

SIS104

# Identity Service from SAP – Identity Provider for the Cloud

Martin Raeppe / SAP NetWeaver Cloud Platform

Marko Sommer / SAP NetWeaver Identity Management & Security



# 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

---

## Getting Started: Single Sign-On and SAML

- **Demo:** Single Sign-on to SAP Travel OnDemand and Amadeus

## ID Service Integration with SAP NetWeaver Cloud

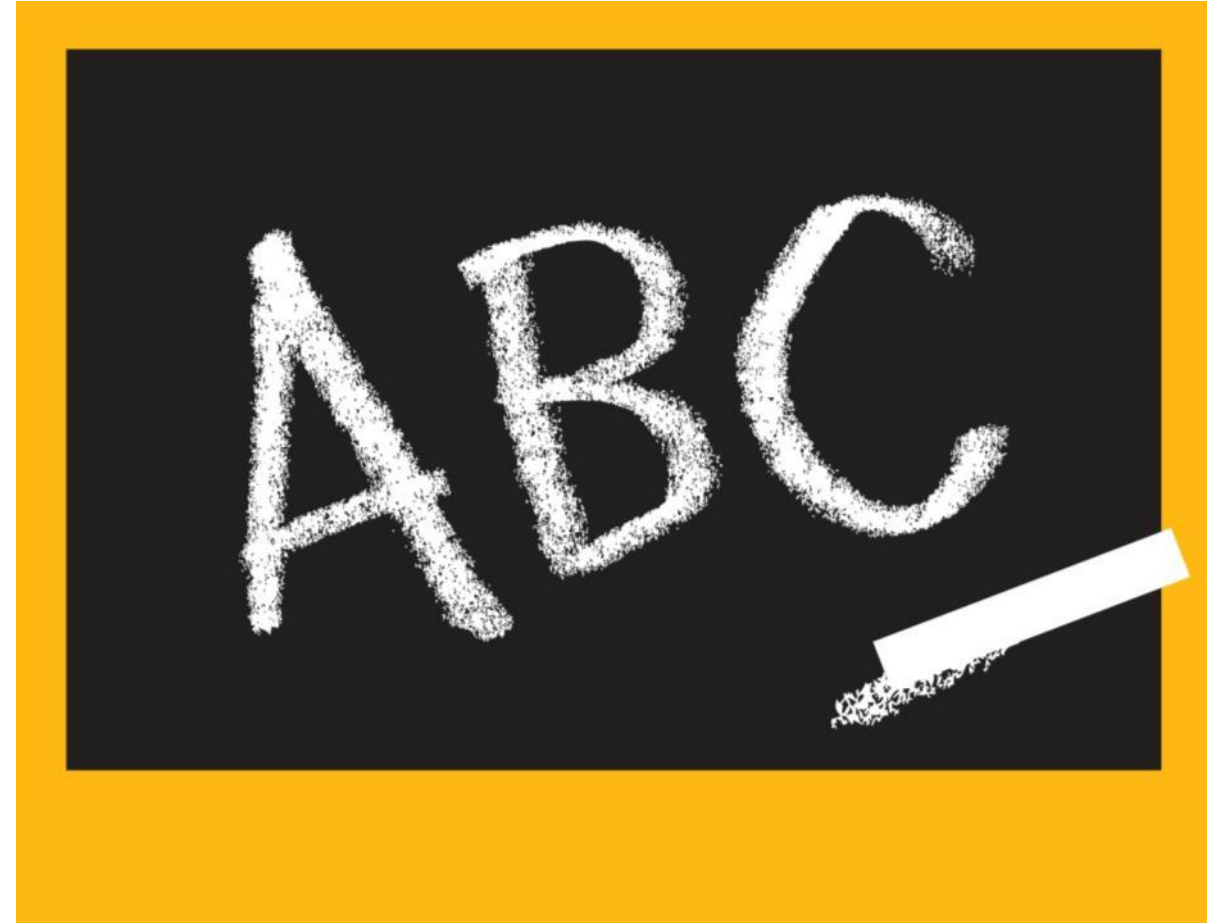
- **Demo:** Delegate Authentication to ID Service in your Application on SAP NetWeaver Cloud
- **Demo:** Working with User Profile Attributes in your SAP NetWeaver Cloud-based application



# After this lecture session, you will know...

---

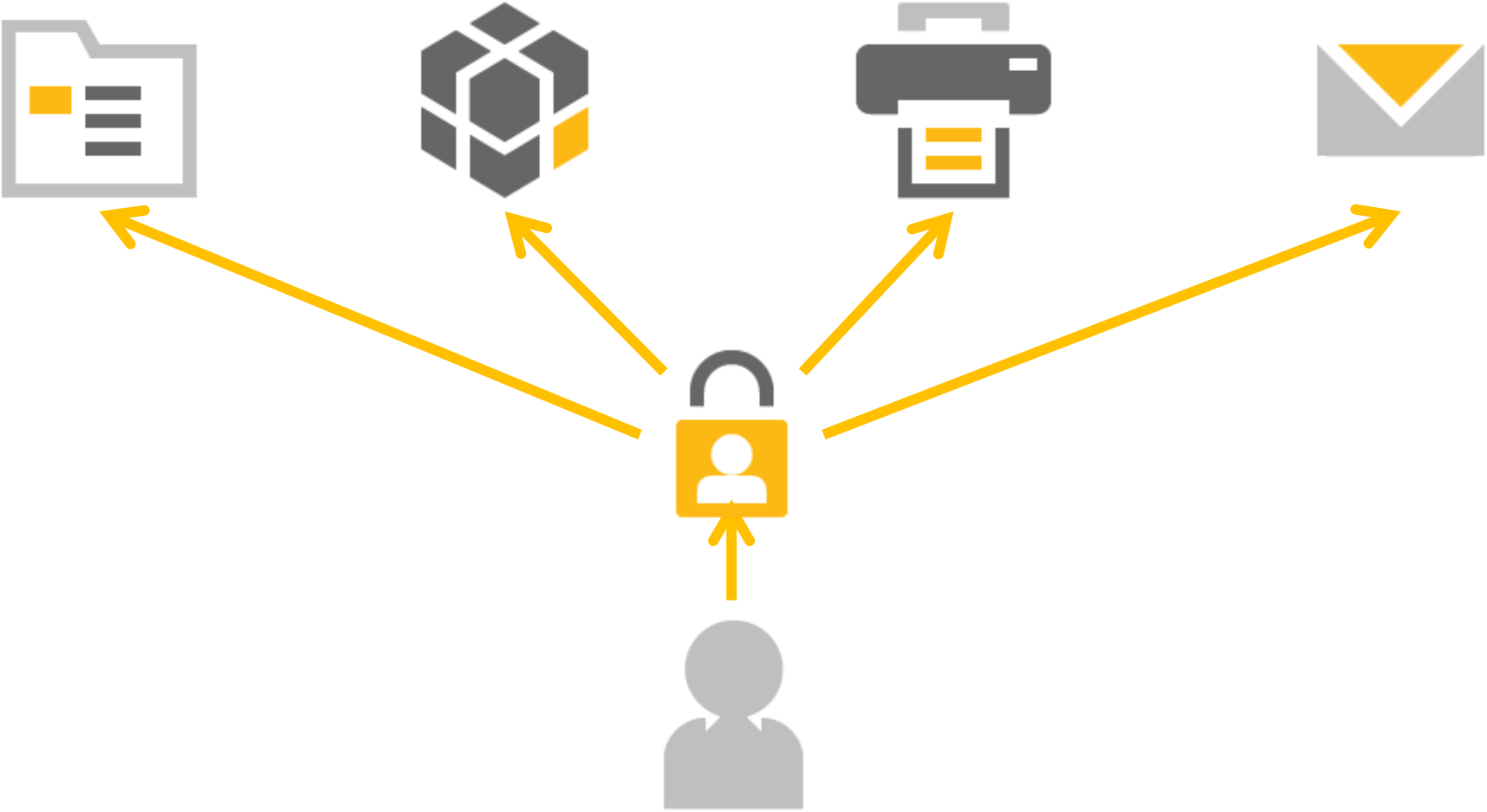
- ... more about user authentication in the Cloud**
- ... details about the ID Service from SAP**
- ... how ID Service can be used in your applications running on SAP NetWeaver Cloud**



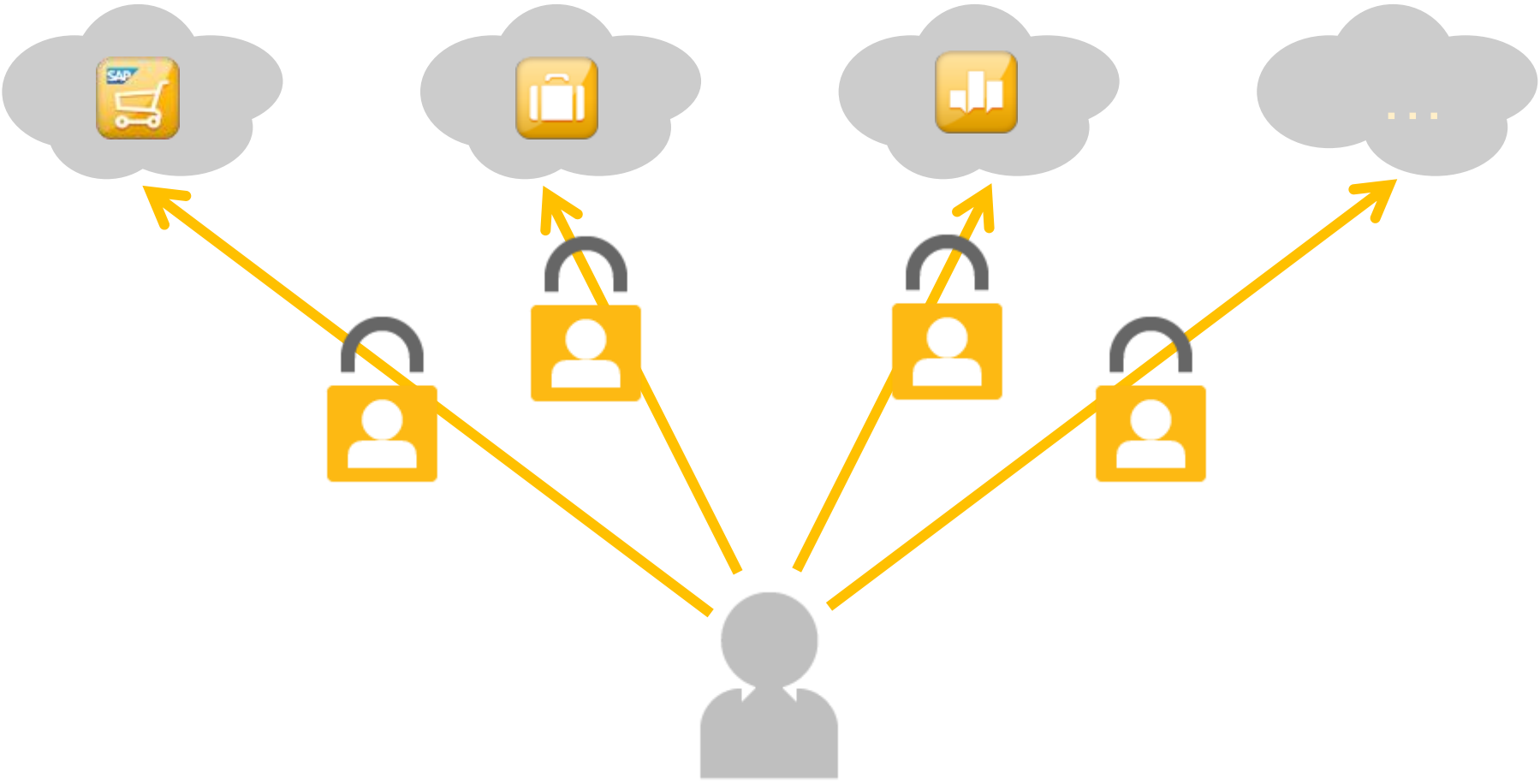


# Getting Started: Single Sign-On and SAML

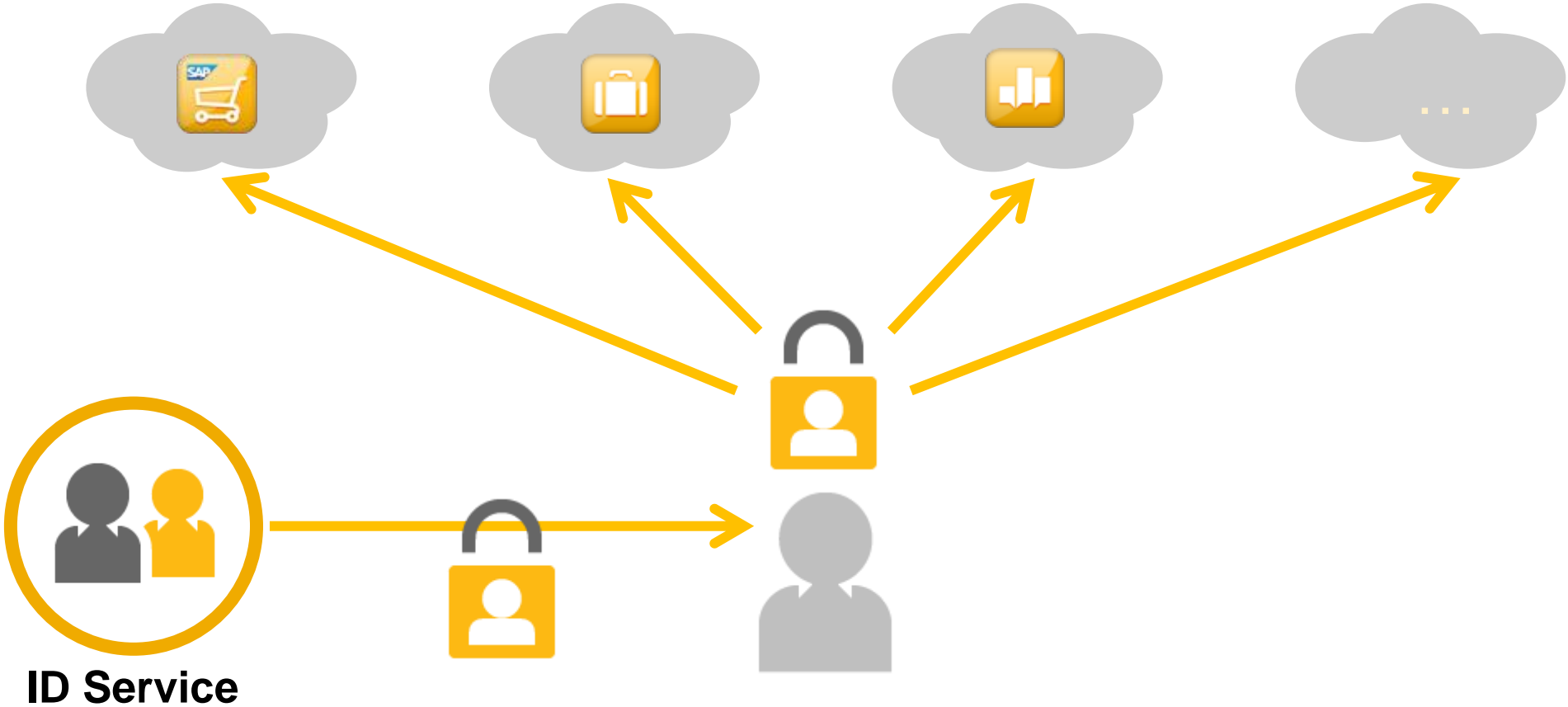
# Single Sign-On: The Corporate User's Perspective



# Single Sign-On: The Cloud User's Dilemma

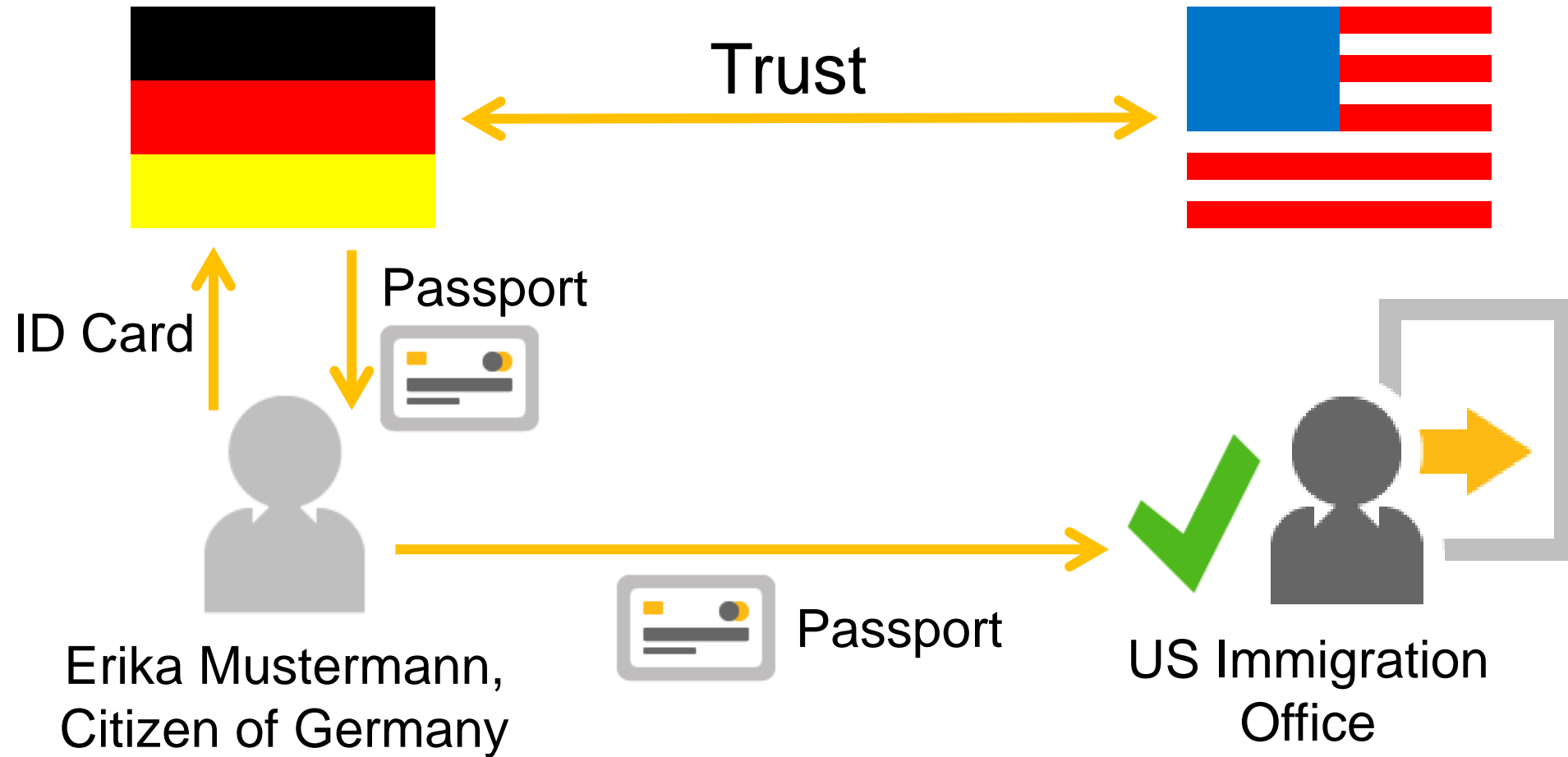


# Single Sign-On for the Cloud with ID Service from SAP

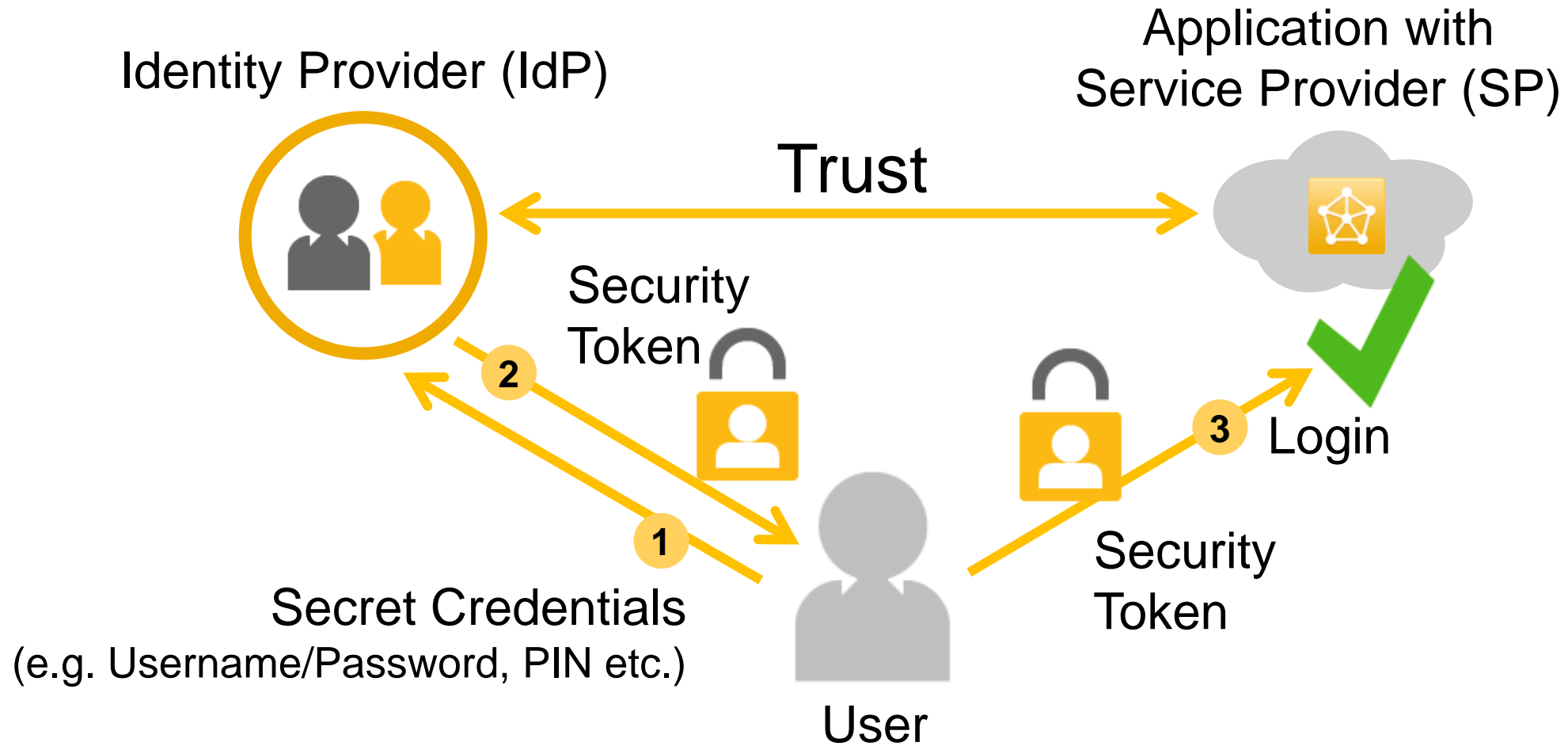




# Cross Boundary Travel – An Analogy for Single Sign-On



# Single Sign-On Fundamentals



# SAML – a Standard for Single Sign-On

## Security Assertion Markup Language

**XML-/HTTP-based protocol for web-based Single Sign-On and Single Log-Out**

## **SAML Security Token: Assertion**

- contains a user's authentication statement
- identifies the party who has issued the assertion with the statement
- may contain additional statements about the user's identity, i.e., role or group memberships of the authenticated user



### **Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0**

**OASIS Standard, 15 March 2005**

**Document identifier:**  
saml-core-2.0-os

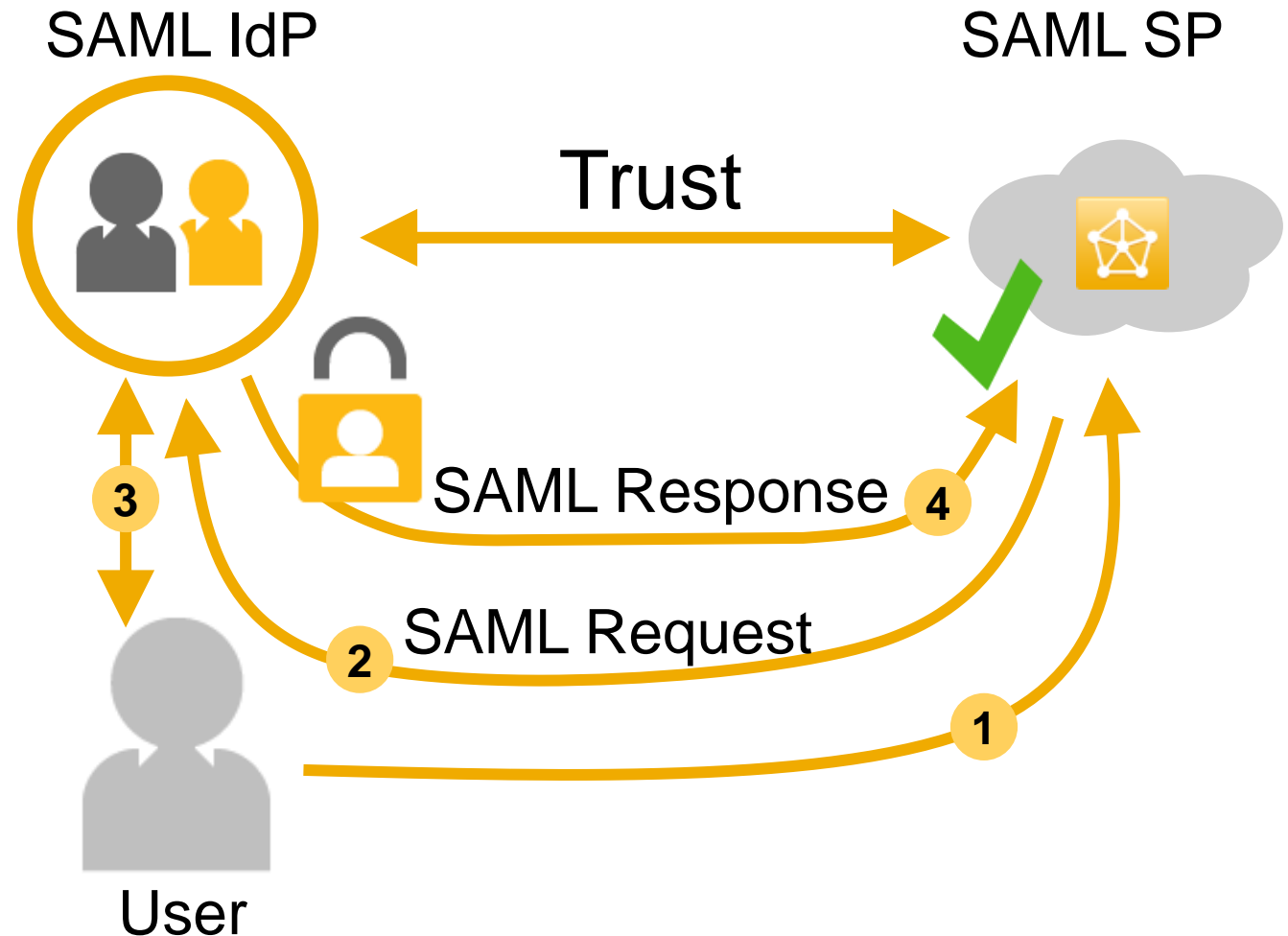
**Location:**  
<http://docs.oasis-open.org/security/saml/v2.0/>

**Editors:**  
Scott Cantor, Internet2  
John Kemp, Nokia  
Rob Philpott, RSA Security  
Eve Maler, Sun Microsystems

**SAML V2.0 Contributors:**  
Conor P. Cahill, AOL  
John Hughes, Atos Origin  
Hal Lockhart, BEA Systems  
Michael Beach, Boeing  
Rebekah Metz, Booz Allen Hamilton  
Rick Randall, Booz Allen Hamilton  
Thomas Wisniewski, Entrust  
Irving Reid, Hewlett-Packard  
Paula Austel, IBM  
Maryann Hondo, IBM  
Michael McIntosh, IBM  
Tony Nadalin, IBM  
Nick Ragouzis, Individual  
Scott Cantor, Internet2  
RL 'Bob' Morgan, Internet2  
Peter C Davis, Neustar  
Jeff Hodges, Neustar  
Fredrik Limb, NetScout

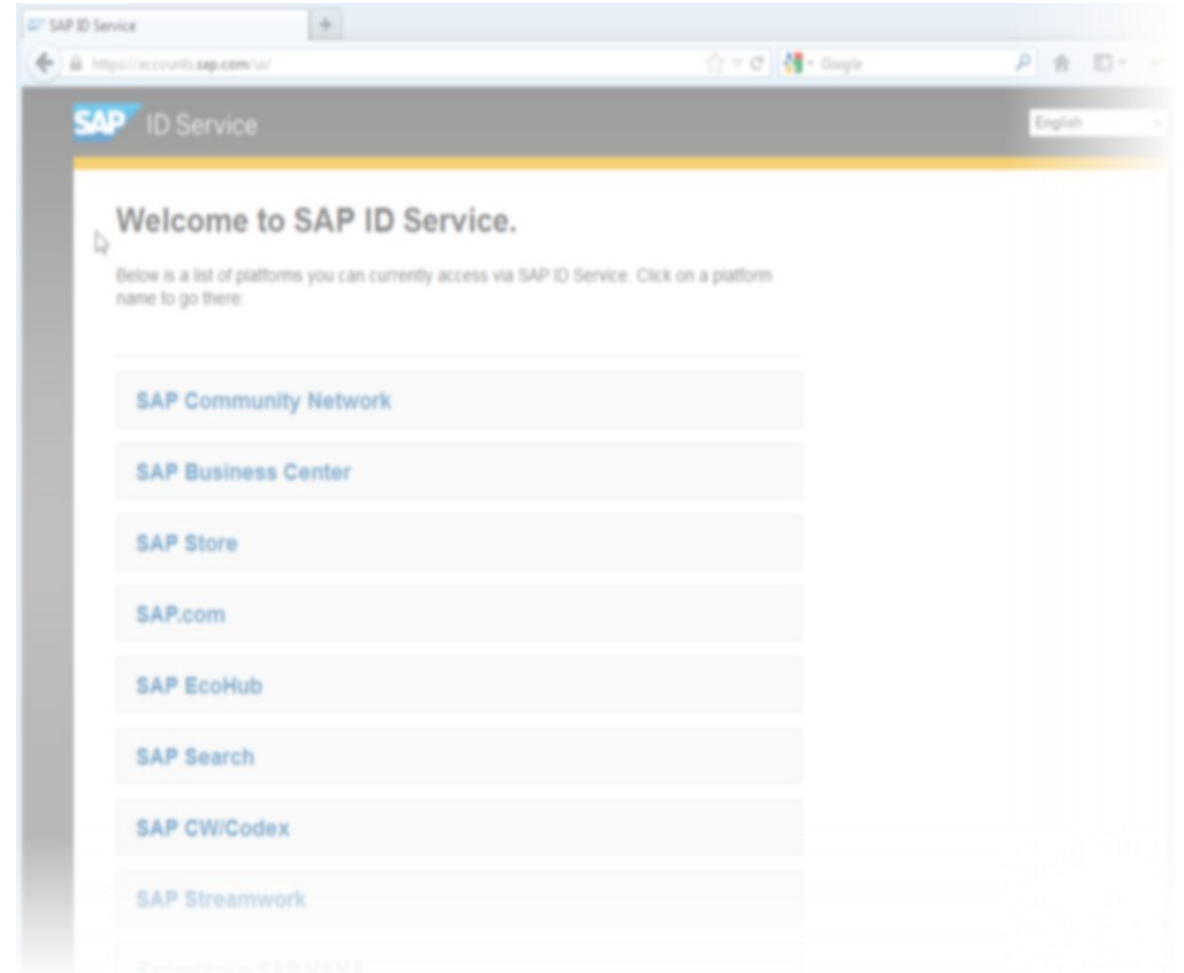
# Single Sign-On with SAML

- 1 User accesses protected web resource on Service Provider (SP)
- 2 SP sends SAML Authentication Request via HTTP redirect to trusted Identity Provider (IdP)
- 3 IdP authenticates the user (if not done already)
- 4 Upon successful authentication, IdP sends SAML Response (which includes the SAML Assertion) to the SAML Service Provider via HTTP POST



# ID Service: SAML-based IdP for the SAP Cloud

- **SAML2**-compliant Identity Provider
- A central store for identities related to **all on-demand applications** and **public web sites**
- Central management of **identity information** (including user information, such as name, descriptor, email address, customer relation, passwords, etc.)
- **Single Sign-On** between SAP on-demand applications and integration with third-party on-demand applications







# Demo

Single Sign-On to SAP Travel OnDemand and Amadeus with ID Service

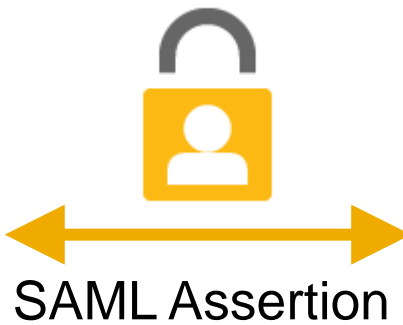


# ID Service: SAML-based IdP for the SAP Cloud (cont.)

ID Service  
(SAML-compliant  
IdP)



~4.2 Million Users

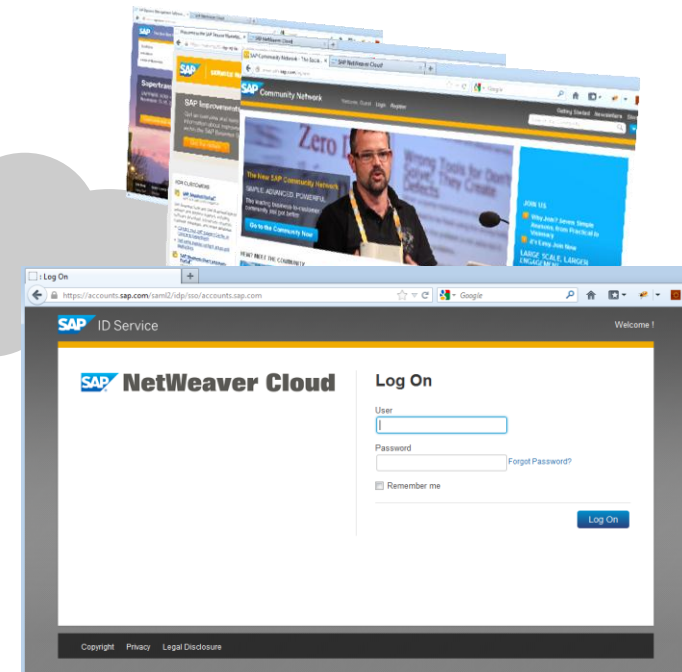


User  
(Individual, Customer, Partner)  
with *one* SAP identity

SSO



- SAP Public Web Sites (SAP.com, SMP etc.)
- SAP Business ByDesign Platform
- SAP Store
- ....




... and **SAP NetWeaver Cloud**




# **ID Service integration with SAP NetWeaver Cloud**



# SAP NetWeaver Cloud: An open, standards-based Platform as a Service for rapid development of on-demand applications

 Standards-based development and run-time environment

 Persistency service leveraging the speed of HANA

 Scalable Document Service for managing unstructured data

 Connectivity service enabling seamless integration with SAP and other systems

 Federated identity management (e.g. via the ID service)

 Remotely monitored and managed via a web-based Operations Console

 Mail Service enables messages to be sent directly from NW Cloud apps

 Built around the SAP Store

# Why using ID Service for SAP NetWeaver Cloud-based Applications?

---

## ID Service from SAP ...

- ... is an **instant user store** for all your identities that require access to protected resources of your SAP NetWeaver Cloud-based applications
- ... provides standards-based **SSO** that enables users to log on only once and get seamless access to all your applications deployed in the Cloud
- ... is an easy way for your Cloud-based applications to **delegate authentication and identity management to a central service** that is highly optimized for this task
- ... essentially keeps your developers **focused on the business logic**



# Supported scenarios to use ID Service an SAP NetWeaver Cloud deployed application

**Declarative authentication:** Resource protection as defined for the web.xml descriptor by the Java EE servlet API

→ **DEMO**

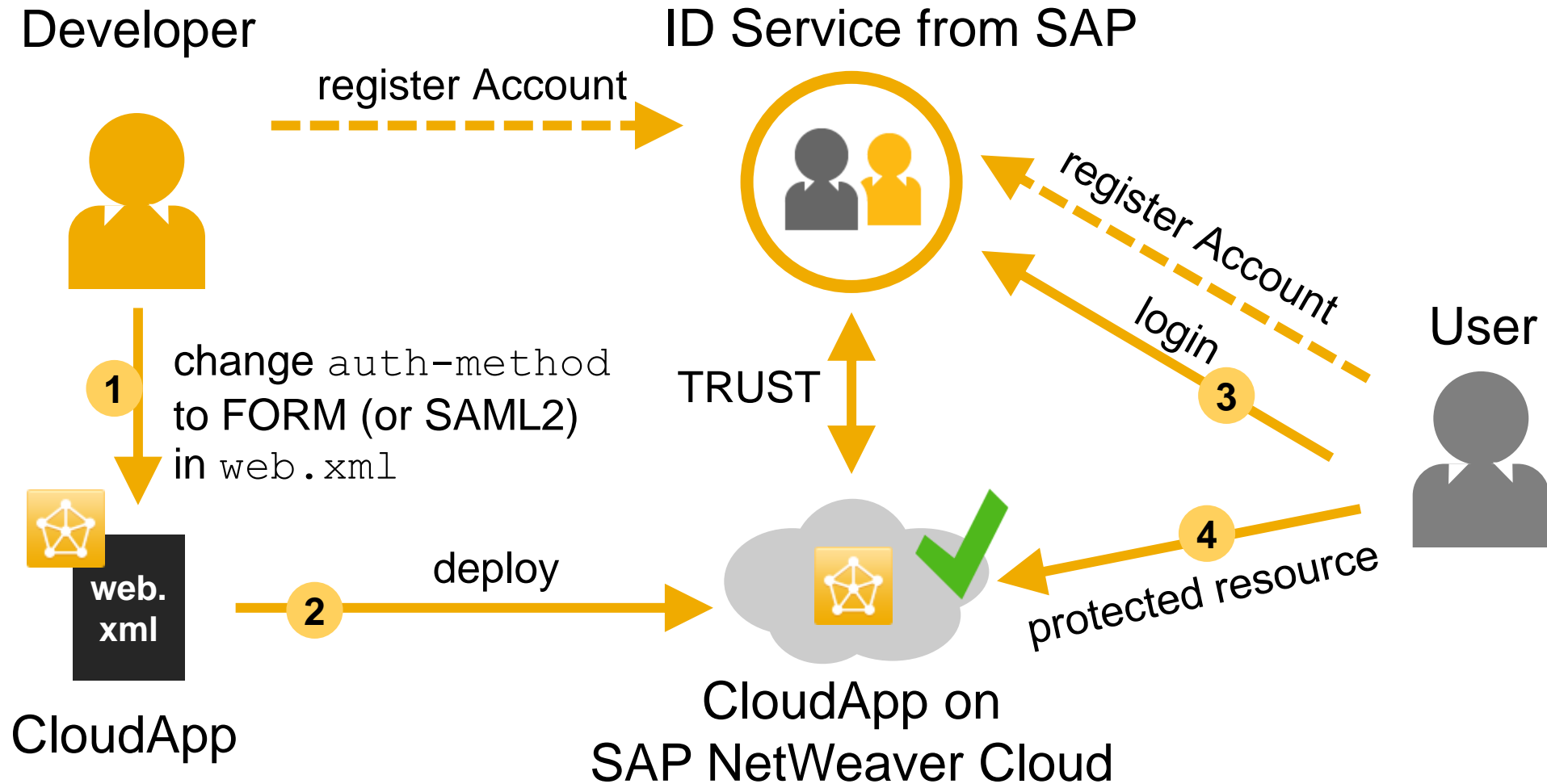
**Programmatic authentication:** Resource protection handled by the application code

**Programmatic logout:** Explicit logout within applications from a logout button or link

**User Profile Data:** Getting specific user attributes → **DEMO**

The screenshot shows the SAP NetWeaver Cloud login interface. At the top left, the SAP logo and 'ID Service' are visible. In the top right corner, there is a 'Welcome !' message. The main content area is split into two sections. On the left, the 'SAP NetWeaver Cloud' logo is displayed. On the right, the 'Log On' section contains a 'User' input field, a 'Password' input field with a 'Forgot Password?' link, and a 'Remember me' checkbox. A blue 'Log On' button is positioned at the bottom right of the login form. The footer of the page includes links for 'Copyright', 'Privacy', and 'Legal Disclosure'.

# Declarative authentication in the Cloud Application





# Demo

Delegate Authentication to ID Service in your Application on SAP NetWeaver Cloud



# Supported Authentication Methods for Applications deployed on the SAP NetWeaver Cloud Platform

<b>Scenario</b>	<b>Recommended &lt;auth-method&gt;</b>	<b>Comment/Constraints</b>
Web Application requiring SSO for external users and/or partners	<b>FORM/SAML</b>	-
Non-Browser Client (e.g. Command Line Tools)	<b>BASIC</b>	For SAML, JavaScript and HTML support by the Client/User Agent is required
AJAX Client (e.g. SAP UI5)	<b>FORM/SAML</b> or <b>BASIC</b>	AJAX calls must be within an existing session

**ID Service-supported Authentication Methods:  
SAML 2.0, BASIC AUTHENTICATION**

# Working with User Profile Attributes

Developer



1

Use `com.sap.security.um.user.*`  
User Management APIs



CloudApp

2

deploy

ID Service from SAP



`first_name`  
`last_name`  
`mail`  
`display_name`

3

Query  
Attributes of logged-in  
User



CloudApp on  
SAP NetWeaver Cloud



User



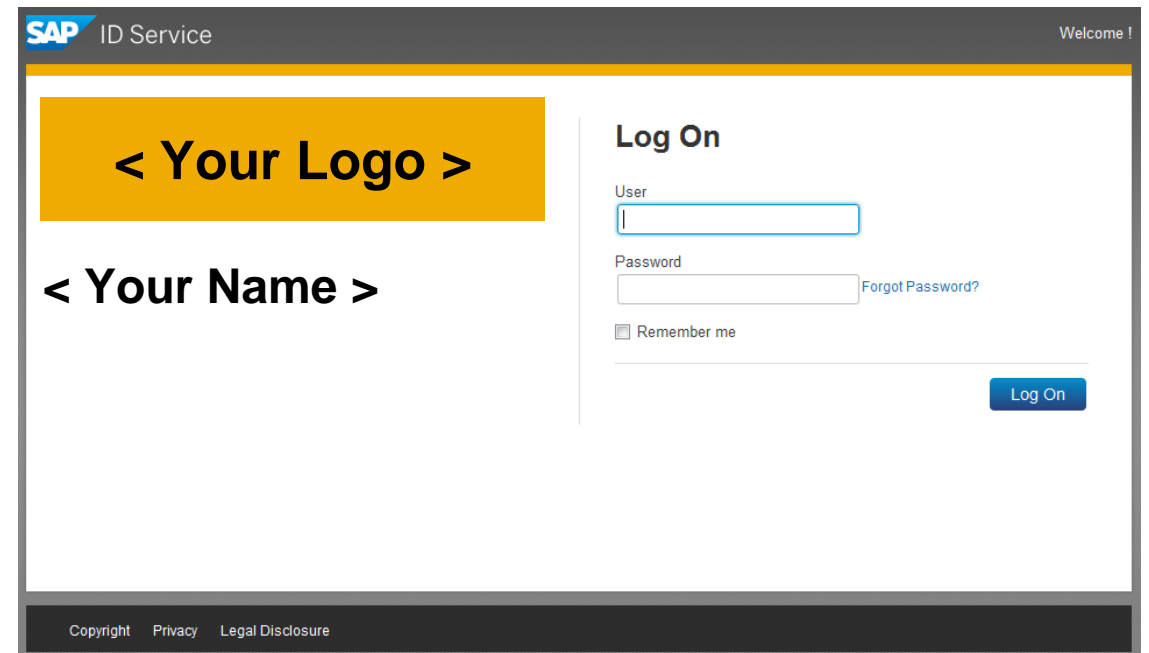


# Demo

Working with User Profile Attributes in your SAP NetWeaver Cloud-based application

# Outlook

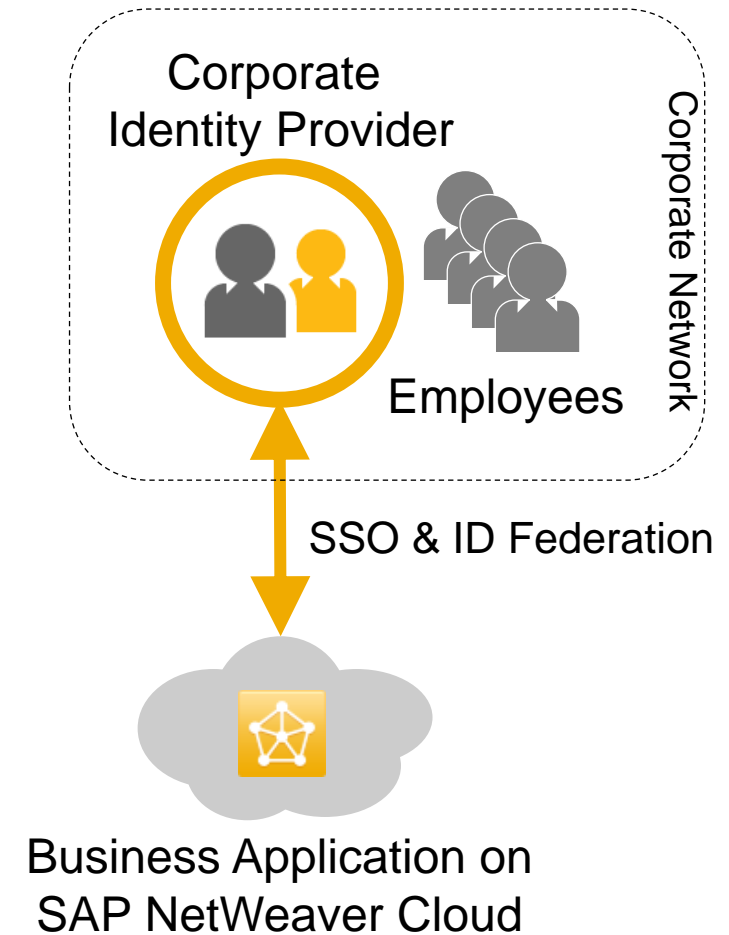
- (Mass) User Account Provisioning to ID Service from SAP NetWeaver Cloud
- Support for tenant-specific ID Service UI Customization in SAP NetWeaver Cloud
- SSO to SuccessFactors Cloud Applications



# Outlook (cont.)

- Managing Authorizations (Role Assignments) in the Cloud
- SSO and Identity Federation with corporate Identity Provider

→ Please join us for Session **CD260**



# Further Information

---

## SAP Public Web

SAP Insider Article: [Enable Secure Single Sign-On in the Cloud](#)

SAP NetWeaver Cloud Developer Center: <http://scn.sap.com/community/developer-center/cloud-platform>

SAP NetWeaver Cloud Identity Service:

[https://help.netweaver.ondemand.com/default.htm?id\\_service.html](https://help.netweaver.ondemand.com/default.htm?id_service.html)

## SAP Education and Certification Opportunities

[www.sap.com/education](http://www.sap.com/education)

## Watch SAP TechEd Online

[CD260](#) The Sky's the Limit – Cloud Single Sign-On and On-Premise Identity Federation  
Hands-On Workshop (2hr)

[CD261](#) Hands-On with SAP NetWeaver Cloud  
Hands-On Workshop (2hr)



# Feedback

Please complete your session evaluation for [SIS104](#).

**Thanks for attending this SAP TechEd session.**



# © 2012 SAP AG. 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 AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, PowerPoint, Silverlight, and Visual Studio are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, z10, z/VM, z/OS, OS/390, zEnterprise, PowerVM, Power Architecture, Power Systems, POWER7, POWER6+, POWER6, POWER, PowerHA, pureScale, PowerPC, BladeCenter, System Storage, Storwize, XIV, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, AIX, Intelligent Miner, WebSphere, Tivoli, Informix, and Smarter Planet are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and its affiliates.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems Inc.

HTML, XML, XHTML, and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Apple, App Store, iBooks, iPad, iPhone, iPhoto, iPod, iTunes, Multi-Touch, Objective-C, Retina, Safari, Siri, and Xcode are trademarks or registered trademarks of Apple Inc.

IOS is a registered trademark of Cisco Systems Inc.

RIM, BlackBerry, BBM, BlackBerry Curve, BlackBerry Bold, BlackBerry Pearl, BlackBerry Torch, BlackBerry Storm, BlackBerry Storm2, BlackBerry PlayBook, and BlackBerry App World are trademarks or registered trademarks of Research in Motion Limited.

Google App Engine, Google Apps, Google Checkout, Google Data API, Google Maps, Google Mobile Ads, Google Mobile Updater, Google Mobile, Google Store, Google Sync, Google Updater, Google Voice, Google Mail, Gmail, YouTube, Dalvik and Android are trademarks or registered trademarks of Google Inc.

INTERMEC is a registered trademark of Intermec Technologies Corporation.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

Bluetooth is a registered trademark of Bluetooth SIG Inc.

Motorola is a registered trademark of Motorola Trademark Holdings LLC.

Computop is a registered trademark of Computop Wirtschaftsinformatik GmbH.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase Inc. Sybase is an SAP company.

Crossgate, m@gic EDDY, B2B 360° , and B2B 360° Services are registered trademarks of Crossgate AG in Germany and other countries. Crossgate is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.