ITM115 – UCON – A New Approach to Making Your RFC Communication More Secure

Juergen Adolf PM Platform Products
Martin Plummer PM Platform Products

SAP TechEd && d-code

Public

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Agenda
Unified Connectivity (UCON) RFC Security Basic Scenario

Motivation and Scope

Basic Concepts

The Practice of UCON: Logging and Blocking – Demo

Setup && Configuration

How to handle System Updates

How to Cope With the Restrictions of Productive Systems

Summary

Unified Connectivity

Motivation and Scope

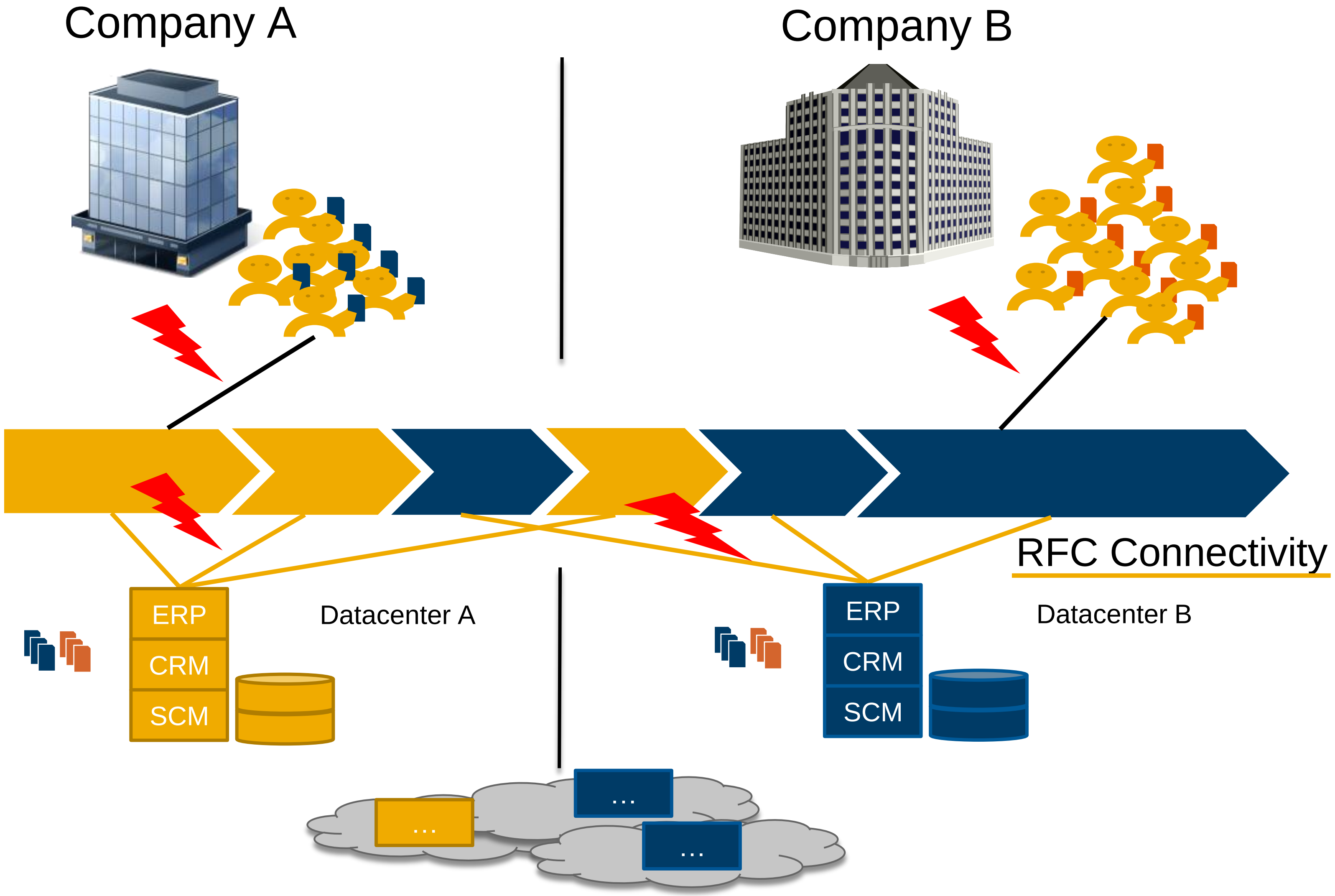
The Scope of UCON RFC Basic Connectivity

Different Companies

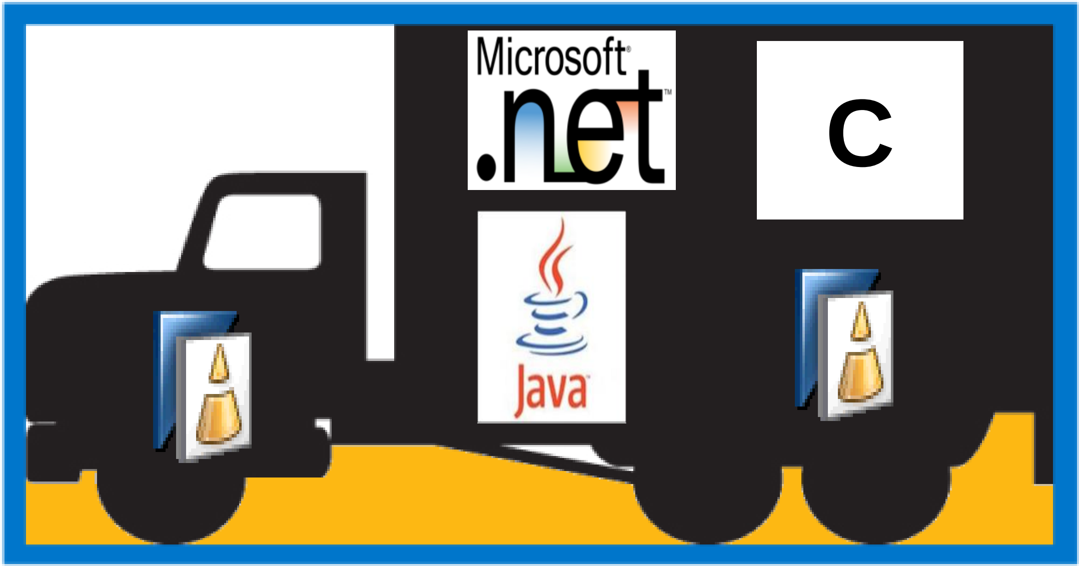
Complex Business Processes

Heterogeneous IT Infrastructures

Cloud



The Scope of UCON RFC Basic Connectivity



High-performing,
for local high load scenarios,
across all ABAP releases,
close integration into ABAP

RFC-Based Connectivity

UCON – A Simple Approach to Make RFC More Secure

Reduce the overall attack surface of your remote-enabled function modules (RFMs). Enhance RFC security by blocking the access to a large number of RFMs!

Facts:

- Most SAP ERP customers run just a limited number of the business (&technical) scenarios for which they need to expose some RFMs
- A lot of RFMs are only used to parallelize within a system

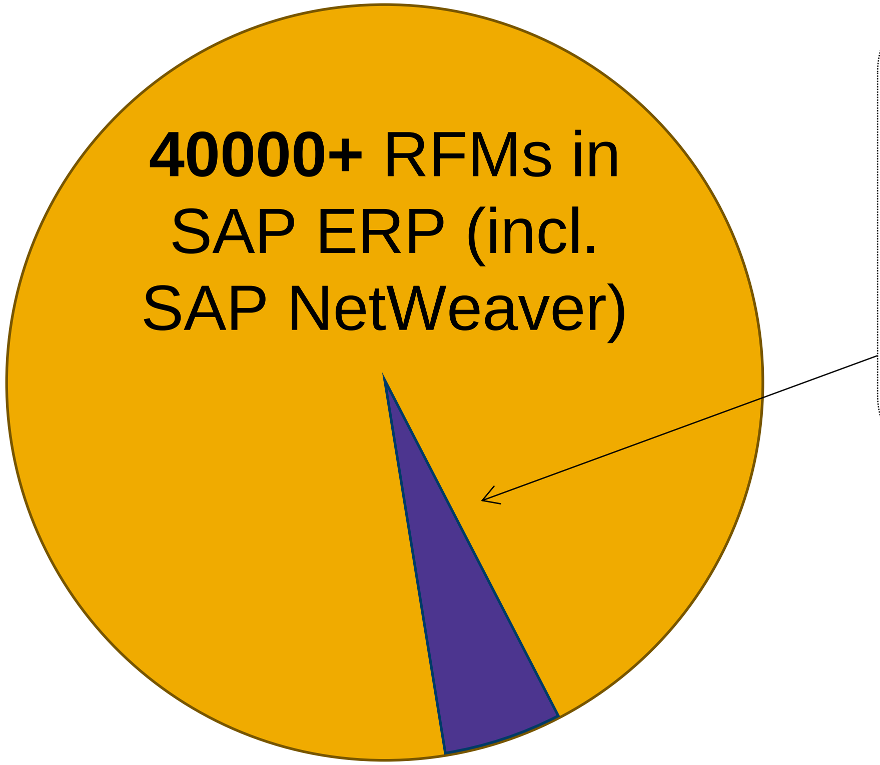
Solution

- Find out which RFMs need to be exposed for the scenarios of a customer
- Block the access to all other RFMs

The Basic Strategy of UCON to Solve These Problems

Reduce the number of RFMs exposed to the outside world

Expose only and exactly those RFMs a customer needs to run their business scenarios



40000+ RFMs in SAP ERP (incl. SAP NetWeaver)

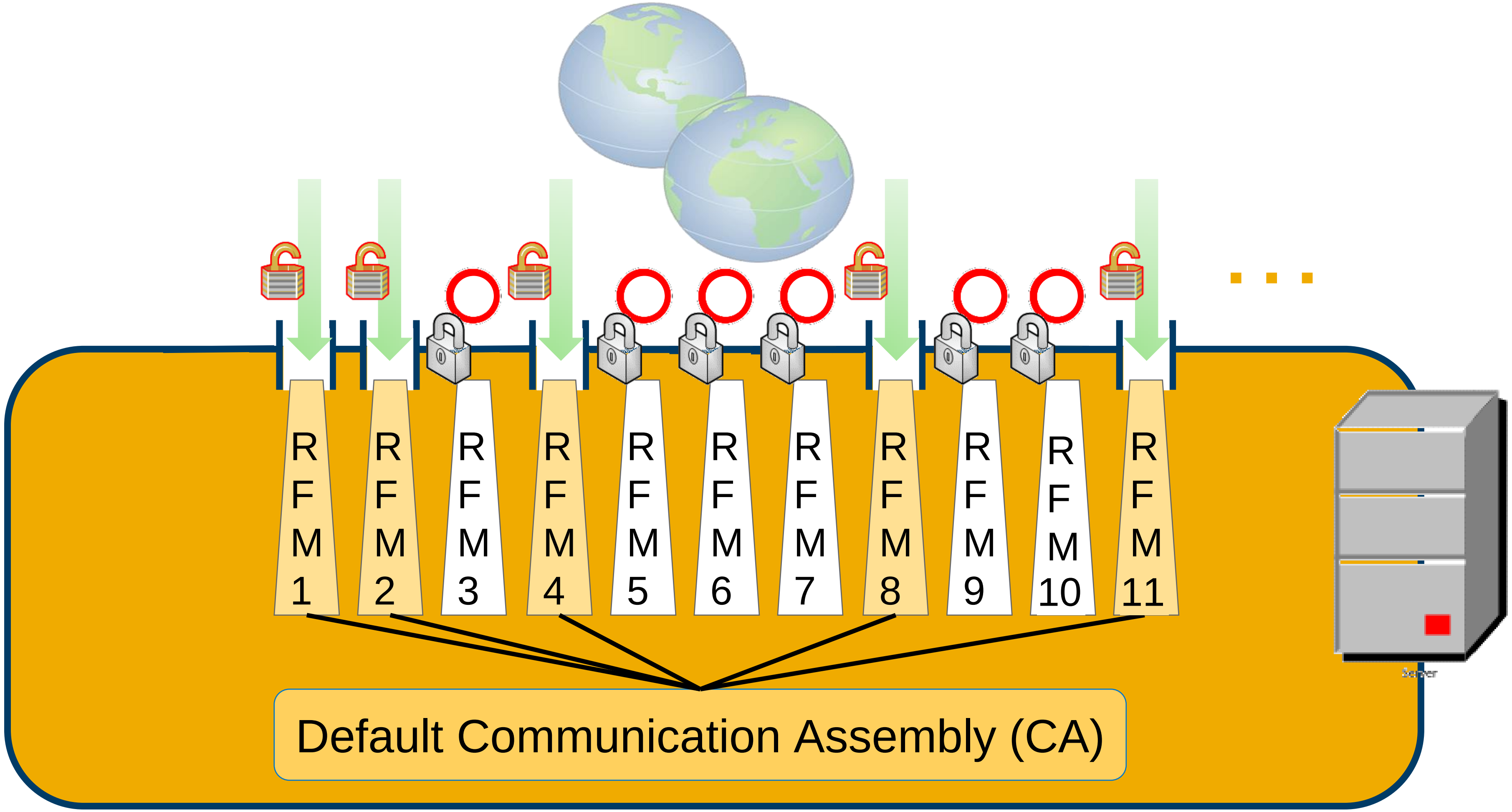
A typical SAP customer only needs to expose a **few hundred** RFMs for their business scenarios

Unified Connectivity

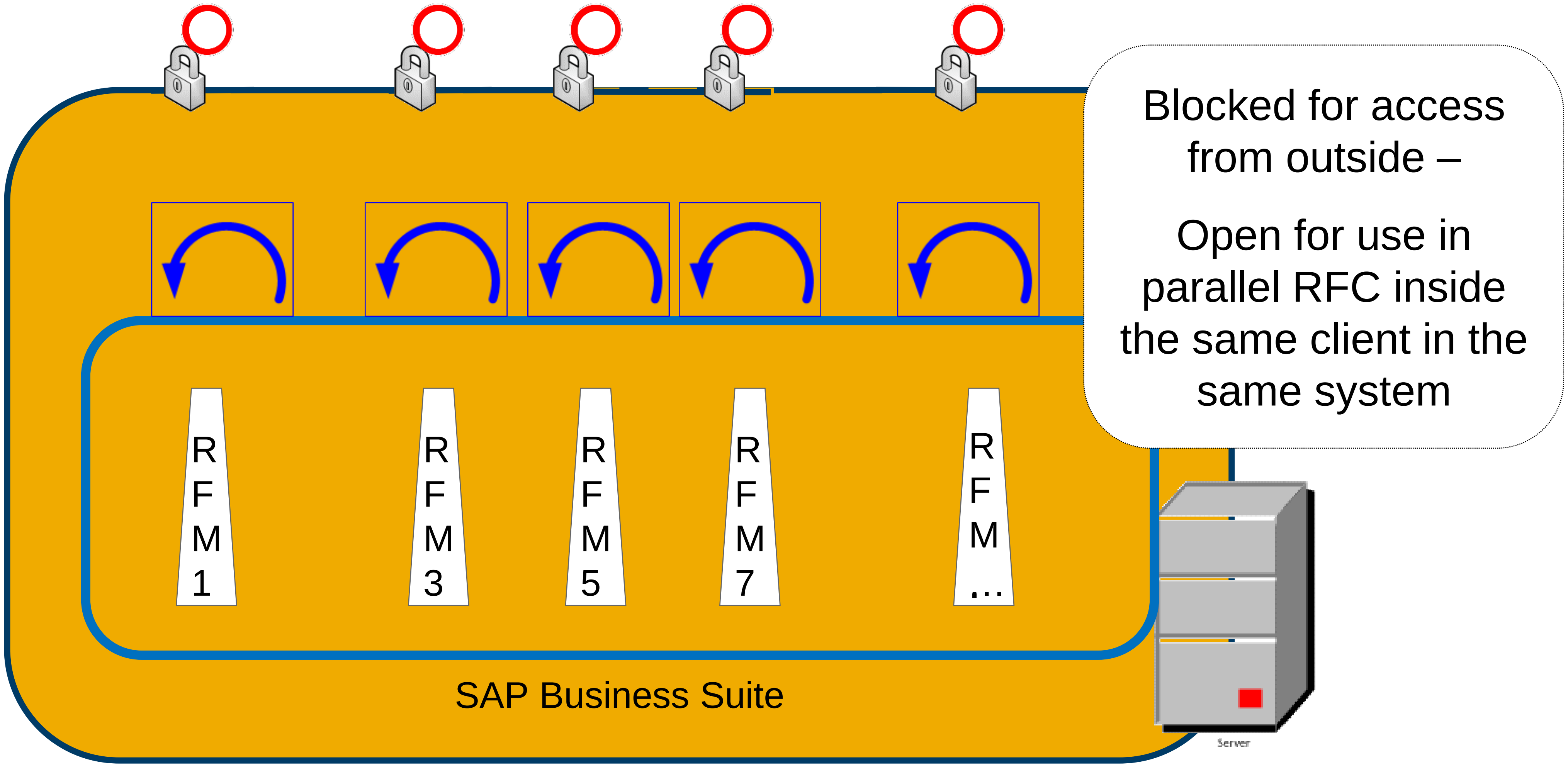
Basic Concepts

The UCON Way to Security: Expose Only Those

Function Modules You Need to the Outside World



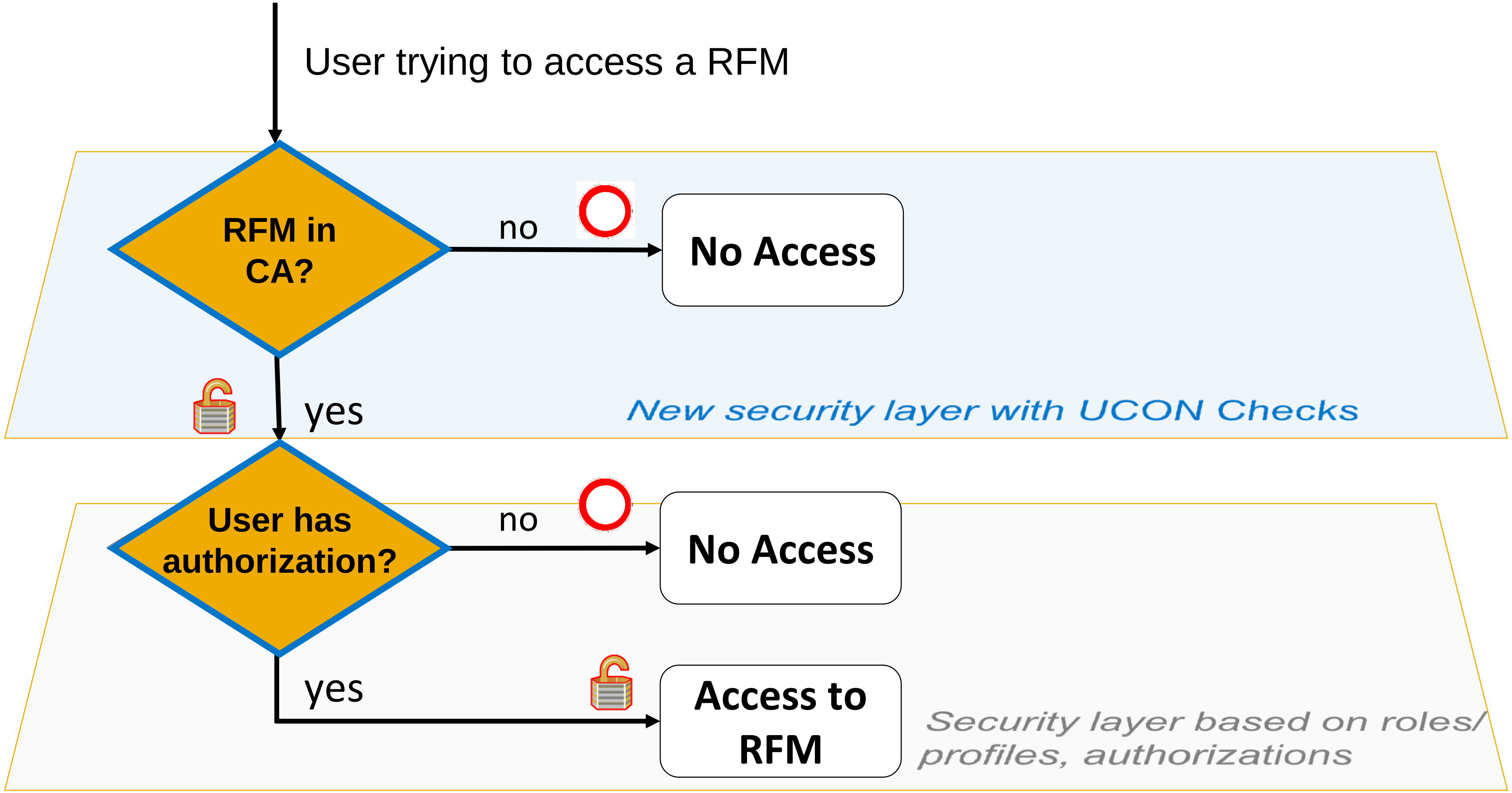
UCON Checks Do not Interfere with Calls Within the Same
Client and System



Blocked for access from outside –

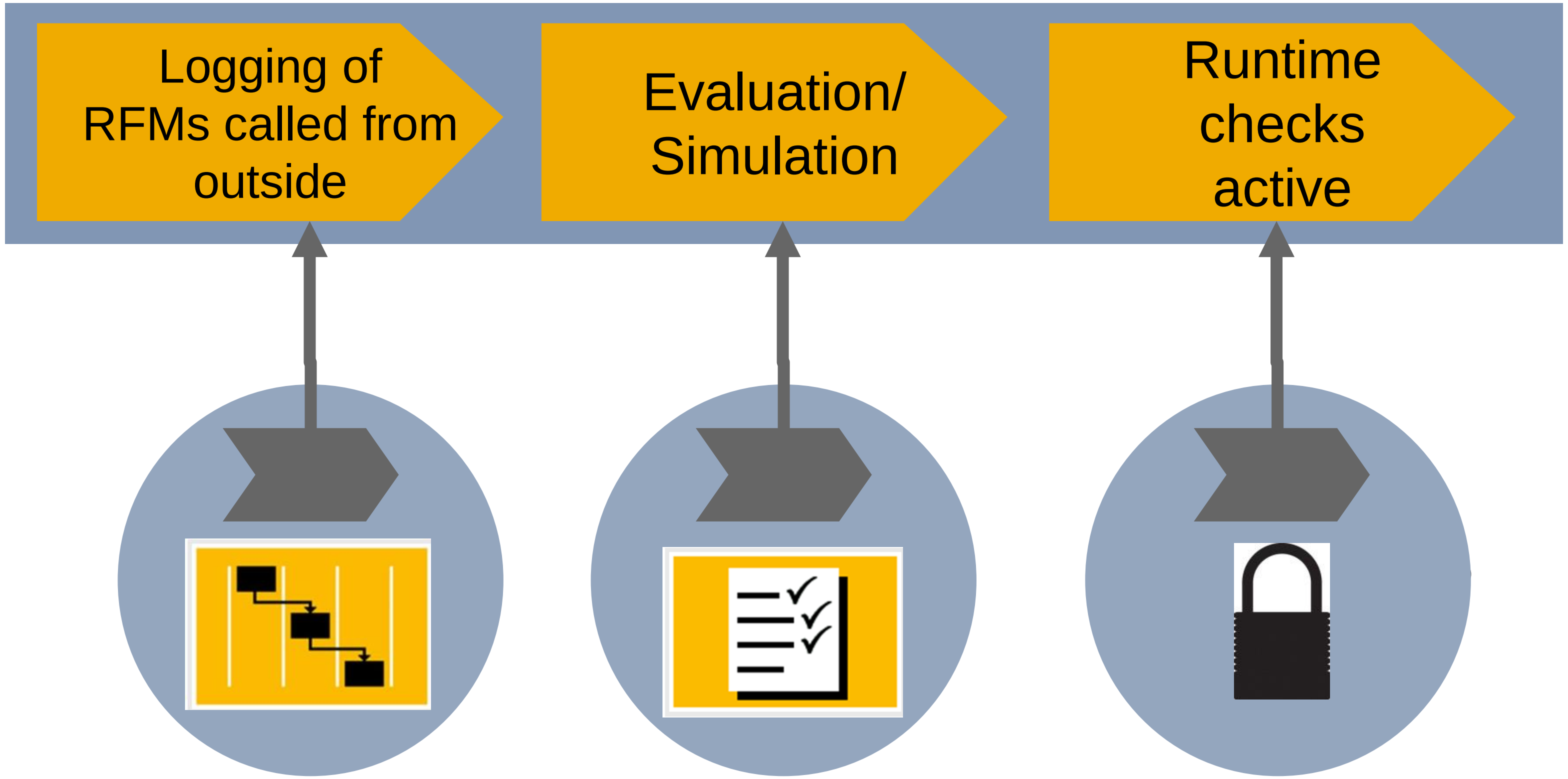
Open for use in parallel RFC inside the same client in the same system

UCON – An Additional Role/User-Independent Layer of Security Checks


User trying to access a RFM
RFM in CA?
no
No Access
yes
New security layer with UCON Checks
User has authorization?
no
No Access
yes
Access to RFM
Security layer based on roles/ profiles, authorizations

UCON RFC Security

Easy Customer Adoption in Three Steps



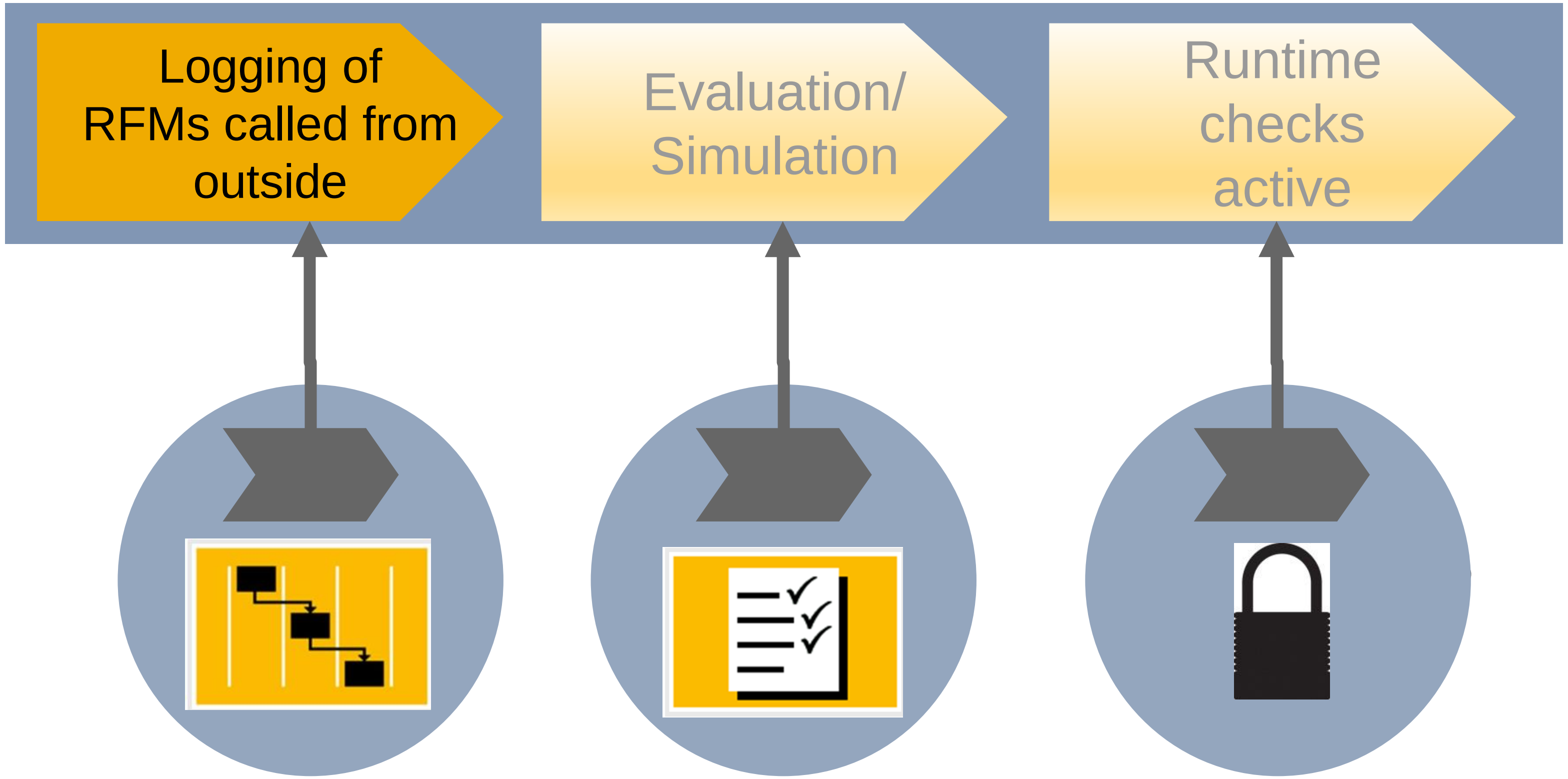
Logging of RFMs called from outside

Evaluation/ Simulation

Runtime checks active

UCON RFC Security

Easy Customer Adoption in Three Steps



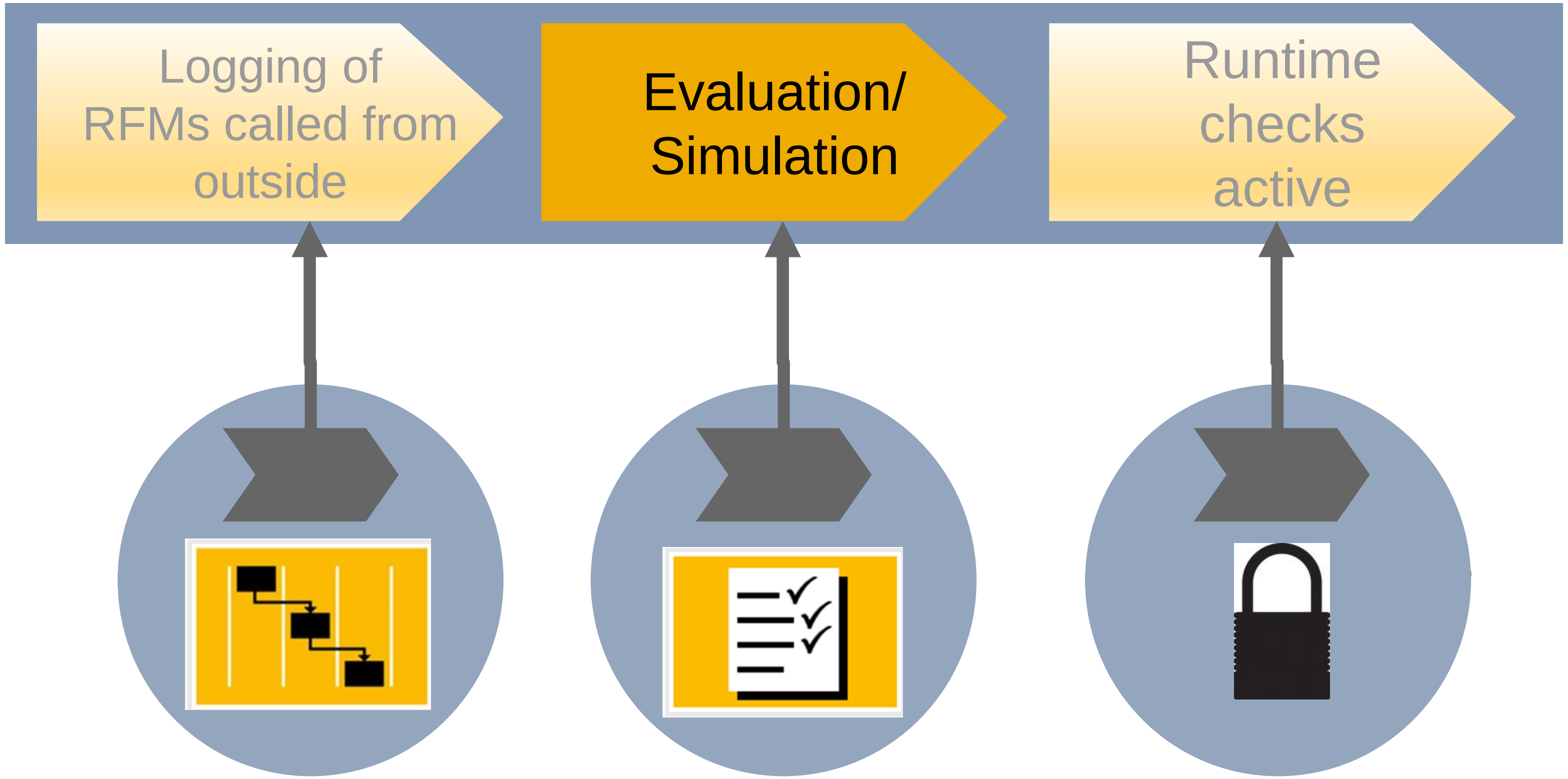
Logging of RFMs called from outside

Evaluation/ Simulation

Runtime checks active

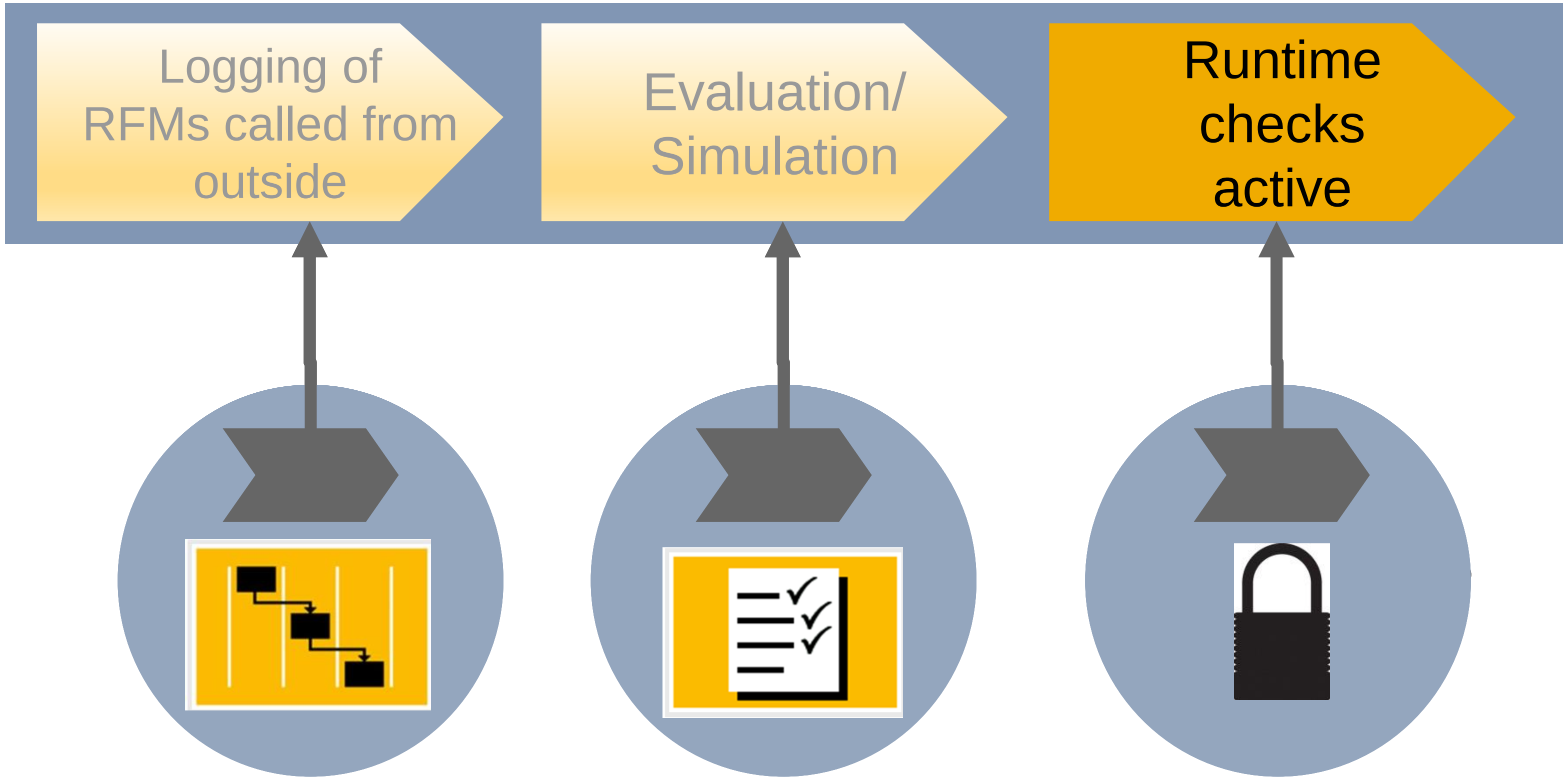
UCON RFC Security

Easy Customer Adoption in Three Steps



UCON RFC Security

Easy Customer Adoption in Three Steps

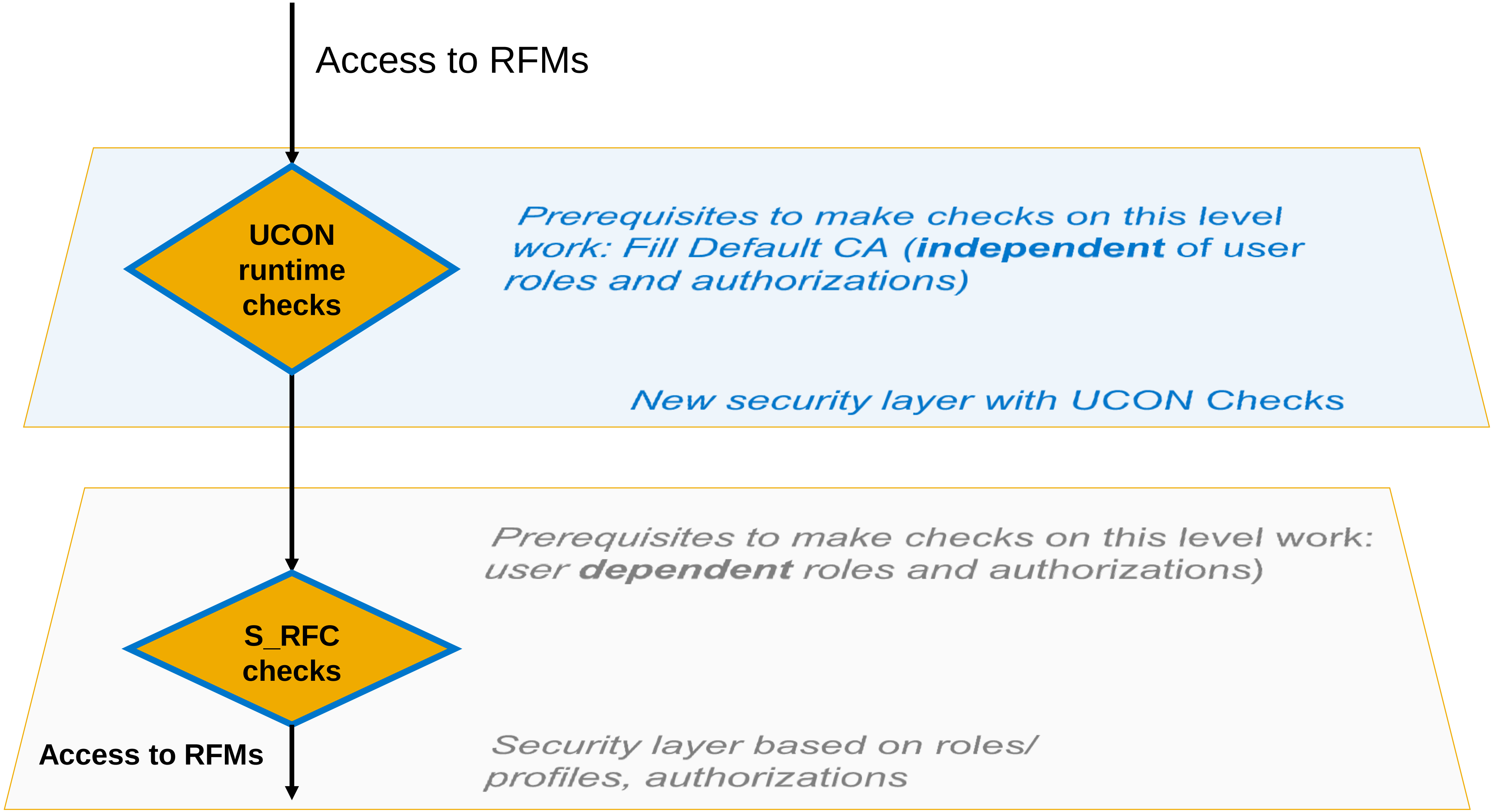


Logging of RFMs called from outside

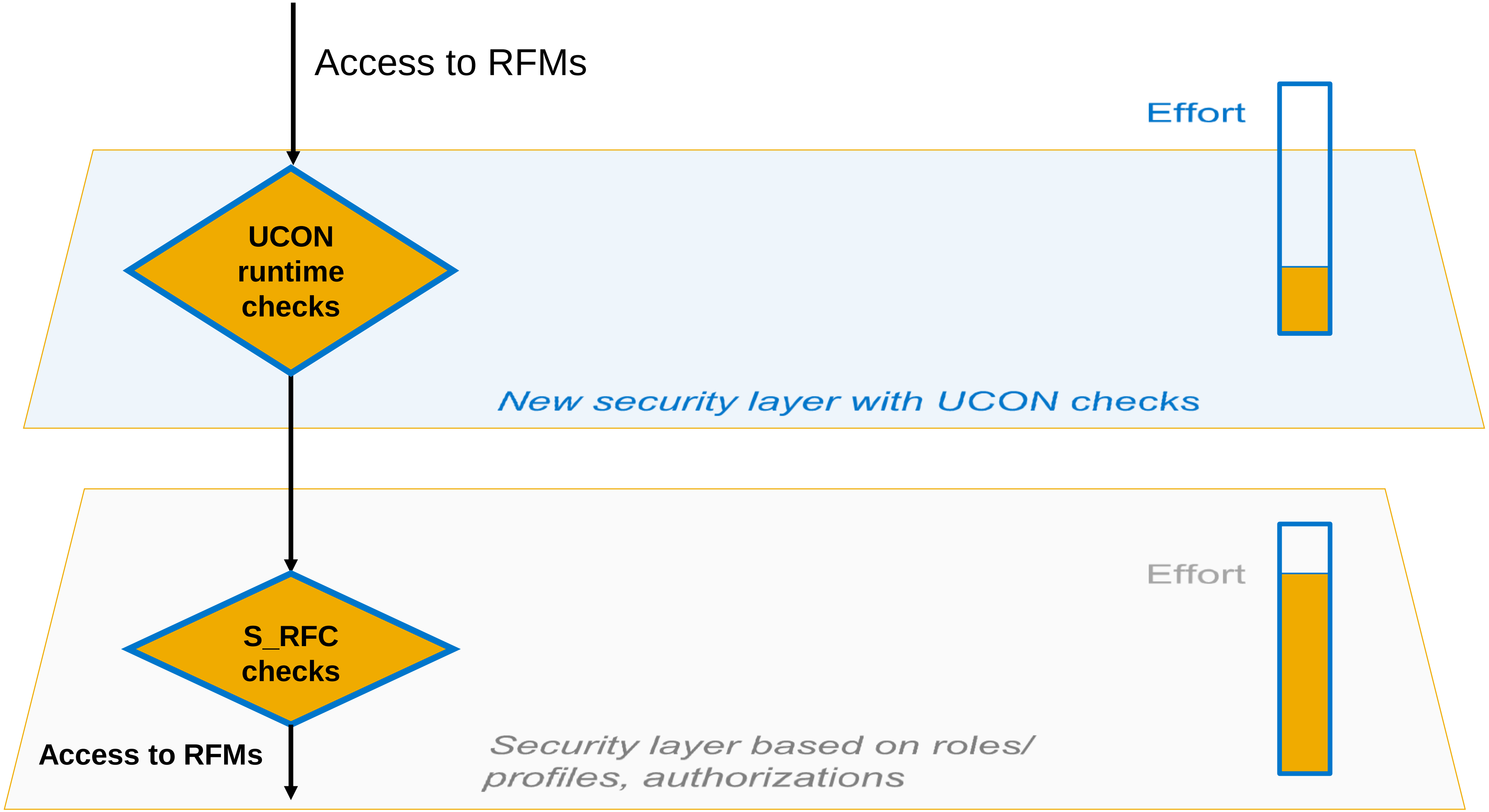
Evaluation/ Simulation

Runtime checks active

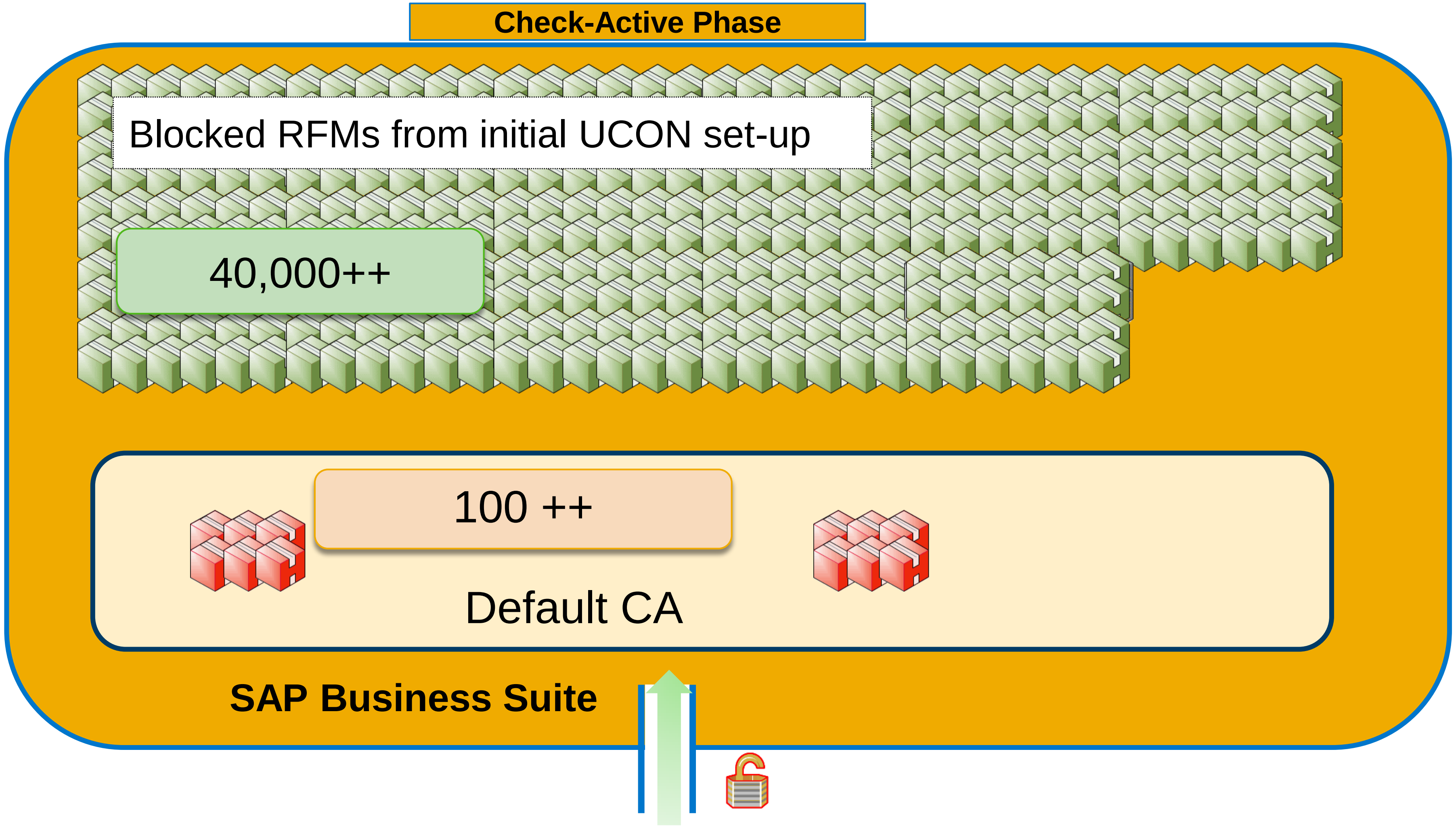
Prerequisites for the Different Security Layers


Access to RFMs
UCON runtime checks
*Prerequisites to make checks on this level work: Fill Default CA (**independent** of user roles and authorizations)*
New security layer with UCON Checks
S_RFC checks
*Prerequisites to make checks on this level work: user **dependent** roles and authorizations)*
Security layer based on roles/ profiles, authorizations
Access to RFMs

Efforts Required for the Different Security Layers


Access to RFMs
Effort
UCON runtime checks
New security layer with UCON checks
Effort
S_RFC checks
Access to RFMs
Security layer based on roles/ profiles, authorizations

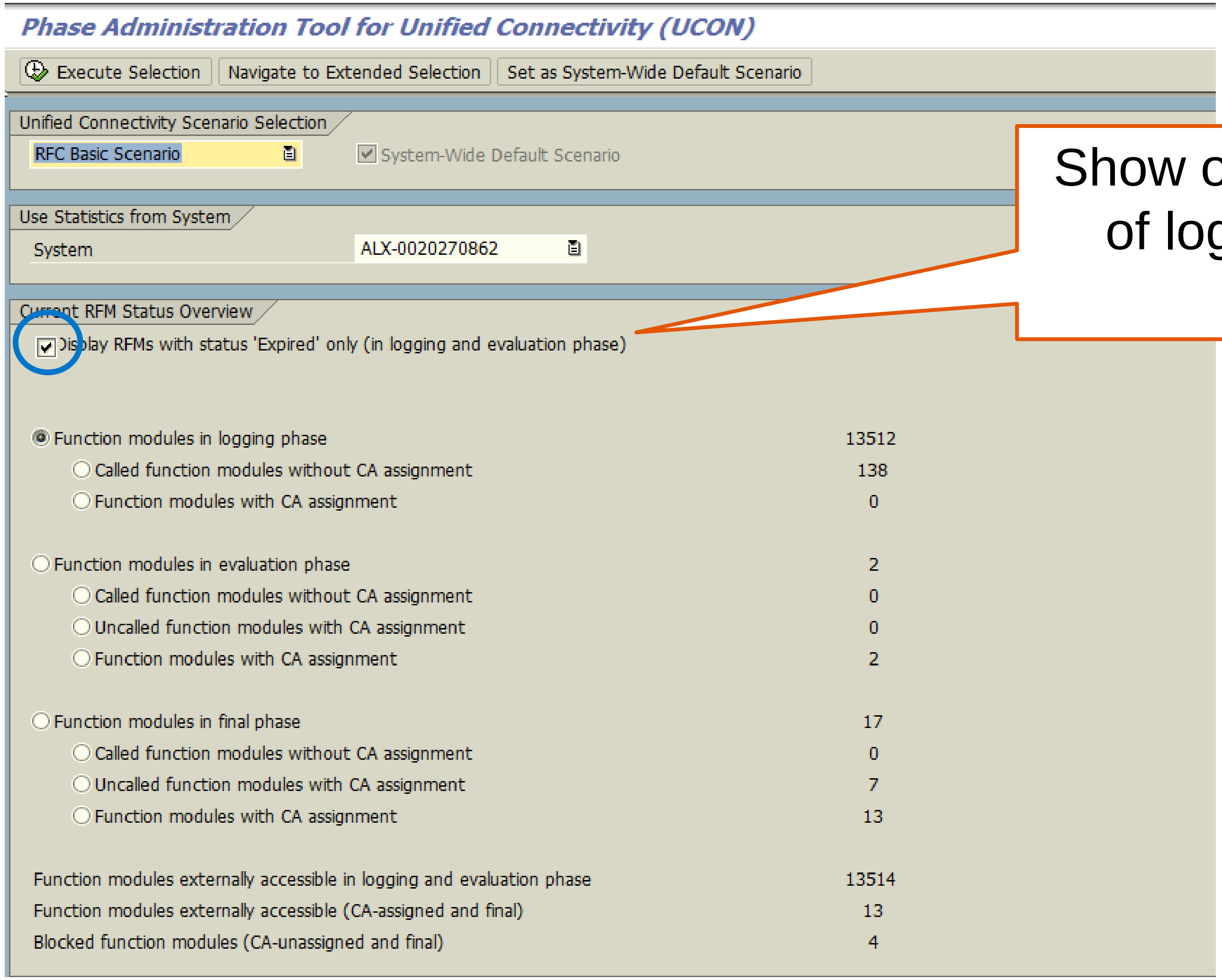
UCON Protection After the Initial UCON Security Classification



Demo

The Practice of UCON: Logging and Blocking

Logging and Blocking in the UCON Phase Tool



Phase Administration Tool for Unified Connectivity (UCON)

Execute Selection
Navigate to Extended Selection
Set as System-Wide Default Scenario

Unified Connectivity Scenario Selection

RFC Basic Scenario ☑ System-Wide Default Scenario

Use Statistics from System

System ALX-0020270862

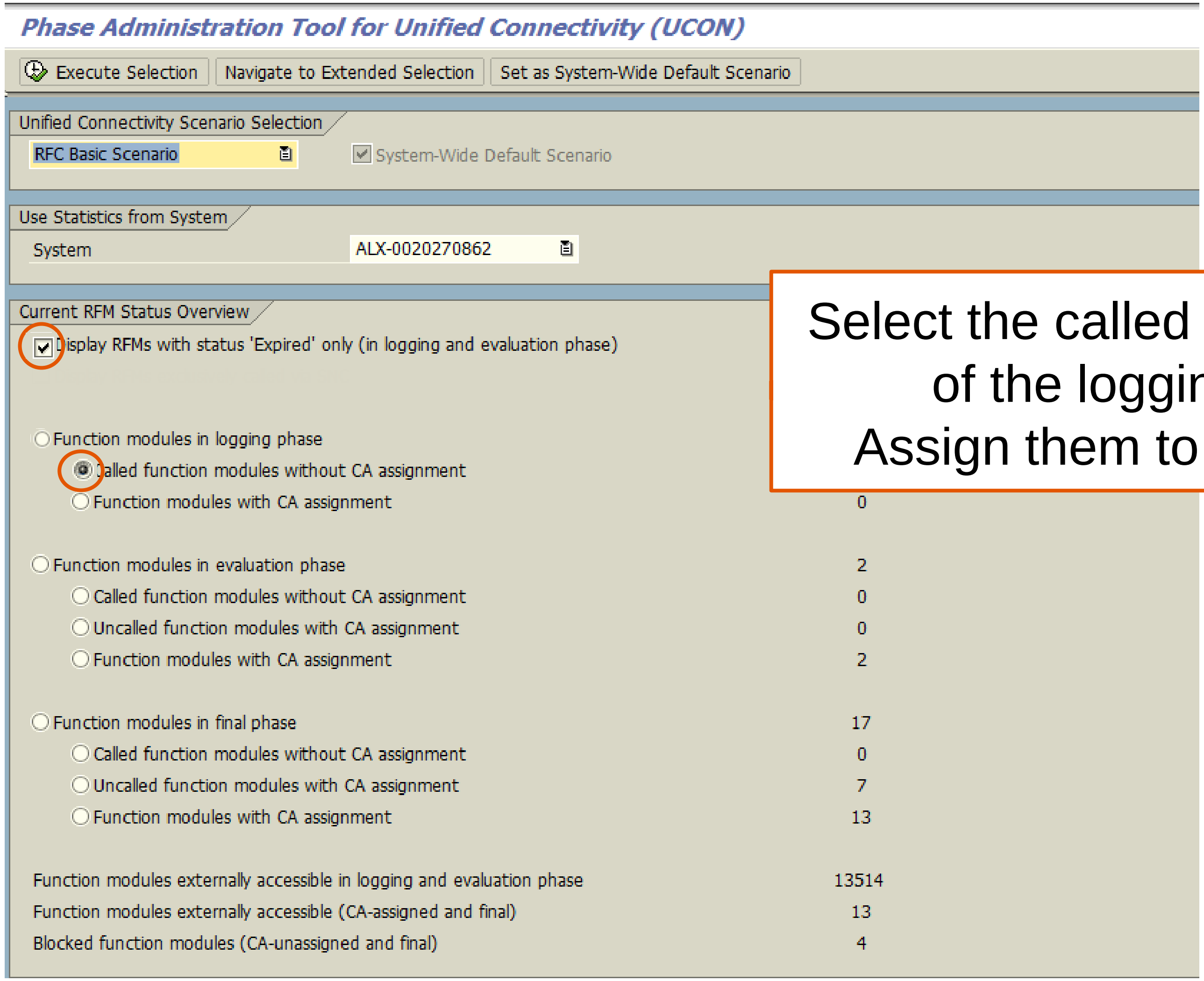
Current RFM Status Overview

☑ Display RFMs with status 'Expired' only (in logging and evaluation phase)

● Function modules in logging phase	13512
○ Called function modules without CA assignment	138
○ Function modules with CA assignment	0
○ Function modules in evaluation phase	2
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	0
○ Function modules with CA assignment	2
○ Function modules in final phase	17
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	7
○ Function modules with CA assignment	13
Function modules externally accessible in logging and evaluation phase	13514
Function modules externally accessible (CA-assigned and final)	13
Blocked function modules (CA-unassigned and final)	4

Show only RFMs at the end of logging or evaluation phase

Logging and Blocking in the UCON Phase Tool



Phase Administration Tool for Unified Connectivity (UCON)

Execute Selection
Navigate to Extended Selection
Set as System-Wide Default Scenario

Unified Connectivity Scenario Selection

RFC Basic Scenario ☑ System-Wide Default Scenario

Use Statistics from System

System ALX-0020270862

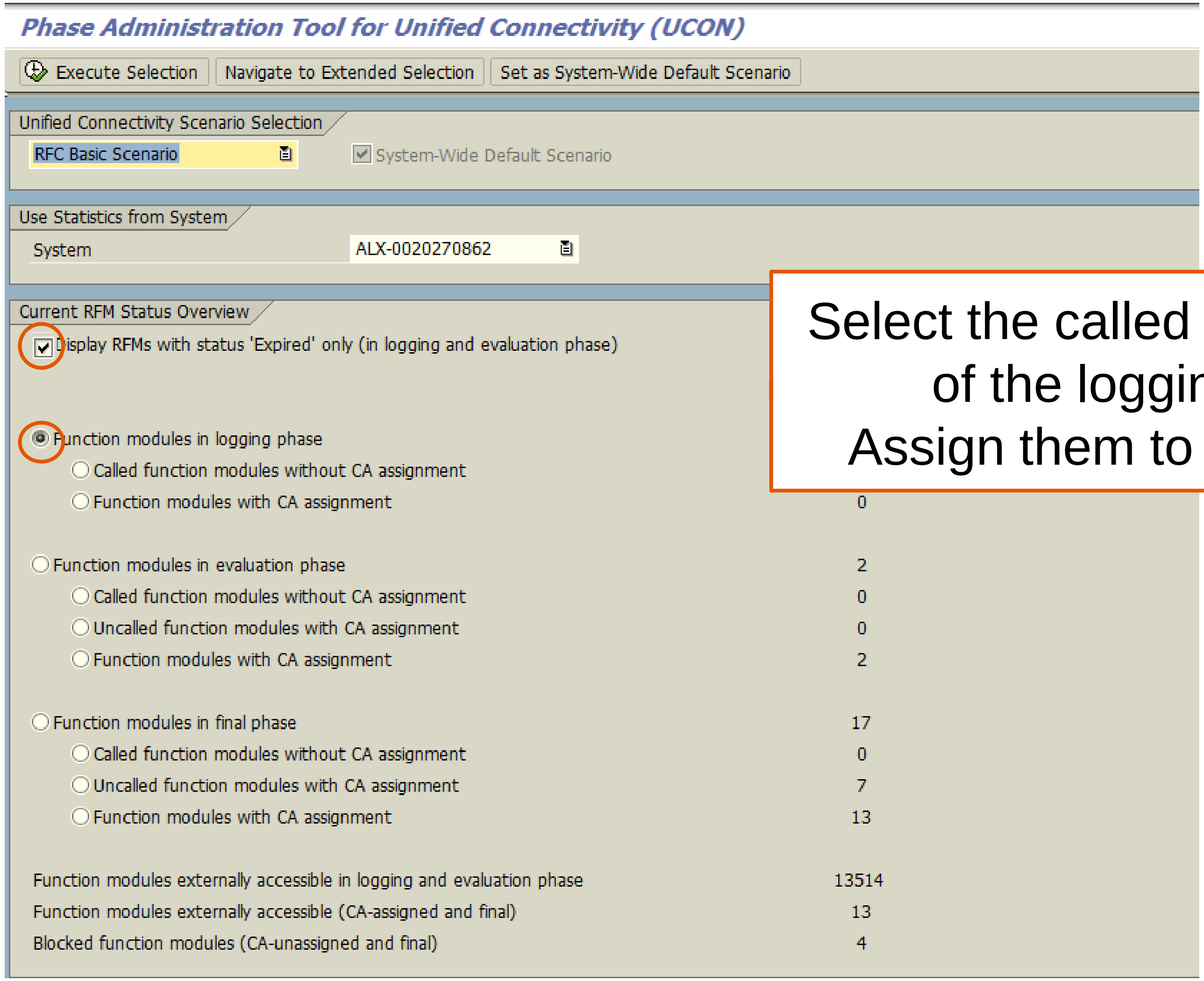
Current RFM Status Overview

☑ Display RFMs with status 'Expired' only (in logging and evaluation phase)

○ Function modules in logging phase	
● Called function modules without CA assignment	
○ Function modules with CA assignment	0
○ Function modules in evaluation phase	2
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	0
○ Function modules with CA assignment	2
○ Function modules in final phase	17
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	7
○ Function modules with CA assignment	13
Function modules externally accessible in logging and evaluation phase	13514
Function modules externally accessible (CA-assigned and final)	13
Blocked function modules (CA-unassigned and final)	4

Select the called RFMs at the end of the logging phase → Assign them to the default CA

Logging and Blocking in the UCON Phase Tool



Phase Administration Tool for Unified Connectivity (UCON)

Execute Selection
Navigate to Extended Selection
Set as System-Wide Default Scenario

Unified Connectivity Scenario Selection

RFC Basic Scenario

☑ System-Wide Default Scenario

Use Statistics from System

System ALX-0020270862

Current RFM Status Overview

☑ Display RFMs with status 'Expired' only (in logging and evaluation phase)

● Function modules in logging phase	
○ Called function modules without CA assignment	
○ Function modules with CA assignment	0
○ Function modules in evaluation phase	2
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	0
○ Function modules with CA assignment	2
○ Function modules in final phase	17
○ Called function modules without CA assignment	0
○ Uncalled function modules with CA assignment	7
○ Function modules with CA assignment	13
Function modules externally accessible in logging and evaluation phase	13514
Function modules externally accessible (CA-assigned and final)	13
Blocked function modules (CA-unassigned and final)	4

Select the called RFMs at the end of the logging phase → Assign them to the next phase

Unified Connectivity

Setup && Configuration

UCON Setup and Configuration

It is simple to set up and configure Unified Connectivity (UCON):

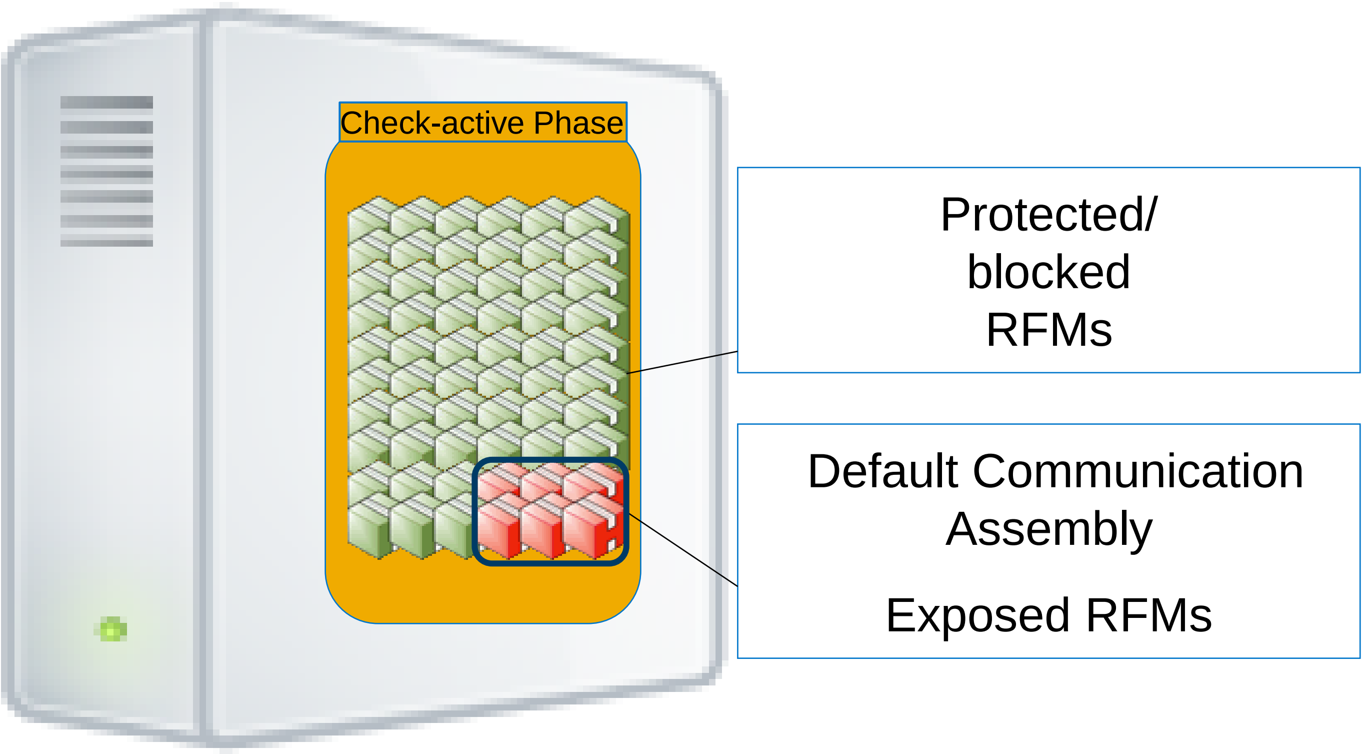
1. Create the UCON profile parameter ucon/rfc/active and set it to 1 to enable UCON runtime checks for RFMs in the final check-active phase
2. Choose a suitable duration of the logging and evaluation phase
3. Run the UCON setup to generate a default communication assembly (CA) and other required entities
4. Schedule the batch job SAP_UCON_MANAGEMENT that selects and persists the RFC statistic records required by the UCON phase tool on the database

Unified Connectivity

How to handle System Updates

Coverage of New Remote-Enabled Function Modules

UCON Protection After Initial Security Classification

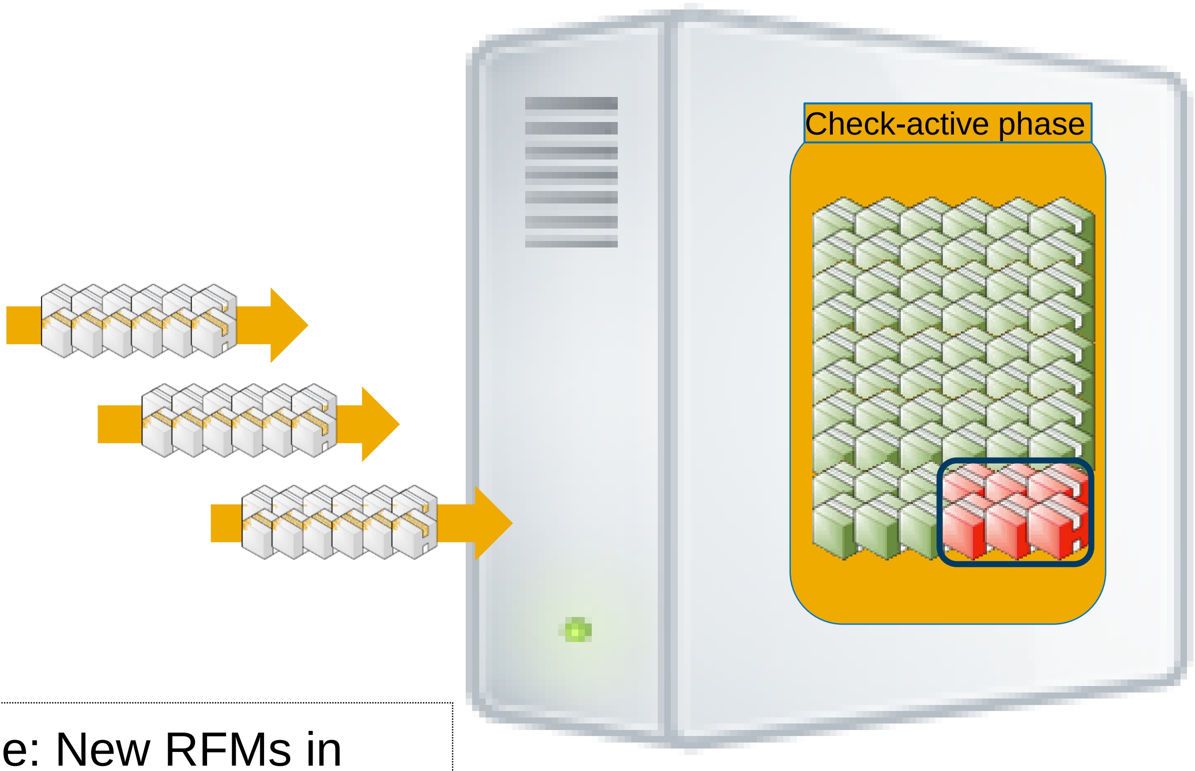


Protected/
blocked
RFMs

Default Communication Assembly

Exposed RFMs

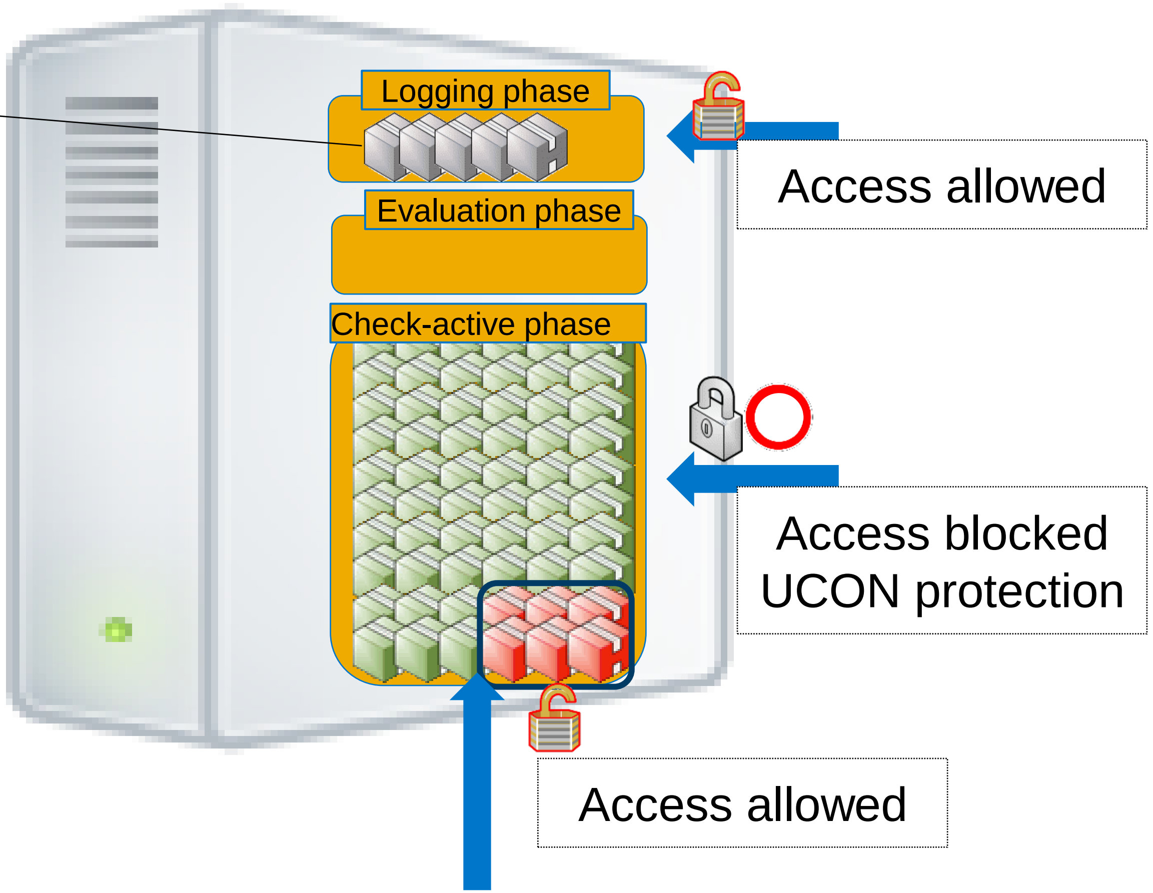
New RFMs Arrive at a UCON-Protected System



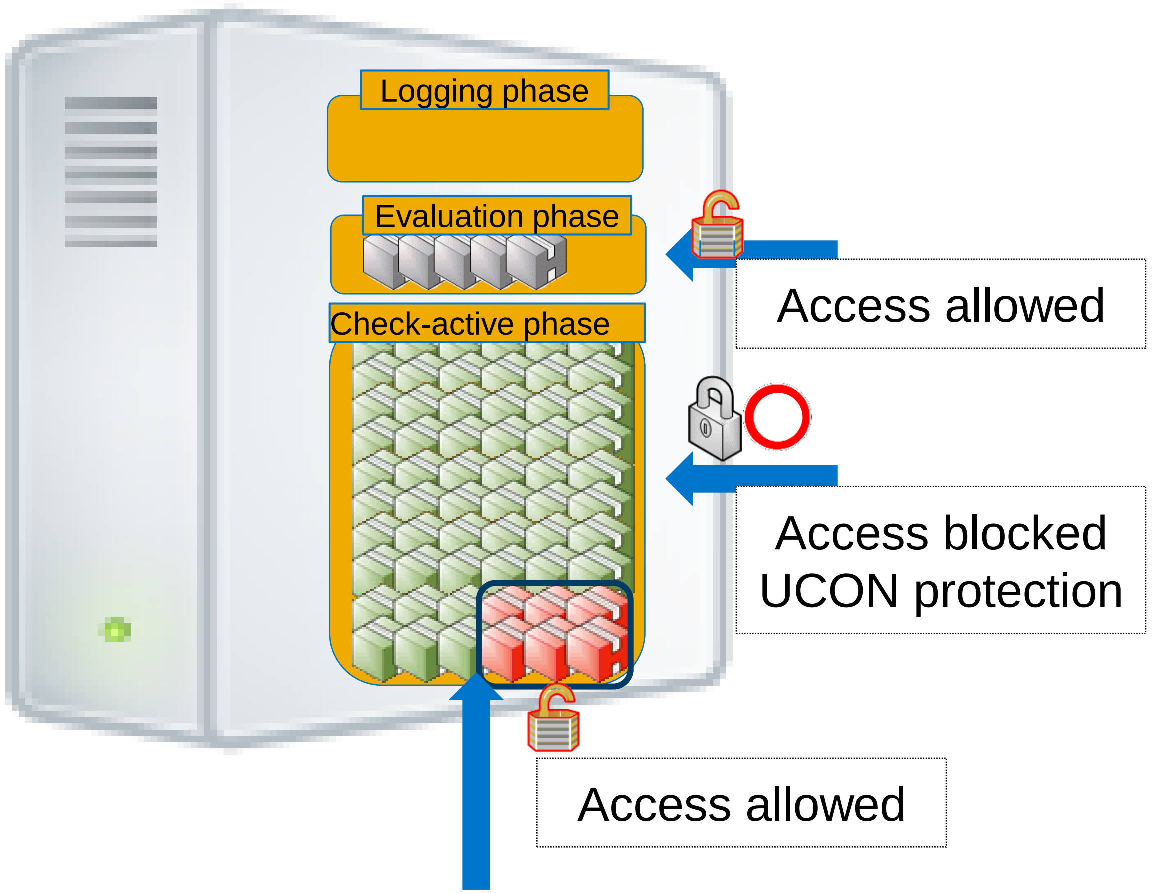
Over time: New RFMs in transports, SPs, EhPs …

New RFMs on Their Way to UCON Protection – Logging Phase

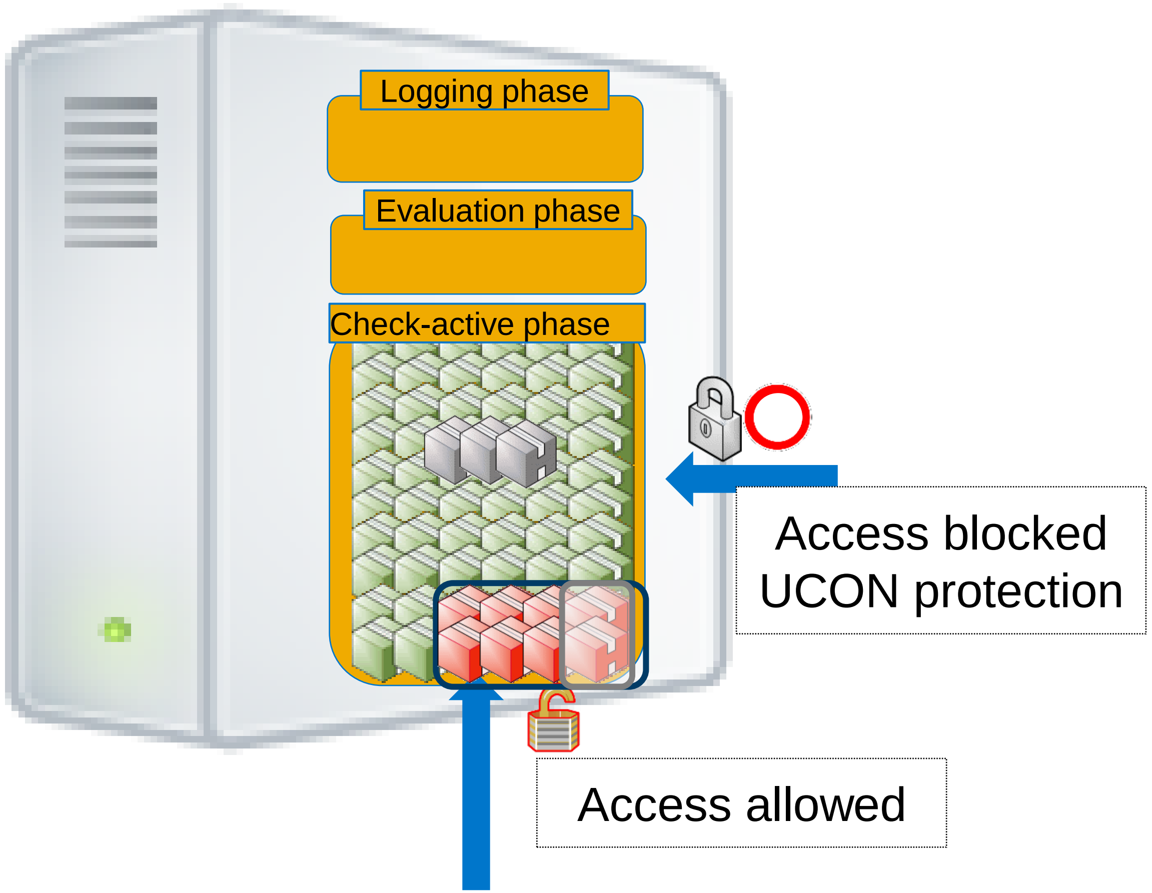
New RFMs are automatically assigned to the logging phase



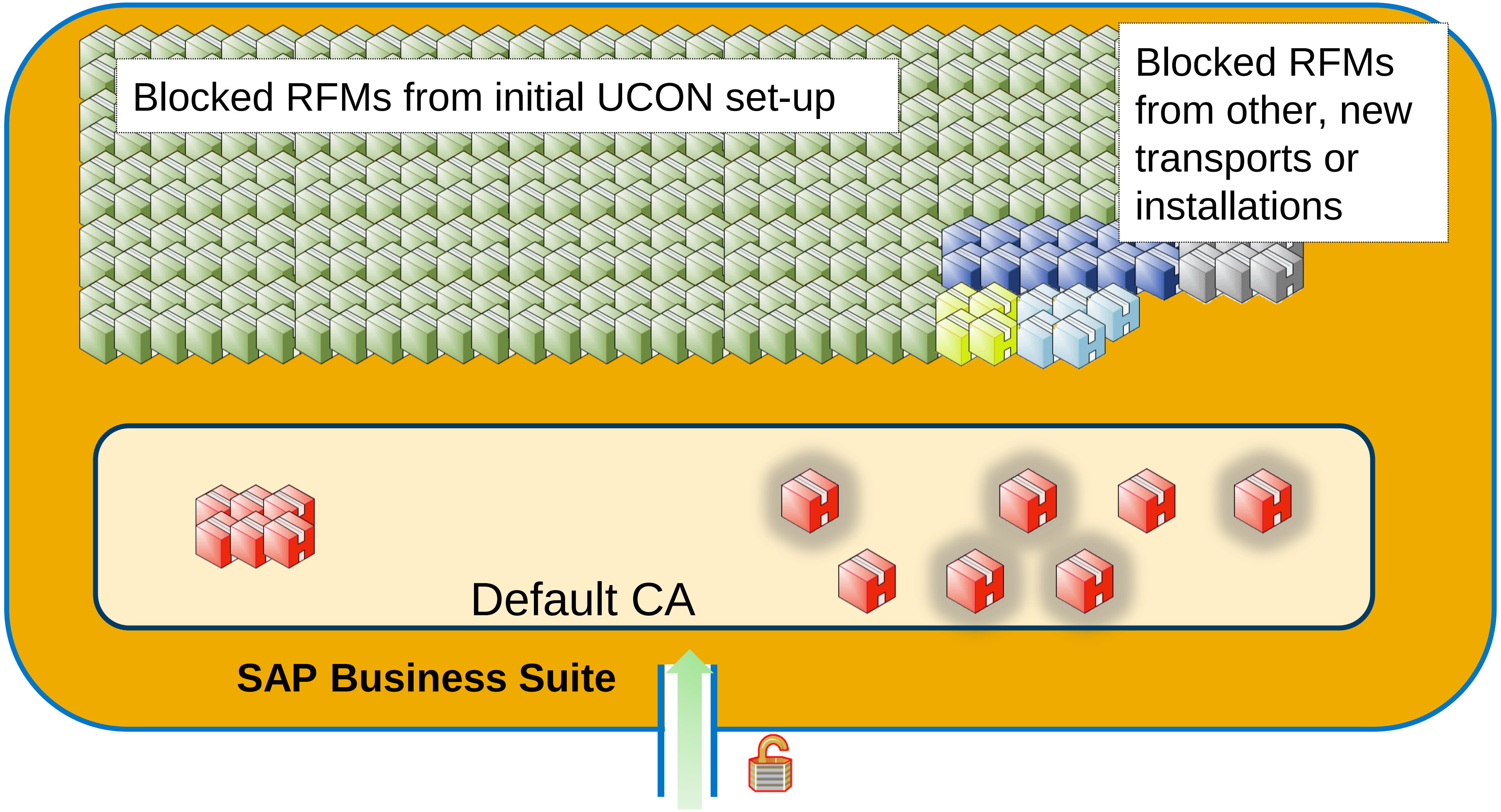
New RFMs on Their Way to UCON Protection – Evaluation Phase



New RFMs Have Achieved UCON Protection – Check-Active Phase



The Ever-Growing Scope of UCON Protection


Blocked RFMs from initial UCON set-up
Blocked RFMs from other, new transports or installations
Default CA
SAP Business Suite

Unified Connectivity

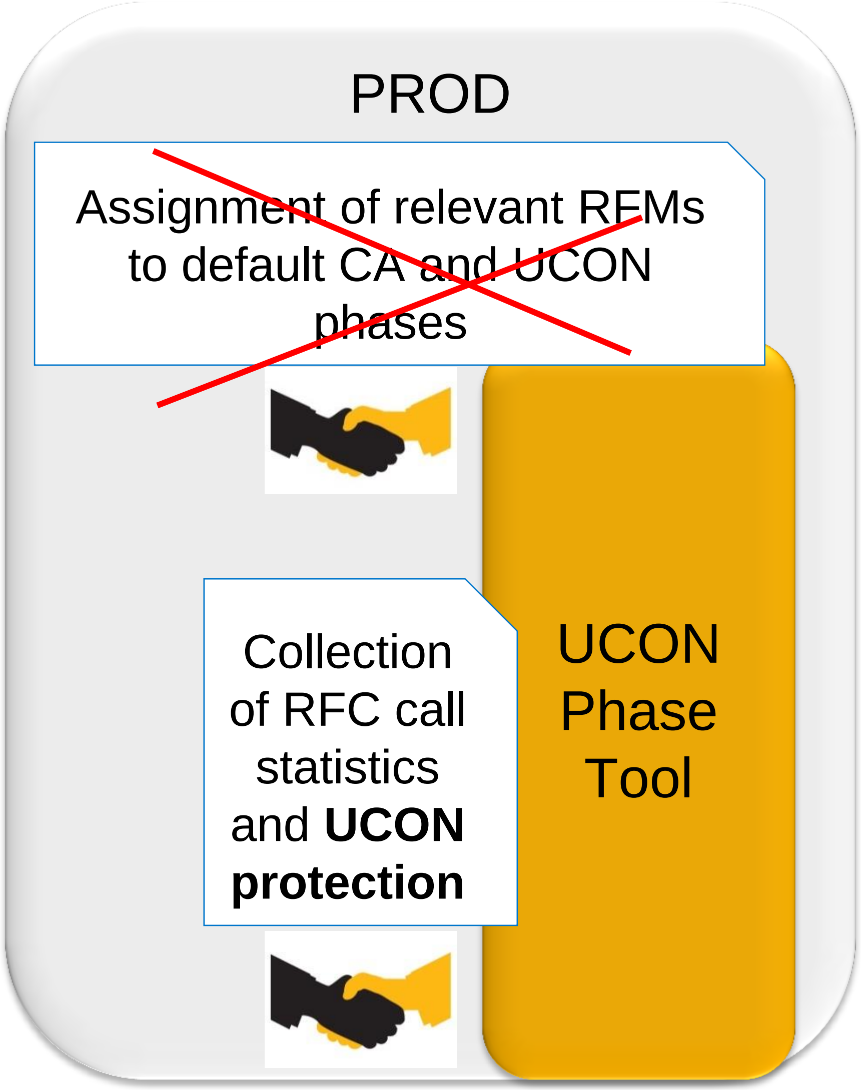
How to Cope With the Restrictions of Productive Systems

SAP TechEd && d-code

UCON and the Restrictions in a Productive System

Challenges

Authorizations and system change options in Productive Systems are not sufficient for UCON Operations



PROD

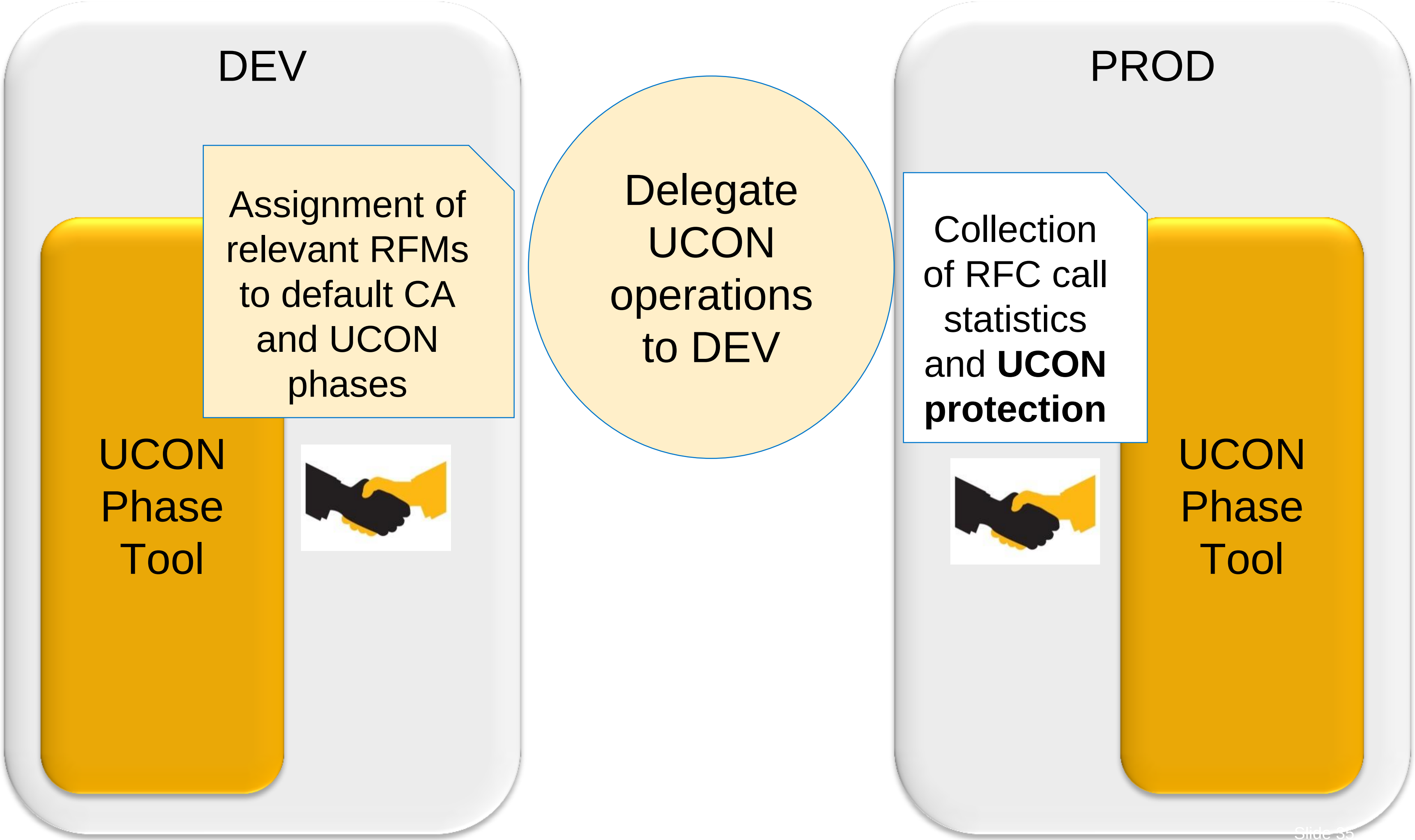
~~Assignment of relevant RFMs to default CA and UCON phases~~

Collection of RFC call statistics and **UCON protection**

UCON Phase Tool

UCON and the Restrictions in a Productive System

Solution



DEV

UCON Phase Tool

Assignment of relevant RFMs to default CA and UCON phases

Delegate UCON operations to DEV

PROD

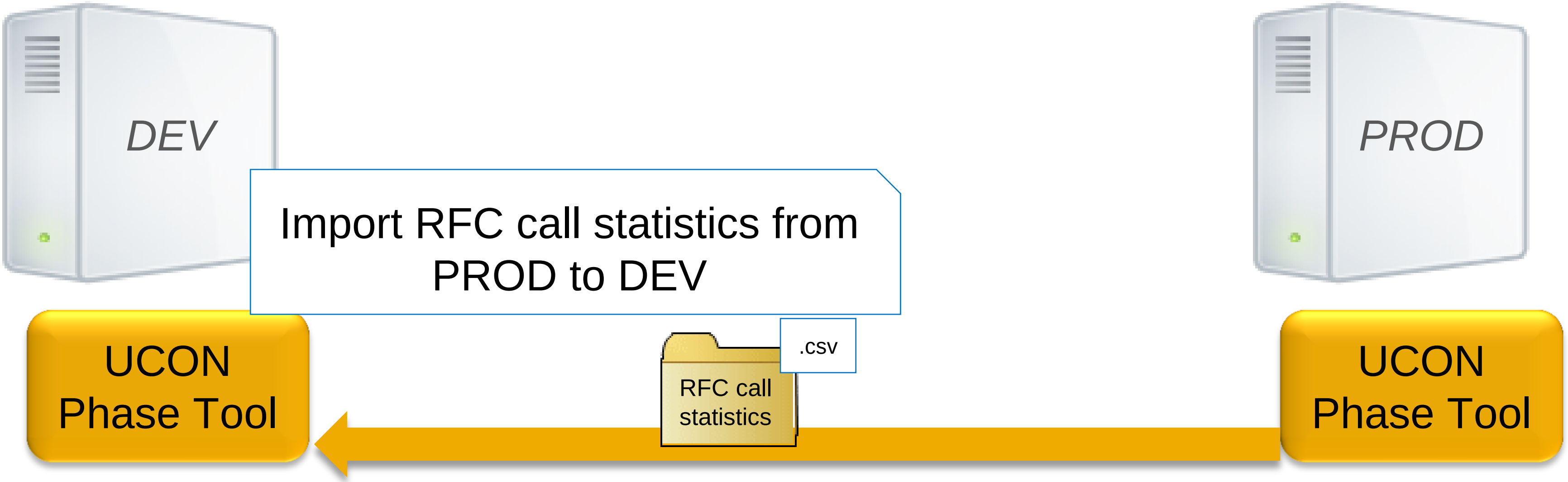
Collection of RFC call statistics and **UCON protection**

UCON Phase Tool

UCON and the Restrictions in a Productive System

How to Delegate UCON Operations to DEV – Step 1

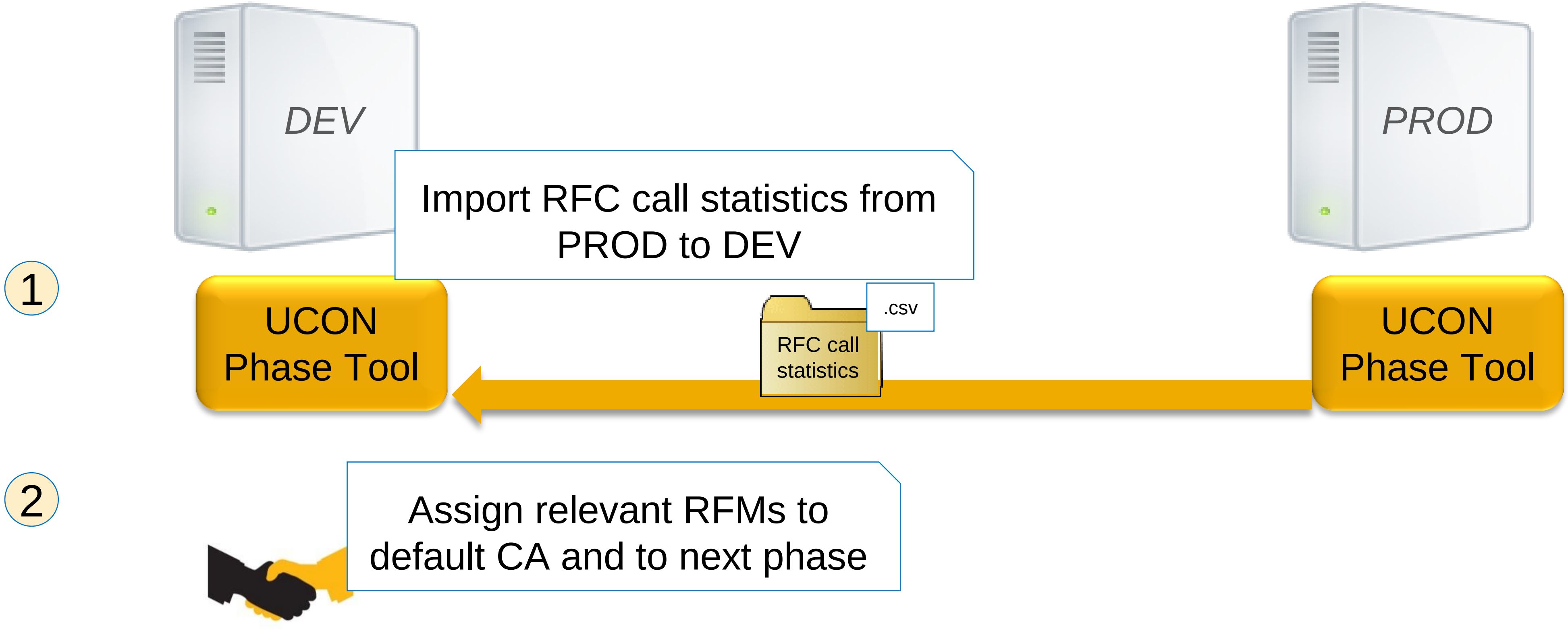
1



Import RFC call statistics from PROD to DEV

UCON and the Restrictions in a Productive System

How to Delegate UCON Operations to DEV – Step 2

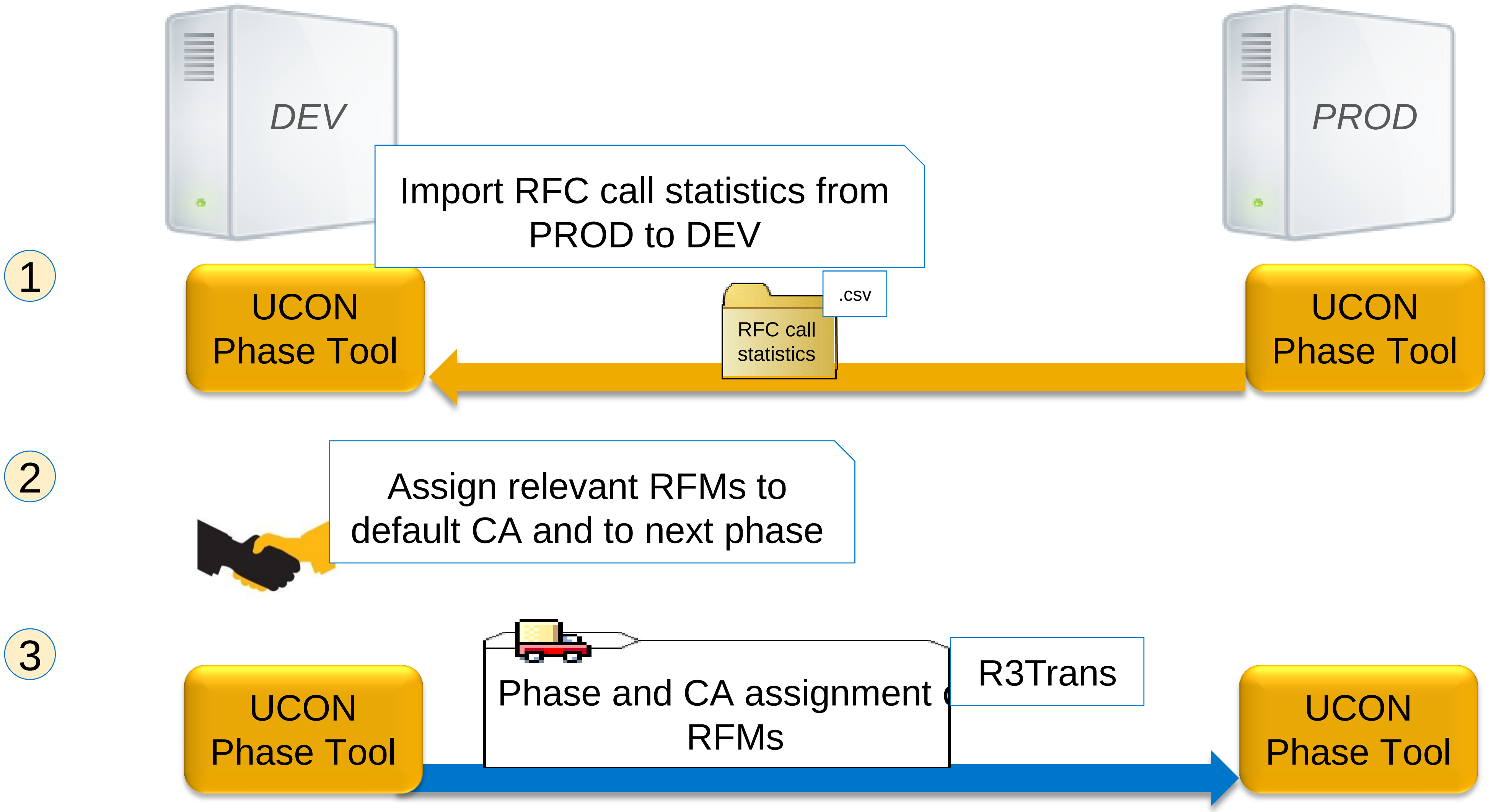


Import RFC call statistics from PROD to DEV

Assign relevant RFMs to default CA and to next phase

UCON and the Restrictions in a Productive System

How to Delegate UCON Operations to DEV – Step 3



1

DEV

PROD

Import RFC call statistics from PROD to DEV

UCON Phase Tool

RFC call statistics

.csv

UCON Phase Tool

2

Assign relevant RFMs to default CA and to next phase

3

UCON Phase Tool

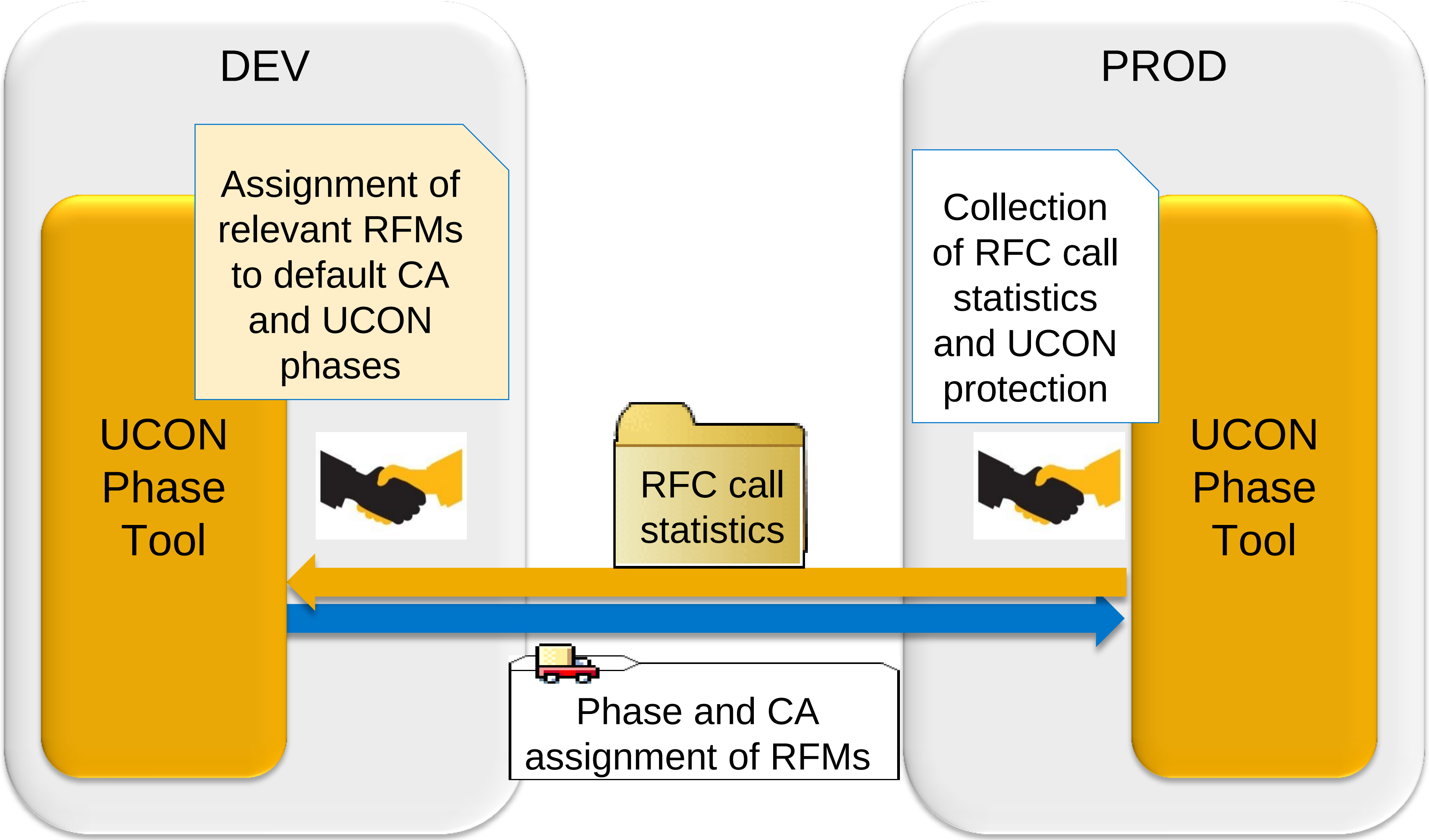
Phase and CA assignment
RFMs

R3Trans

UCON Phase Tool

UCON and the Restrictions in a Productive System

How to Delegate UCON Operations to DEV in a Nutshell


DEV
Assignment of relevant RFMs to default CA and UCON phases
UCON Phase Tool
RFC call statistics
Phase and CA assignment of RFMs
PROD
Collection of RFC call statistics and UCON protection
UCON Phase Tool

Unified Connectivity

Summary

Summary – It is simple to set up and configure Unified Connectivity (UCON)

- The UCON framework offers a simple, straightforward approach for enhancing the security of your RFCs. It allows you to minimize the number of RFMs on ABAP-based servers exposed to other clients and systems, reducing the available attack surface in your RFC communications
- The UCON phase tool guides and supports the administrator in the four-step setup and the three-phased process
- UCON covers new function modules entering the system via Support Packages, Enhancement Packages, transports, or new developments
- UCON is fully enabled for life-cycle management to ensure consistent RFC security across your system landscape

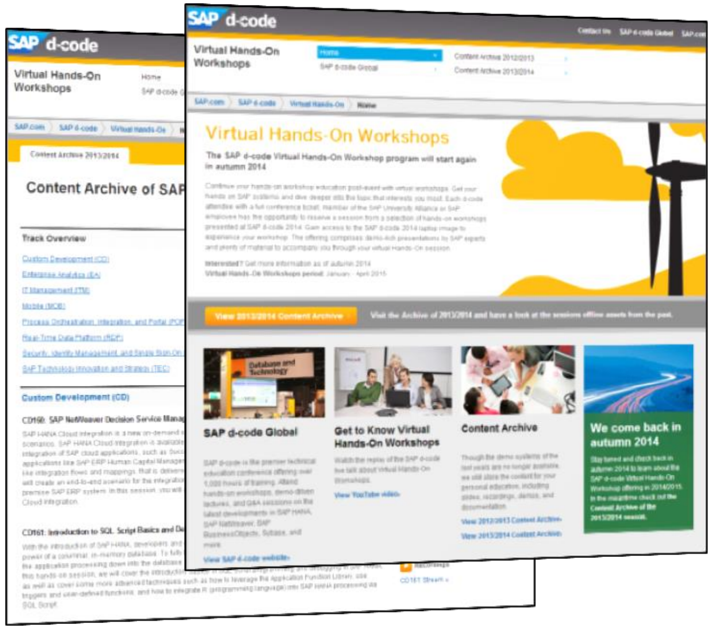
SAP d-code Virtual Hands-on Workshops and SAP d-code Online

Continue your SAP d-code education after the event!

SAP d-code Virtual Hands-on Workshops

- Access hands-on workshops post-event
- Starting January 2015
- Complementary with your SAP d-code registration

http://sapdcodehandson.sap.com



Virtual Hands-On Workshops

The SAP d-code Virtual Hands-On Workshop program will start again in autumn 2014

Interested? Get more information as of autumn 2014

Virtual Hands-On Workshops period: January - April 2015

View 2013/2014 Content Archive

Visit the Archive of 2013/2014 and have a look at the sessions offline assets from the past.

SAP d-code Global

Get to Know Virtual Hands-On Workshops

View YouTube video

Content Archive

View 2012/2013 Content Archive

View 2013/2014 Content Archive

We come back in autumn 2014

Content Archive of SAP

Track Overview

Custom Development (CD)

Enterprise Analytics (EA)

IT Management (ITM)

Mobile (MOB)

Process Orchestration, Integration, and Portal (POI)

Real-Time Data Platform (RDP)

Security, Identity Management, and Single Sign-On

SAP Technology Innovation and Strategy (TEC)

Custom Development (CD)

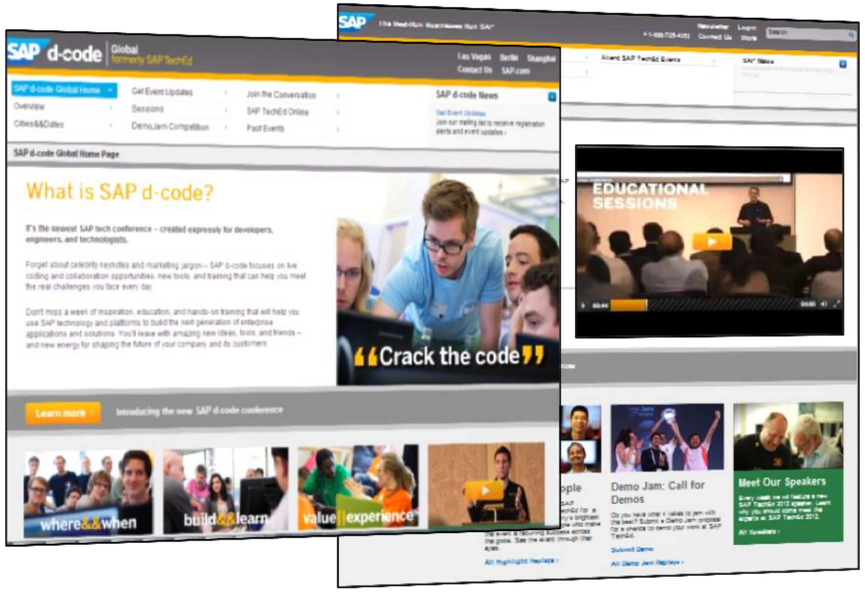
CD160: SAP NetWeaver Decision Service Manag

CD161: Introduction to SQL Script Basics and De

SAP d-code Online

- Access replays of keynotes, Demo Jam, SAP d-code live interviews, select lecture sessions, and more!
- Hands-on replays

http://sapdcode.com/online



SAP d-code Global Home Page

What is SAP d-code?

It's the newest SAP tech conference – created expressly for developers, engineers, and technologists.

Forget about celebrity keynotes and marketing jargon – SAP d-code focuses on live coding and collaboration opportunities, new tools, and training that can help you meet the real challenges you face every day.

Don't miss a week of inspiration, education, and hands-on training that will help you use SAP technology and platforms to build the next generation of enterprise applications and solutions. You'll leave with amazing new ideas, tools, and friends – and new energy for shaping the future of your company and its customers.

Learn more

Introducing the new SAP d-code conference

Demo Jam: Call for Demos

Meet Our Speakers

Further Information

SAP Public Web

http://scn.sap.com/docs/DOC-53844

http://scn.sap.com/community/security

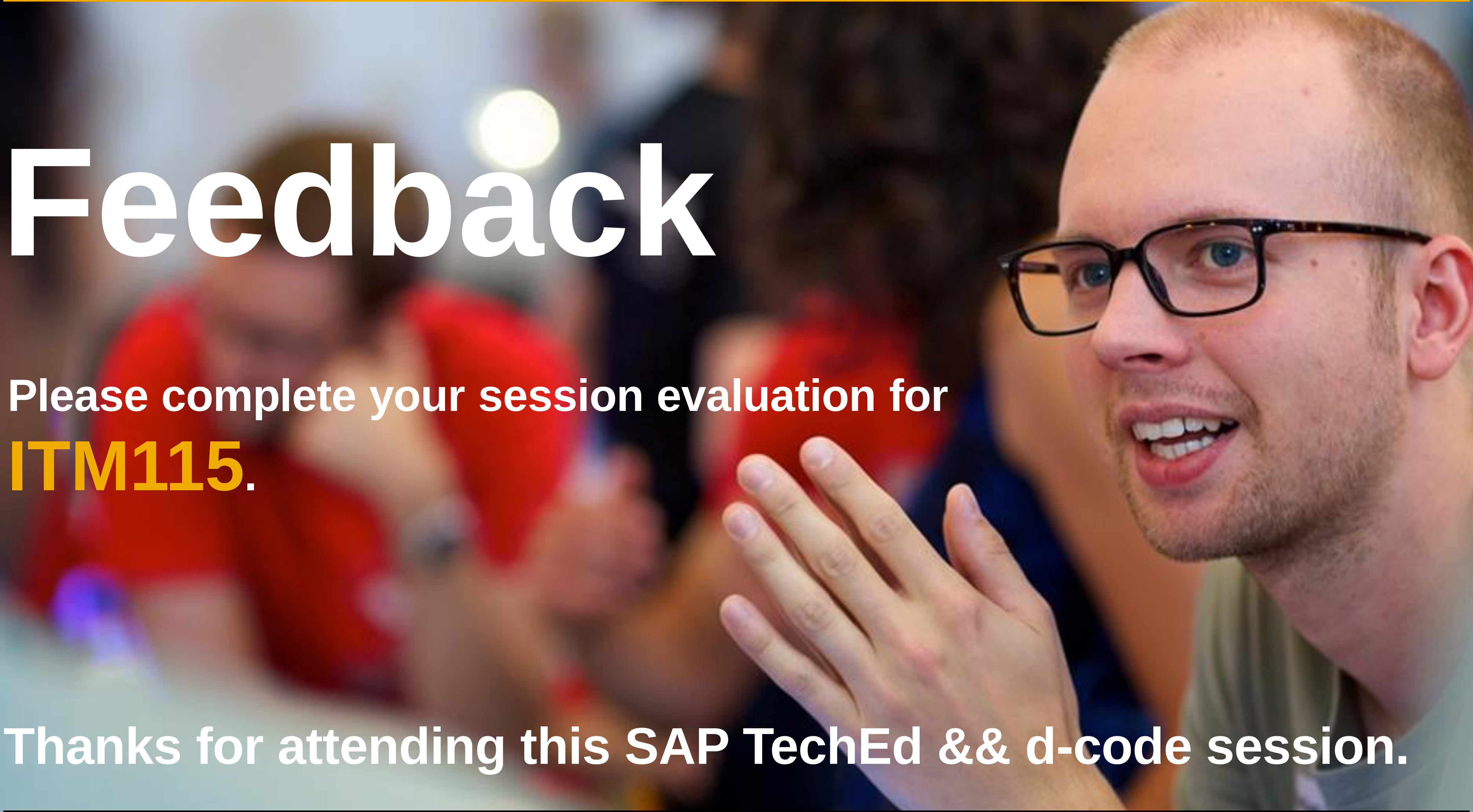
www.sap.com

SAP Education and Certification Opportunities

www.sap.com/education

Watch SAP d-code Online

www.sapcode.com/online



Feedback

Please complete your session evaluation for

ITM115.

Thanks for attending this SAP TechEd && d-code session.

© 2014 SAP SE or an SAP affiliate company. All rights reserved.