Trust Metrics
TAS3 Approach

Sampo Kellomäki (sampo@symlabs.com)
European Identity Conference
Munich, May 6, 2009

TAS3 and Symlabs

- Sampo Kellomäki, TAS3 Architecture Lead
- TAS3 - **Trusted Architecture for Securely Shareable Services**
- EC FP7 funded research project, started Jan 2008, 4 year project
- Symlabs is member of the consortium

Trust in TAS3

Generic requirement "secure"

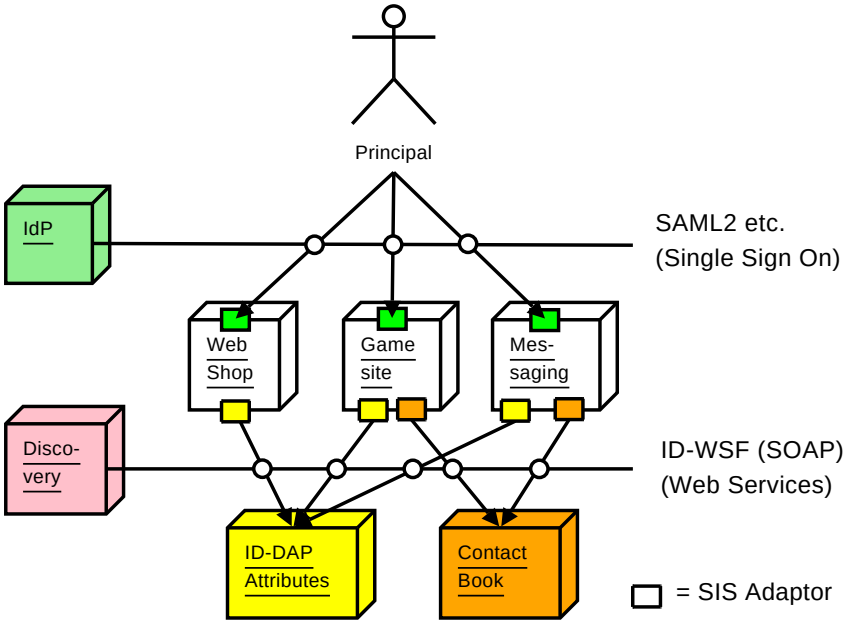
- Goal 1: Be **perceived** as trustworthy
  - Get Users to use it because they trust it
  - Get companies to use it because they trust it
- Goal 2: Actually **be** trustworthy
  - Earn trust in the long run
  - Avoid scandals
  - Keep costs down by avoiding abuse and fraud
- Goal 3: Allow trust to be formed dynamically

Building User Trust

- Dashboard
  - Transparency
  - Understandability
  - User has control
  - Auditability
- Nonrepudiation (user gets receipt)
  - Hold parties responsible
  - Well articulated with legal and contractual framework
- Explicit commitment to privacy and security
- Certified implementations
- Vetting or certification of other players
- Ongoing compliance validation
- Works correctly and as expected

Building Trust Between Systems

- Liability
- Auditability
- Nonrepudiation
  - Hold parties responsible
  - Well articulated with legal and contractual framework
- Certified implementations
- Vetting or certification of other players
- Ongoing compliance validation


Principal
IdP
SAML2 etc.
(Single Sign On)
Web Shop
Game site
Mes-saging
Disco-very
ID-WSF (SOAP)
(Web Services)
ID-DAP Attributes
Contact Book
= SIS Adaptor

Front Channel Trust

- Which web site to use?
  - User needs to decide on this
- Web site (SP): which IdP to use?
  - Trust as factor in IdP discovery
  - User's trust preception in choosing IdP (if choice is given)
- How was the user vetted?
- How was the user registered?
- How was the user authenticated?
- What is the trustworthiness of the attributes or claims received from the front channel?
  - How were they collected?
  - From what source?
  - Tampered in storage or transit?

SAML Approach: Trust Network (CoT) management

- Ultimately trust is determined by whether you trust digital signature
- SAML Well Known Location (WKL) metadata provisioning is great mechanism for distributing certificates, but not trustworthiness
- Explicit listing of acceptable public keys (certificates) most common
- Externally managed explicit list (push or pull)
- PKI + Revocation lists or OCSP (Online Certificate Status Protocol)
  - what's the win: explicit list vs. revocation list?

SAML Approach: Trust in SSO

- Authentication Contexts combine both "hows"
  - Initial vocabulary too vague and limited
  - You can invent your own
- Possibility of using separate attributes to convey "hows" separately
- Either way, the ontology problem remains: what authentication levels to use and how to rank them

XACML Approach to Trust

- PDP is generally fully trusted by definition
- Trustworthiness of the inputs to PDP is the real problem
  - Signed attributes or claims is mechanism
  - Still need to solve whether to trust the attributes and how they were collected.

Summary of SSO Trust

1. Trust signatures, but do not automatically trust transaction
2. Use some metric to trust IdP (or not)
3. Use some metric to trust the authentication and registration
4. Use some metric to trust the attributes and claims
   - Vetting or profiling of user appears as attributes
5. Trust PDP blindly and feed 2-4 to it so that policy based ponderation of the metrics can be made.

Back Channel Trust

- Instead of simple SP-IdP trust relationship, more complex constellation.
- Never-the-less, same methods of Trust Network management as in front channel, fundamentally work
- The discovery mechanism for back channel can easily use trust score as a factor in selecting a service

Dynamic Trust Score

- Users
  - Credit score or similar
  - User's track record
  - Other reputation systems designed for users
- Systems
  - Compliance history
  - Other reputation systems

Eventually Dynamic Scoring can also address Trust Network membership

Roaming and Proxying Trust

- Introduction of trust by locally trusted indemediary
  - IdP Proxying
  - Discovery Proxying
- Problems in mapping metrics from one Trust Network to Another
- Perhaps Dynamic Trust Score can solve this

Trust Ontology Research

- Agreement on authentication or assurance levels is still lacking despite years of effort on the problem
- Most probably we need to live with multiple systems and provide mappings between them
- Ability to join Trust Network based on reputation?
- What metrics are useful to describe attributes?

Thank You

Sampo Kellomäki (sampo@symlabs.com)
+351-918.731.007
www.symlabs.com
www.tas3.eu

Questions?