



Providing access to IT-services for “guests”

Two solutions for «guest» users provisioning



Background

- University of Oslo
 - About 7 500 employees (staff and faculty)
 - About 33 000 students
 - About 2 000 PhD
 - Between 6 000 and 8 000 "others"
 - Several affiliated research centers, hospitals etc
 - Wide research cooperation (both in Norway and abroad)
 - Euroam and FEIDE member



Identity management at the University of Oslo

- Authoritative information about people
 - An HR system based on SAP
 - A student registry
- Authoritative organizational data
 - Recorded in the HR system
- Centralized management directory providing
 - Credentials for all users
 - Access control for all IT services
 - Base data for authentication services (including the norwegian federation)
 - Updates for IT systems used throughout the University



The problem

- People affiliated to educational institutions travel around (hopefully) acquiring knowledge
 - This is good but challenging for the IT service providers at the institutions
 - Federations are to solve this, but while we are waiting we need to do something else. And, not all the problems will be solved with federations.



Guest users, who are they?

- For now, we have managed to identify three major categories of guests:
 - Guests in need of short-lived credentials
 - Long-term guests
 - Aliens :-)



Short-lived credentials

- Typically people attending conferences or given lectures
- Our “research” indicated that they needed:
 - Network access
 - Printing services
 - Temporary data storage
- Sponsors are usually easy to identify



Long-term guests

- Typically researchers doing field work, working on short-lived projects etc
- We found out that they want:
 - Well, everything
 - Mostly treated as employees
 - Access to most available IT services
 - Access needed for longer periods of time (from one month and up)
 - Sponsors available



Aliens

- These are the really difficult cases, usually people who are allowed to use an office or a study room for a while without having any connection to the University
- We have not found an appropriate solution for them yet, and it seems that Eduroam is fixing the problem for us.



Technology and policy – a fair warning

- Provisioning “guests” is really a policy issue
- Small organizations may make do with a set of registration routines, no new technology needs to be introduced.
- But technology will help you keep track of registrations and make sure de-provisioning is done in a correct and timely manner



Short-lived credentials

- Implemented as a module in the IdM
 - Can be obtained by local IT via the same administration tool used for other administrative tasks
 - Used a lot during conferences, seminars etc
- Implementation
 - A pre-created set of credentials with generic user names and automatically produced passwords
 - Pre-created storage (blank home directories)
 - Owned by a restricted group
 - Limited validity
 - A set of reports is implemented to help keep track credentials in use



Implementation

- At request local IT registers who is using the credentials
 - The ownership of the credentials is temporarily given to the organizational unit where the request came from (via an appropriate group)
 - The access privileges may be extended by the local IT (but there are restrictions to that, local login servers are allowed, while administrative system privileges are not)
- The validity period for the credentials is defined at request-time (default is three days), but it may be extended to 14 days



Implementation

- The credentials have three possible states:
 - Active (in use right now)
 - Quarantined (cannot be issued for a period of time)
 - Inactive (may be used)
- If the “pool” of the available credentials is empty (all the credentials are in use or quarantined) a warning is issued to the service administrators (that would be us :-):
 - The pool may be expanded by the service administrators



Implementation

- Several reports are implemented and statistics are produced to monitor usage of the short-lived credentials
 - Twice a day active-report
 - Nightly quarantined-report
 - Use of temporary credentials per organizational unit
 - Validity period choosen



Implementation

- Administration
 - With exception of request procedure and the expansion of the credentials set everything happens automatically
 - When the validity period for a set credentials is over the home directory is wiped (after backup) and the password is reset
 - This backup troubles us a whole lot
 - After 40 days all the extra privileges are removed, the backup of the home directory is deleted and the credentials are released for use



Does it work?

- This service has been in use for about four years
- General it does work very well
 - Low maintenance costs
 - Easy to use
 - Easy to monitor
 - Easy to administer
- But there are some problems
 - We allow local IT to request several sets of credentials in one go (up to any number sets available). This makes it a challenge to register who is using the different credentials.
 - We have had problems related to guests coming back and asking for the data they stored after the validity and quarantine period is over



Long-term guest credentials

- Implemented as a part of the IdM
- More procedural than technical
- More complicated



How does it work

- The IdM system is a support system for this service, and most of the implementation is actually reuse of the functionality connected to person data management
- Guests are registered as any employee would be with the exception:
 - Employment data
 - Affiliation



Registration process

- The sponsor contacts personell administration officers locally and information about the guest via a webinterface
 - Name
 - Date of birth
 - NIN (if one is present, otherwise a fake but a uniq one will be provided by the HR-system)
 - Duration of stay
 - Reasons for registration
 - Any special needs (but we have not used this yet so we don't really know how it will work :-))



Maintenance and deprovisioning

- An expire date corresponding with the last day of the stay registered in the HR system is registered in the IdM (and updated if changed in the HR system)
 - 90 days before this date is reached a warning is sent to the guest as well as to the local IT
 - Another warning is sent 30 days before expiration as well
- If no action is taken by the guest or sponsor:
 - The credentials are invalidated seven days after expiration date
 - All access privileges are removed
- The home directory is backed up and removed after a while and the guest is gone



Does it work?

- The service has been in use for around 4 years
- It does work to a degree
 - We can use mostly the same automatic procedures to properly maintain the credentials (we use the same procedures for our ISP service)
 - Sponsoring is real easy for the faculty (most work is done by staff)
- There are some challenges:
 - Time (it may take a few days to get the person registered)
 - The registration process is complicated
 - Higher support load locally (well, they get to deal with more users)
 - Restricted access to administrative systems can be a problem