The new Account Management
Identity, Authentication, Authorization Policies

ACCU

March 9, 2010

IT-OIS
Account Management
What’s new?

• On 22 November 2010, a new Account Management system was introduced
  – Replacing old CRA system
  – Introduced new policies and concepts

• Next objectives
  – Medium to long term: policies review
  – Procedures are being adapted, optimized and reviewed
  – Massive cleanup of data and rules being done
  – Consolidation of all the services involved
## IAA Definition

<table>
<thead>
<tr>
<th>Answer the questions</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>“Who are you?”</td>
</tr>
<tr>
<td>Authentication</td>
<td>“Ok, how can you prove it?”</td>
</tr>
<tr>
<td>Authorization</td>
<td>“What can I do?”</td>
</tr>
</tbody>
</table>

- **Identity:**
  - Human Identity: FOUNDATION (GS/AIS)
  - Computer Identity (accounts): FIM (IT/OIS)

- **Authentication:**
  - Active Directory, Kerberos, Single Sign-On, LDAP, SOAP (IT/OIS)

- **Authorization:**
  - E-Groups to maintain access control lists (GS/AIS)
Account Model

Account types

- **Primary account**
  - Automatically created
  - Call Service Desk to enable

- **Secondary account**
  - *Belongs* to the user
  - Deleted when the user leaves CERN

- **Service account**
  - *Assigned* to the user
  - Can be *reassigned*
  - Reassigned to supervisor when user leaves CERN
End-User Perspective

What’s new?

• **Actions are either Automated or Self-Service based**
  – The end-user connects to a **Self-Service Web Portal**

• **User Arrival**
  – The Primary account is automatically created
  – First activation through Service Desk
  – Follow course and sign OC5 security rules within 5 days maximum

• **Account Management**
  – Users can create and manage **optional** Secondary and Service accounts through the Web Portal
  – Ownership of Service accounts can be transferred
    • to avoid orphan accounts

• **Service Management**
  – Service Management Web page presents to the user a global view of:
    • the computing resources he owns,
    • the list of services he has subscribed to
    • and the available options for each of them

• **User Departure**
  – Service accounts are reassigned to the supervisor - if the user has not reassigned them proactively.
  – Account disabled 2 months after departure, deleted after 6 months
## Operating Systems & Information Services

### User Experience

**Self Service tools**

[Image of a computer screen showing an account management interface with sections for personal details, account properties, and account tasks.]

#### Account Management

<table>
<thead>
<tr>
<th>Personal details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emmanuel Ormancey</td>
</tr>
<tr>
<td>Group</td>
</tr>
<tr>
<td>Team Leader</td>
</tr>
<tr>
<td>Supervisor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account</td>
</tr>
<tr>
<td>Emmanuel Ormancey</td>
</tr>
<tr>
<td>ormancey</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emmanuel Ormancey</td>
</tr>
<tr>
<td>svcn18</td>
</tr>
<tr>
<td>adormin</td>
</tr>
<tr>
<td>adfssrv</td>
</tr>
<tr>
<td>Emmanuel Ormancey</td>
</tr>
<tr>
<td>svcnt01</td>
</tr>
<tr>
<td>svcn1h</td>
</tr>
<tr>
<td>Emmanuel Ormancey</td>
</tr>
<tr>
<td>svcnt01</td>
</tr>
<tr>
<td>svcnt01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADFS SqReplication</td>
</tr>
<tr>
<td>adfssvre</td>
</tr>
<tr>
<td>CERNCA ServiceAccount01</td>
</tr>
<tr>
<td>svcn01</td>
</tr>
<tr>
<td>CERNCA ServiceAccount02</td>
</tr>
<tr>
<td>svcn02</td>
</tr>
<tr>
<td>HyperV ServiceAccount01</td>
</tr>
<tr>
<td>svcn1h</td>
</tr>
<tr>
<td>VMV ServiceAccount002</td>
</tr>
<tr>
<td>svcn02</td>
</tr>
<tr>
<td>VMV ServiceAccount003</td>
</tr>
<tr>
<td>svcn03</td>
</tr>
<tr>
<td>Xidap ServiceAccount</td>
</tr>
<tr>
<td>svcx01</td>
</tr>
<tr>
<td>YukserviceAccount</td>
</tr>
<tr>
<td>yukserv</td>
</tr>
</tbody>
</table>

#### Create a new account

**Account type:** Secondary

To create a secondary account you only need to provide a login name.

**Login name:** [Input field]

[Create button]
Account Management

Change or Reset CERN Account password
This operation will change the specified CERN Account password, and the operation is immediately effective on CERN Account based services.
To avoid errors you are asked to enter your current password. Please note that this operation cannot be reversed and all usage is accounted. This form will also change the APSS/PLUS password at the same time.

User name: ormancay
Reset password:
Current password:
New password: **********
Confirm new password:
Strength:
Password strength validation: Weak
For your password to be accepted, it must match the following criteria:
- Minimum 8 characters in length
- Contains at least 3 of the 4 categories of characters:
  - Lowercase letters (a, b, ...)
  - Uppercase letters (A, B, ...)
  - Numbers
  - Symbols (For example: !@#$%
- I confirm that I have read and understood the Computing Rules
  (http://cern.ch/ComputingRules)

EDH Signature (AIS Authorization) password
The EDH Signature password, also called AIS Authorization password, is a specific “signature password” which is not the same as the CERN Account password for security reasons:

Change AIS Authorization password.

Password hints
For more information about the CERN Computing Rules and a safe password choice, please read the password rules help page here:

Otherwise, here are some suggestions unique to this page of safe passwords that you can use:

- Wire-Bama
- Phukul00
- Ceceleke3
- Niu-Tone
- Tuxa21
- ZeruiRule4
- Siku-Kiga
- Huputa70
- Nikuhagul
- Beme-Xiki
- Mikro88
- KulMoju9
- Zabe-Zia
- Tangul02
- FineKudu0

Last update: March, 2011 - Contact: servicedesk@cern.ch
### Windows Desktops

The Windows desktop service provides support for managed Windows desktops and laptops at CERN using the HPC infrastructure. This provides a consistent environment through which Windows users at CERN can obtain resources, applications, and managed operating system services.

#### Service common properties

- **Automatic Subscription:** True
- **Associated E-Groups:** WindowsDesktops-Denied-Users (denied users)
- **Home Page:** [http://cern.ch/winservices](http://cern.ch/winservices)

#### Service personal properties for account ormancay

**Home Directory**
- **Home directory folder:** /users/ormancy
- **Quota:**
  - **2560 MB (2.50 GB)**
  - **1800 MB (1.8 GB) used**
- **Increase Quota To:**
  - **3072 MB**
  - [Request]

**Folder Redirection**
- **Desktops:** /users/ormancy/Desktop
- **Favorites:** /users/ormancy/Favorites
- **My Documents:** /users/ormancy/Documents

**Remote Assistance**
- **Can offer remote assistance:** true

**Password-protected Screen Saver**
- **Is enforced:** true

Last update: March 2011 - Contact: servicedesk@cern.ch
• Computing Groups were migrated to E-Groups
  - Specific Unix/AFS groups
• Group administrators decide how to manage their groups:
  - Static membership
  - Dynamic criteria
  - Both (nested groups)
Multiple Computing Groups
New Feature

Users changing Experiment was not easily covered by the old system

- **Users can now be member of several computing groups**
  - When working on several Experiments
  - No need to create many secondary accounts

- **Tools now allow easily to change the primary Computing Group**
  - Permanently, the old remains available anytime
  - Temporarily
Users’ departure policy

- When a user’s contract ends + 2 months:
  - Primary and secondary accounts disabled
  - Same policy for everyone
  - Decreasing to 1 month will increase security

- Supervisor can ask for an extension to the Service Desk
  - Such a Blocking Exception should become a new HR feature / status (investigation in progress)

- Decrease exceptions
  - Understanding the need for exception will help to cover them with normal procedures.
A few numbers to conclude

- Total: 42264 Accounts
- Since FIM started on 22 November:
  - 876 Accounts activated
    - Primary : 555
    - Secondary : 118
    - Service : 200
  - Primary Accounts activated per month (new persons):
    - November 2010 : 51
    - December 2010 : 112
    - January 2011 : 199
    - February 2011 : 162
    - March 2011 : 111
Questions?