



Week 1: What's New in SAP HANA 2.0 SPS 03

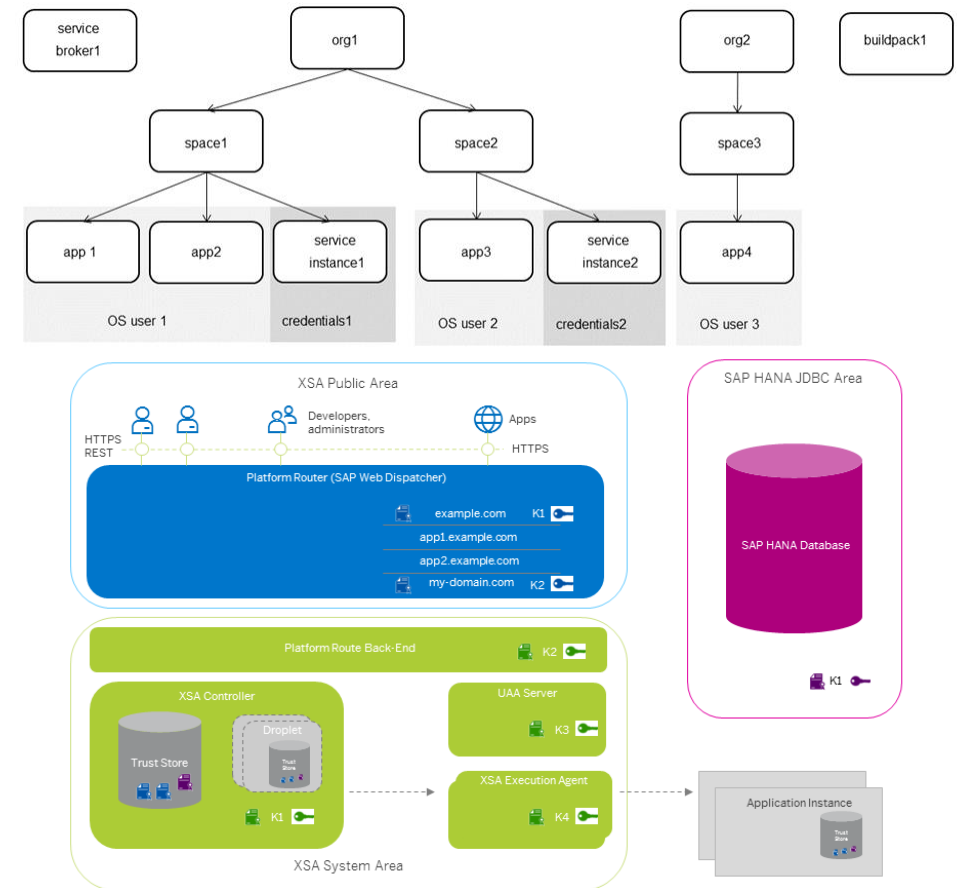
Unit 5: Security Improvements

Security Improvements

Key challenge – Isolation

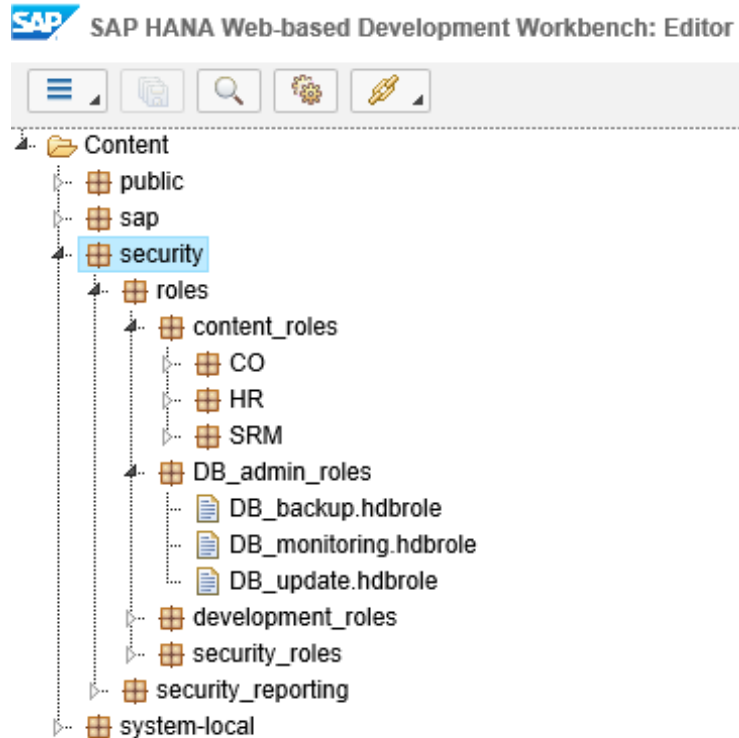
XSA applications can run native code on the server (Node.js, Java) (OS commands, network)

- Application level isolation
 - Based on token infrastructure
- Administration/development isolation
 - Based on orgs and space concept
- Operating system level isolation
 - Based on separate OS users
 - for applications and system components
 - per applications based on orgs/space concept
- Network level isolation
 - Based on system PKI between applications and system components
 - Network separation between application layer and database layer
- Database layer isolation
 - Based on separate HDI containers



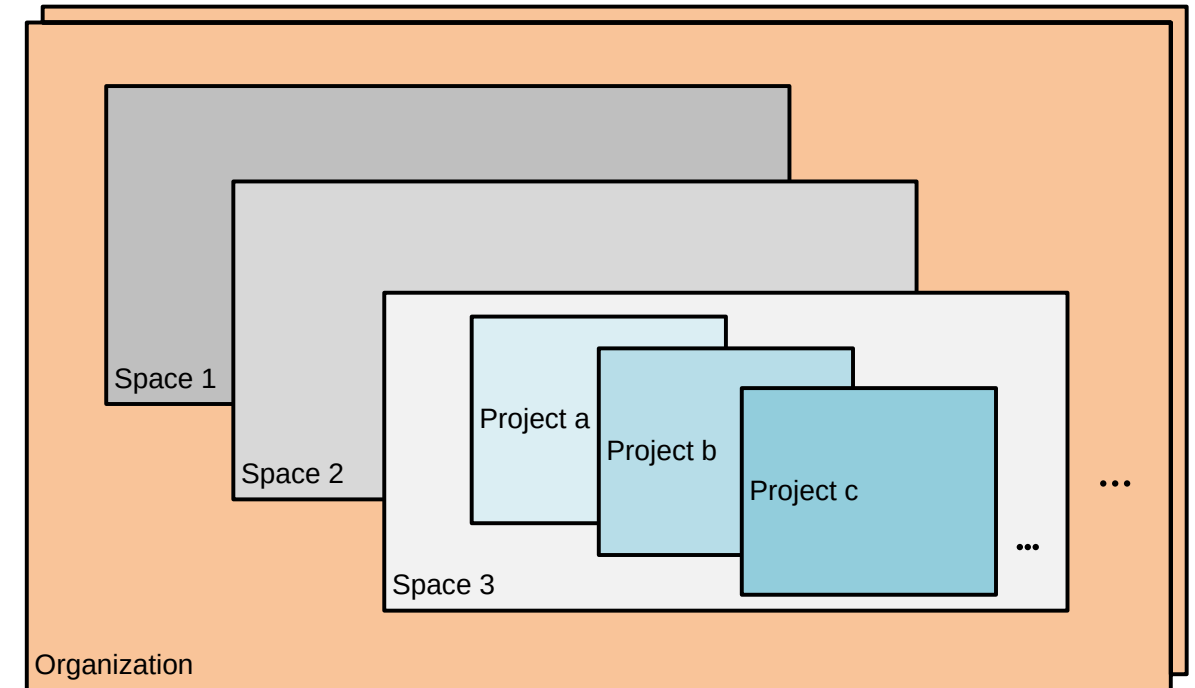
Security Improvements

Application structure XSC vs. XSA



XSC:

- Package structure
- All development shares privileges of `_SYS_REPO`



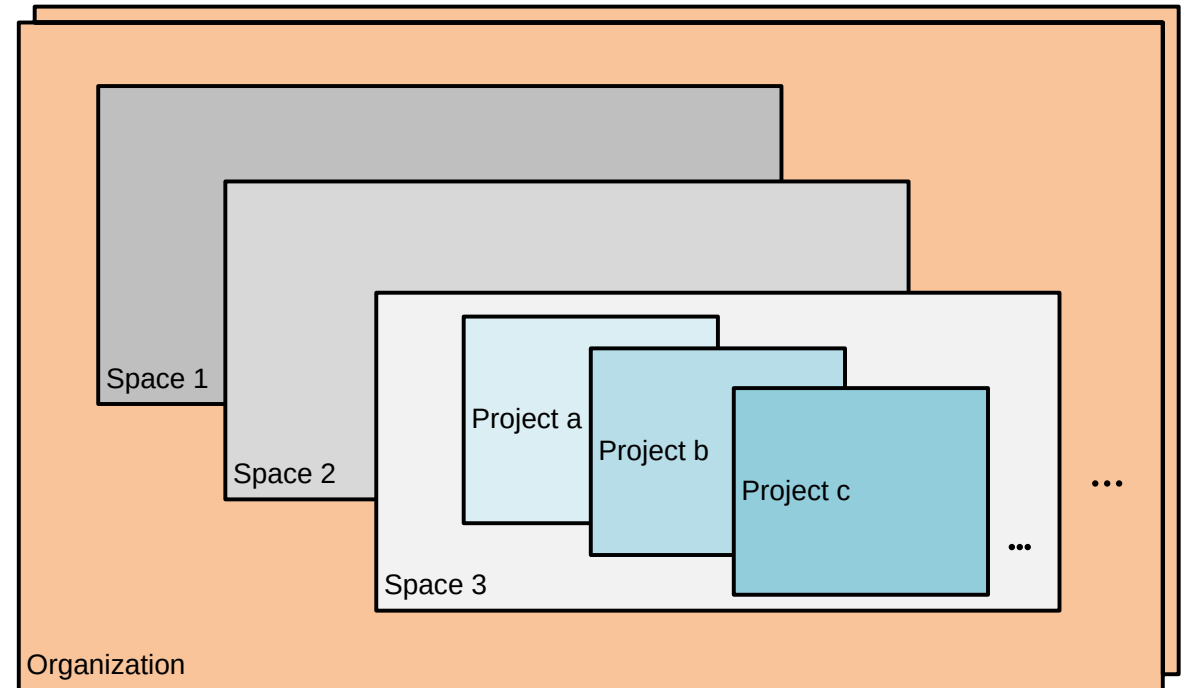
XSA:

- Org-space hierarchy
- Privileges separated by space

Security Improvements

XS advanced – Orgs, spaces, and projects

- Organizations can be used for example to
 - Logically group line-of-business development
 - Logically group security-related development from other development
- Spaces can be used for example to
 - Separate line-of-business development
 - Separate security-related development from other development
 - Separate privileges for role development
- Projects can be used for example to
 - Separate sets of roles for different target systems

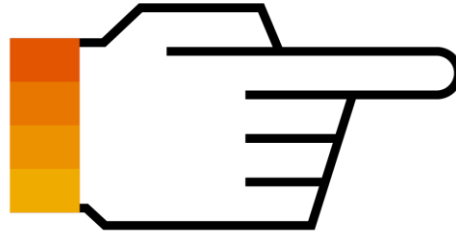


Security Improvements

Names in the new world

XS classic & SAP HANA

- Role
- Application privilege
- Analytical privilege



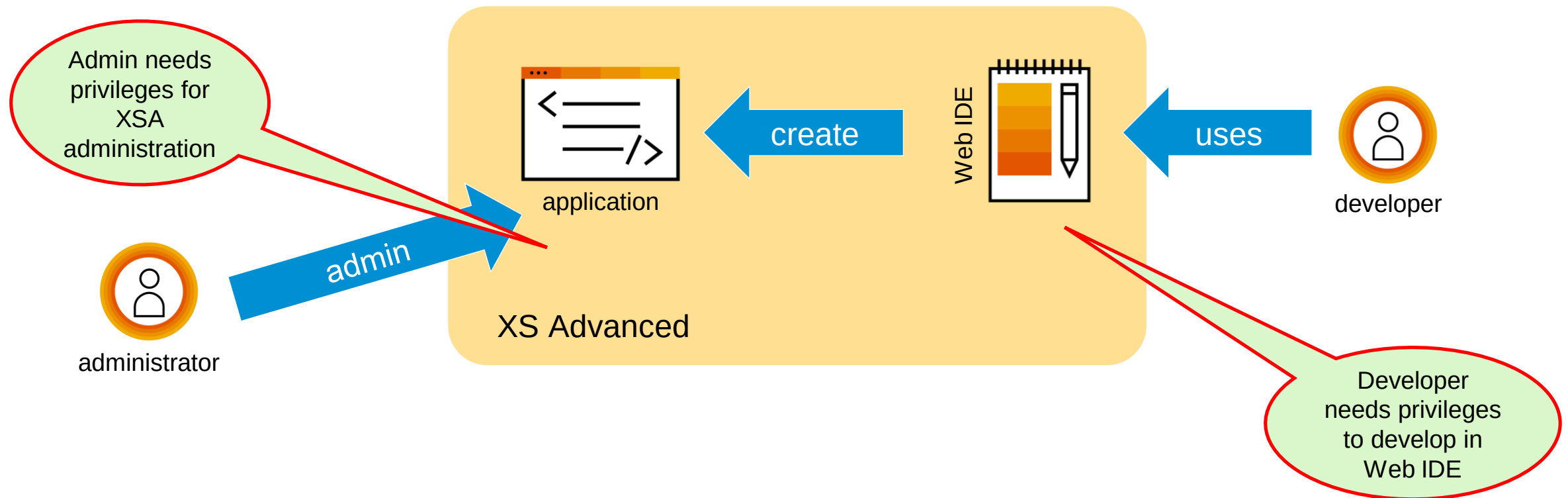
XS advanced

- Role collection / role
 - Scope
 - Attribute
-
- Role collection = role + role + ...
 - Role = role template + attribute value
 - Role template = scope + attribute definition

Security Improvements

Assign XS advanced privileges

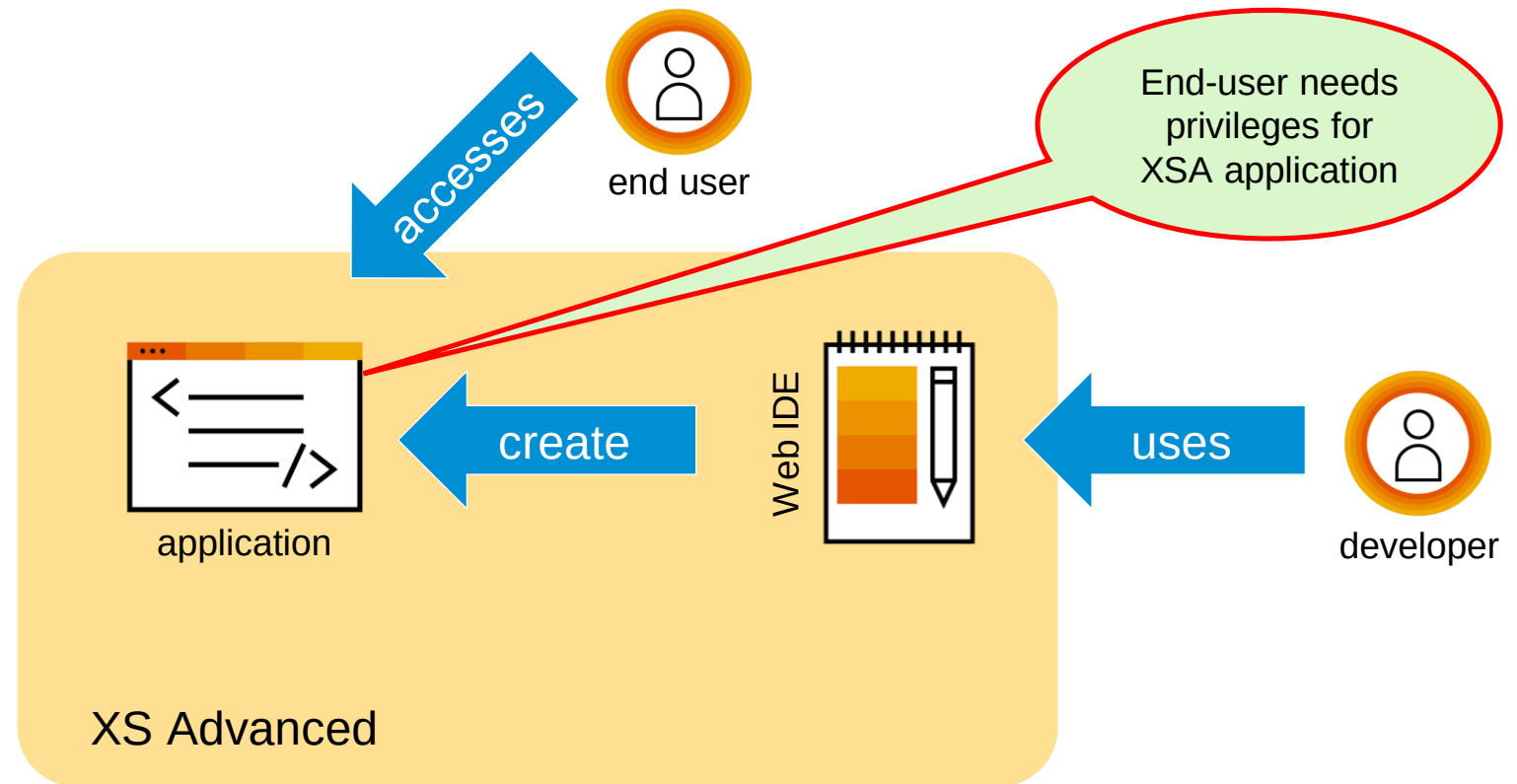
- For XSA administration and XSA Web IDE development, SAP provides predefined role collections
- Role collections have to be assigned



Security Improvements

Create XS advanced privileges

- For XSA applications, end users need to have role collections
- Privileges in XSA applications (created during development)
 - Developer implements scope and defines attributes in XSA application coding
 - Developer creates role templates with scope and attribute definition
- Role administrator builds and assigns role collections
 - Administrator creates roles out of role templates with specific attribute values
 - Different XSA application roles can be combined into role collections



Security Improvements

xs-security.json example

EVENTS APP

ROLE TEMPLATE: "Event Reader"

SCOPE: "Read Events"

SCOPE: "Comment Events"

ROLE TEMPLATE: "Event Manager"

SCOPE: "Read Events"

SCOPE: "Comment Events"

SCOPE: "Manage Events"

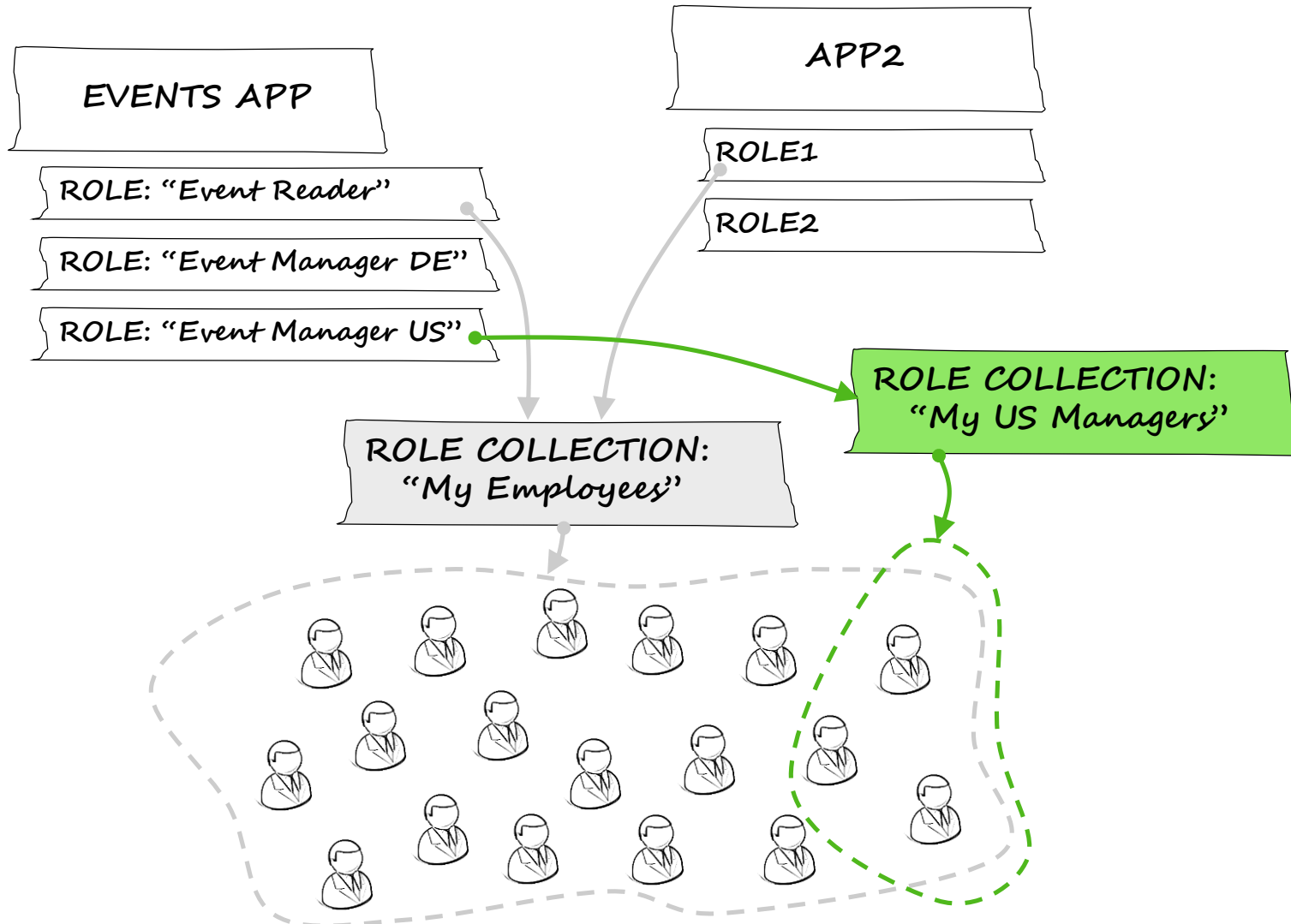
ATTRIBUTE: "Country"

Sample *xs-security.json* File:

```
{
  "xsappname"      : "events",
  "scopes"         : [ { "name"                : "$XSAPPNAME.ReadEvents",
                        "description"          : "Read events" },
                        { "name"                : "$XSAPPNAME.CommentEvents",
                        "description"          : "Write comments for events" },
                        { "name"                : "$XSAPPNAME.ManageEvents",
                        "description"          : "Create new or delete existing events" }
                      ],
  "attributes"     : [ { "name"                : "Country",
                        "description"          : "Country where employees live",
                        "valueType"            : "s"
                      } ],
  "role-templates": [ { "name"                : "EventReader",
                        "description"          : "Template for reading events",
                        "scope-references"     : [ "$XSAPPNAME.ReadEvents",
                                                  "$XSAPPNAME.CommentEvents" ] },
                      { "name"                : "EventManager",
                        "description"          : "Template for managers managing events",
                        "scope-references"     : [ "$XSAPPNAME.ReadEvents",
                                                  "$XSAPPNAME.CommentEvents",
                                                  "$XSAPPNAME.ManageEvents" ],
                        "attribute-references": [ "Country" ] } ]
}
```

Security Improvements

Managing authorizations



An administrator can define **role collections** using the administrative UIs

Multiple roles from different applications can be assigned to a single role collection

Using the SAP HANA XSA cockpit, a role collection can be **assigned** to a **user**

Security Improvements

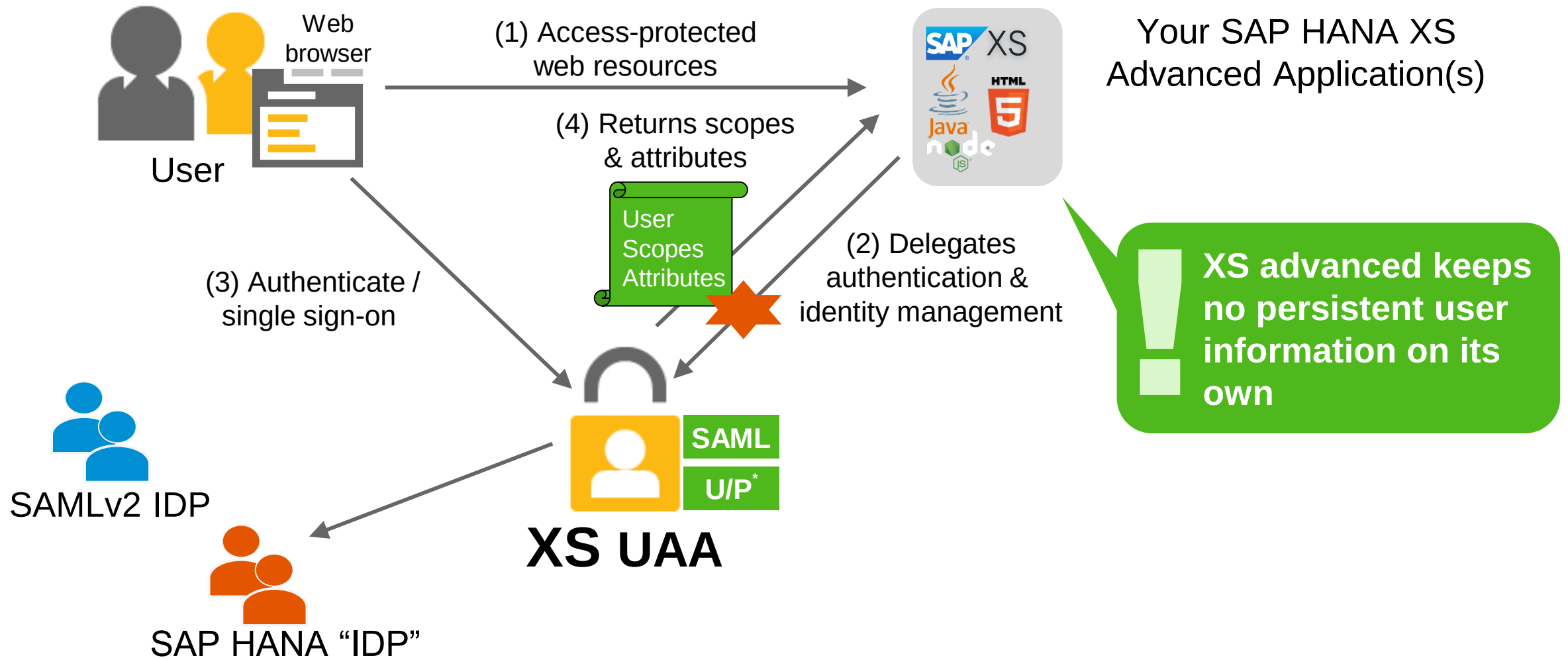
DON'Ts with XSC and XSA

- Don't put XSC roles in XSA roles
- Don't put XSA roles in XSC roles
- Don't use XSC roles to grant privileges to HDI container
- Don't equip XSA administrators with XSC roles
- Don't put XSC application privileges in XSA roles
- Don't use objects belonging to `_SYS_REPO` (repository) for XSA authorizations



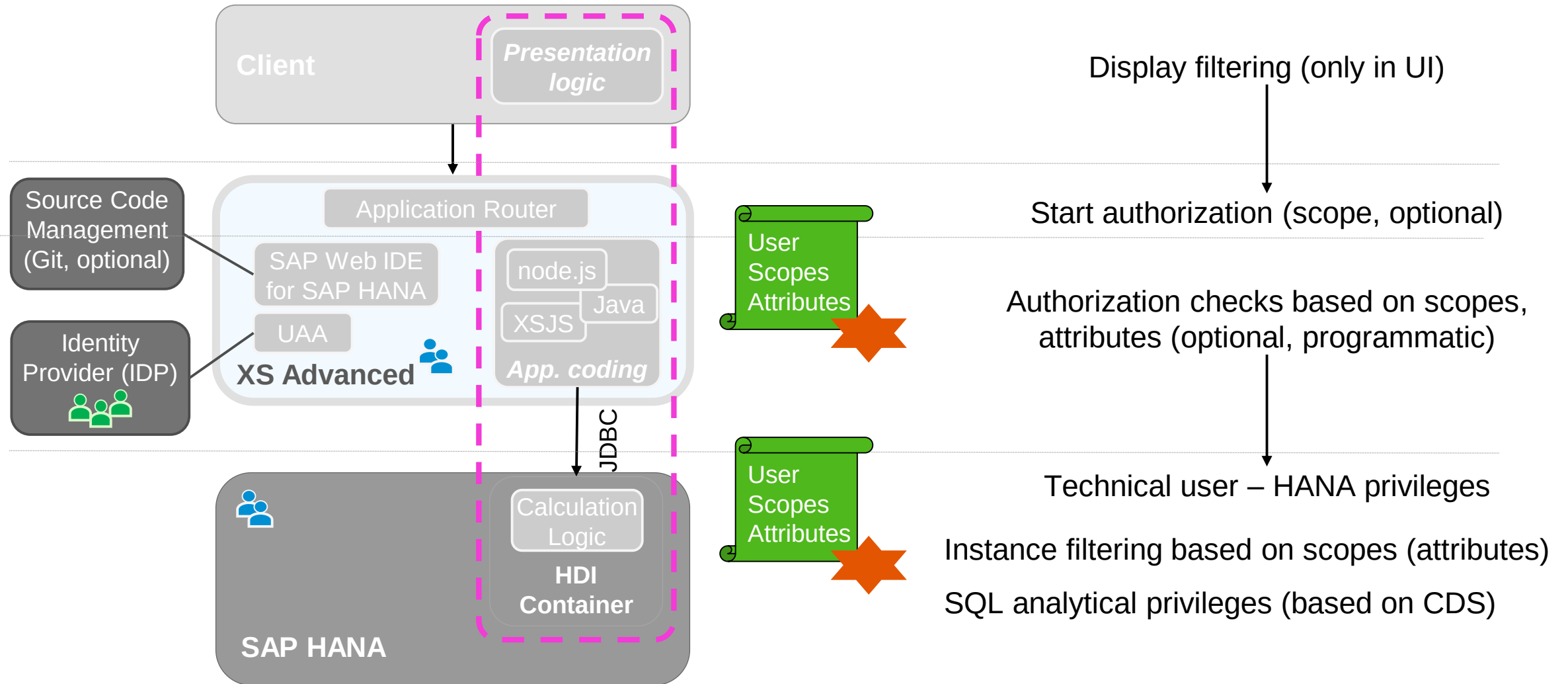
Security Improvements

Federated authentication and SSO in SAP HANA XS, advanced model



Security Improvements

Authorization checks SAP HANA XS, advanced model applications



Thank you.

Contact information:

open@sap.com

Follow all of SAP



www.sap.com/contactsap

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.