

**Virtual Directory Services
for Web Access Management
with RSA Cleartrust**

at Ringier AG / Zürich

Gerald Kaufhold, KOGIT GmbH, Germany

Authentication and Authorization for RSA and SAP with Radiant One Virtual Directory Server

Team

- Customer



- RSA Implementation



- VDS Implementation



Company profile

- Ringier AG is a worldwide acting media company (Print, TV, NewMedia)
- Ringier has a Swiss-based IT department (about 5000 users) and has due to M&A many subsidiaries in different countries (each up to 5000 users)
- Each country has an independent IT department
- There exists no global directory

Business needs

- WW Corporate Portal (Intranet)
- Reduced SignOn
- Consolidation (Content, Data, User)
- Smooth integration of IT-Ressources

Architectual Reqs.

- For authentication/authorization (SSO) of internal web portal and other applications, Ringier choosed RSA Cleartrust
 - RSA Cleartrust needs one central directory
- For authorization of internal SAP web portal Ringier needs one central directory
 - SAP uses one directory configuration.
- Different locations uses Microsoft Active Directory, Novell eDirectory and some OpenLDAP
 - The solution must handle all kinds of directories from various vendors

Options

- A meta directory approach
 - Build up a central directory and synchronize the existing directories with the new one
 - Use one existing Active Directory and synchronize the existing directories of the subsidiaries into that Active Directory
- A virtual directory approach
 - No synchronization at all
 - Use a cache and synchronize this cache with the existing directories

Why Radiant One?

- Virtual Directory with the highest out-of-the-box functionality
- RSA recommends Radiant One
 - No changes in RSA
- No changes in existing directories
- No changes in SAP
- Support of all existing directories at Ringier

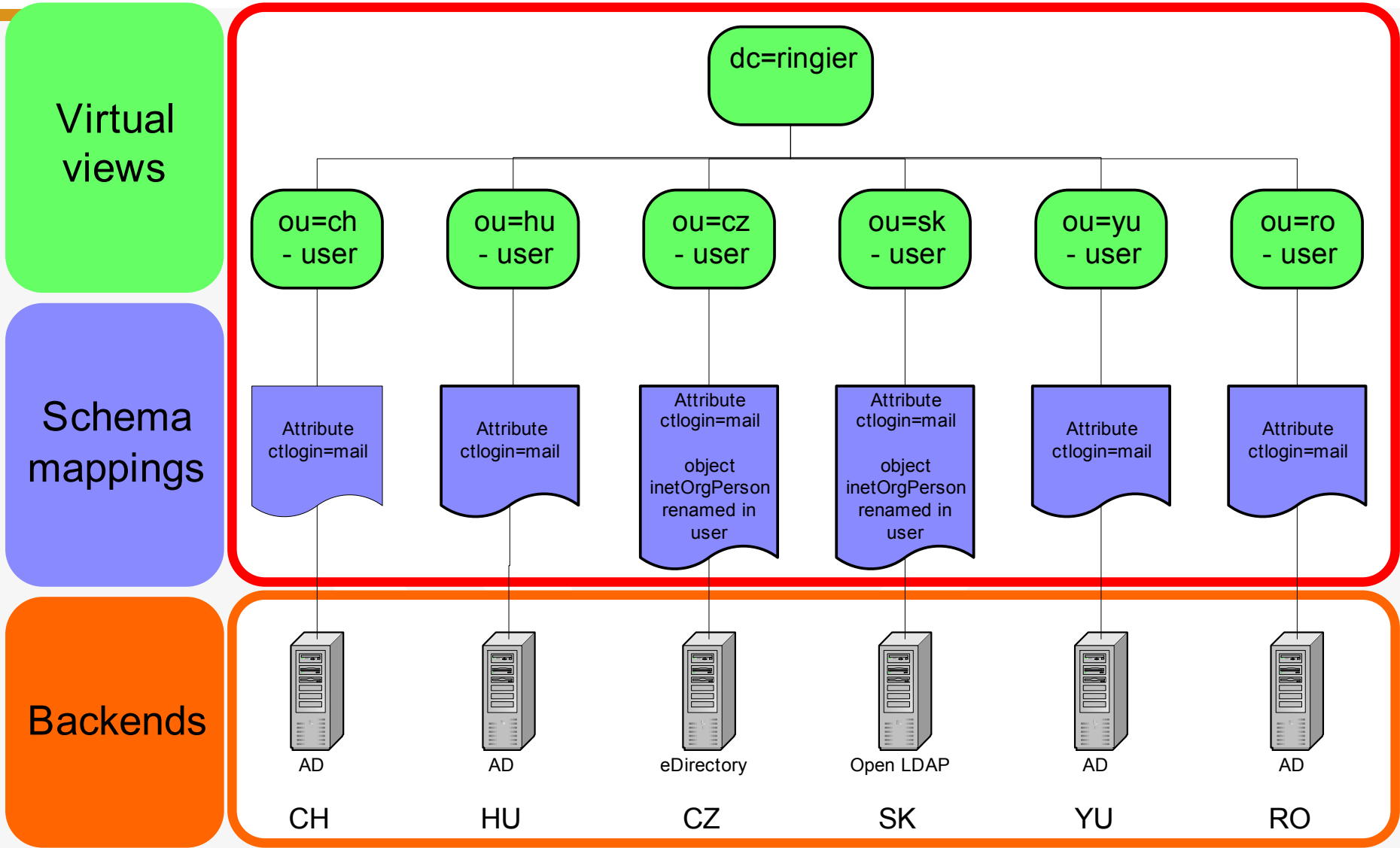
Project steps

- Configuration of virtual views of the subsidiaries directories to act as flat user repositories for RSA Cleartrust
- Extending the virtual view, to also act as a flat user repository for the internal SAP portal
- Setting up a cache for the virtual views
- Setting up a cache refresh with the ICS server functionality

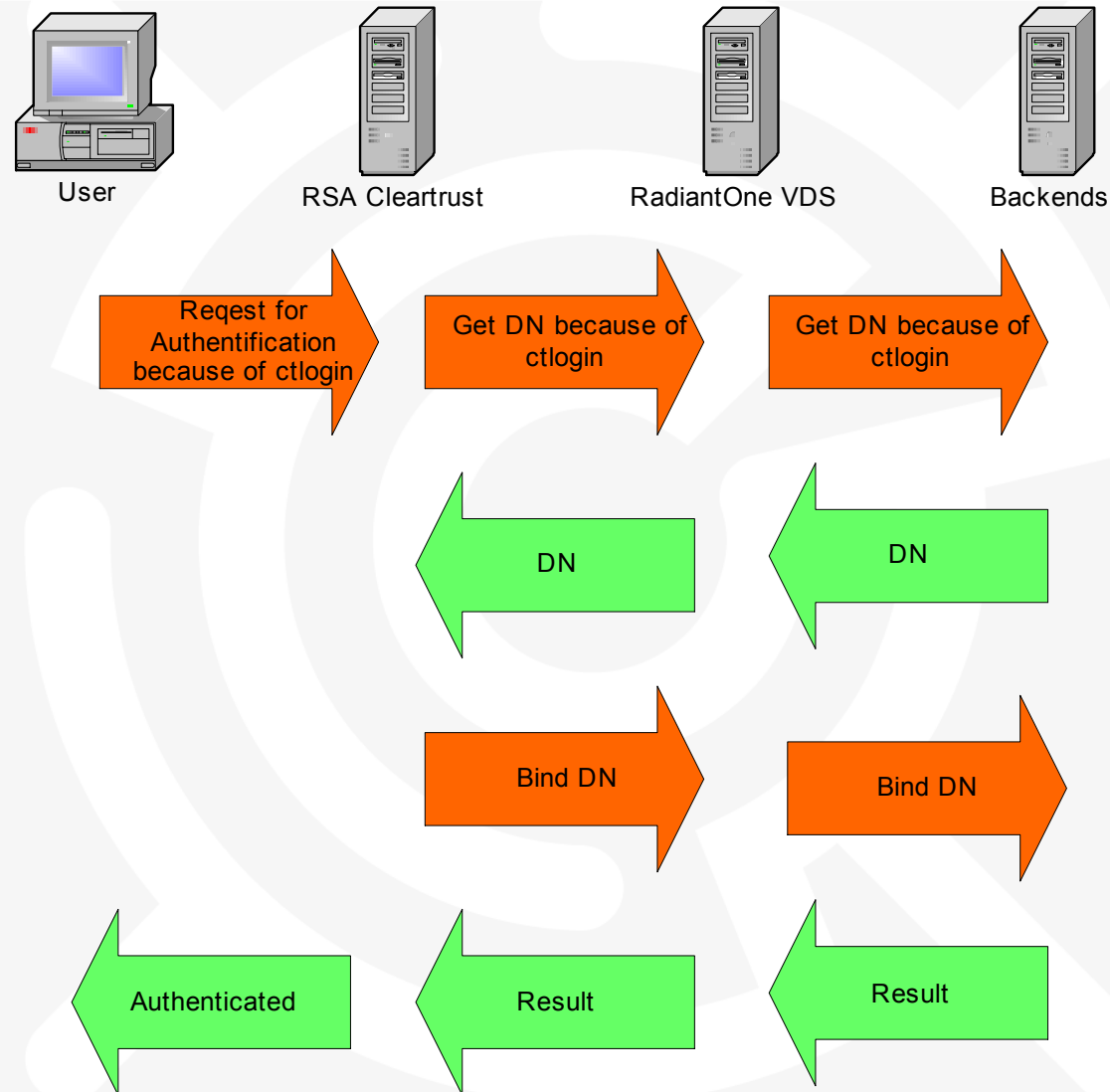
Step 1: Virtual flat user repository for RSA Cleartrust

- The RSA team created a LDAP store inside the VDS for the RSA internal configuration
 - They used the documentation from the RadiantLogic webpage
- Virtual views of the user objects of each directory were created
- For Novell eDirectory and Open LDAP the object names were mapped to the Microsoft Active Directory names
- One attribute was added to all user objects in each country for enabling RSA to find the user in the directory
- One central view was created, that has a link for each virtual user object

Configuration context RSA



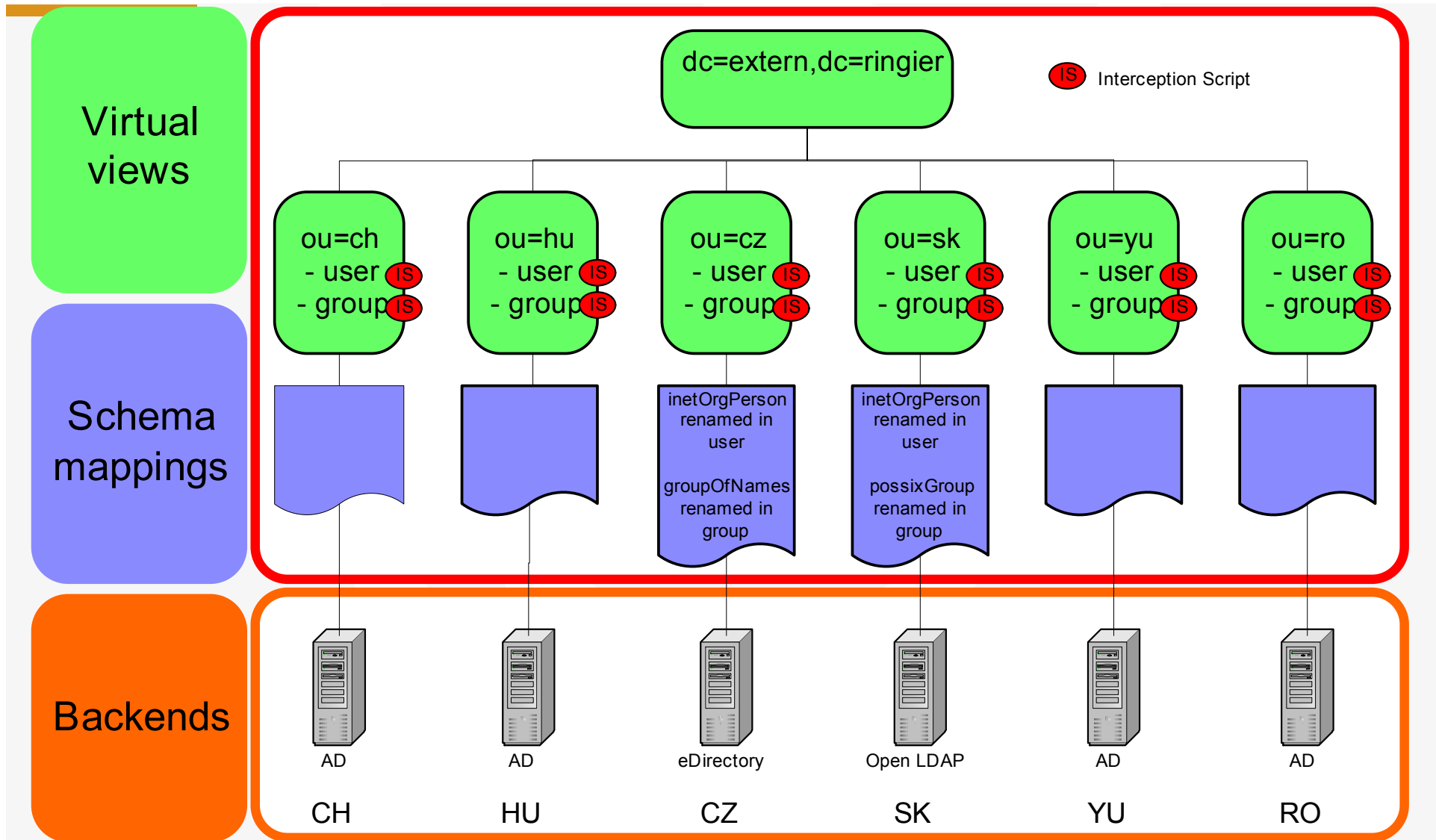
Workflow authentication



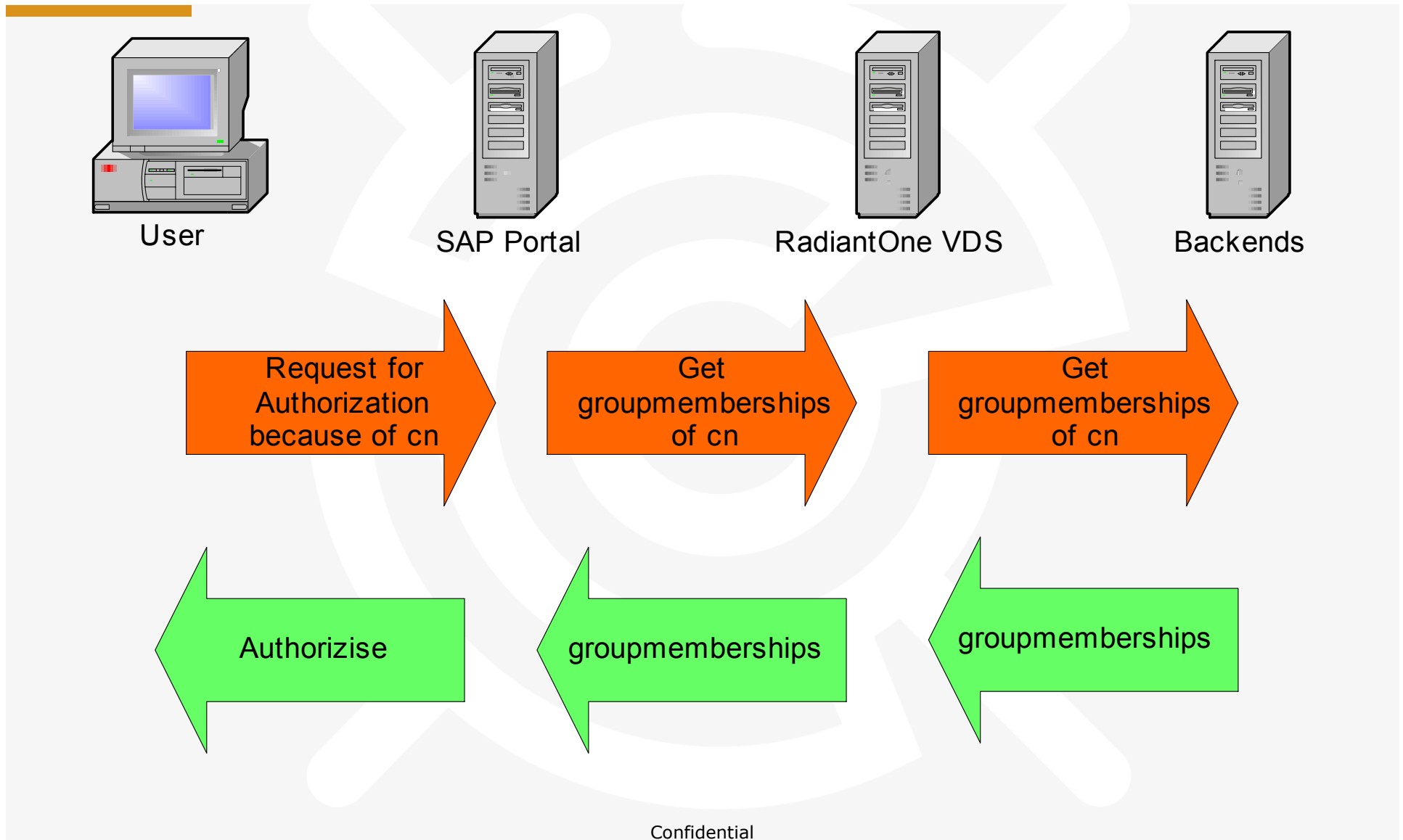
Step 2: Extending the virtual view, for the internal SAP portal

- Creation of virtual views for group objects of each directory
- Configuration of these virtual views as links into the central view
- Creation of interception scripts
 - Link users and groups correctly
 - Comply to the SAP interface specification
 - Let eDirectory and OpenLDAP behave like a Active Directory .

Customization context SAP



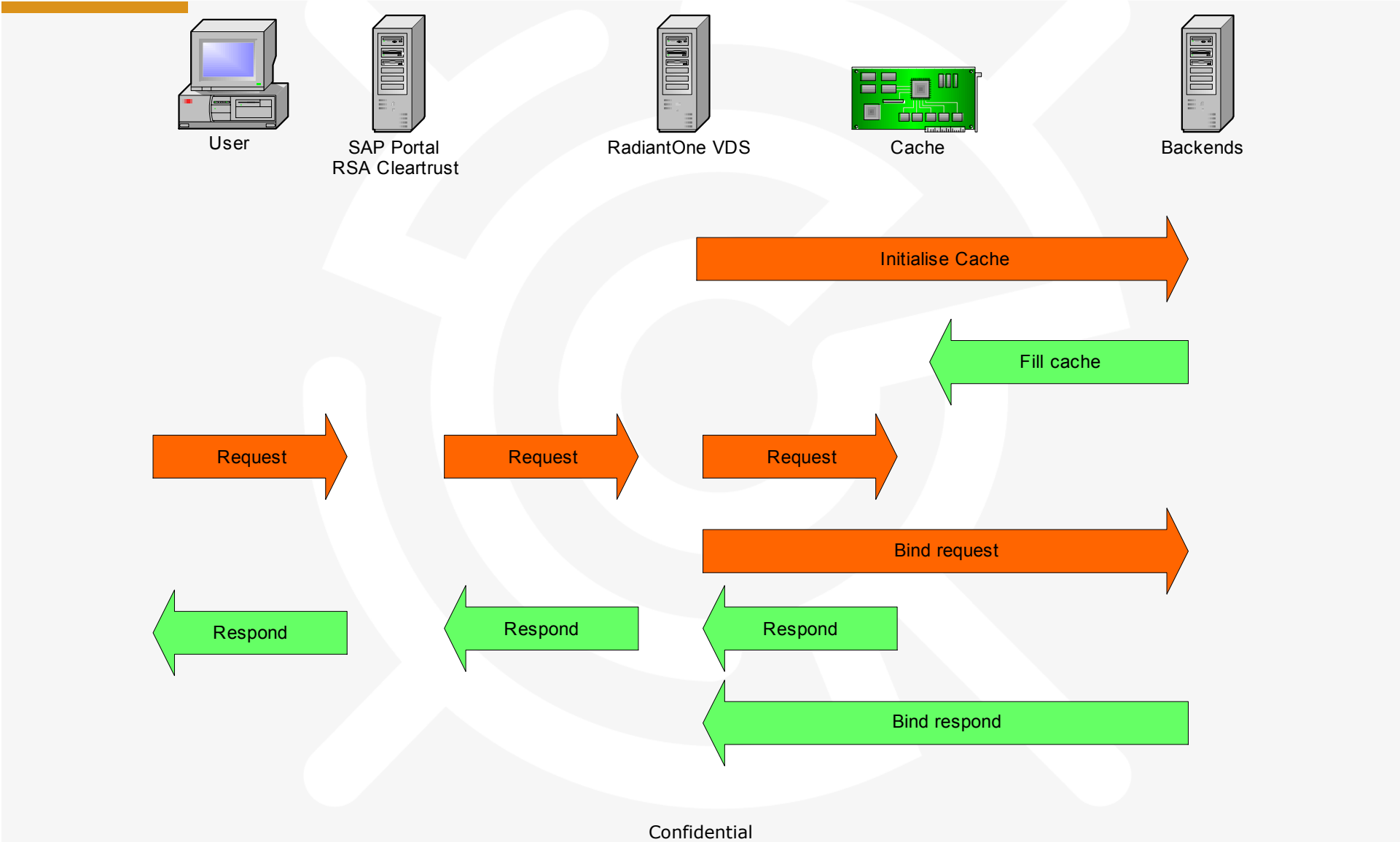
Workflow authorization



Step 3: Setting up a cache for the virtual views

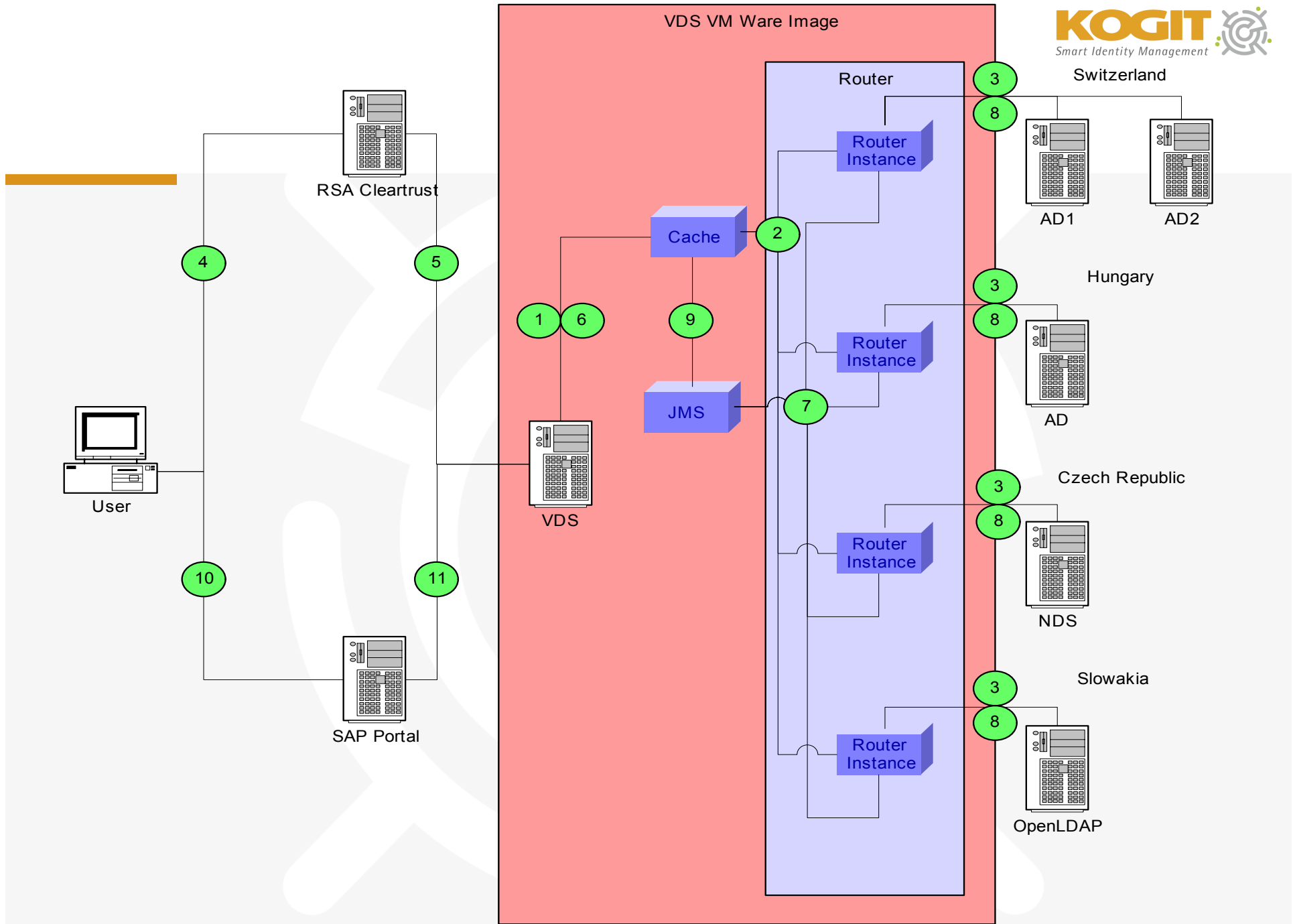
- After the use of Radiant One version 4.5 this feature was out of the box.
- One cache for each directory

Cache



Step 4: Setting up a cache refresh with the ICS server functionality

- To ensure high availability, a fail over scenario was setup
 - One Radiant One router service is running
 - One router instance inside the router service for each directory
- After the use of Radiant One Version 4.5 the creation of the cache refresh logic was a out of the box feature.
 - Customize a transformation script to detect groupmembership changes in AD



Benefits

- No changes in existing directories
 - No communication overhead with the IT departments of the subsidiaries
(overcome political and organizational boundaries)
- Use of out of the box interfaces in RSA Cleartrust and SAP
 - No customization need in these products
 - Less customization by scripting in the product
 - Easy to maintain by customer
- Higher performance in case of Authorization because of the use of a cache compared to connection to each directory directly