A Meta Model for Trust Frameworks

Rainer Hörbe, 28-March-2011

License: http://creativecommons.org/licenses/by-nc-sa/3.0/
What is a Trust Federation?

**Trust Federation**

- **Constellation (High-level Use case)**
  - user-centric
  - service-centric
  - appears in some

- **Parties/Actors**
  - Relying Party
  - Identity Provider
  - Attribute Provider
  - Subject
  - Federation Operator
  - legally binds parties

**Trust Federation Users**

- Service Providers
- Service Consumers

**Trust Framework**

- defines
- is established by
- provides interoperability
- is broken down into domains or components

**Security Objectives**

- Confidentiality
- Integrity
- Accountability
- Authenticity
- Availability

**Interop Levels**

- legal
- operational
- technical

**Trust domains**

- Identity Assurance
- Privacy & user rights
- Authorization
- ...
## Trust Framework Capabilities

<table>
<thead>
<tr>
<th>ANSI/NASPO</th>
<th>Identity</th>
<th>AuthN</th>
<th>Session</th>
<th>AuthZ</th>
<th>Accountability</th>
<th>Privacy</th>
<th>User Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT eGov Fed</td>
<td>Individuals</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>epSOS</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>eSignature</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FIPS201 (PIV-I)</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IGTF/APC</td>
<td>NPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 29101</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ISO 29115</td>
<td>all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kanrara PF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Kantara IAF</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>KYC</td>
<td>all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-63</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>STORK</td>
<td>Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Mittwoch, 30. März
Risk management in enterprises the risk as cross section of assets, vulnerabilities and threats is determined and mitigated by safeguards and other methods. Service providers and consumers are part of the organization. IT Security is managed by handling IT-related risk. Policies can be managed and enforced centrally.
Risk management: Federation with SP-centric view

Risk management across enterprises disrupts the risk management process as known from enterprise risk management. Assets cannot be related to threats, mitigating vulnerabilities by safeguards to adjust risk to an acceptable level is and other methods. As autonomous actors handle their risk at a time, there is no common process for risk management. To resolve the issue, Trust Frameworks provide a baseline security policy, frequently with several assurance levels, to map the complexity of vulnerabilities and threats to a defined set of controls (or assurance criteria).
Meta Model: A basis to assess Trust Frameworks

- **Trust Framework Meta Model**
  - Context Analysis
  - Terminology
  - Actor Model
  - Catalogue of Protect. Requ.
  - Catalogue of Controls
  - Categorizations
  - Functions
  - Purpose
  - Mapping
  - Gap Analysis
  - Granularity Analysis
  - Public Policy Guidance
  - Justification of Controls

- **Purpose**
  - Delimitation of Components
  - identity assurance, privacy, ..

- **Mapping**
  - Automated policy negotiation

- **Context**
  - high-level use cases

- **Terminology**
  - controlled vocabulary, mapping

- **Catalogue of Controls**
  - by area of control, actor, ..

**Risk/Value Balance**

**Risk/Value Balance**
Trust Relationships
Actor Model

The previous federation models with three actors fit nicely into Venn diagrams, but many federation constellations have more actors. This diagram includes Attribute Providers (AP), a Federation Operator (FO), Registration Authority (RA), Attribute Authority (AA) and a Policy Management Authority (PMA).

The key objective of a Trust Federation is to support all these relationships.