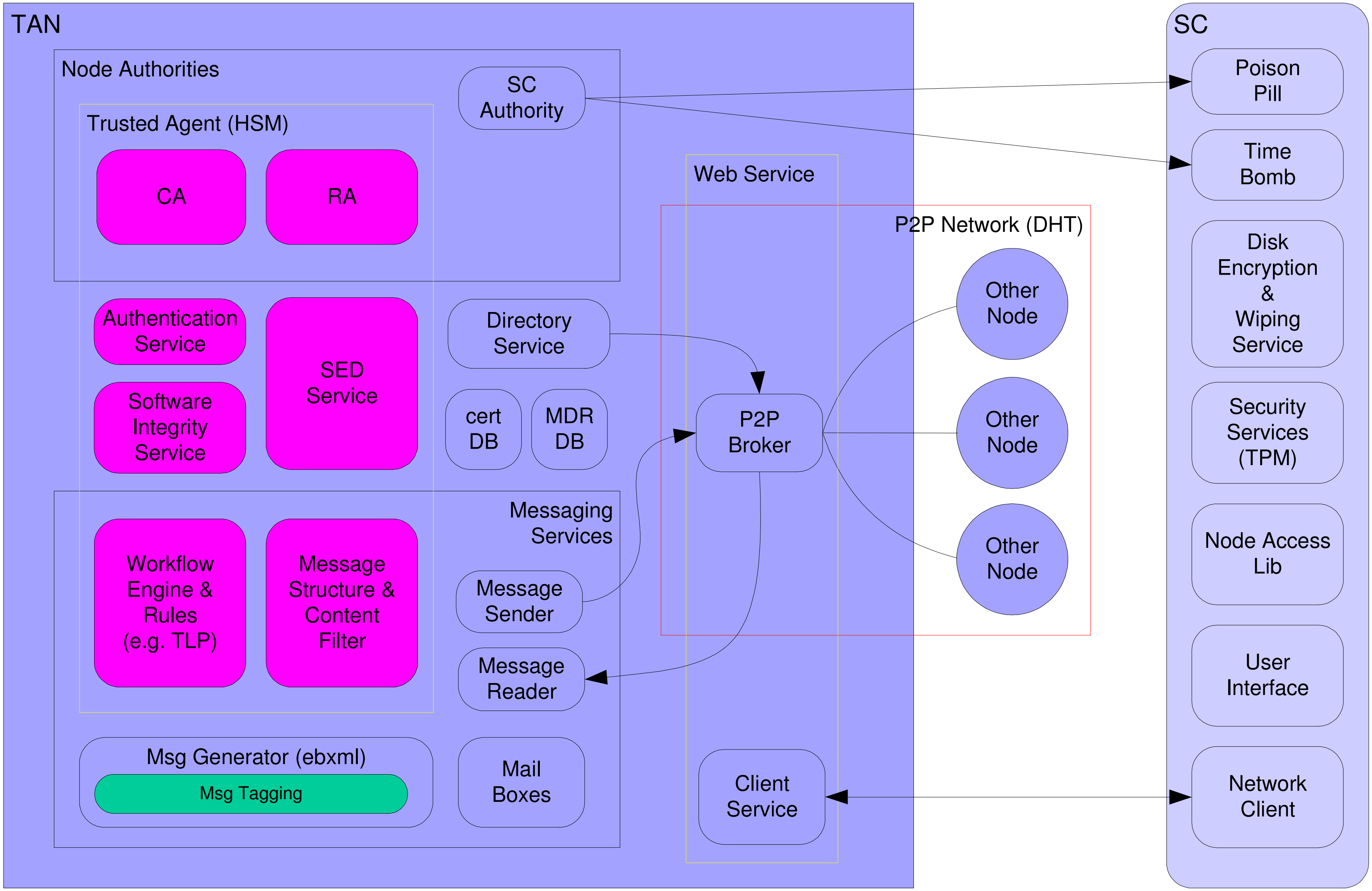
Sender TAN's signature

Encrypted to recipient's PK

Sender's Signature

Msg

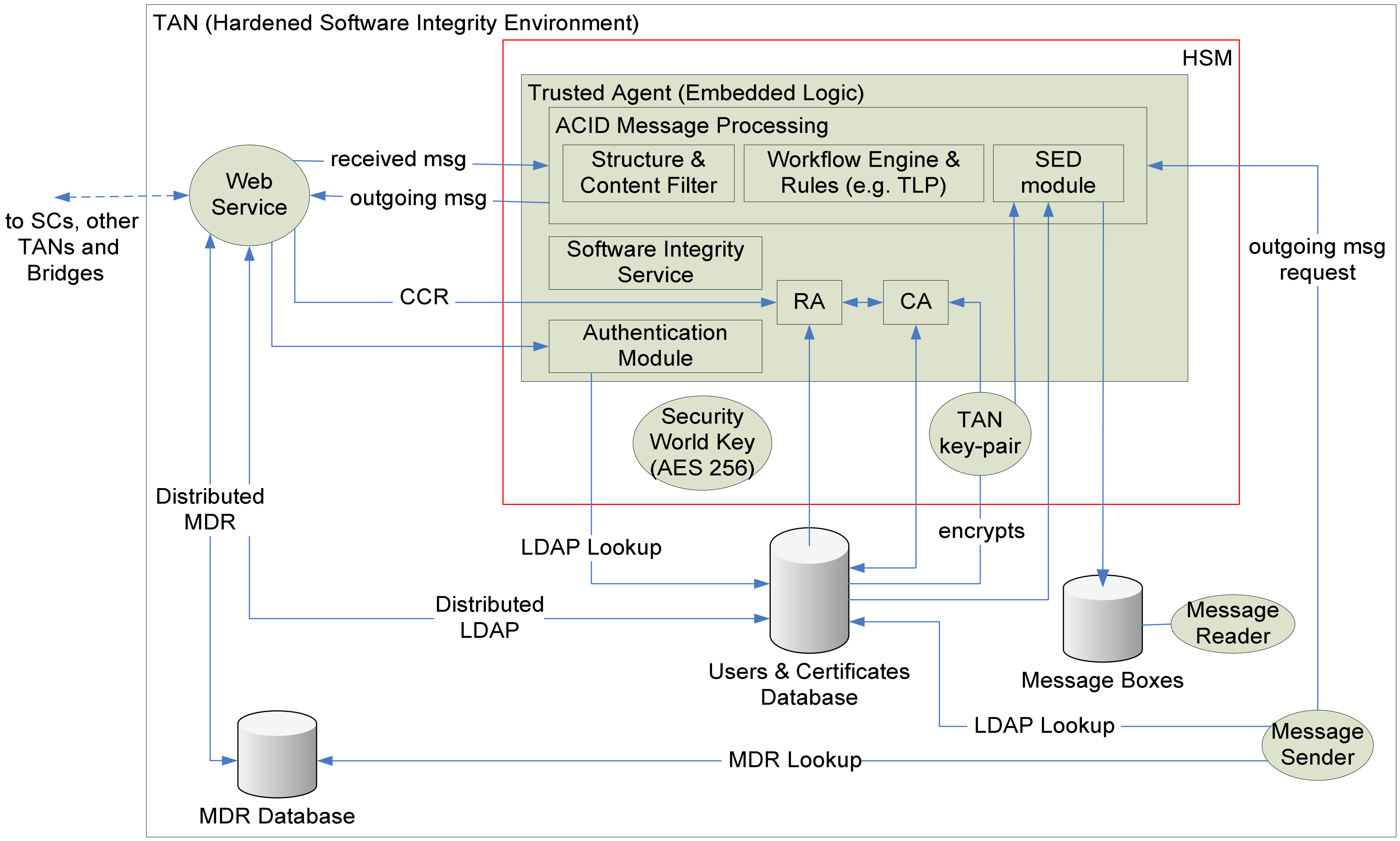
Functional structure of TAN & SC



Note: Directory service performs trust and metadata related lookups

SED = Signature, Encryption, Decryption

TAN Functional Architecture



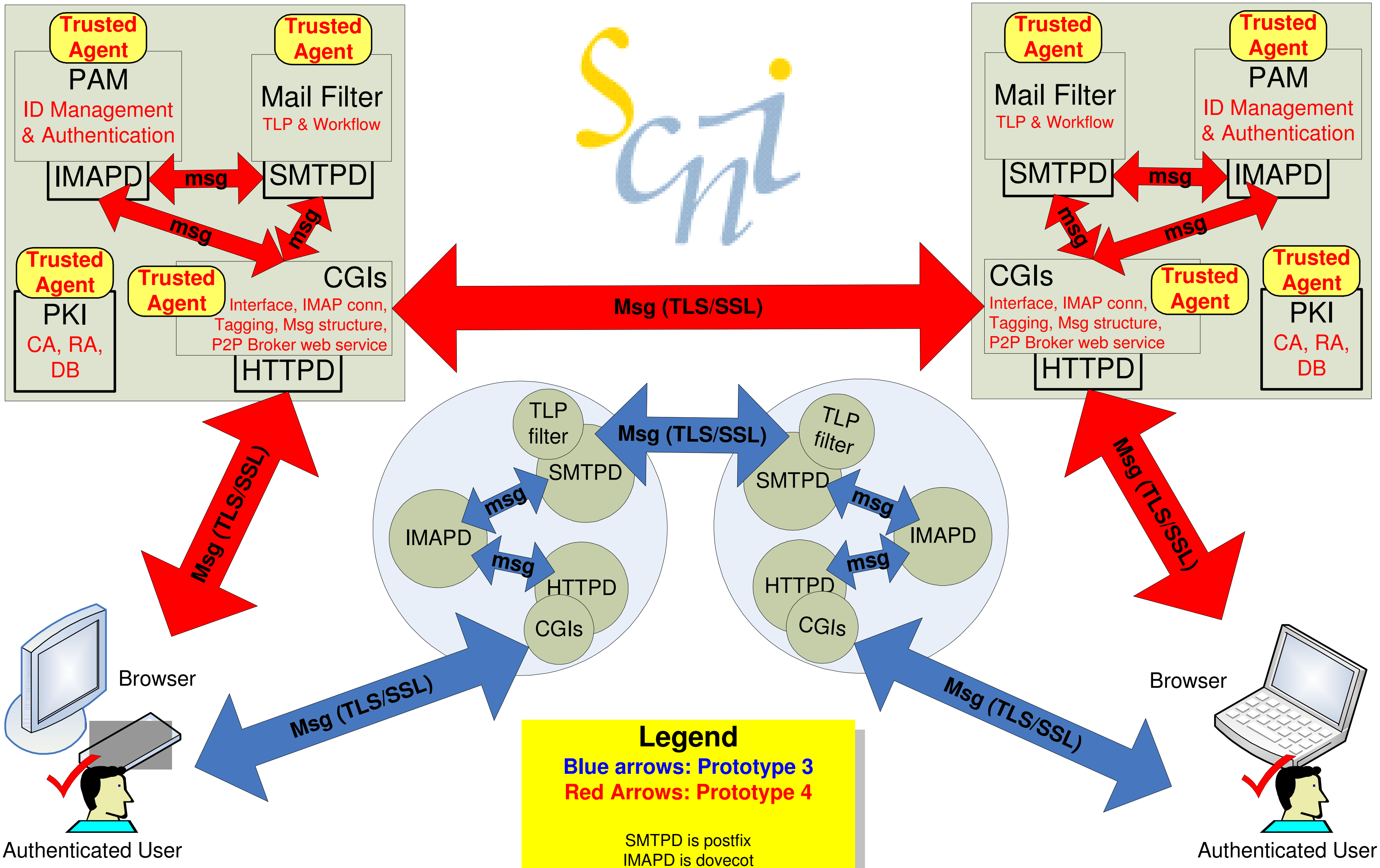
Note: the MDR (MetaData Registries) DB is continuously updated from peer TAN MDR DBs as well as its SecNet-IE Bridge's MDR DB
Note2: Distributed LDAP DB is also a peer mirror of certs and forwards lookups for unknown ones to the appropriate remote peer TAN's LDAP, over the web service. Kknowledge of all certs and their certification paths could become sensitive knowledge.

TAN = Trusted Agent Node
TA = Trusted Agent
SC = Secure Client
ACID = Atomicity, Consistency, Isolation, Durability

CA = Certification Authority
RA = Registration Authority
CCR = Cross Certification Request
HSM = Hardware Security Module

SecNet-IE Prototype 3 & Prototype 4 Messaging

6/20/2008



Legend

Blue arrows: Prototype 3

Red Arrows: Prototype 4

SMTPD is postfix
IMAPD is dovecot
HTTPD is apache
In proto 3 the CA is openSSL based

Issues

A central authority still exists!?

- A CA compromise (in hierarchical PKIs) & BCA or TANA compromise in SecNet-IE do not have the same consequences
- In TANA there is no root key whose compromise would mean someone would be able to upset trust chains.
- Even if the TAN setup material (at the TANA) was to be compromised, there would be no BCA entry of the forged TAN's certificate and therefore the node would never initialize
- BCA entry of new node certs requires a mutual strong authentication, between TANA & BCA, that includes procedural social controls.
- Problem: How to detect forged compromised BCA node from joing the network?
- Same problem with TANs. How to prevent TAN network poisoning and propagation of the poisoning (poisoning of the distributed data).
- Obviously, a compromised BCA does not prevent a TAN from trusting other nodes (like a compromised root ca would) on its own right via peer Cross-Certification.

Issue: Code calling HSM

- How is the integrity of the software initiating the HSM calls ensured? Possibilities
  - Tripwire and split knowledge of hashes
  - Also hardened OS and TPM based trusted system (system integrity)
  - The HSM embedded Trusted Agent somehow checks integrity of the whole system or calling process? Ideas anyone?

User Authentication

- Ideally, how should the user authenticate to the system?
- Desirably: using a smart card holding a cert, supplying PIN to the smart card and a biometric separately (multi-factor auth)
- The user would authenticate to the Secure Client, the SC to the TAN, the TAN to another TAN.
- Current experimental prototype: user & pass

Reporting vulnerabilities & incidents

- Companies and organizations most often unwilling to make public incidents that have occurred or vulnerabilities that have been discovered.
- anon messaging capabilities become important. But how?
- Mixmaster/Cypherpnk paradigm?
- P2P a great platform for anon messaging implementations

Message Semantics potentially weak

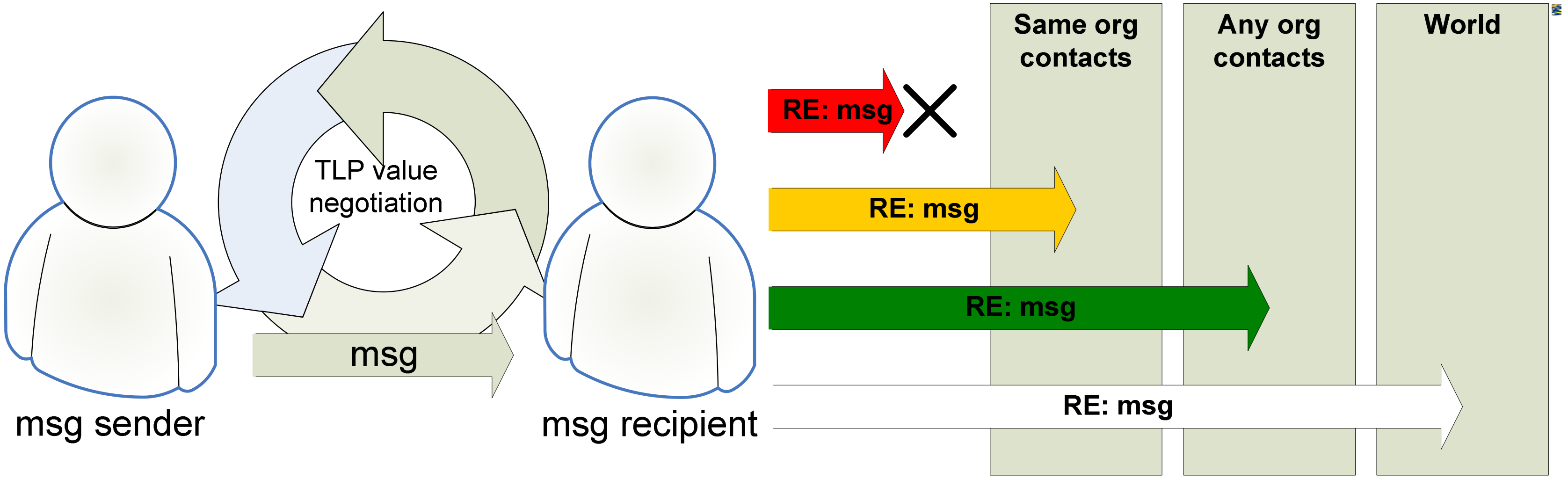
- Multi-lingual issues
- Multi-cultural issues
- No security ontology
- Use of multiple taxonomies may be confusing
- Use of one taxonomy may be restrictive

Annexes

Factors Affecting Interoperability

- Numerous autonomous agencies
- Multiple trust domains
- Heterogeneous environments
- Varied governance structures
- Significant investment in legacy environments
- Inconsistent or non-existent security policies & procedures
- Disparate and incompatible security mechanisms

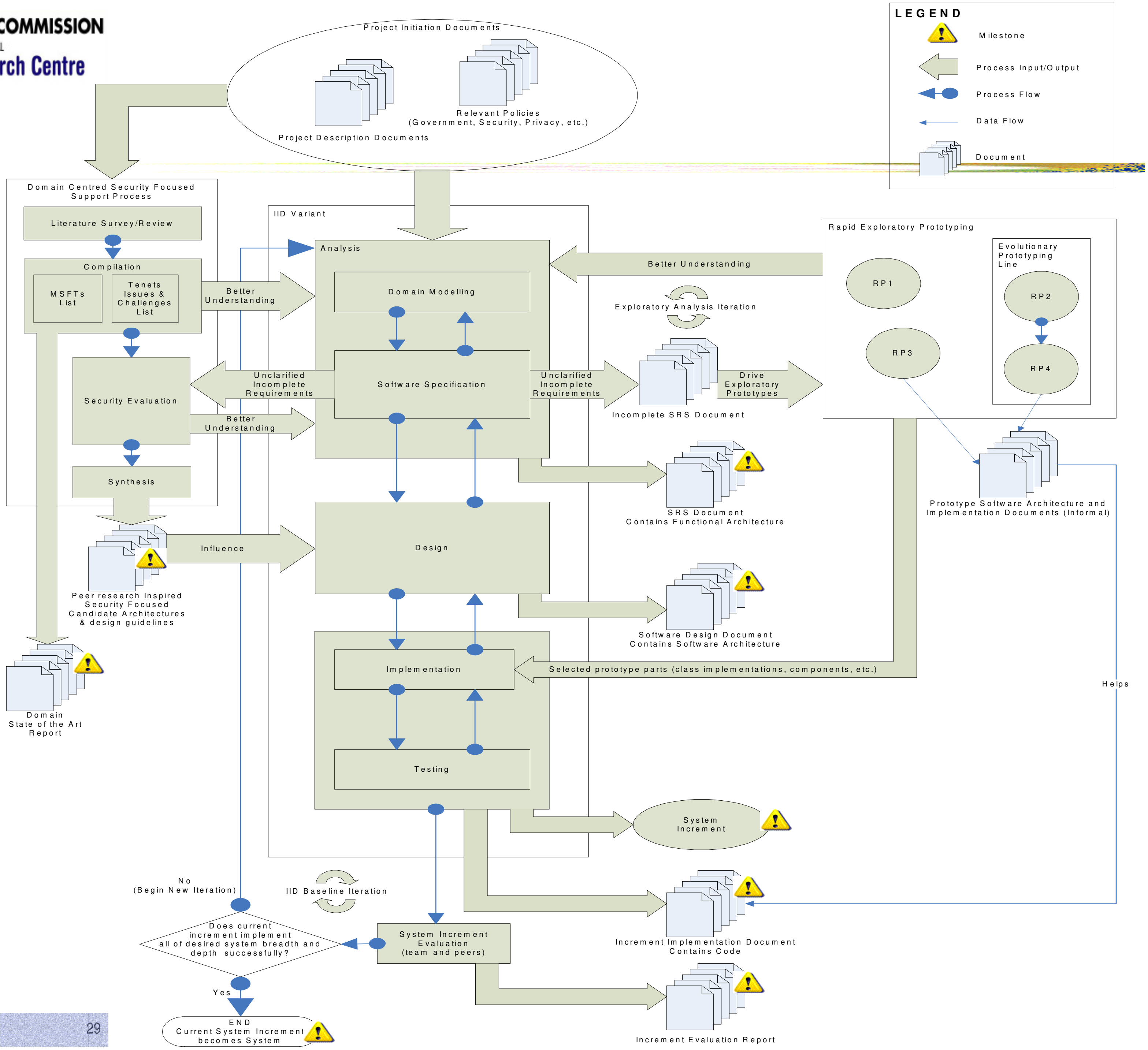
Traffic Lights Protocol



- An email metaphor is used for SecNet messaging in initial prototypes.
- Negotiation is currently envisioned as being done manually using traditional email replies. If negotiation results in both parties agreeing to a different TP value, the original message is resent as a new message with a different TLP value.
- However, if deemed necessary after testing of system's first increment, we could implement a GUI based TLP value negotiation process that uses special email messages transparently

ROSF Process

- ROSF is a process for “Research Oriented, Security Focused” software development that I have developed and actively updating and polishing while using it for SecNet-IE’s development.
- Software development as part of a research effort is usually subject to significantly different conditions than in the typical commercial environment. Such software is often only built as proof of concept for some novel approach to solving the involved problems. As such:
  - It is not constrained by deadlines or quality requirements that are as stringent
  - The need for a proven, systematic and effective approach to addressing an often fuzzy set of requirements is paramount.
  - Further, to secure peer interest and continued project funding as well as satisfy internal organization bureaucracy and management a series of working prototypes and accompanying documentation often need to be produced throughout the development lifecycle.
- Our group (SCNI) performs such research oriented software development with a special focus on the security aspects of it.
- The following slide depicts ROSF, a process for software development that satisfies the particularities of our work. The process is the product of the synthesis of two proven models for software development - the IID paradigm and especially the Unified Process and Rapid Prototyping - with a concurrently running support process for funnelling domain literature survey generated knowledge into the SDLC while utilizing a heuristic for the security evaluation of identified requirements and proposed designs.
- ROSF will be fully presented in an upcoming presentation/publication.



LEGEND
Milestone
Process Input/Output
Process Flow
Data Flow
Document

Project Initiation Documents
Project Description Documents
Relevant Policies
(Government, Security, Privacy, etc.)

Domain Centred Security Focused Support Process
Literature Survey/Review
Compilation
MSFTs List
Tenets Issues & Challenges List
Security Evaluation
Synthesis
Peer research Inspired Security Focused Candidate Architectures & design guidelines
Domain State of the Art Report

IID Variant
Analysis
Domain Modelling
Software Specification
Design
Implementation
Testing
Better Understanding
Unclarified Incomplete Requirements
Better Understanding
Influence

Exploratory Analysis Iteration
Unclarified Incomplete Requirements
Incomplete SRS Document
Drive Exploratory Prototypes
Better Understanding

Rapid Exploratory Prototyping
RP1
RP3
Evolutionary Prototyping Line
RP2
RP4
Prototype Software Architecture and Implementation Documents (Informal)

SRS Document
Contains Functional Architecture
Software Design Document
Contains Software Architecture
Selected prototype parts (class implementations, components, etc.)
Helps

System Increment
IID Baseline Iteration
System Increment Evaluation
(team and peers)
Increment Implementation Document
Contains Code
Increment Evaluation Report

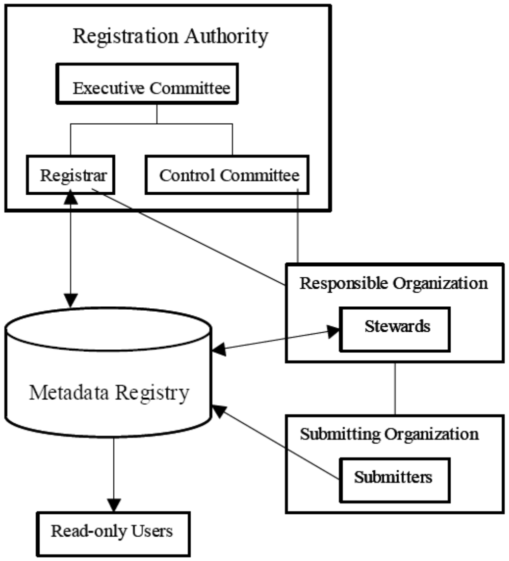
Does current increment implement all of desired system breadth and depth successfully?
No
(Begin New Iteration)
Yes
END
Current System Increment becomes System

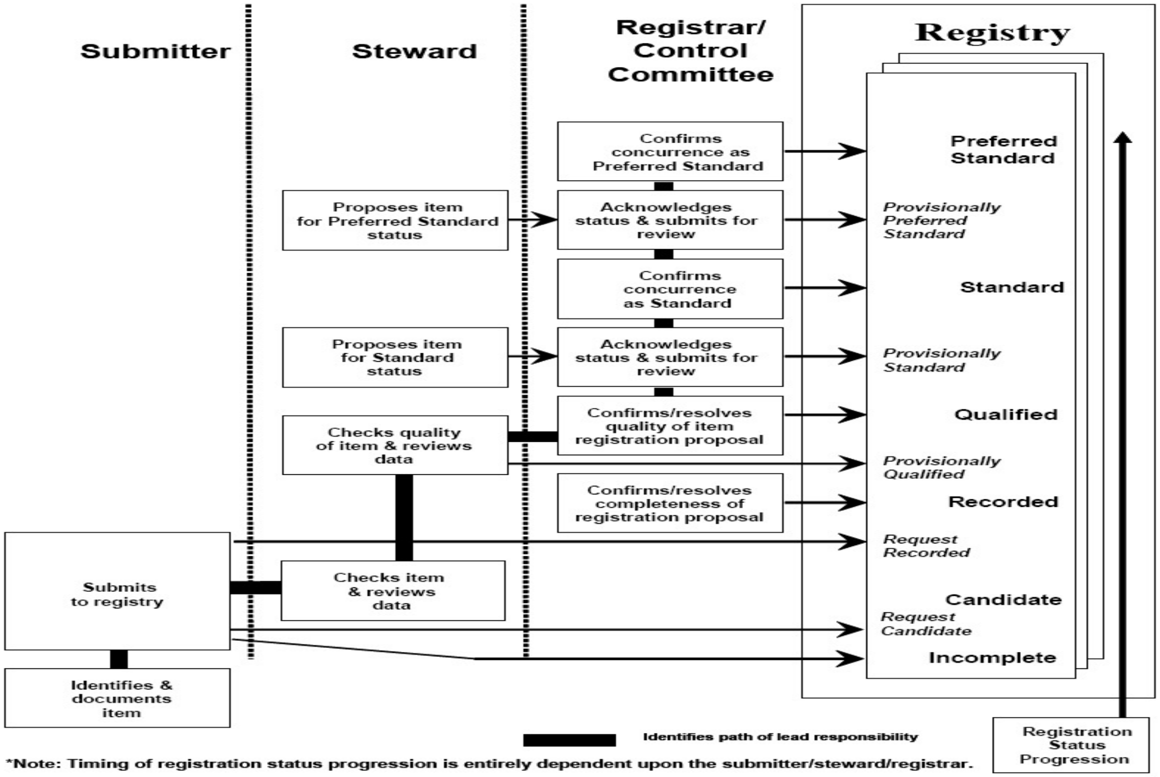
MDR

- ISO/IEC 11179 is one of the few mature standards for storing enterprise metadata in a controlled environment.
- An ISO metadata registry consists of a hierarchy of "concepts" with associated properties for each concept. Concepts are similar to classes in object-oriented programming but without the behavioral elements. Properties are similar to Class attributes. ISO standards require that each concept and property have a precisely worded data element definition.
- The use of metadata standards is strongly encouraged by organizations that exchange large amounts of data. Organizations such as the United Nations and the US Government are large users of 11179 standards.

MDR Registration

Structure & Process




Submitter
Steward
Registrar/ Control Committee
Registry
Confirms concurrence as Preferred Standard
Proposes item for Preferred Standard status
Acknowledges status & submits for review
Confirms concurrence as Standard
Proposes item for Standard status
Acknowledges status & submits for review
Checks quality of item & reviews data
Confirms/resolves quality of item registration proposal
Confirms/resolves completeness of registration proposal
Submits to registry
Checks item & reviews data
Identifies & documents item
Preferred Standard
Provisionally Preferred Standard
Standard
Provisionally Standard
Qualified
Provisionally Qualified
Recorded
Request Recorded
Candidate
Request Candidate
Incomplete
Registration Status Progression
Identifies path of lead responsibility

*Note: Timing of registration status progression is entirely dependent upon the submitter/steward/registrar.

FEA

- The Federal Enterprise Architecture (FEA) aims to provide a common set of references for information technology (IT) acquisition in the United States federal government
- It is designed to ease sharing of information and resources across federal agencies, reduce costs, and improve citizen services.
- The FEA is currently a collection of reference models that develop a common taxonomy and ontology for describing IT resources.
- The DRM (Data Reference Model) is of particular interest for Information Exchange. It enables agencies to describe the types of interaction and exchanges that occur between the Federal Government and citizens.
- A common data model will streamline information exchange processes within the Federal government and between government and external stakeholders.
- The DRM is the starting point from which data architects should develop modeling standards and concepts. The combined volumes of the DRM support data classification and enable horizontal and vertical information sharing.

FEA and MDR Implementation Examples

- FEA is already used in such frameworks and systems as:
  - NIEM (National Information Exchange Model)
    - Based on G-JXDM (Global Justice XML Data Model)
    - A joint DHS and DoJ venture
  - DoI (Department of Interior) Pilot system for FEA based NIE
- NIEM, besides FEA and ISO 11179 (MDR), also makes some use of Dublin Core's Abstract Model
- FEA and MDR are generic and abstract enough to be used to solve some of the SecNet-IE problems.

NIEM 1/2

- The National Information Exchange Model (NIEM) is designed to develop, disseminate, and support enterprise wide information sharing standards and processes across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise at all levels and across all branches of government.
- The result is more efficient and expansive information sharing between agencies and jurisdictions, more cost effective development and deployment of information systems, better quality decision making as a result of more timely, accurate, and complete information, and tangible improvements in public safety and homeland security.
- NIEM leverages the data exchange standards efforts successfully implemented by DOJ’s Global Justice Information Sharing Initiative (Global) and extends the Global Justice XML Data Model (Global JXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise.

NIEM 2/2

- Rather than nationwide integration of all local, state, tribal, and federal databases, NIEM focuses on cross-domain information exchanges between key domains and communities of interest (COIs), across all levels of government
- The fundamental building block of NIEM is the *data component*. Data components are the basic business data elements that represent real-world objects and concepts.
- Some sources of data components include data models, databases, data dictionaries, schemas, and exchanges. In NIEM, these objects and constructs are represented using XML Schema for the purpose of consistent definition and transmission of information exchange packages (IEPs). The model, however, is independent of any particular technology and in the future could be depicted in any number of representations (e.g., Resource Definition Framework (RDF) or Web Ontology Language (OWL)),

NIEM Domains & COIs

- In NIEM, each domain traditionally includes a cohesive group of data stewards who are subject matter experts (SMEs), have some level of authority within the domains they represent, and participate in the processes related to harmonizing conflicts and resolving data component ambiguities.
- Domains are expected to:
  - Provide content to NIEM;
  - Provide domain subject matter expertise to support content development;
  - **Have existing COIs or the ability to enroll or formulate COIs;**
  - Possess the ability to perform outreach to relevant COIs;
  - Agree to the principles and practices of NIEM (including conformance to NIEM Naming and Design Rules
  - Maintain alignment with the NIEM taxonomy
- Communities of interest (COIs) are collaborative groups of users who exchange information in pursuit of shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they exchange.
- Generally, COIs are formally constituted through an organizational charter, a memorandum of understanding (MOU), articles of incorporation
- COIs reuse data components and artifacts found in NIEM to document their information exchanges.

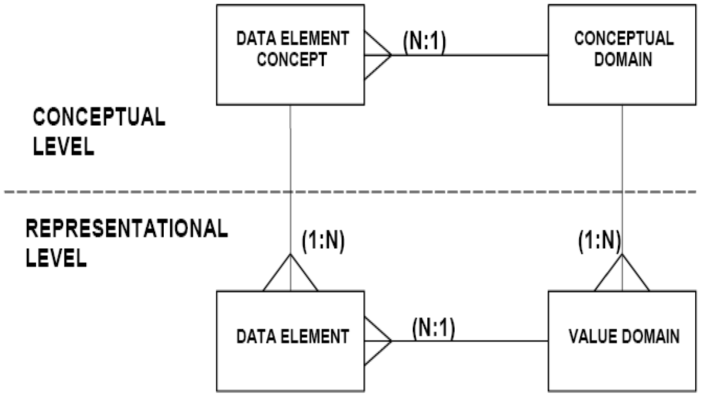
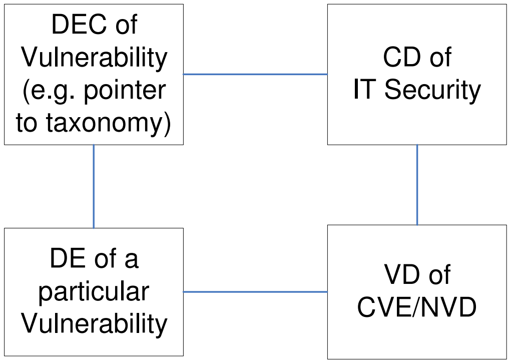


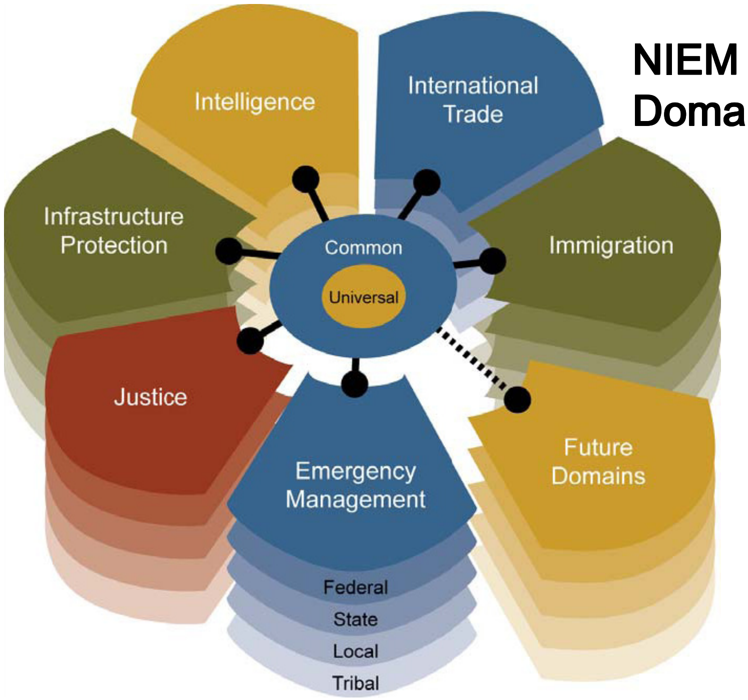
Figure 4 — Overview Model for ISO/IEC 11179 Metadata Registry

For Example in SecNet-IE

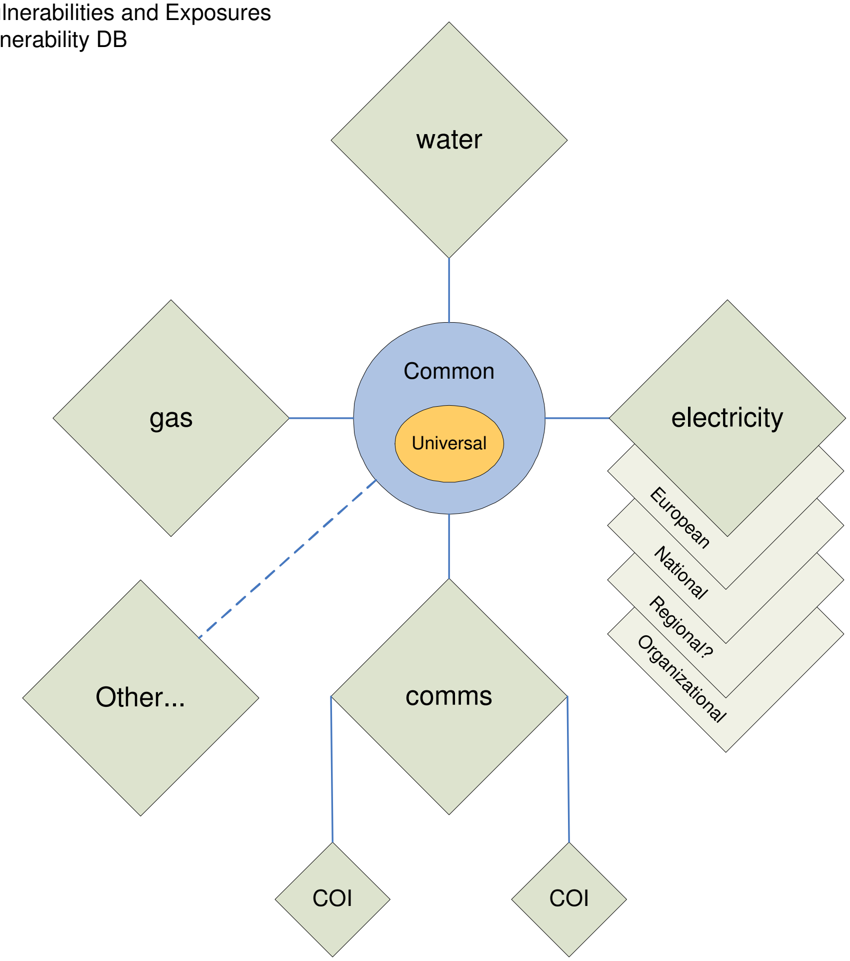

DEC of Vulnerability (e.g. pointer to taxonomy)
CD of IT Security
DE of a particular Vulnerability
VD of CVE/NVD

CVE = Common Vulnerabilities and Exposures
NVD = National Vulnerability DB

NIEM Domains



For Example in SecNet-IE



Note: Common and Universal refer to metadata artifacts that are Common and Universal among some and all domains respectively

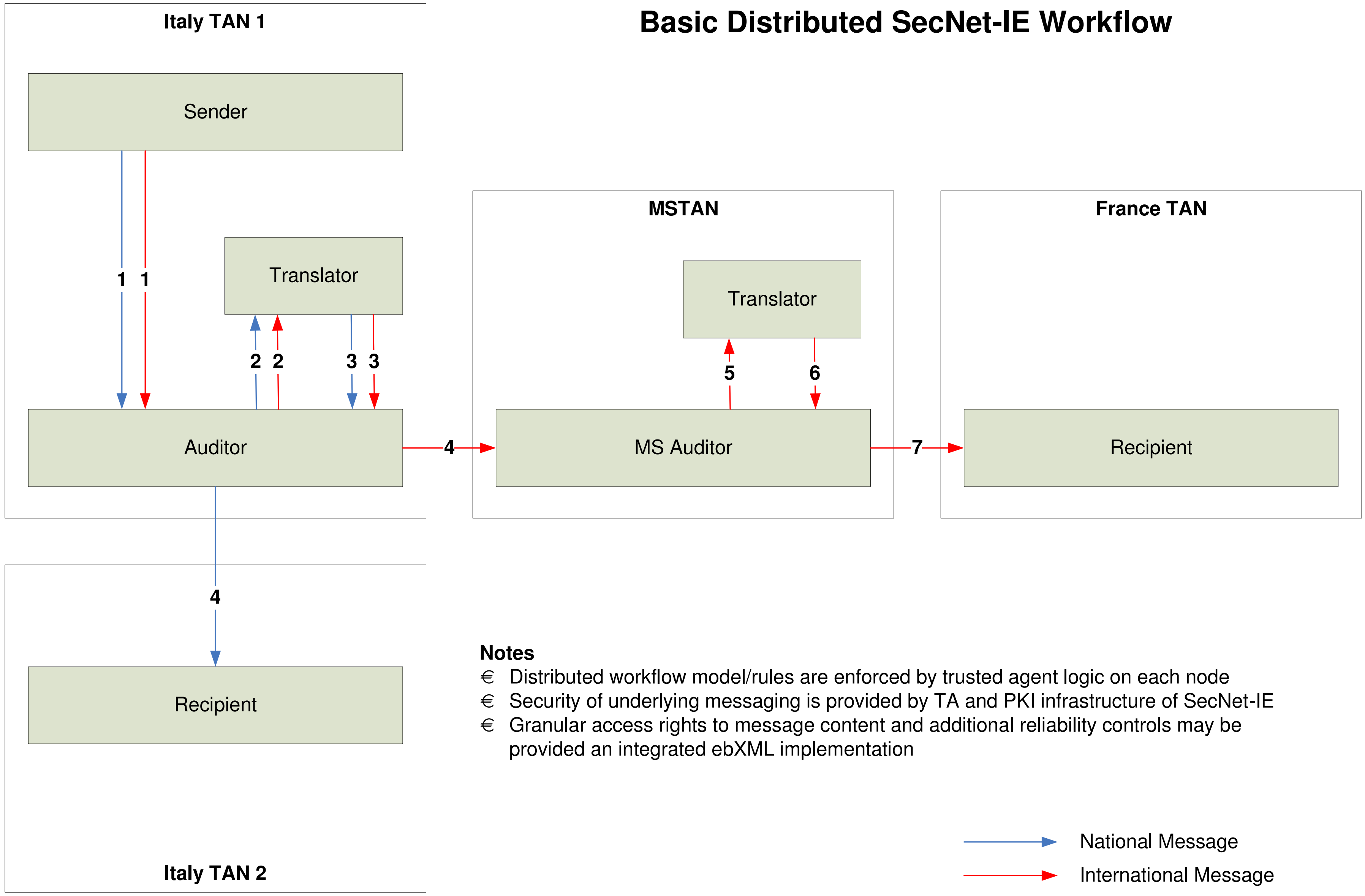
ebXML – The EDI successor

- Focuses on defining a communications-protocol neutral method for exchanging electronic business messages.
- It defines specific enveloping constructs supporting reliable, secure delivery of business information.
- The specification defines a flexible enveloping technique, permitting messages to contain payloads of any format type.
- It’s XML security characteristics make it a great platform for document based workflow.
- ebXML RIM (Registry Information Model) defines an ebXML meta-model

ebXML Security Properties

- **Persistent Digital Signature (XMLDSIG)**
  - Persistent because parts of an xml doc can be selectively signed, thus permitting the xml doc to be changed without the signature being invalidated
- **Persistent Signed Receipt**
- **Non-persistent Authentication**
  - Non-persistent auth and integrity may be implemented at the communication protocol layer (e.g. TLS – Transport Layer Security)
- **Non-persistent Integrity**
- **Persistent Confidentiality (XML encryption std not yet fully specified)**
  - Persistent confidentiality is basically persistent encryption
- **Non-persistent Confidentiality (e.g. TLS based)**
- **Persistent Authorization (SAML)**
- **Non-persistent Authorization (e.g. TLS based)**
- **Trusted Timestamp (under development)**
- **Reliable Messaging Module**
  - ack, retry and duplicate detection and elimination, resulting in the *To Party* receiving the message Once-And-Only-Once
- **Persistent Storage and System Failure recovery**
  - Persistent storage is technology agnostic but places certain requirements on what is kept in persistent storage or is recoverable in case of system failure

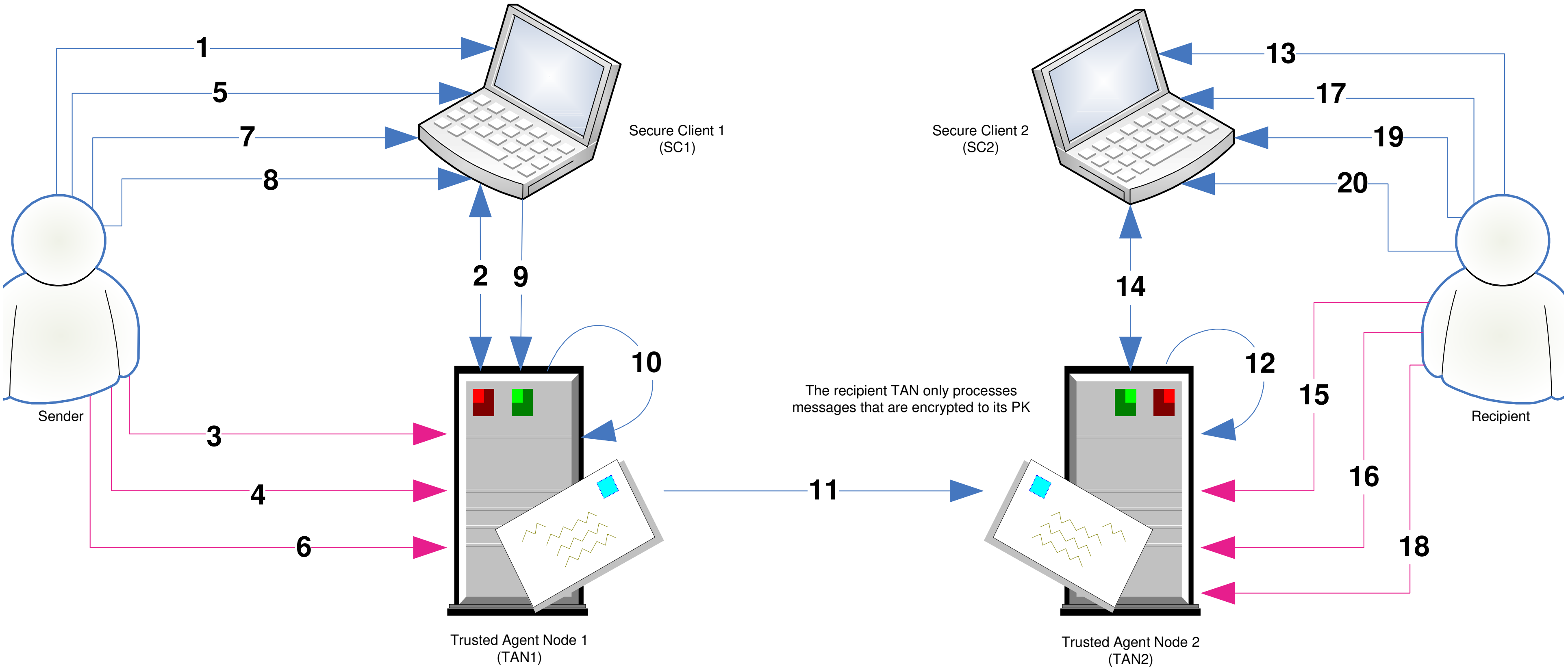
Basic Distributed SecNet-IE Workflow



Notes

- Distributed workflow model/rules are enforced by trusted agent logic on each node
- Security of underlying messaging is provided by TA and PKI infrastructure of SecNet-IE
- Granular access rights to message content and additional reliability controls may be provided an integrated ebXML implementation

User perspective of SecNet-IE messaging



Direct Interaction

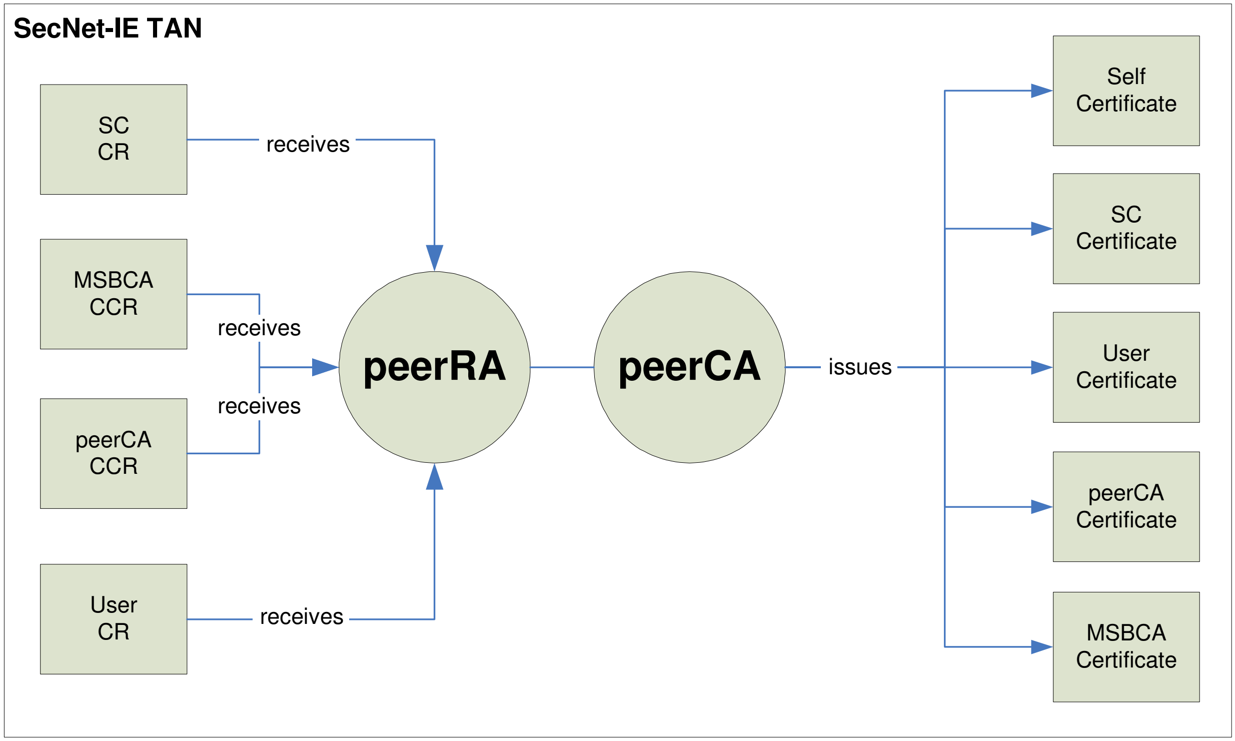
Virtual Interaction

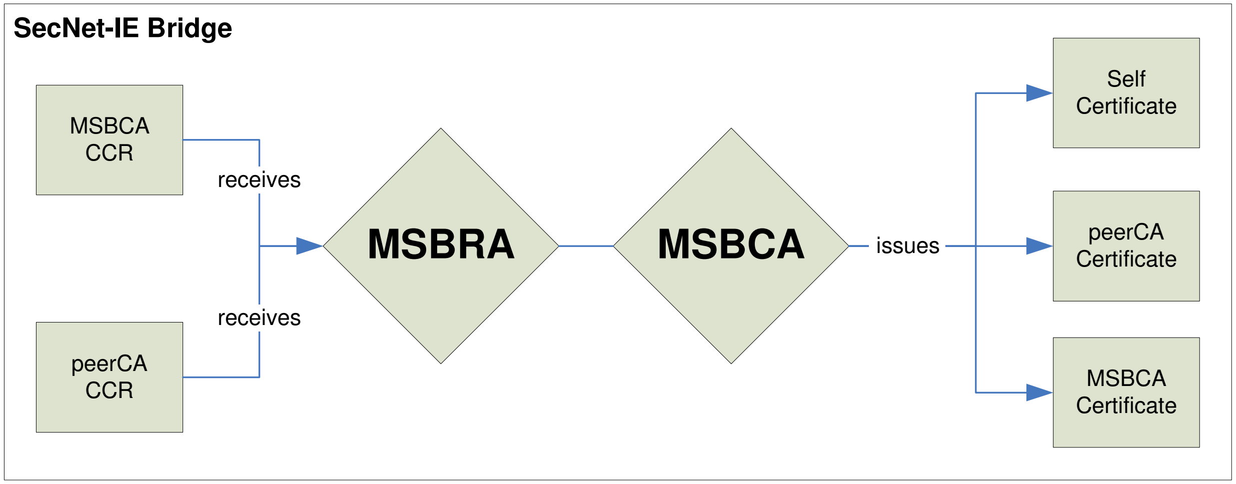
Note: It may be deemed desirable to provide trusted yet fully anonymous messaging capability in order to deal with situations where a company may avoid reporting an incident and related security info fearing market repercussions. SecNet's P2P network architecture provides a good platform for the use of a variety of anonymizing techniques like those used in mixmaster, cypherpunk and nym anon remailers.

Interactions

1. Sender authenticates to SC1 (Multi-factor authentication: Smart card containing user SK and a biometric registered during user-SC coupling)
2. SC1 and TAN1 perform mutual authentication (i.e. SC1 holds TAN1's cert and TAN1 holds SC1's cert – they challenge each other)
3. Sender authenticates to TAN1 (i.e. TAN issues challenge to Sender's cert that it holds and it has actually created)
4. Sender performs a distributed LDAP lookup and receives the trusted certificate of intended recipient
5. Sender composes a free text message
6. Sender performs distributed MDR lookups for dynamic metadata
7. Sender attaches to the message the chosen metadata, a TLP value and, optionally, a request for translation and binary attachments
8. Sender signs the message with his/her SK and encrypts it to TAN1's PK
9. SC1 sends the packaged message to TAN1 over the secure connection (e.g. TLS)
10. TAN1 unencrypts the message, verifies its signature, checks it for structural integrity, enforces TLP and other distributed workflow (e.g. auditing) and then encrypts the signed message to the recipient's trusted PK, signs it with its own SK and finally encrypts it to TAN2's trusted PK
11. TAN1 sends the message package to TAN2 over a secure connecton (e.g. TLS)
12. TAN2 receives the message package, decrypts it, checks the signature and verifies the sending node, and delivers the message, still encrypted to the recipient's PK, to his/her messagebox
13. Recipient authenticates to SC2
14. SC2 and TAN2 perform mutual authentication
15. Recipient authenticates to TAN2
16. Recipient accesses messagebox and downloads message
17. Recipient decrypts message using his/her SK
18. Recipient performs an LDAP lookup and receives sender's trusted certificate
19. Recipient verifies Sender's signature
20. Recipient reads the message, and understands it helped by attached metadata and a possible translation to his/her language

Note: Used certificates are trusted because their issuing CA is certified by either the local TAN's CA or by the TAN's MSBCA. This trust-path check is done by an implicit call not shown here.





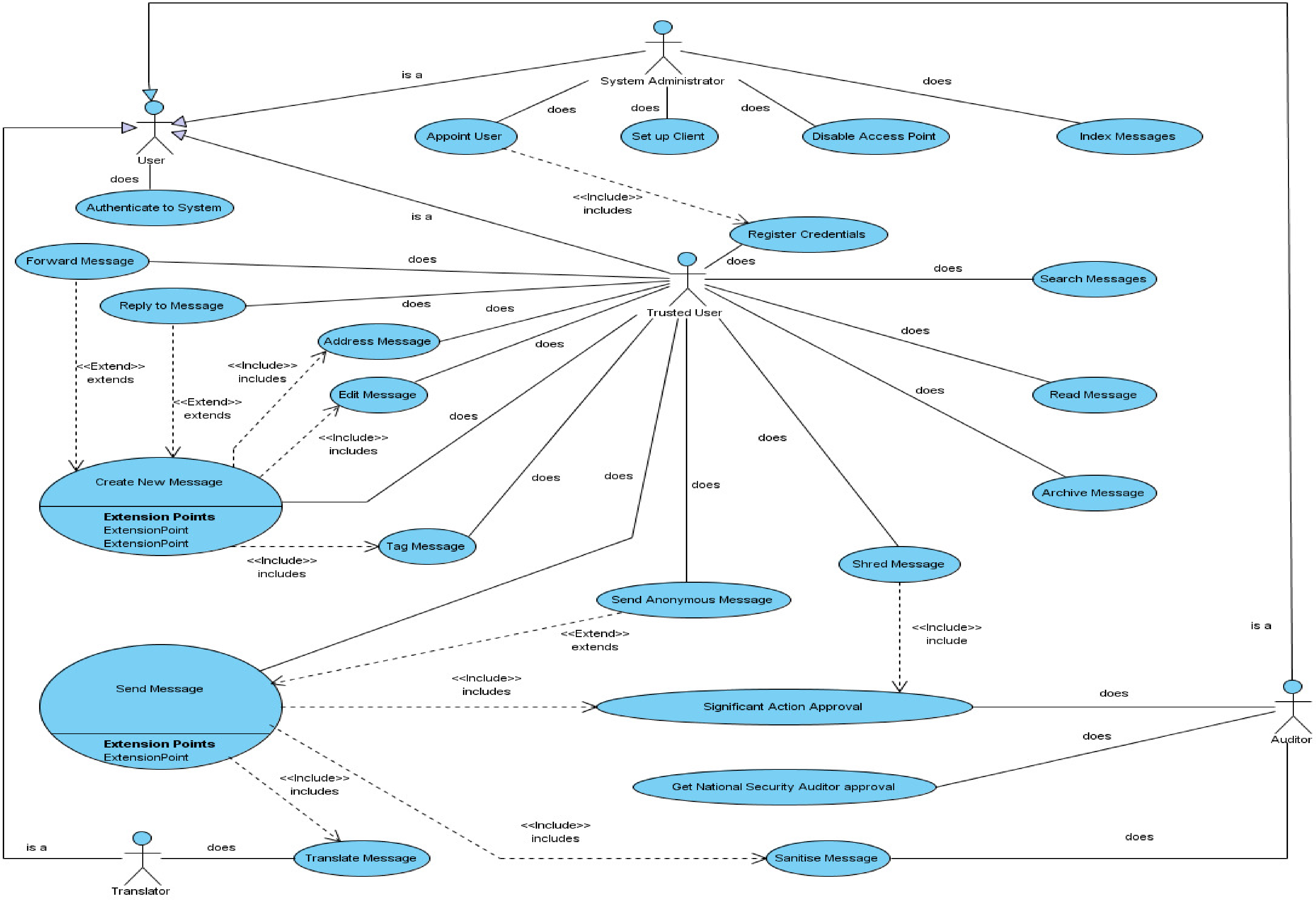
TAN = Trusted Agent Node

CCR = Cross Certification Request

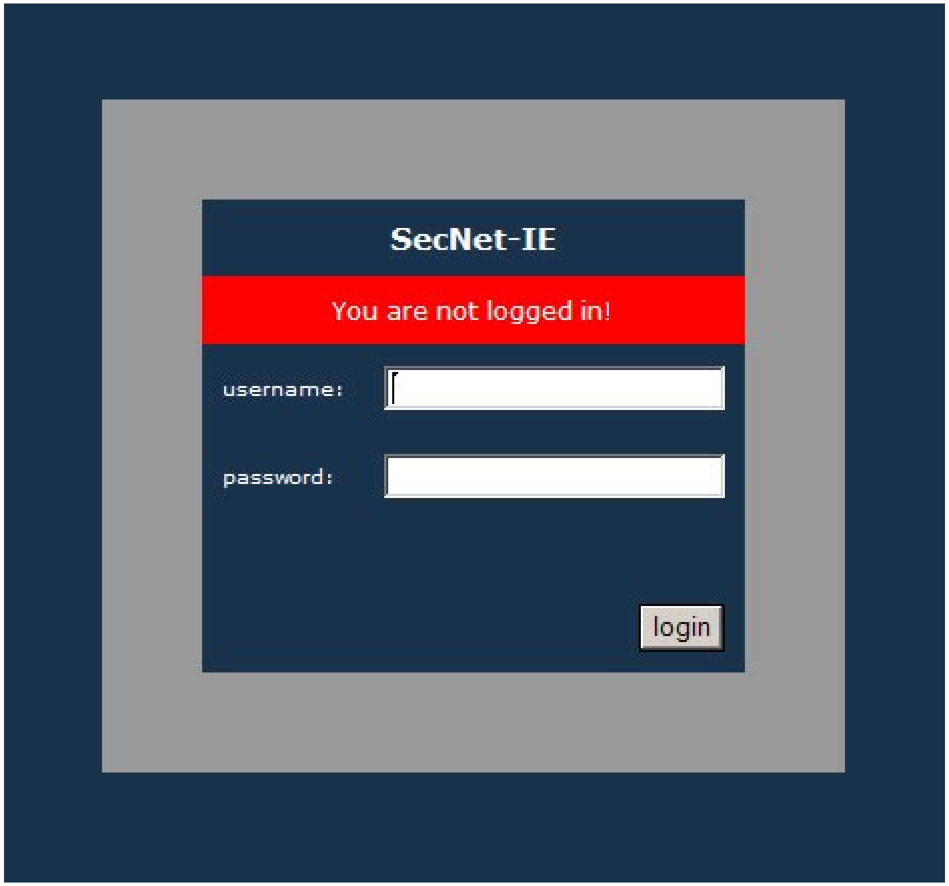
SC = Secure Client

CR = Certification Request

Name	**Analysis - Domain Modelling - Use Case Model**
Project	**SecNet-IE**

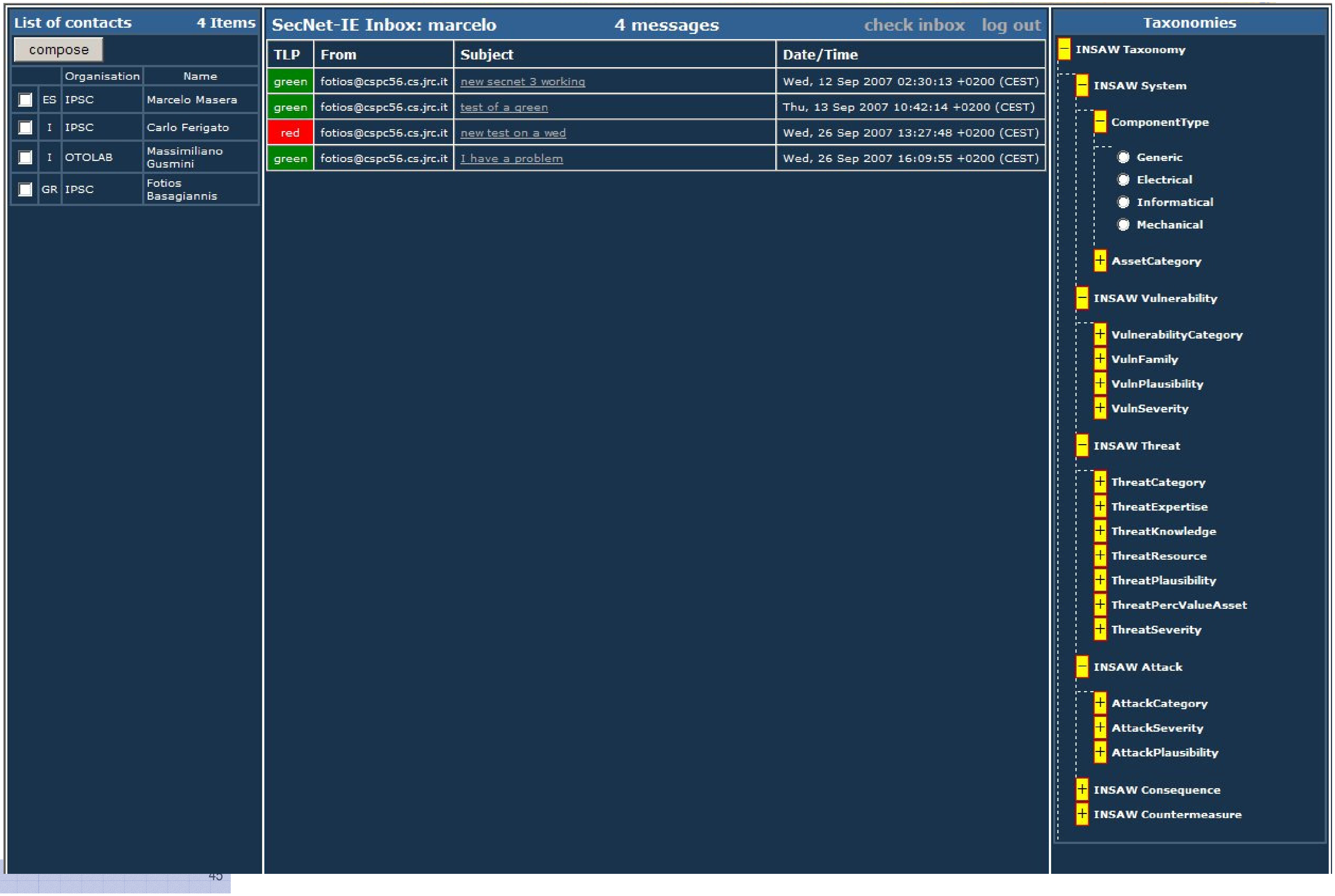


SecNet-IE Prototype 3: Login



You are not logged in!

SecNet-IE Prototype 3: Inbox



List of contacts 4 Items

compose

		Organisation	Name
□	ES	IPSC	Marcelo Masera
□	I	IPSC	Carlo Ferigato
□	I	OTOLAB	Massimiliano Gusmini
□	GR	IPSC	Fotios Basagiannis

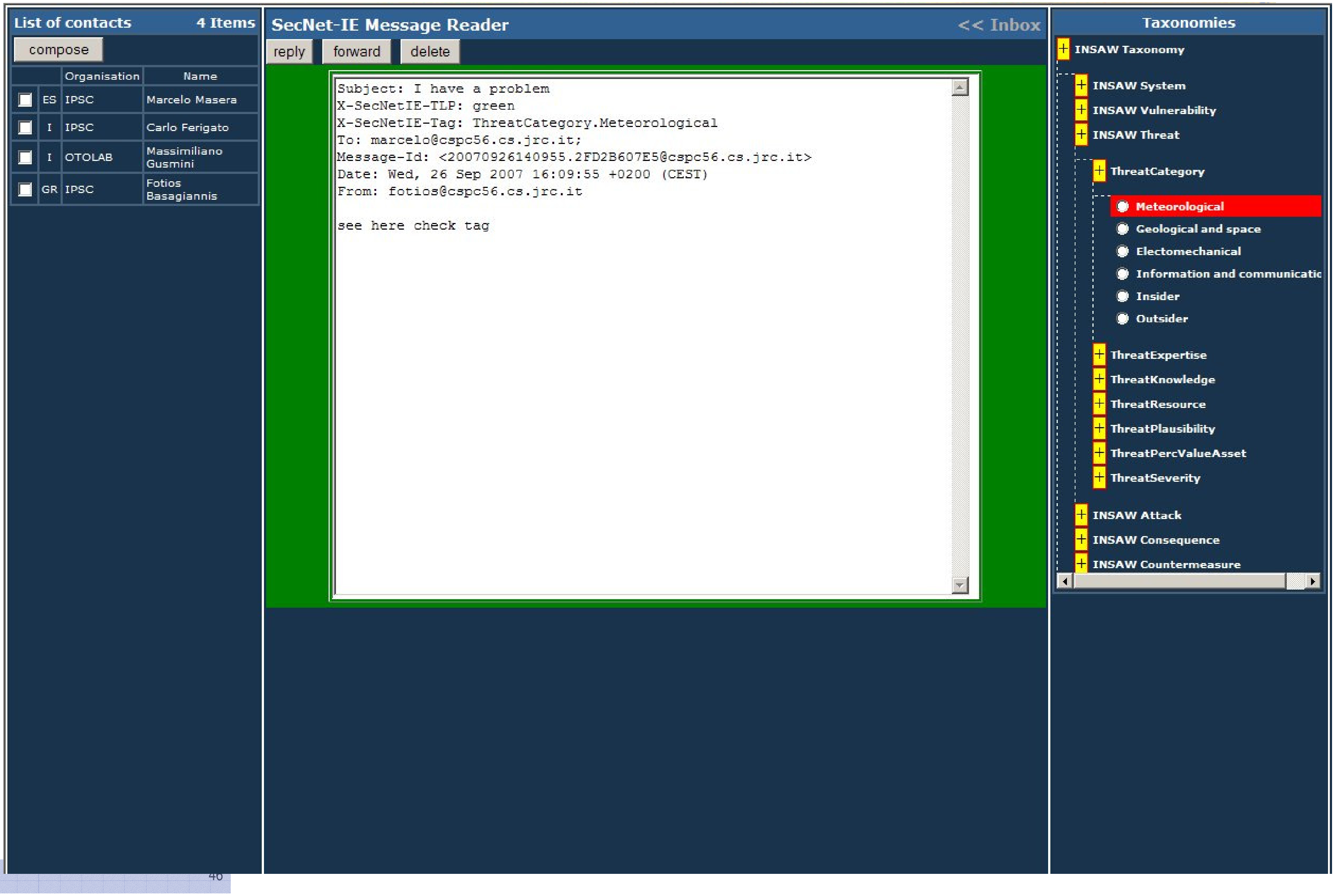
SecNet-IE Inbox: marcelo 4 messages check inbox log out

TLP	From	Subject	Date/Time
green	fotios@cspc56.cs.jrc.it	new secnet 3 working	Wed, 12 Sep 2007 02:30:13 +0200 (CEST)
green	fotios@cspc56.cs.jrc.it	test of a green	Thu, 13 Sep 2007 10:42:14 +0200 (CEST)
red	fotios@cspc56.cs.jrc.it	new test on a wed	Wed, 26 Sep 2007 13:27:48 +0200 (CEST)
green	fotios@cspc56.cs.jrc.it	I have a problem	Wed, 26 Sep 2007 16:09:55 +0200 (CEST)

Taxonomies

- − INSAW Taxonomy
  - − INSAW System
    - − ComponentType
      - ○ Generic
      - ○ Electrical
      - ○ Informatical
      - ○ Mechanical
    - + AssetCategory
  - − INSAW Vulnerability
    - + VulnerabilityCategory
    - + VulnFamily
    - + VulnPlausibility
    - + VulnSeverity
  - − INSAW Threat
    - + ThreatCategory
    - + ThreatExpertise
    - + ThreatKnowledge
    - + ThreatResource
    - + ThreatPlausibility
    - + ThreatPercValueAsset
    - + ThreatSeverity
  - − INSAW Attack
    - + AttackCategory
    - + AttackSeverity
    - + AttackPlausibility
  - + INSAW Consequence
  - + INSAW Countermeasure

SecNet-IE Prototype 3: View message



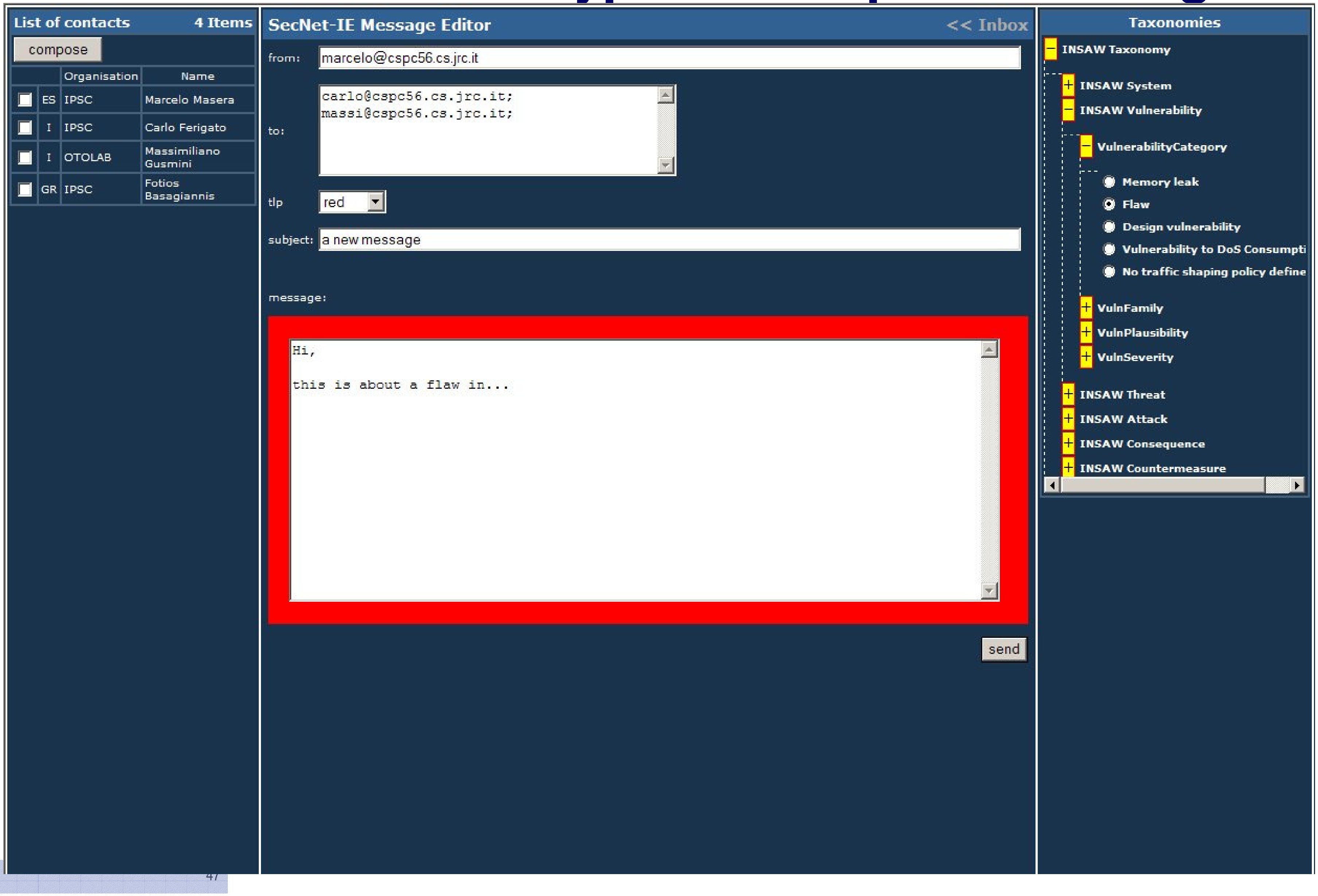
		Organisation	Name
□	ES	IPSC	Marcelo Masera
□	I	IPSC	Carlo Ferigato
□	I	OTOLAB	Massimiliano Gusmini
□	GR	IPSC	Fotios Basagiannis

```
Subject: I have a problem
X-SecNetIE-TLP: green
X-SecNetIE-Tag: ThreatCategory.Meteorological
To: marcelo@cspc56.cs.jrc.it;
Message-Id: <20070926140955.2FD2B607E5@cspc56.cs.jrc.it>
Date: Wed, 26 Sep 2007 16:09:55 +0200 (CEST)
From: fotios@cspc56.cs.jrc.it

see here check tag
```

- + INSAW Taxonomy
  - + INSAW System
  - + INSAW Vulnerability
  - + INSAW Threat
    - + ThreatCategory
      - ● Meteorological
      - ○ Geological and space
      - ○ Electomechanical
      - ○ Information and communicatic
      - ○ Insider
      - ○ Outsider
    - + ThreatExpertise
    - + ThreatKnowledge
    - + ThreatResource
    - + ThreatPlausibility
    - + ThreatPercValueAsset
    - + ThreatSeverity
  - + INSAW Attack
  - + INSAW Consequence
  - + INSAW Countermeasure

SecNet-IE Prototype 3: Compose message



List of contacts 4 Items

compose

		Organisation	Name
□	ES	IPSC	Marcelo Masera
□	I	IPSC	Carlo Ferigato
□	I	OTOLAB	Massimiliano Gusmini
□	GR	IPSC	Fotios Basagiannis

SecNet-IE Message Editor << Inbox

from: marcelo@cspc56.cs.jrc.it

to: carlo@cspc56.cs.jrc.it; massi@cspc56.cs.jrc.it;

tlp: red

subject: a new message

message:

Hi,

this is about a flaw in...

send

Taxonomies

- INSAW Taxonomy
  - INSAW System
  - INSAW Vulnerability
    - VulnerabilityCategory
      - ○ Memory leak
      - ● Flaw
      - ○ Design vulnerability
      - ○ Vulnerability to DoS Consumpti
      - ○ No traffic shaping policy define
    - VulnFamily
    - VulnPlausibility
    - VulnSeverity
  - INSAW Threat
  - INSAW Attack
  - INSAW Consequence
  - INSAW Countermeasure

P2P & DHT 1/2

- The P2P overlay network consists of all the participating peers as network nodes. There are links between any two nodes that know each other: i.e. if a participating peer knows the location of another peer in the P2P network, then there is a directed edge from the former node to the latter in the overlay network. Based on how the nodes in the overlay network are linked to each other, we can classify the P2P networks as unstructured or structured.

- An unstructured P2P network is formed when the overlay links are established arbitrarily. Such networks can be easily constructed as a new peer that wants to join the network can copy existing links of another node and then form its own links over time. In an unstructured P2P network, if a peer wants to find a desired piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. The main disadvantage with such networks is that the queries may not always be resolved. Popular content is likely to be available at several peers and any peer searching for it is likely to find the same thing. But if a peer is looking for rare data shared by only a few other peers, then it is highly unlikely that search will be successful. Since there is no correlation between a peer and the content managed by it, there is no guarantee that flooding will find a peer that has the desired data. Flooding also causes a high amount of signaling traffic in the network and hence such networks typically have very poor search efficiency. Most of the popular P2P networks such as Gnutella and FastTrack are unstructured.

- Structured P2P network employ a globally consistent protocol to ensure that any node can efficiently route a search to some peer that has the desired file, even if the file is extremely rare. Such a guarantee necessitates a more structured pattern of overlay links. By far the most common type of structured P2P network is the distributed hash table (DHT), in which a variant of consistent hashing is used to assign ownership of each file to a particular peer, in a way analogous to a traditional hash table's assignment of each key to a particular array slot. Some well known DHTs are Chord, Pastry, Tapestry, CAN, and Tulip. Not a DHT-approach but a structured P2P network is HyperCuP.

- Distributed Hash Table (DHT) networks has been widely utilized for accomplishing efficient resource discovery for Grid computing systems, as it aids in resource management and scheduling of applications. Resource discovery activity involve searching for the appropriate resource types that match the user’s application requirements. Recent advances in the domain of decentralized resource discovery have been based on extending the existing DHTs with the capability of multi-dimensional data organization and query routing. Majority of the efforts have looked at embedding spatial database indices such as the Space Filling Curves (SFCs) including the Hilbert curves, Z-curves, k-d tree, MX-CIF Quad tree and R*-tree for managing, routing, and indexing of complex Grid resource query objects over DHT networks. Spatial indices are well suited for handling the complexity of Grid resource queries. Although some spatial indices can have issues as regards to routing load-balance in case of a skewed data set, all the spatial indices are more scalable in terms of the number of hops traversed and messages generated while searching and routing Grid resource queries.

P2P & DHT 2/2

- Distributed hash tables (DHTs) are a class of decentralized distributed systems that provide a lookup service similar to a hash table: (name, value) pairs are stored in the DHT, and any participating node can efficiently retrieve the value associated with a given name. Responsibility for maintaining the mapping from names to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows DHTs to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

- DHTs form an infrastructure that can be used to build more complex services, such as distributed file systems, peer-to-peer file sharing and content distribution systems, cooperative web caching, multicast, anycast, domain name services, and instant messaging. Notable distributed networks that use DHTs include BitTorrent (with extensions), eDonkey network, YaCy, and the Coral Content Distribution Network.

- DHTs characteristically emphasize the following properties:
  - Decentralization: the nodes collectively form the system without any central coordination.
  - Scalability: the system should function efficiently even with thousands or millions of nodes.
  - Fault tolerance: the system should be reliable (in some sense) even with nodes continuously joining, leaving, and failing.

- A key technique used to achieve these goals is that any one node needs to coordinate with only a few other nodes in the system – most commonly, Θ(logn) of the n participants (see below) – so that only a limited amount of work needs to be done for each change in membership.

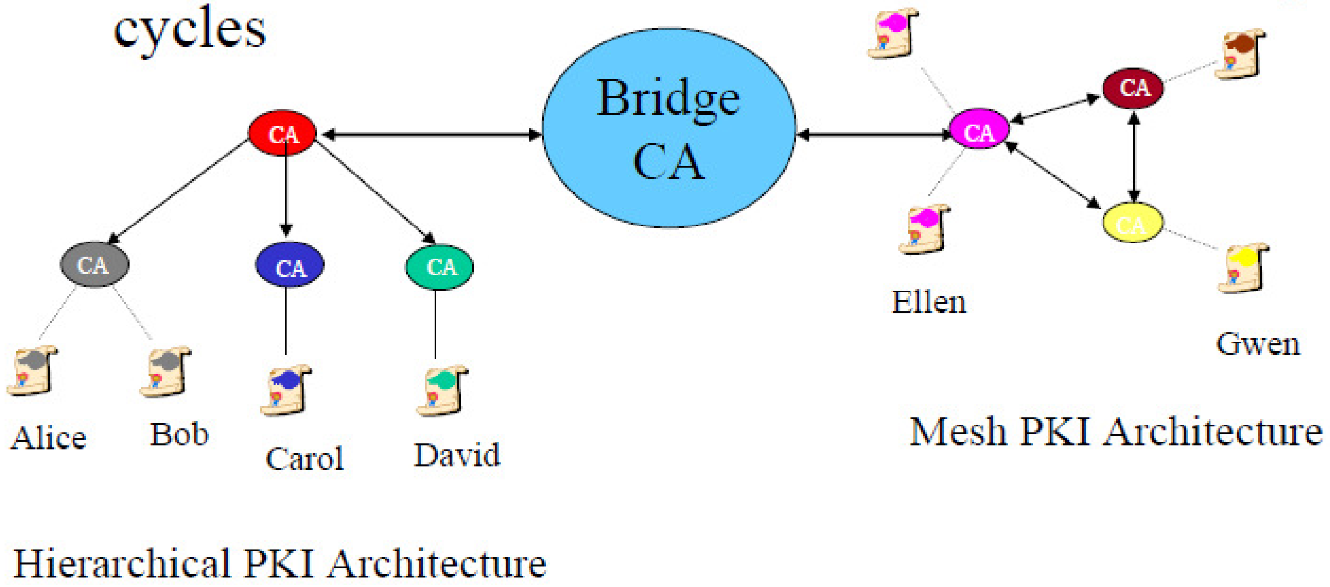
- The structure of a DHT can be decomposed into several main components.[2][3] The foundation is an abstract keyspace, such as the set of 160-bit strings (actually, number of bits is a parameter of DHT and could vary). A keyspace partitioning scheme splits ownership of this keyspace among the participating nodes. An overlay network then connects the nodes, allowing them to find the owner of any given key in the keyspace.

- Once these components are in place, a typical use of the DHT for storage and retrieval might proceed as follows. Suppose the keyspace is the set of 160-bit strings. To store a file with given filename and data in the DHT, the SHA1 hash of filename is found, producing a 160-bit key k, and a message put(k,data) is sent to any node participating in the DHT. The message is forwarded from node to node through the overlay network until it reaches the single node responsible for key k as specified by the keyspace partitioning, where the pair (k,data) is stored. Any other client can then retrieve the contents of the file by again hashing filename to produce k and asking any DHT node to find the data associated with k with a message get(k). The message will again be routed through the overlay to the node responsible for k, which will reply with the stored data.

- The keyspace partitioning and overlay network components are described below with the goal of capturing the principal ideas common to most DHTs; many designs differ in the details.

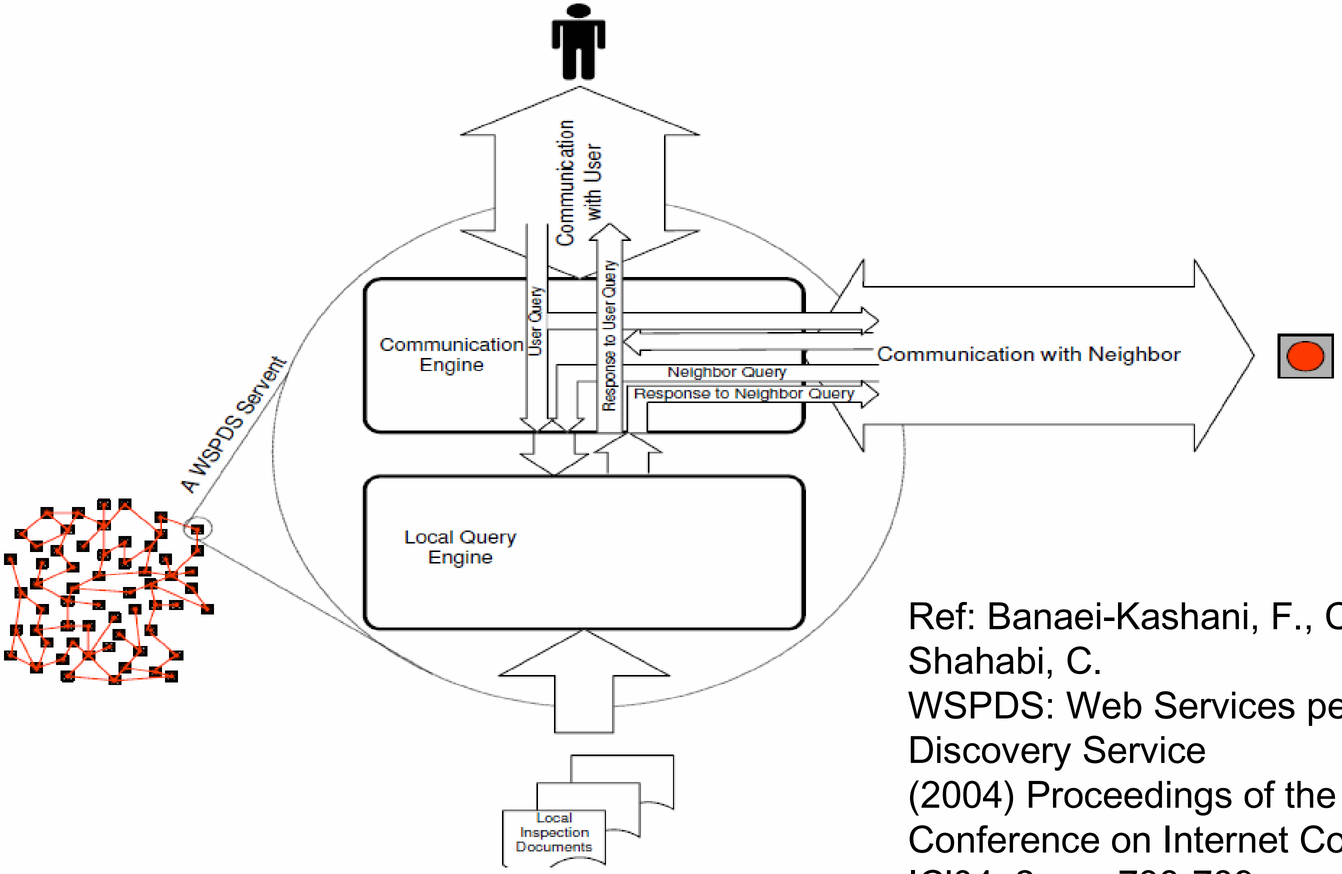
PKI Architectures

- There may be dead-ends and cycles



Unlike a mesh PKI CA, the BCA does not issue certificates directly to users. In addition, the BCA is not intended to be used as a trust point by the users of the PKI, unlike the “root” CA in a hierarchy. The BCA establishes peer-to-peer trust relationships with the different user communities, which elevates political issues between organizations and allows the users to keep their natural trust points. These relationships are combined to form a “bridge of trust” enabling users from the different user communities to interact with each other through the BCA with a specified level of trust (Ref: NIST)

P2P Web Service 1/2

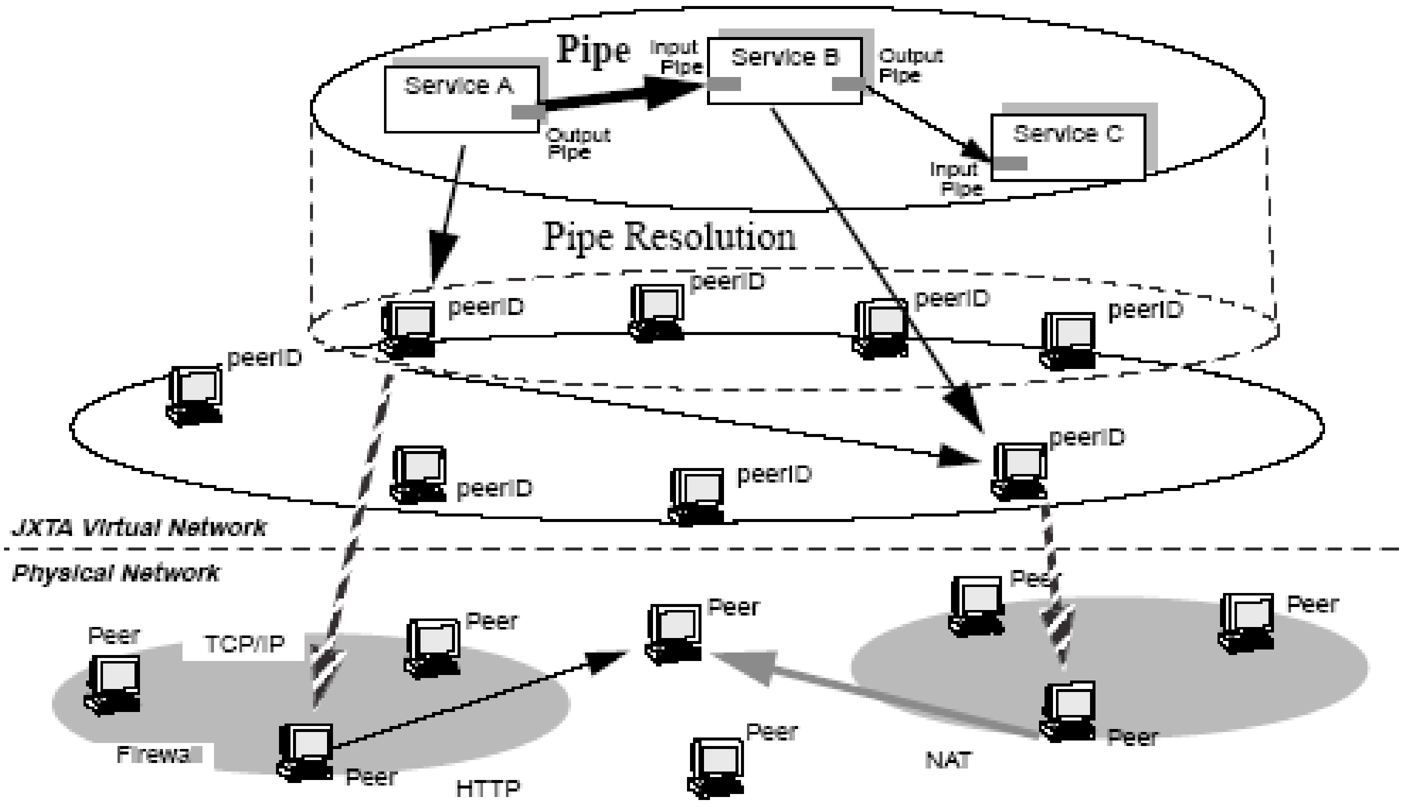


Ref: Banaei-Kashani, F., Chen, C.-C., Shahabi, C.
WSPDS: Web Services peer-to-peer Discovery Service
(2004) Proceedings of the International Conference on Internet Computing, IC'04, 2, pp. 733-739.

Fig. 1. WSPDS Architecture

P2P Web Service 2/2

Could be JXTA based. Ref: sun.com


Pipe
Service A
Input Pipe
Service B
Output Pipe
Output Pipe
Service C
Input Pipe
Pipe Resolution
peerID
peerID
peerID
peerID
peerID
peerID
peerID
peerID
JXTA Virtual Network
Physical Network
Peer
TCP/IP
Peer
Peer
Peer
Peer
Firewall
Peer
HTTP
Peer
NAT
Peer