FFI Forsvarets forskningsinstitutt

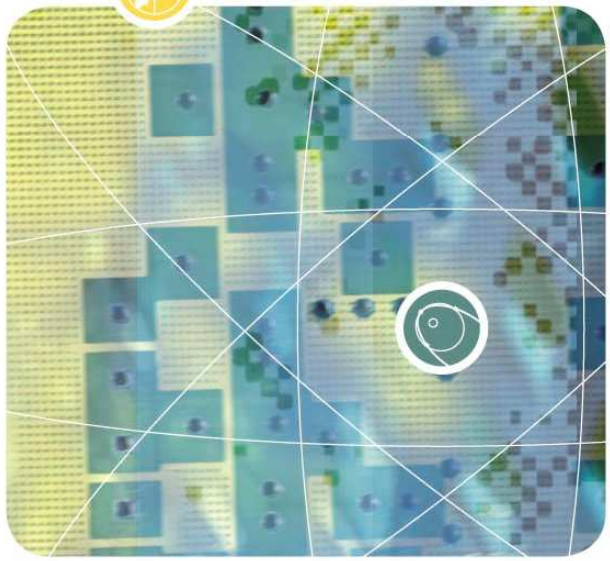
Architecture Patterns for a Ubiquitious Identity Management System

NISNET Finse School 2011

Anders Fongen, PhD

Norwegian Defence Research Establishment

May 2011



Identity Management (IdM)

- Identity:
  - Set of properties associated with an *Entity*
- Identifier:
  - Subset of properties to *distinguish* identities
- Identity Statement:
  - Attestation of the subject's identifier
- Identity Provider (IdP)
  - Service which issues identity statements
- Identification
  - Establishment of identity

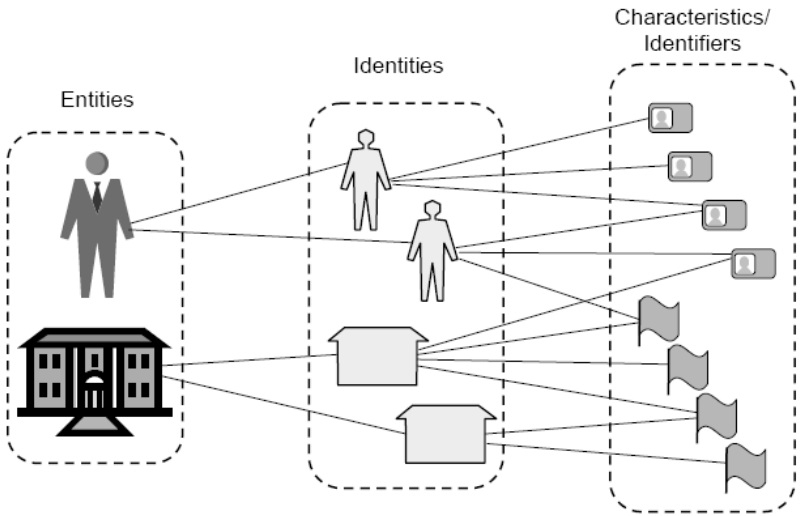


Figure 1: Correspondence between entities, identities and characteristics/identifiers.

IdMs are suffering from:

- Discarding existing investments
  - need separate user registries
- High coupling between domains
  - guest users individually registered
  - autonomy delegated for federation
- Visibility of user identities
  - access given to identities, not roles
- Driven by security excellence, not networking excellence
  - protocols too costly for ”narrow and bumpy” networks

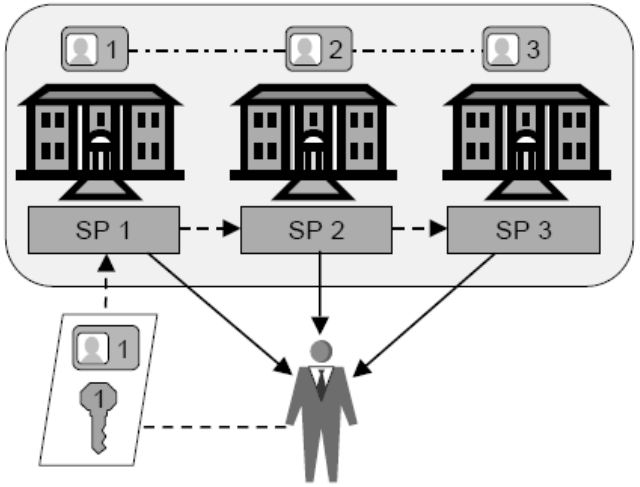


Figure 3: Federated user identity model.

IdM systems should

- Protect investments and knowledge
  - Employ existing enrollment procedures and data storage
- Allow federation for ”guest access”
  - Should not need to enroll guests
- Give access rights to *roles*, not identities
  - RBAC, ABAC
- Protect domain autonomy
  - owner of service decides the access control
- Allow system latency
  - trust has a lifetime
- Limit the trust relationships
  - minimize the ”trust anchors”
- Balance requirements between security and network economy

Cross Domain Identity Management

- Inside each domain:
  - User key/certificate management
  - User roles/privileges management
- Between domains:
  - Trust in others' authentication process
  - Trust in integrity of user attributes
  - No management of foreign users
- Role based authorization process
  - since identity of guests are ”unmanaged” in host domain

Tactical networks – ubiquitous computing

- Mobile, wireless, based on military radio technology
  - spread spectrum, strong encryption
- Low bandwidth (< 100 kb/s, depending on range)
- Multi-hop, Ad-hoc
  - latency
  - packet loss
  - link loss

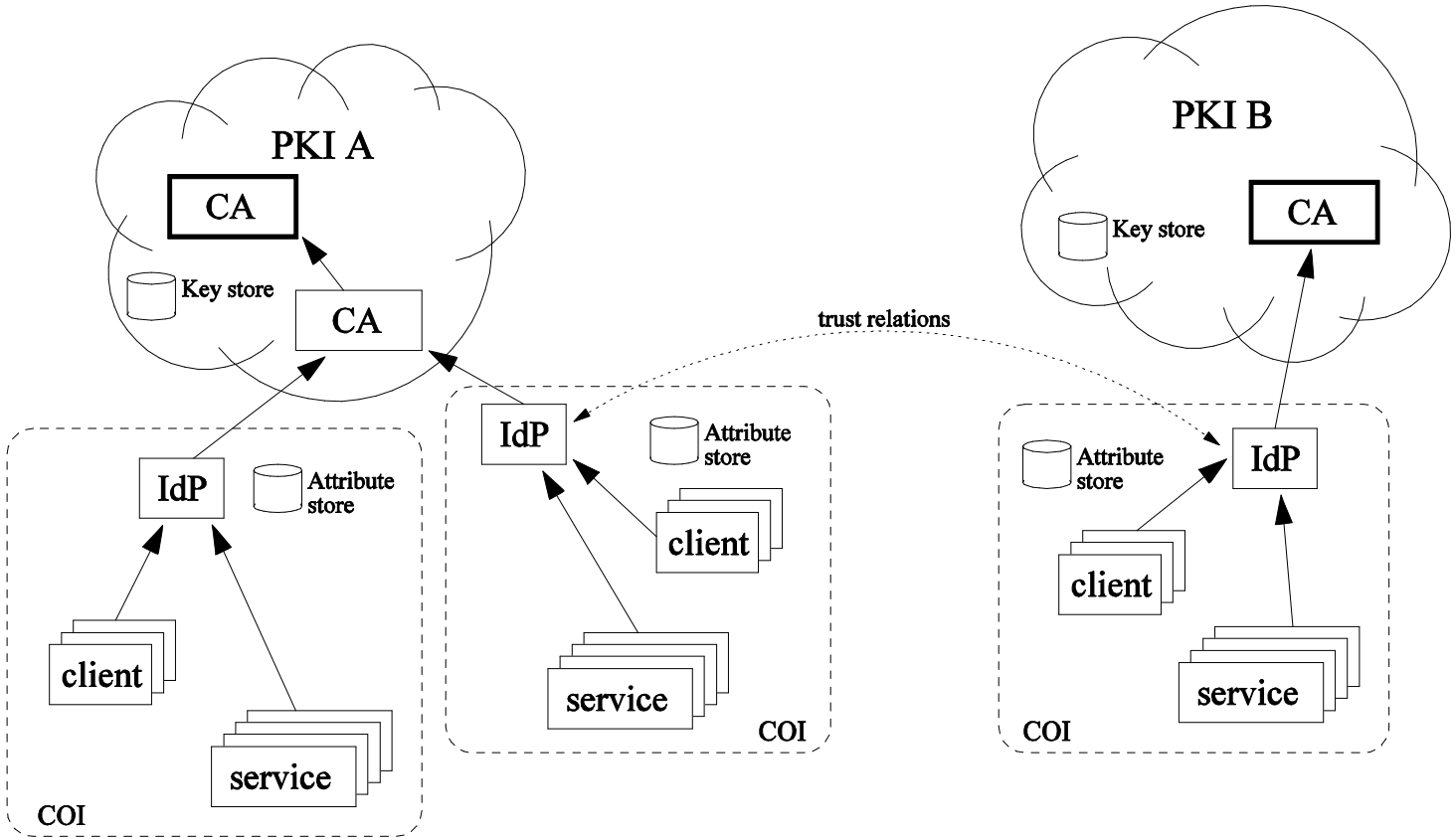
- Applications adapted for tactical networks are frugal, robust and perserverant, which are desirable properties everywhere
  - ***tactical applications are fit for ubiquitous computing***

Revocation and Tactical Networks

- Identity credentials may need to be *revoked*
- Revocation of identity information requires bandwidth and connectivity
- Revocation checking is expensive and error-prone
  - since one actually asks the *opposite question*

- The work presented
  - relies on short-lived ***”identity statements”*** which require no revocation scheme,
  - the identity statements are derived from X.509 certificates maintained in a PKI

The GISMO IdM Architecture



The Identity Statement

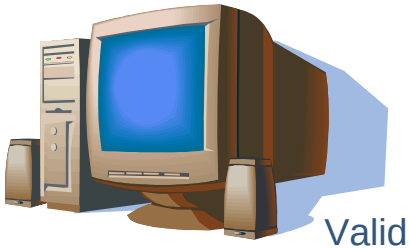
- Attested binding between properties and identifier
  - public key, attributes
- Signed by a trusted issuer
- Expires
- Both clients and services presents their identity statements in order to provide *mutual* authentication

Subject identifier
Subject public key/x509 cert
Subject attribute 1..n
Validity period (from-to)
Issuer identifier
Issuer public key/x509 cert
Issuer’s signature

Identity establishment example 1

Client

Identity provider



Harry Olsen

Harry Olsen's identity statement
(identity, roles, public key)

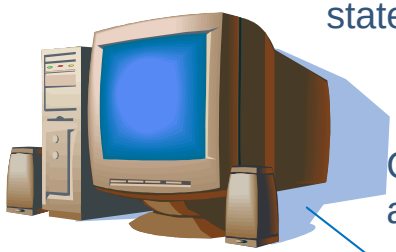
Validate Harry Olsen's certificate

PKI

Identity statement, signature, service parameter

Service response, signed by server, server's identity statement

Control of identity statement and signature



Service provider

Control of user roles against policy statements

Policy

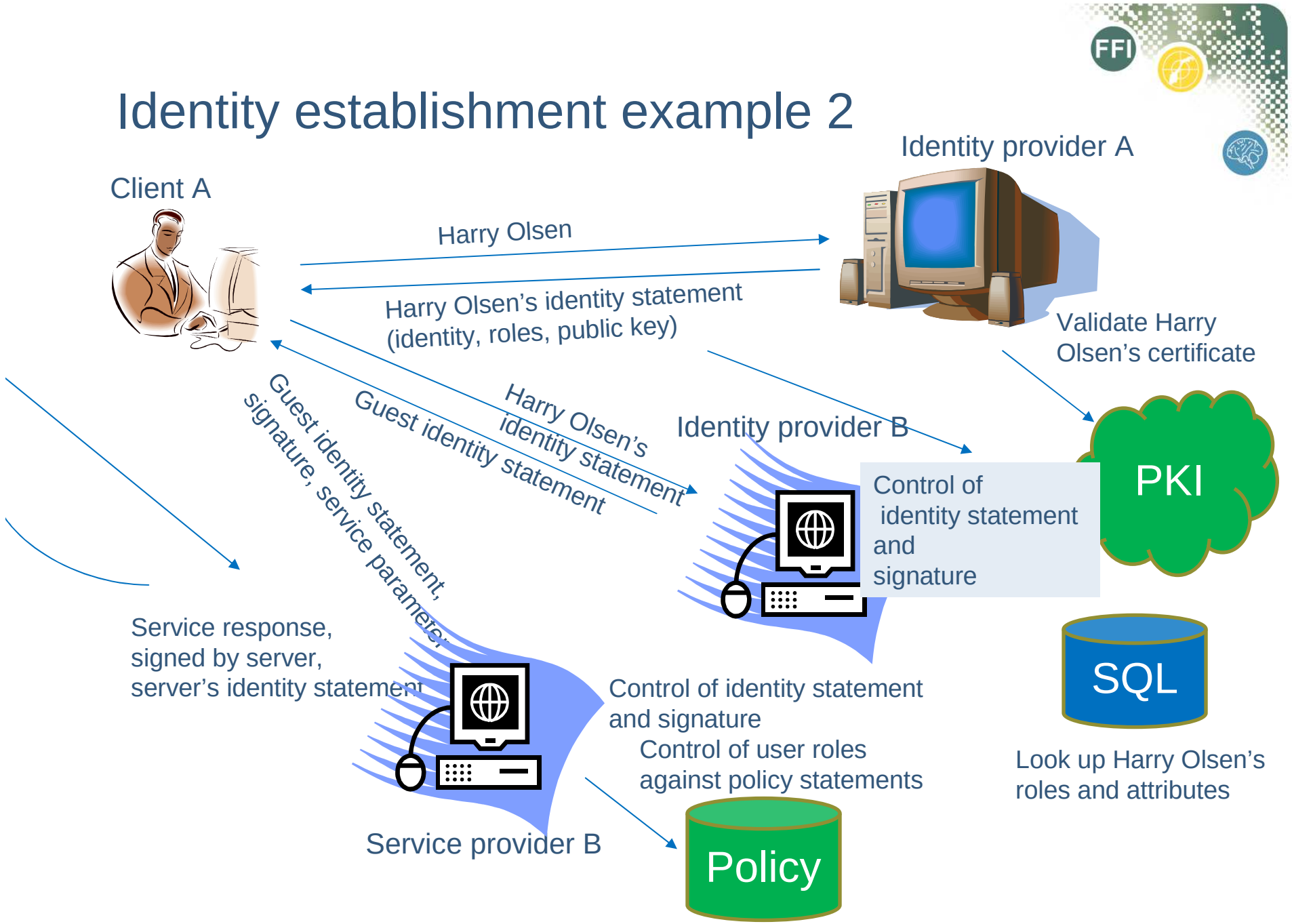
SQL

Look up Harry Olsen's roles and attributes

Trust assumptions

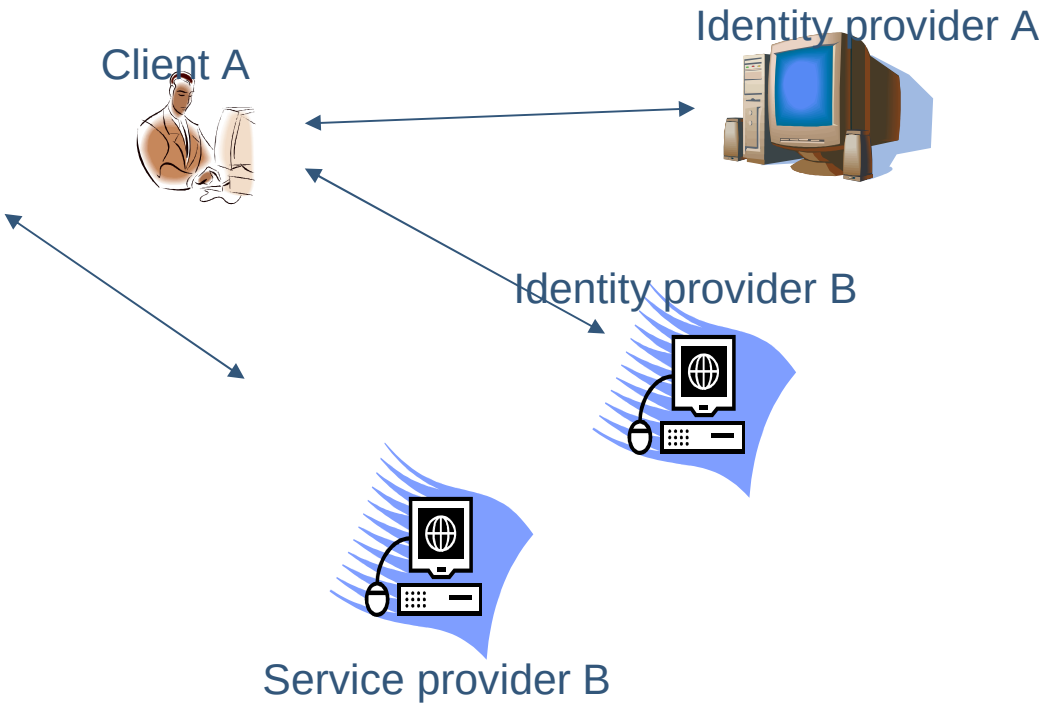
- The identity statement is issued (and signed) by the IdP
  - The service providers need trust in the IdP
    - that the identity statement are ”correct”
- The service providers trust the authenticity of a client who demonstrates a private key (proof-of-possession)

Identity establishment example 2



Trust relations

- IdP-B (Identity provider in domain B) trusts the authentication process of IdP-A.
  - it vouches for IdP-A by *re-signing* the identity statement
    - makes it into a domain-B security document



Advantages of GISMO IdM

- Administrative and Authority Issues
  - autonomy of domains and COI
  - loose coupling between domains (certificate pair)
- Scalability issues
  - no CRL distribution
  - single domain user management
- Mobility / Tactical issues
  - occational service invocations with IdP
  - client-A and server-B can connect independent on IdP reachability

Planned experiment: Protected service invocations for Android