Data Separation Reference Implemenation
– Quick Overview of the Solution –

Conclusion

Behavior is analogue to ServiceNow Domain Separation, but:

- pure data separation

- no process deviations

- simplified configuration

- Implementation based on Query Business Rules

- no domain-picker

To be highlighted common features:

- hierarchical domain model

- Contains-Domains (enhances the pure tree-like hierarchy for cross-connections)

- Visibility Groups (allows single user to access more than just their own domain and the domainsbelow the own domain)

Implementation (Basic)

- **1 controlling table (in the menu at System Security → Data Domains)**

- **per data separated (base) table:**
  - 1 Feld (u_data_domain)

  - 3 Business Rules:

    - „Data Domain Query" → *enhance* every Query to include the user's domains

    - „Data Domain Update Checker" → prevent unauthorized manipulations

    - „Data Domain Cascade Domain" → rule to determine the default domain of a new record at creation time

Implementation (reflecting security)

Query Business Rule prevent retrieval of records of foreign domains

**Before Update/Delete Business Rule *additionally* prevent manipulations,
even if a record of a foreign domain was retrieved somehow
(check of the previous recrods, so the before-the-changed-happend, domain field value)**

Therefor no changes/enhancements to ACLs and the role model are neccessary.

changes/enhancements to ACLs wouldn't even be feasible:

ACLs on the same level are OR'd

To project domains to ACLS, *all* ACLs would need a rework

Implementation (Sequence at login / retrieval of a record)

At login time all domains a user has access to are stored in the Session Cache
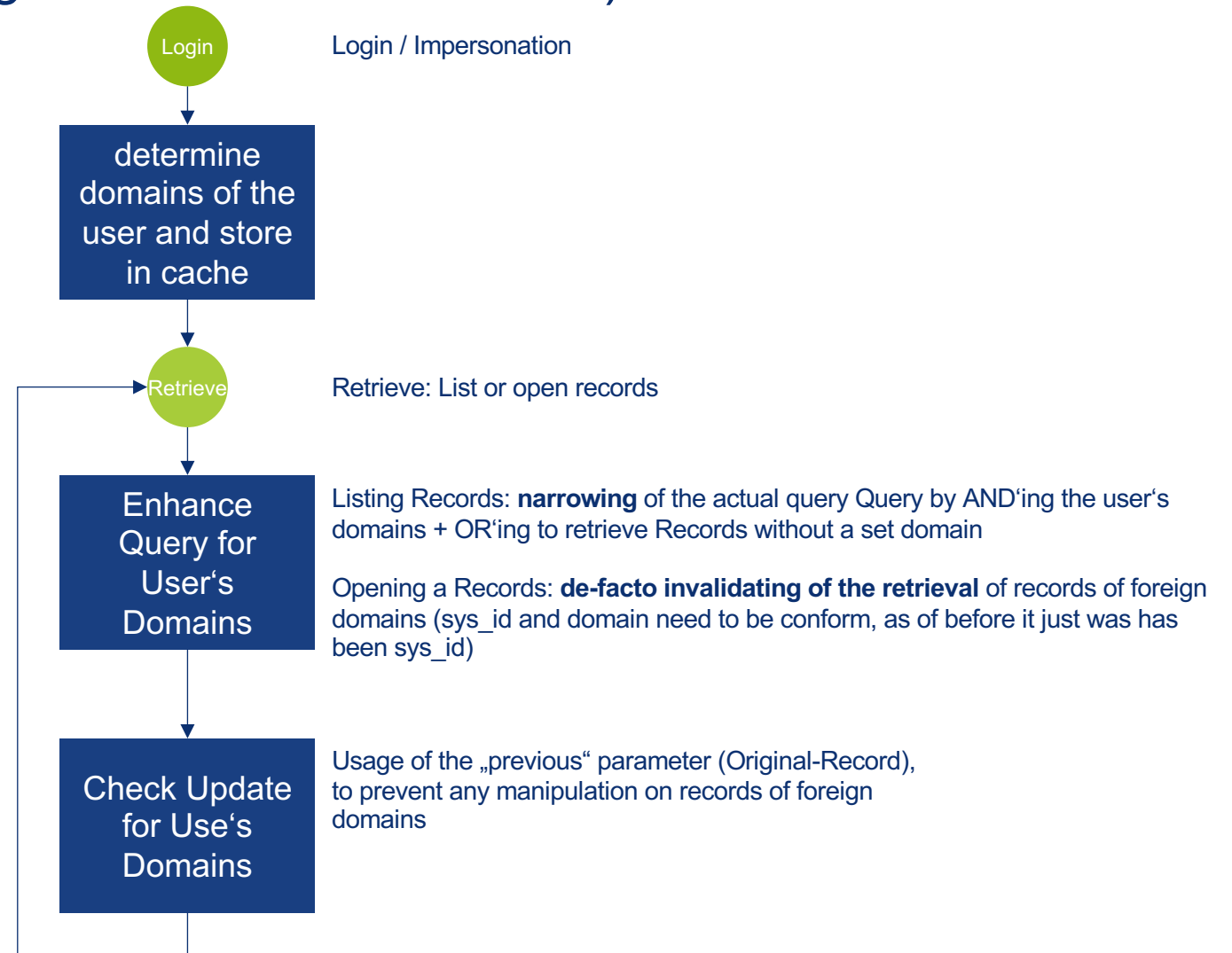
Business Rules are triggering only, if:

User doesn't have the admin role

User has at least one domain

Table is not excluded from separation

Record has a domain set

Business Rules are using the Session Cache (good performance)

Login

Login / Impersonation

determine domains of the user and store in cache

Retrieve

Retrieve: List or open records

Enhance Query for User's Domains

Listing Records: **narrowing** of the actual query Query by AND'ing the user's domains + OR'ing to retrieve Records without a set domain

Opening a Records: **de-facto invalidating of the retrieval** of records of foreign domains (sys_id and domain need to be conform, as of before it just was has been sys_id)

Check Update for Use's Domains

Usage of the „previous" parameter (Original-Record), to prevent any manipulation on records of foreign domains

Thanks for your attention!

Ibrahim-Ben Faruhn

Berlin I Karl-Pokern-Str. 30 I 12587 Berlin

Tel. +49 176 29 47 48 87

hello@cbc-faruhn.com I www.cbc-faruhn.com