Squaring the Circle.
Reflections on Identities, AuthN & AuthZ at CERN

Dr. Stefan Lüders
(CERN Computer Security Officer)
37th TF-CSIRT Meeting 20120928
Overview

The Problem: Legacy of the Past.
Eligibility of accounts, ownership of computing resources and AuthZ for using computing services (or not) are undefined and uncontrolled.

The Present: Regain control.
Define who is eligible for owning computing accounts/resources and using computing services. Have a full lifecycle for accounts and resources.

The Future: Federation, anyone?
Opening up for external identities.
The Problem: Legacy of the Past.

There is no policy who is eligible to use CERN computing resources. *Nada.*

Once you’re in you can own/use/eat what you want.

_Yum-Yum._
Academic Freedom at CERN

CERN’s user community:

▷ ...from 100s of universities worldwide
▷ Pupils, students, post-docs, professors, technicians, engineers, physicists, ...
▷ High turn-over (~10k per year)
▷ Strong characters, know-it-alls, nerds & individualists
▷ “Security” is usually not part of their mindset.

Academic Freedom in Research:

▷ Open campus attitude
  No boundaries if possible: free communication & freedom to publish
▷ Merge of professional and private life (we have hostels on site):
  Social networks, Dropbox, Gmail, LinkedIn, ...
▷ CERN is an ISP!
  The CERN IT department provides central services for their convenience.
CERN accounts for your dog

Today, no rules who can obtain a CERN computing account:

- You just need to be registered with CERN HR.

**Staff & Fellows**
- Apprentices & Trainees
- Students
- Children of Staff
- Honorary members
- Associates

**Researchers ("Users")**
- Professional visitors
- Members of official CERN clubs
- Lecturers
- Retirees

**Temporary labour & contractors**
- Industrial liaison officers
- Host state’s authorities
- Committee members
- Official guides

- That account allows owning plenty of CERN computing resources...
  (e.g. a mailbox, websites, other accounts, DFS/AFS disk space)

- ...and enables use of many (~all!) CERN computing facilities
  (e.g. LXPLUS/LXBATCH, Windows PCs, INDICO/CDS, EDH)

- That account will remain being still valid for two months after leaving CERN.
  Even if you just worked two days at CERN painting a wall!
More accounts for your dog

In addition, there are more accounts:

▶ “Secondary accounts” for the usage of a different computing profile; or for access to critical resources (e.g. admin access)

▶ “Service accounts” for running computing services & control systems; its password is usually hardcoded and shared between peers 😐

▶ “Lightweight accounts” for accessing public services (e.g. CERN Market or for blogs); these are usually clones of Gmail, ... accounts with a dedicated CERN password

A clear definition is needed of

▶ who can use CERN computing facilities, and
▶ who can own CERN computing resources.

A proper split needs to be done between AuthN & AuthZ.

▶ Having logged in shouldn’t imply you can access/use everything
The Present: Regain Control.

Separate AuthN and AuthZ.
Align eligibility of computing resources with SLDs, service catalog, and have a lifecycle.
# Ground Rules for Eligibility

<table>
<thead>
<tr>
<th>Staff &amp; Fellows</th>
<th>Researchers (&quot;Users&quot;)</th>
<th>Temporary labour &amp; contractors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apprentices &amp; Trainees</td>
<td>Professional visitors</td>
<td>Industrial liaison officers</td>
</tr>
<tr>
<td>Students</td>
<td></td>
<td>Host state’s authorities</td>
</tr>
<tr>
<td>Children of Staff</td>
<td></td>
<td>Committee members</td>
</tr>
<tr>
<td>Honorary members</td>
<td></td>
<td>Official guides</td>
</tr>
<tr>
<td>Associates</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### "Staff" / "Users" (REFEDS: "Faculty"*):
- Get an identity by default; Can own resources; Can use services
- Some can get a CERN certificate (in-line with EUgridPMA)

### "Retirees" ("Affiliate"*?) / "Contributors" ("Unpaid Workers"*?):
- Can get an identity; Can subscribe to some services; Won’t get a certificate

### (none):
Nothing; can use *public* services, only

*REFEDS categories don’t really work for us...
Adapt Current Infrastructure

IdP / Attribute Authority

Register

Opt-in [ID, attr]

AuthZ-groups

Configure [ID, attr]

IdP / LDAP/AD

HRDB

LDAP

AD

AuthN

Login

[ID, credentials]

SSO

AuthZ

LDA

PAD

AuthZ

Resource Broker

Configure [ID, attr]

FIM+

Resource Broker

IdP / LDAP/AD

HRDB

LDAP

AD

AuthN

Login

[ID, credentials]

SSO

AuthZ

LDA

PAD

AuthZ

SP

FIM+
A Central AuthZ Framework

SPs (+Security Team) define...

- ...eligibilities, i.e. whether AuthZ is granted by default or user needs to subscribe (→ RB)
- ...which attributes are needed for AuthZ (e.g. HR/REFEDS categories, roles, organizational units, experiments, institutes)
- ...which LoA is needed for AuthZ (→ last slides)
- ...whether a second AuthN factor is needed (e.g. for critical LHC settings, admin access, signatures for 100kCHF++)
- ...outer boundaries of who is denied AuthZ (e.g. secondary or service accounts)

Uses LDAP/AD with custom configuration interface for AuthZ rights management based on either dynamic attributes or static individual user names.
One CERN Single Sign On Portal...

...for all computing services

► Current focus on web applications
► Integration of Kerberos/NTLM and x509, certificate
► One single defined SSO API for non-web applications
► Migration of all non-SSO applications has started
► Phase-Out of ad-hoc HTTP logins (and move to HTTPS)

Looking for suitable solutions for non-web applications

► e.g. Project Moonshot, mapping of Grid x509 certificates
...enabling Two-Factor AuthN

Plus SSH ForceCommand option for SMS OTP and Yubikey
The Future: Federation, anyone?

CERN is not the center of the world. Why shouldn’t a FNAL/DESY/PSI/… person use his FNAL/DESY/PSI/… identity at CERN?
Joining ID Federation(s)

Most CERN users have IDs with their home university, lab or inst.

- They work from there, are used to their SSO portal, regularly forget the CERN password, and even forward their CERN mail “home”
- Permit them using their home ID instead of the CERN one (which they still have)

We won’t need external attributes:

- Their inconsistent usage makes life complicated.
- Due to legal reasons, users need to be registered with CERN and with the CERN greybook (for experiment affiliations)
- Their home email address would be the handle (like for CERN mail forwards)

Thus, CERN is already IdP and AA

- Define public / private attributes and share
- (SSO Portal still needs to be adapted to obtain user consent when sharing)
### Classes of Identities

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERN Registered</td>
<td>Currently active CERN primary accounts.</td>
</tr>
<tr>
<td>HEP Trusted</td>
<td>HEP people registered with CERN/HR, AuthN using their HEP systems through ID Federations.</td>
</tr>
<tr>
<td>CERN Shared</td>
<td>Currently active CERN secondary and service accounts.</td>
</tr>
<tr>
<td>Verified External</td>
<td>Ex-members of personnel, like retirees, former staff, etc. They still have an entry with CERN/HR but no primary account anymore.</td>
</tr>
<tr>
<td>Unverified External</td>
<td>Anonymous unverified people, like lightweight accounts, Google accounts, unregistered Federation accounts.</td>
</tr>
</tbody>
</table>

**Five LoAs:**

- Up to the SP to decide which ID to AuthZ access (e.g. HR or finance applications vs. LXPLUS/BATCH vs. CERN Market or blogs)
- Taking advantage of the CERN AA

**Extending beyond ID Federations: Permitting OpenIDs**
Proofs-of-Concept

Choices will be remembered using cookies.
Of course this doesn’t scale...

More IdPs, more icons, more bilateral agreements 😞

We need to establish a network of trust à la IGTF
► ...before CERN seriously joins more ID Feds (in parallel we’ll extend our pilot)
► Requirements defined in collaboration with many other sectors at the last “FedID Management” workshop
  (https://indico.cern.ch/conferenceDisplay.py?confId=191892)
► Next one is in March 20/21 2013 at PSI, Villigen Switzerland

Plus:
► How would the Grid x509’s fit into this all?
  ➤ Needs security token translation service (e.g. EGI STS)
► How would ORCID* fit into this all?
  (*tagging publications such that the author is uniquely identified, and his/her publications are properly assigned)
Summary

The Problem: Legacy of the Past.
Eligibility of accounts, ownership of computing resources and AuthZ for using computing services (or not) are undefined and uncontrolled.

The Present: Regain control.
Clean up has started. Eligibilities are defined. Two-factor AuthN deployed. Basic framework for AuthZ ready. Up to SPs now to apply.

The Future: Federation, anyone?
Pilots launched with Switch, BNL, INFN, Google and others. Wider trust framework discussed with peers at the FIM workshop series.