

## FEDERATED IDENTITY WORKSHOP

*Wednesday 29Apr09 at the Pittsburgh Supercomputer Center (PSC)*

Round Table Introductions: 25 attendees.

### MILAN SOVA (CESNET): IDENTITY FEDERATIONS IN EUROPE

Milan presented on behalf of Diego Lopez from RedIRIS, Licia Florio from TERENA and himself from CESNET. Eduroam is the 1<sup>st</sup> pan-European Identity Federation. Goal: "Open your laptop and be connected!" Used only for network access, it employs 802.1X/EAP + hierarchical (domain name based) RADIUS: If Local RADIUS server realizes that user is unknown from domain name, then traverse Root RADIUS Server + Country RADIUS server + ORG RADIUS server to find that user. This simple identity federation doesn't use many attributes (The EU maintains stringent controls over personal data, and this limits attribute exchange.), and only regulates peering among national federations. The SSID is always *eduroam*. Metadata is exchanged as large XML files without versioning controls or revocation, but with "Valid until" expiry. Wireless APs must support 802.1X; any RADIUS implemented on a PC works. Milan: preconfigured packages for institutions are used/needed

Some Useful Federation Definitions:

- Assertions: AuthN, and AuthZ attributes
- Protocol: Request and Response elements for packaging assertions
- Bindings: how SAML protocols map onto standard message or communication Protocols
- Profiles: How SAML protocols, bindings and assertions combine to support a defined use case.

Federation Options:

- Bilateral federation (classical model)
- Confederation
- Inter-federation
- Leveraged federations
- Gateway of federations (eduGAIN) – loosely-coupled via abstract device service; set of interconnection points (Bridging Element, BE) at each federation (this was before SAML2). Metadata service (MDS) distributes info via eduGAINMetaQuery API delivered to the requesting BE. BEs then exchange data using eduGAIN SAML-based profile. Here MDS serves as a refinement on downloading the entire XML.
- eduGAIN-ng: because everybody speaks SAML: removes BEs and uses dynamic metadata instead; gain trust via metadata publishers. (Milan supports this)
  - Others ...

## DEB BLANCHARD (VERIZON BUSINESS (CYBERTRUST)): IDENTITY AND ACCESS MANAGEMENT

Deb has been working in identity management for 15 years. She is also associated with the just announced Four Bridges Forum (4BF) that includes:

- **Federal PKI Architecture** (Federal Bridge), serving all Federal agencies.
- **CertiPath**, serving the aerospace and defense industries.
- **SAFE-BioPharma Association**, serving the biopharmaceutical and healthcare industries.
- **HEBCA**, serving the higher education sector in the United States

Verizon Managed Security Services 1) Assess; 2) Mitigate; 3) Test & Certify; and 4) Maintain security. Verizon handles 71% of US/federal government IP traffic and 3300 customers worldwide, including many Fortune100s. Verizon recently acquired UniCERT CA (Baltimore Corp. technology) as part of a "10yr plan by Verizon." CyberTrust core business is monitoring hacker chat with 6 SOCs around the world. Her group was recently moved from VerizonBusiness to VerizonCore. Supports pre-verification and web-based access. Delegates an accredited company the capability to issue SSL certs in real-time.

- Personal Identity Cards must be managed right. One fed agency kept retired PIV cards without revoking them.
- Verizon goes through a WebTrust audit every year.
- Note embedded trust point in mobile Phones (including iPhone). Verizon wireless phones carry OTP (NIST 800-63 Level 3)
- InCommon has had difficulty dealing with Fed policies and practices
- Mike Helm: Identity Proofing remains a problem. DHS & NSA: "We don't want to do identity proofing for the nation" Deb: What constitutes id proofing? There are ways to mitigate f2f id checks. MikeH: ID proofing remains intractable. Deb gave example going back to fed or state "antecedent."
- AlanSill: the TAGPMA Bridge group is stalled due to technical issues having to do with identity proofing. BridgePath discussion would be useful. Would Verizon like to federate with IGTF?
- MikeH problem of VO still hasn't been addressed. We would like for InCommon to solve some problems – but this may be too difficult in the USA.
- CyberTrust has ideas about the proxy cert. Portal SW verifies the validity of a user's identity certificate via CRL/OCSP & LDAP. Then proxy registration page pre-populated based on cert or LDAP or entered by the user. Web based software includes report generation, could be setup in 10 days. Discussed certificate lifecycle management. Verizon would be willing to support grid needs.
- MikeH: could we solve a national infrastructure problem? Like an InCommon grid cert service.
- Scott: 4BF infrastructure provides PKI that scales.
- USA is opposed to a National ID card. EU supports the concept.
- CyberTrust supports Belgian and Italian ID cards.
- Obama is looking at ID mgmt!

MICHAL PROCHAZKA, (HPC AT MASARYK UNIVERSITY IN BRNO, CZ): GRID-ENABLED DESKTOP

- Work done with Daniel Kouril, HPC center staff & Tomas Kubina student
- About access to the Grid & Key mgmt & user view of authN mechanisms
- Cred transformation; Network IDM (NIM); Apps for accessing the Grid.
- Private key mgmt has drawbacks.
- Store X.509 cert in the user's web browser; use MyProxy; enables SSH (PuTTY), WINscp, SCP w gsi-ssh or Kerberos/MyProxy
- Special UI Apps with cert on disk (globus?)
- MikeH: x.509 cert mgmt vs password mgmt is an anachronism. People don't understand passwords and they don't do it well.
- Deb: wants to get rid of pages and pages of username/passwords. X.509 cert is better for me.
- Hide PKI from the users; focused on Windows OS for now
- voms-proxy-init ported to Windows & GSSAP
  - support Windows CertStore
  - support for VOMS
  - support for PKCS#11
- Jens: Java 1.6 can also access Windows CertStore
- AlanS: MS dropped all Kerberos support in Geneva
- Jens: we have a Java app that does what you do but transparently
- Demo: Federated On-line CA: His app has a Federation tab. Work is based on plug-ins, e.g. gsi plug-in for putty.
- NIM still under development. Apple/Linux. V1.x supports Kerberos authN, V2 supports many types of credentials
- FNAL has a contract to develop Apple/Linux port of NIM with Secure Endpoints.
- MikeH: what about InfoCards? Too many geeky things in this app?
- Irwin: NIM is widely deployed and has enabled Windows users to use certs.
- AlanS: referenced GRIX Java front-end \*\*\* switching to Shib only \*\*\*
- Jens has a Java interface based on myProxy.
- MikeH: what is the availability? NIM is open-source project.

DARIAN WOODFORD (SAFENET): SAFENET UPDATE

Darian has a lot of identity Management experience: Safe-Net; Aladdin; Oracle; Baltimore Technologies; AT&T; NCSA (where he worked on Mosaic).

- He usually does commercial – wants to understand academic needs.
- DRM & Enterprise Security Mgmt
- SafeNet + Aladdin are now the 4<sup>th</sup> largest security company in the world
- Strong presence as token provider for higher education
- Tokens don't do federation specifically, but tokens enable/support PKI. (“something the user has”)
- How strong is strong? The range of technologies for storing tokens:
  - PRNG – one-time password tokens – nothing happens on the token itself; “something I have” + “something I know”

- TPM Trusted Privacy Modules (secure-ish storage) all new Macs have TPMs in them for secure storage (but no crypto)
- Token storage on Encrypted drive + SW app
- Smartchips / SmartCards = encrypted ops + secure storage
  - Signing, key gen,
  - Embedded OS
  - Tamper resistant / evident / proof
- FIPS 140 and Common Criteria: CC EAL Level 4
- Everything with a USB connector is a SmartCard @ FIPS Level3
- All new tokens are Java-based OS instead of CardOS
- SafeNet no longer sells Alladin 64K tokens to new customers. (Pro-64 token with Java is more flexible. Gov customers can still get the CardOS version)
- Hybrid: USB drive & FLASH 72K storage portion with one chip to support encryption while another chip supports 1-2GB of the FLASH to encrypt just that USB drive
- Plan to merge to a single mgmt interface that supports APIs: CAPI / PKCS#11 / DTAPI / PCSC / APDU / OATH
- Can integrate with Mac KeyChain or can be managed by AD, LDAP or customer DB
- ScottR: federations are policy and stds driven i.e. 800-63. DebB: You can operate at Level 4, but Med/HW is the highest that the 4BF will accept. PKI cred may end up as Level 2. Feds give no waivers. This applies in Defense and Intelligence (where ActiveIdentity and SafeNet are main players.)
- HSPD-12 ID cards are different and 6.2 Million issued.
- NIST 800-63 considers OTP as Level3; zero-knowledge password?
- What about users who lose keys? Agencies & Enterprise make it so painful that they stop losing it. For example, in the AWACS. forgetting to do something twice will get a person fired. Coddling people allows bad things to happen. Sarbanes-Oxley, HIPAA impose fines as 'motivation'. Policy can address what happens when the private key in the token gets smashed or lost.
- Have folks use a certificate for all access AND store the private key on a HW token. Make it non-exportable on a HW device so that interaction between token and OS is secure. Policy can be burned on the token. Setup PIN timer to require re-authentication.
- AlanS: We need both stronger LoA and weaker LoA. This looks like mature technology and we should reference it in our AUPs.
- Jens: Robot certs require Level 2 hardware tokens
- ScottR: Can you gen keys on a token and export it (encrypted) to HSM? Darian: you can, but you shouldn't. Our eToken system: create your key-pair with our software and stick it on multiple tokens. MikeH: if a key token is in another place, we have to help them get back to work. One way - make a duplicate and throw it in a safe.
- Darian: Alladin previously didn't sell HSMs; their tokens were borderline HSMs. Now they won't stomp on the HSM market
- MikeH: wants an assertion from the device that presents the CSR. Darian - you can see the serial number of the token. Was a token involved in a transaction? Darian: there is also a clientless token w a CDRROM partition - only works on Windows. Creates SSL tunnel. **CD partition fires up a browser with a secure SSL tunnel**

**using an a priori cert on the token itself.** Configure a token – mail it to the user. Issuer sets up the interface. Client gets automatically connected (securely) (SmartCard piece with ROM with a Windows image that runs on VMWare on Mac or a Windows box.) App fires up and phones home. Like an electronic key-ring. Plus escrow yields ‘backup’.

- Discussion about a “browser in the middle” attack. Generates a key-pair elsewhere than in the token. Darian: so the attacker hijacks the session; mimics the communication. But is the browser distributed with the token? What if a bad guy creates a key-pair?
- Irwin suggests adding Darian on one of our conf calls – keep the dialogue going.

#### **LISTEN IN ON TWO TALKS FROM INTERNET2 SPRING 09 MEMBER MEETING:**

##### 1. KEN KLINGENSTEIN (INTERNET2): FUTURE OF INCOMMON AND US FEDERATIONS

- Managing identity for science teams is different than managing students.
- “Hub & spoke” model: **Covisint**, a company who provides federated identity services to the automobile sector and is moving into commercial health care.
- InCommon “soup” is good for groups and members but bad for user confusion and isolation. Elements that cause confusion:
  - What if my campus belongs to several federations? What would the pull-down menu look like? Attrib release policies? Privacy policies?
  - What if my IdP changes federation
  - Metaphors like InfoCards put you directly in contact with your IdPs
  - NIH doesn’t want to sign an agreement with UT-System?
  - Comanage instances need to be configured – distribution of metadata is a problem
- SWITCH Digital ID Card and method for managing attribute releases may be an equivalent or competitor to Windows CardSpace.

##### 2. JACK SEUSS (INCOMMON STEERING COMMITTEE): US FEDERATIONS

- Ken is the good engineer! Jack plays the ‘evil manager’. “We must ship it.”
- Time is of the essence. Also looking for feedback on the future of InCommon.
- <https://spaces.internet2.edu/> Goal: present something by July.
- 141 participants in Spring 2009 & >3Million users served.
- Primary focus will be US higher-ed because of need for mutual trust
- K-12, states, commercial are not current primary focus.
- Partners asked to focus on higher ed R & E mutual interests
- Bob Morgan: We want US government service providers as participants/partners – so this isn’t black and white.
- Asks for an InCommon Governance Model Review because:
  - InCommon was a separate LLC corp with Internet2 as the sole member
  - 2007 Governance & Nominations Committee (GNC) established 4 advisory councils
  - Current oversight lacks accountability and transparency

- A separate group with lawyers should review Governance and make recommendation
  - Partnerships based on range from simple MOU to shared investment
  - EDUCAUSE role?
- Was priced aggressively to encourage orgs to join. Real infrastructure costs more. Need to raise fees for participation. Should be break-even at 200 members. “We are charging too little to make this work.”
- Right now, Option 1: everybody pays the same fee. There should be some variance based on some easy-to-understand criteria.
- Option 2: Tiered pricing based on number of users
- Option 3: ???
- Option 4: Multi-institution discount if a single entity organizes a group of members and is the one trusted point of contact
- Option 5: some hybrid
- Service goal: successfully deploy InCommon Silver in order to address level of assurance to support trust.
  - Core services
  - Promised or in-dev service
  - Adjacent services (training, consulting support)
  - Provide leadership in standards bodies
  - Innovation
- InCommon may consider running a low-cost SSL cert service?
- What services should InCommon NOT pursue?
- Ken asks Scott’s question: how will InCommon provide support for PKI
  - What is the role of InCommon as a CA?
  - NSF staff use 2<sup>nd</sup> factor tokens. Grids use certs.
  - Jack: Until we do Silver – we’re not ready to do Platinum...
  - Jack getting ready to look at Meteor (Lvl 2) NIST 800-63 levels but not all the web ISO’s support 2 factor right now.
  - Ken: 2 factor is slippery slope. They don’t want Lvl 3. Stop keyboard sniffing. But avoid in-person ID vetting.
  - Jack: the other app is ERP: I’ve got auditors concerned about passwords. Can we come up with an infrastructure that supports both science and staff.
  - Question about K-12: the number of IdPs will be so many more and characteristics will be different. But K-12 doesn’t have a code writing group, so will want to leverage InCommon tools and services. Ken: if it’s not InCommon’s job, then whose is it? Person in audience: But states don’t have the \$\$ or resources. Jack: Prove the model works first.
- Why doesn’t InCommon have 2-3000 members? Jack: What if federal student aid required participating in a federation? – That would be a motivator. 300-600 is possible. 3000, not so much.
- Kevin Morooney: We’re inching the refrigerator forward, but now big agencies are saying “This is how we will do it.” We need this & it shows the payback on the investment. This is not news for any institution with a medical center. The medical centers need more outreach.

- TAGPMA mtg (in progress) is already considering one CA request for working with InCommon credentials.

#### KEN KLINGENSTEIN TALKS WITH TAGPMA ID MANAGEMENT WORKSHOP

Ken Klingenstein Phone call:

- ScottR: a lot of people, including reps from organizations are asking “What federation should we be joining?” Can InCommon provide the glue?
- KenK: InCommon will represent an evolving mix of communities. We may see large groups leave InCommon to form their own federations. Only about half of the current members publish their POPs. A lot of NSF related sites use weak Id proofing + 2<sup>nd</sup> factor service. We need a national 2<sup>nd</sup> factor service. Minimally, we require Silver. Impact on InCommon only affects the operators. Gold probably won’t be that hard (after Silver).
- ScottR: Silver puts everybody on the right track. Hard issues are the same with Gold.
- KenK: Jim Basney did some good work comparing InCommon LoAs and. Ken doesn’t think that Silver works for the science comment. Silver can be met by campuses because of flexibility of docs and operational requirements.
- JimB: We will discuss my doc tomorrow – I think that Silver gives us what we need. Silver + 2factor could support long-lived certs.
- KenK: InCommon TAG is frugal in its attribute provision. Ken agrees with the Australian attribute approach better where campuses store attributes from external SOAs in their directories. A National Grid service could require InCommon members to support this. Silver does more than raise LoA – it can introduce new attributes.
- AlanS: Apart from which LoA will meet which needs, what about the mechanism of engagement? InCommon needs a seat at the IGTF table. Join TAGPMA? KenK: sounds like you want TAGPMA to get a place at the InCommon table, and although this seems natural, we don’t have a table yet. Wait until Silver is up and governance gets changed.
- Irwin comment: there is a difference between a CA and an IdP.
- InCommon requires an annual audit for Silver. Audit form is on their website and they are in the process of socializing that form to better map to campus auditor procedures. Issue about what info to publish. Suggests making only access to registered CAs IdPs – maybe a privilege that depends on providing a signed something.
- KenK: there is no federated operational practices document today. What does the Federated operator need to do? 800-63 is a framework for LoA. Silver Profile is approved and an instantiation of 800-63. NIST is talking about producing a revision or audit doc. MikeH: How will InCommon publish this? Ken: at least in meta-data.
- MikeH: He doesn’t see it as too useful to do 2 factor. Mike has been burned by it, but it is required at various places. It would be nice to provide a profile based on assertions that could be made about 2 factor systems. KenK: NIST needs to do a good job of handling mobile phones and SMS and such. But don’t expect to lay down your 2 factor burdens in the next 6-9 months. He suggested incenting federation as

an option. Jens: you can assert LoA now – see UT-System attrib. MikeH: but it's in UT attrib space. Marg: reason for that is that it takes so long to get into the global space, but these attribs can move.

- MikeH: question about Jack's focus? What about DOE labs? Should we continue to campaign to get sister labs to join InCommon. KenK: Absolutely! The government is our 'anchor tenant'.
- KenK: Comanage will get a lot of stuff/support moving towards federation. i.e. grant admin. Don't take "higher ed" to exclude the national labs. They are partners. Also, there are a large number of med schools who want to join InCommon, but their IdP is different from the part of the institution that registered with InCommon.
- JimM: We look forward to working more with InCommon!
- AlanS: the need to document something that works is what drives us.