FFI Forsvarets forskningsinstitutt

Validation of Inferior Identity Credentials

Anders Fongen, PhD
Norwegian Defence Research Establishment
CIT 2014 - Tenerife
ISIC Prosjektrådsmøte 06.03.2014

Scope of research

- How to manage authentication under circumstances where the necessary services are not available?

Outline of presentation

- Basic authentication
- Use and validation of credentials
- Balancing risk in tactical communication
- Representation and processing of inferior identity credentials
- Functional evaluation
- Conclusions and remaining research

Basic authentication relies on *trust*

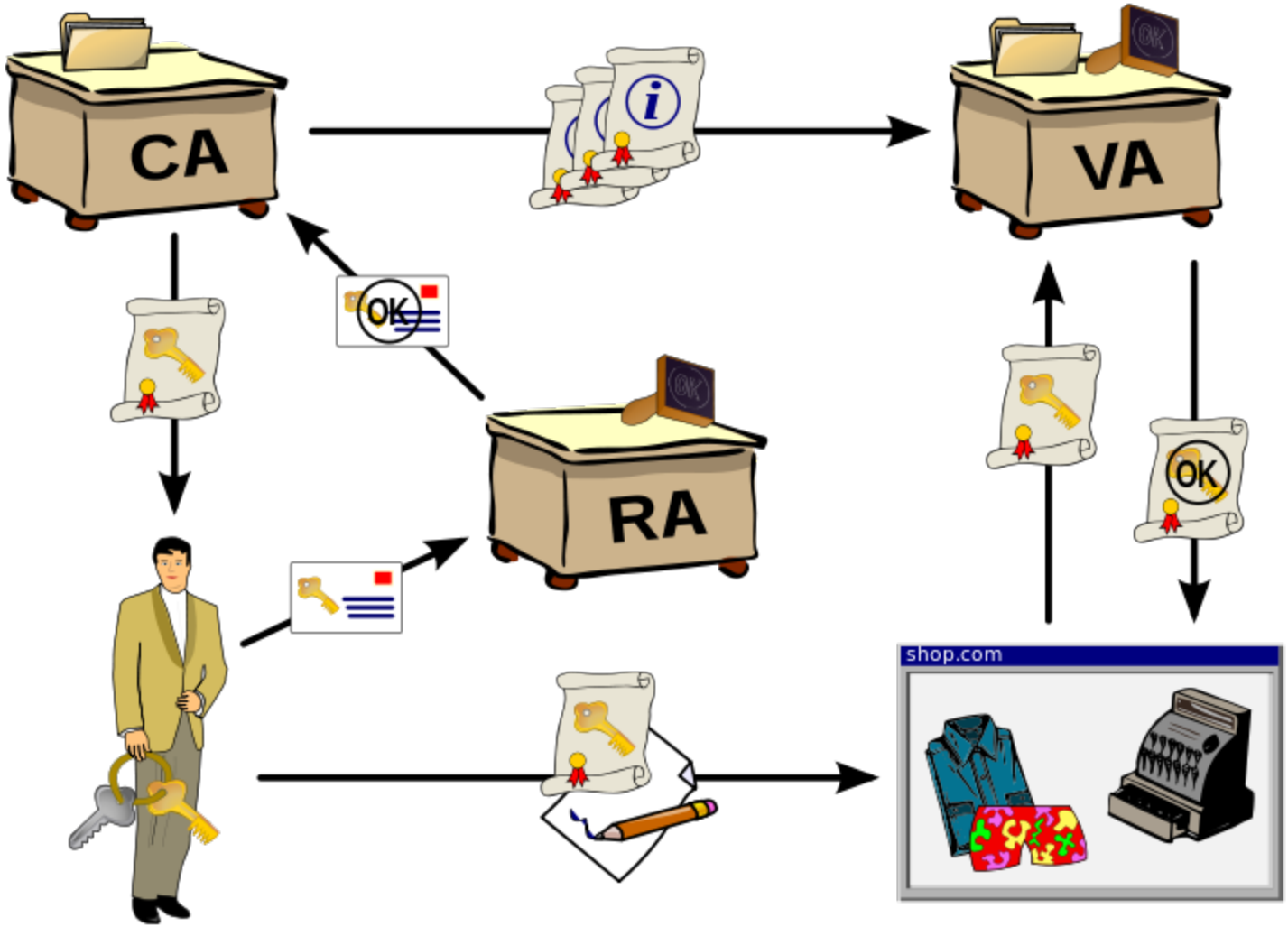
Often used principle: *Proof of possession*

- Direct trust
  - Parties share a secret, e.g. a password
  - Need a pre established secure channel for exchanging keys
- Indirect trust
  - Trust between parties derived from trust in a third party (TTP)

Credentials from Trusted Third Parties

- Today, mostly used with asymmetric crypto (public key)
- Sometimes called a CA (Certificate Authority) or PKI (Public Key Infrastructure)
- Credentials are issued in the form of *Public Key Certificates*
  - Bind *public keys* to *subject identities* and signs/seals with its own *private key*.
  - The signature of the issuer (CA) is trusted by everyone
- Credentials have restrictions:
  - Limited validity period
  - Key usage restrictions
  - Signature path length restrictions
  - etc.

A possible PKI configuration



Validation techniques

When a signature is verified, the corresponding public key must be *validated*:

- The signature should be verified with the key in the certificate
- The validity period of the certificate should be observed
- The usage restrictions should be obeyed
- A certificate path should lead to a *trust anchor* (TTP)
- No auxiliary info should contest its validity (e.g., revocation lists)

Characteristics of tactical communication

- Mobile nodes
- Wireless communication
- Intermittent connectivity
- Limited energy supply
- Low bandwidth
- Weight constraints

- Preparation phase, transport phase
  - abundant network and energy resources
- Operational phase (“dismounted”)
  - limited resources

It is unwise to rely on service availability in the operational phase without a “plan B”

Expired credentials - balancing risks

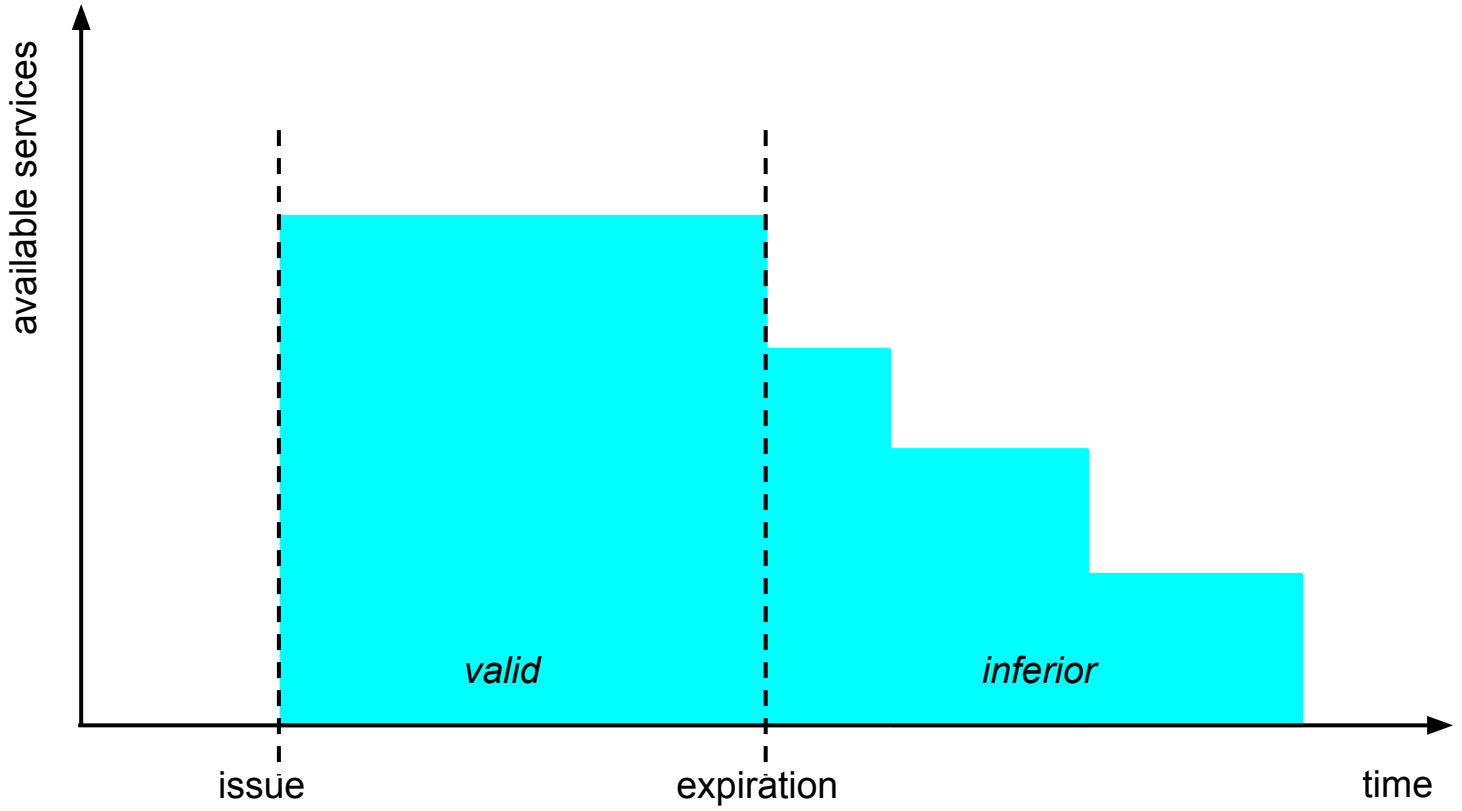
In a tactical environment, credentials may expire if the CA cannot be reached for a new issue.

During a military operation, to deny access to information may cost lives! Allowing access without proper control is also risky.

What to do?

- Deny any service (risky)
- Allow any service (risky)
- Allow a successively smaller subset of vital services
  - “graceful degradation”

Graceful degradation of services



Gismo IdM

In-house IdM made to study

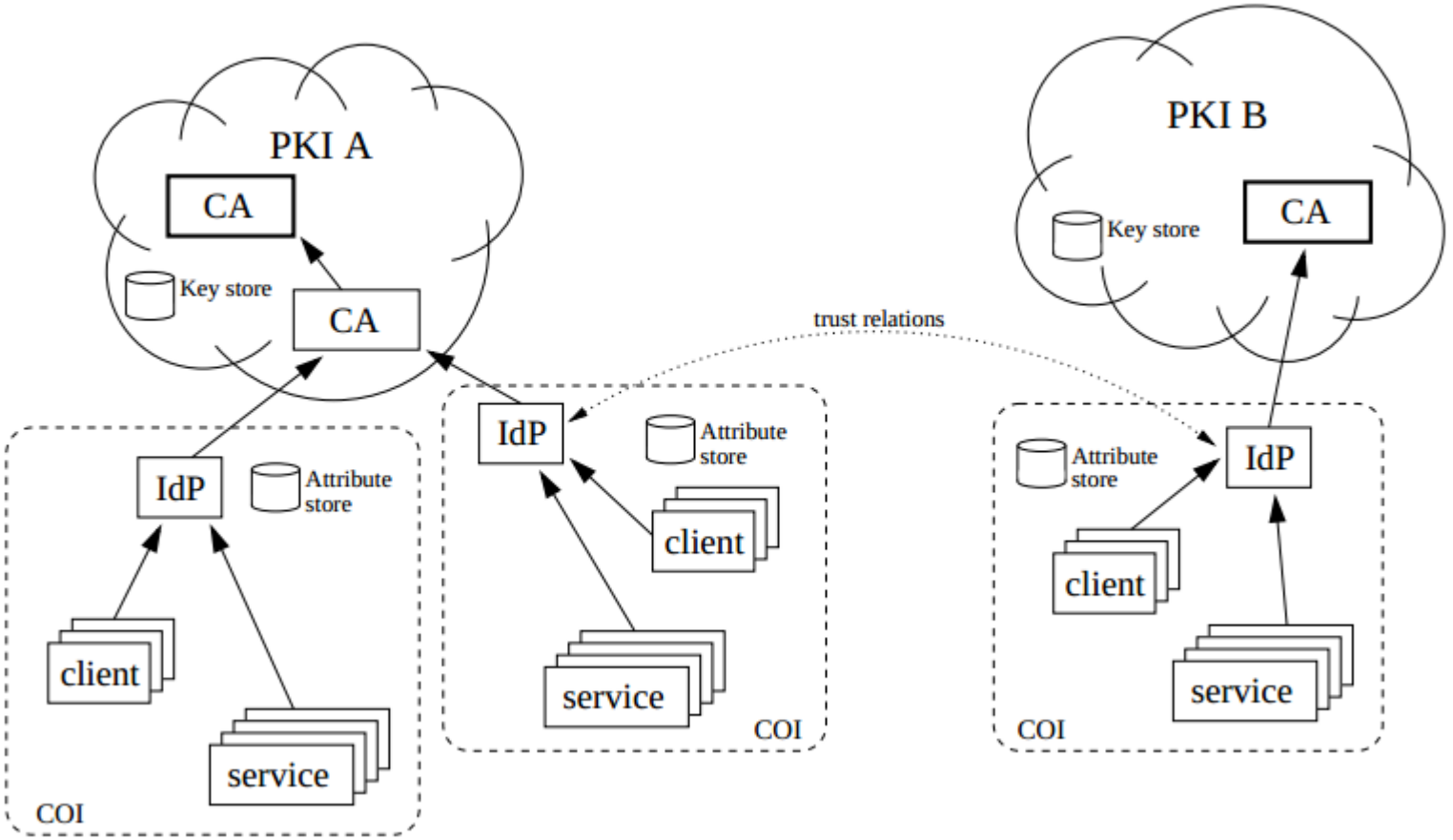
- Identity Management
- Authentication
- Access control
- Message protection
- Software integrity protection
- Service Discovery protection

in a tactical, multi-domain (coalition) network

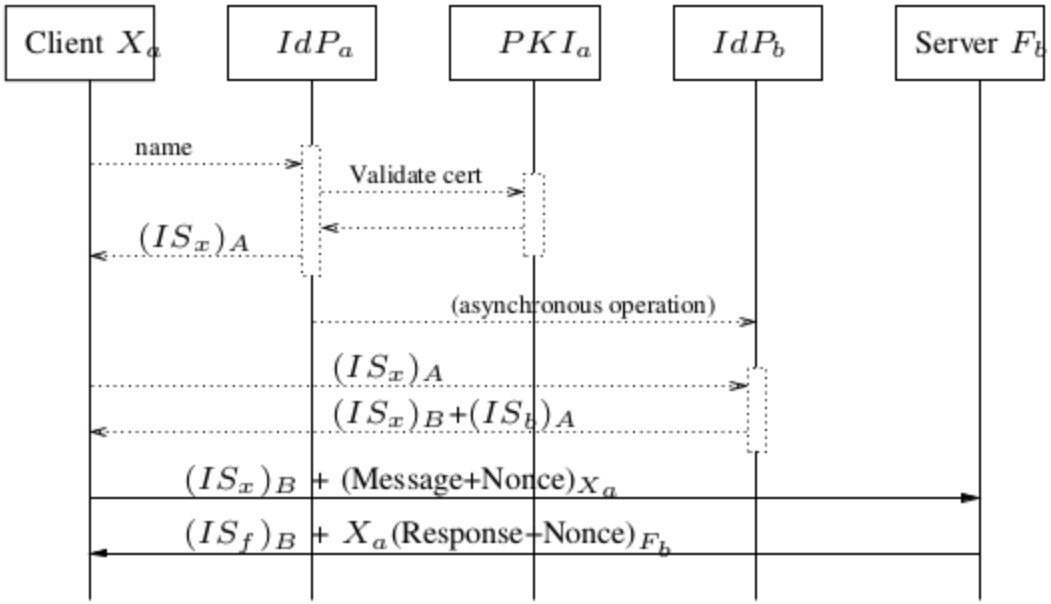
Key properties:

- Short-lived credentials (identity statements) with keys and attributes
- PKI encapsulation
- Straightforward cross-domain operation

Gismo IdM architectural overview



Gismo IdM authentication protocol



(Figure shows a *cross domain* operation)

Where to accept inferior credentials

Credentials should, as far as possible, be issued during the *preparation* and *transport* phase.

Credentials should be given a lifetime longer than the expected duration of the operation

Expired credentials will occur due to unforeseen circumstances

- Duration of operation
- Domain of communication

How to act upon inferior credentials?

Outcome of authentication is always binary: Anders/SomeoneElse

We will never hear “Probably Anders”

Inferior credentials can be represented among the *subject attributes,* given to the service for access control desicions.

```
$nationality=”no” and $clearance=”secret” and  $overdue<#30
```

Integration with service discovery

In Gismo Service Disovery, credential lifetimes are used to control the *liveness property* of services

Services with expired credentials are regarded as *defunct*, and will never be brokered by the discovery service.

Processing inferior credentials and service liveness using the same mechanisms is a hard act.

Functional evaluation

Yes, these mechanisms have been implemented and functionally tested based on the Gismo IdM experimental prototype

There are always surprises during both coding and evaluation, but in general, the idea works as planned.

The mechanism is exposed to clock drift (like validation in general), but using margins in the range of minutes exacerbates any clock drift problem.

Conclusions and remaining research

Summary and conclusions

- Rejecting expired credentials may be risky, and an intermediate mechanism may be justified
- Through the integration of access control and authentication, inferior authentication can be represented as subject attributes
- Access control mechanisms can use attribute information to allow/deny service to “inferior” clients

Remaining research

- A better understanding of how the term “inferior” relates to different operational conditions and events
- More experience on the concept of “graceful degradation” of services
- Field experiments are necessary!