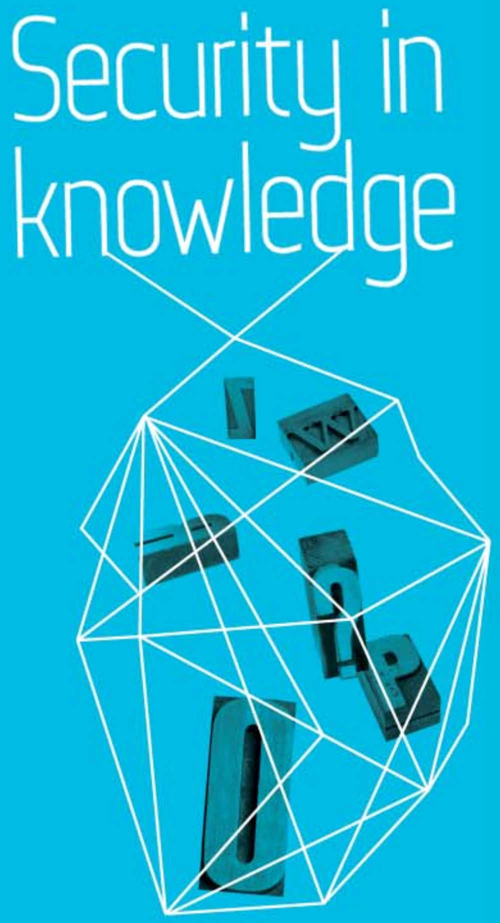
SAML Meets OAuth in the Cloud: A Marriage Made in Heaven



Riaz Zolfonoon

RSA, The Security Division of EMC

RSA CONFERENCE EUROPE 2013

Session ID: ARCH-R08

Session Classification: Intermediate

Agenda

- Introduction
- SAML Overview
- OAuth Overview
- Integration Use Cases

Introduction

IS OAUTH RELEVANT TO ENTERPRISES?

IS OAUTH REPLACING SAML?

WHAT ARE THE INTEGRATION USE CASES?

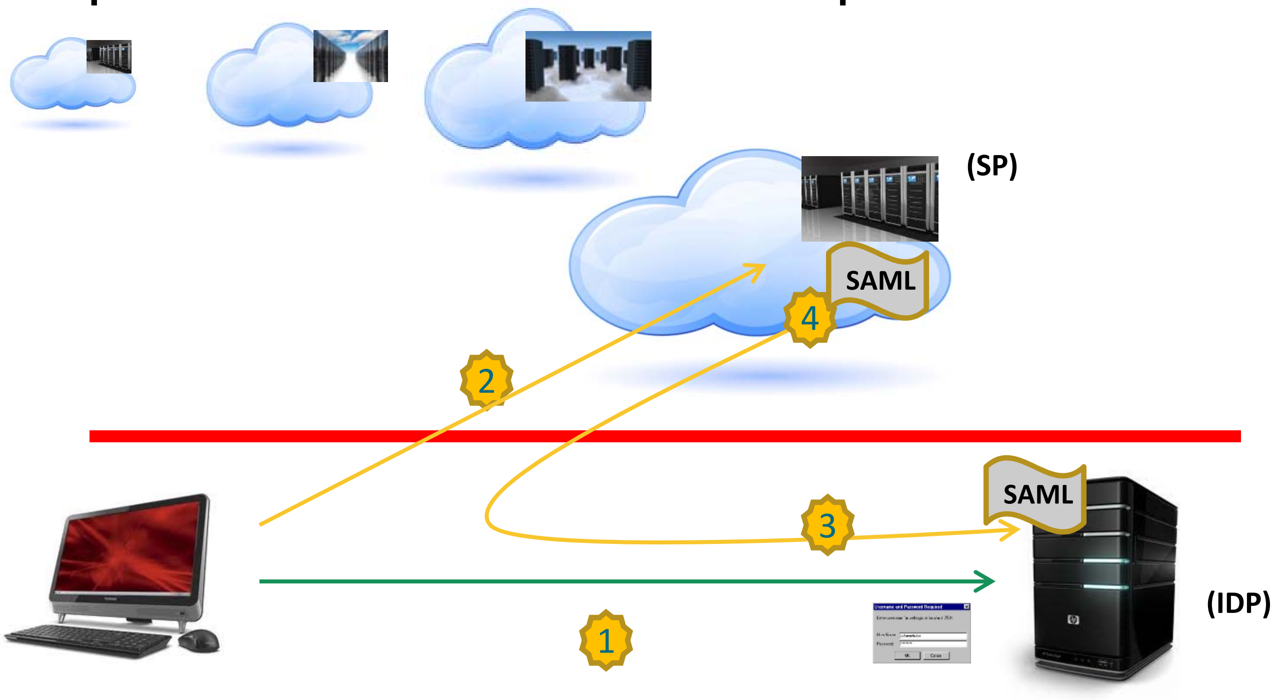
HOW ARE THESE PROTOCOLS HELPING ME WITH BYOI?

SAML Overview

- SAML= Security Assertion Markup Language
- Enables Single Sign-on across domains, using open standards
  - an alternative to proprietary SSO and Cross-Domain SSO solutions
- The Actors:
  - IDP
  - SP
  - Assertion Bearer

SAML Sample Scenario

- Definition: Employees need access to “Storage-in-the-Cloud”. But additional auth (i.e. another logon) are not acceptable. Need SSO with enterprise!



OAuth 2.0 Overview

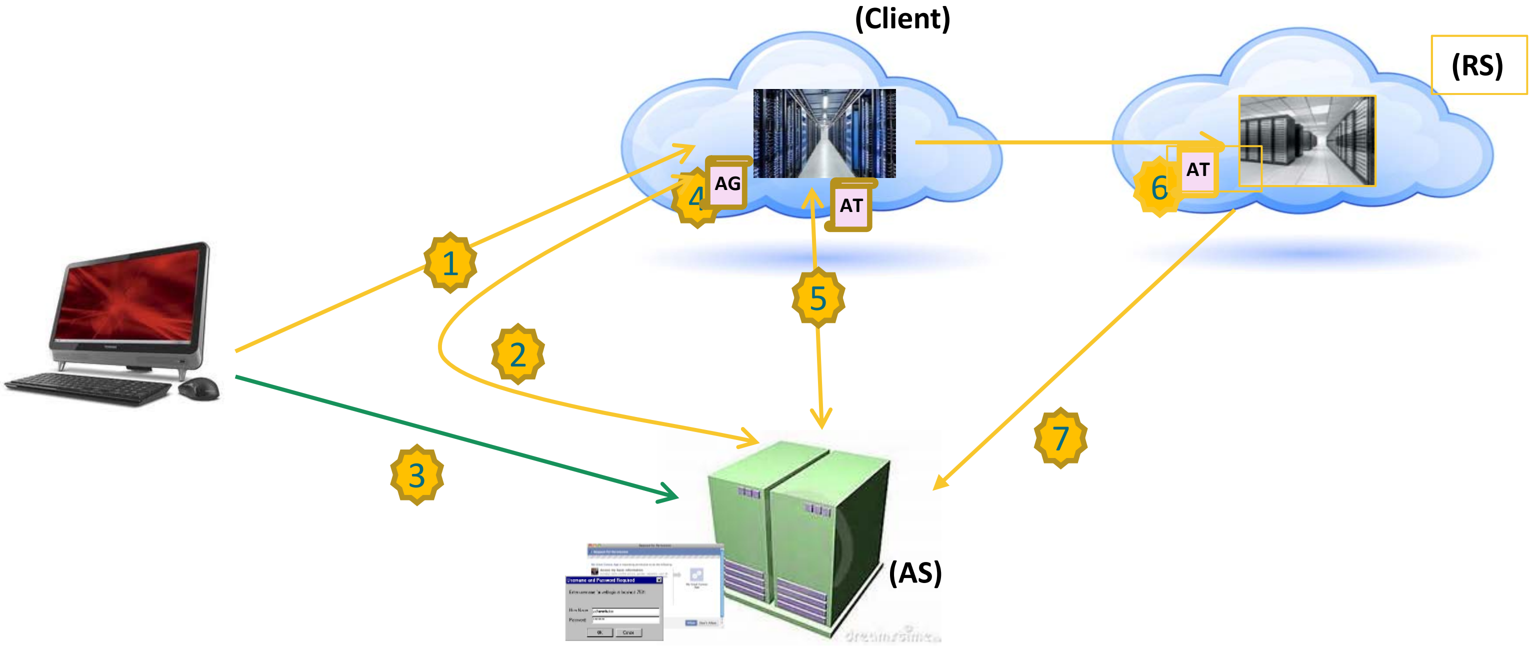
- OAuth = Open Authorization
- An open standard that allows users to share their private resources on one site (RS) with another site (Client) without having to hand out their credentials.
- Standards
  - IETF RFC 5849 - OAuth 1.0 Protocol
  - IETF RFC 6749 - OAuth 2.0 Authorization Framework

OAuth 2.0 Overview

- Actors
  - Resource Owner: end user
  - Resource Server (RS): hosting protected resource
  - Client: accessing resource on behalf of end user
  - Authorization Server (AS): issuing access token after successful auth

OAuth Sample Scenario

- Definition: Users access a “Corporate Benefits” portal which aggregates and presents health plan, 401K, and other corporate benefits from different sites



OAuth & Enterprise Challenges

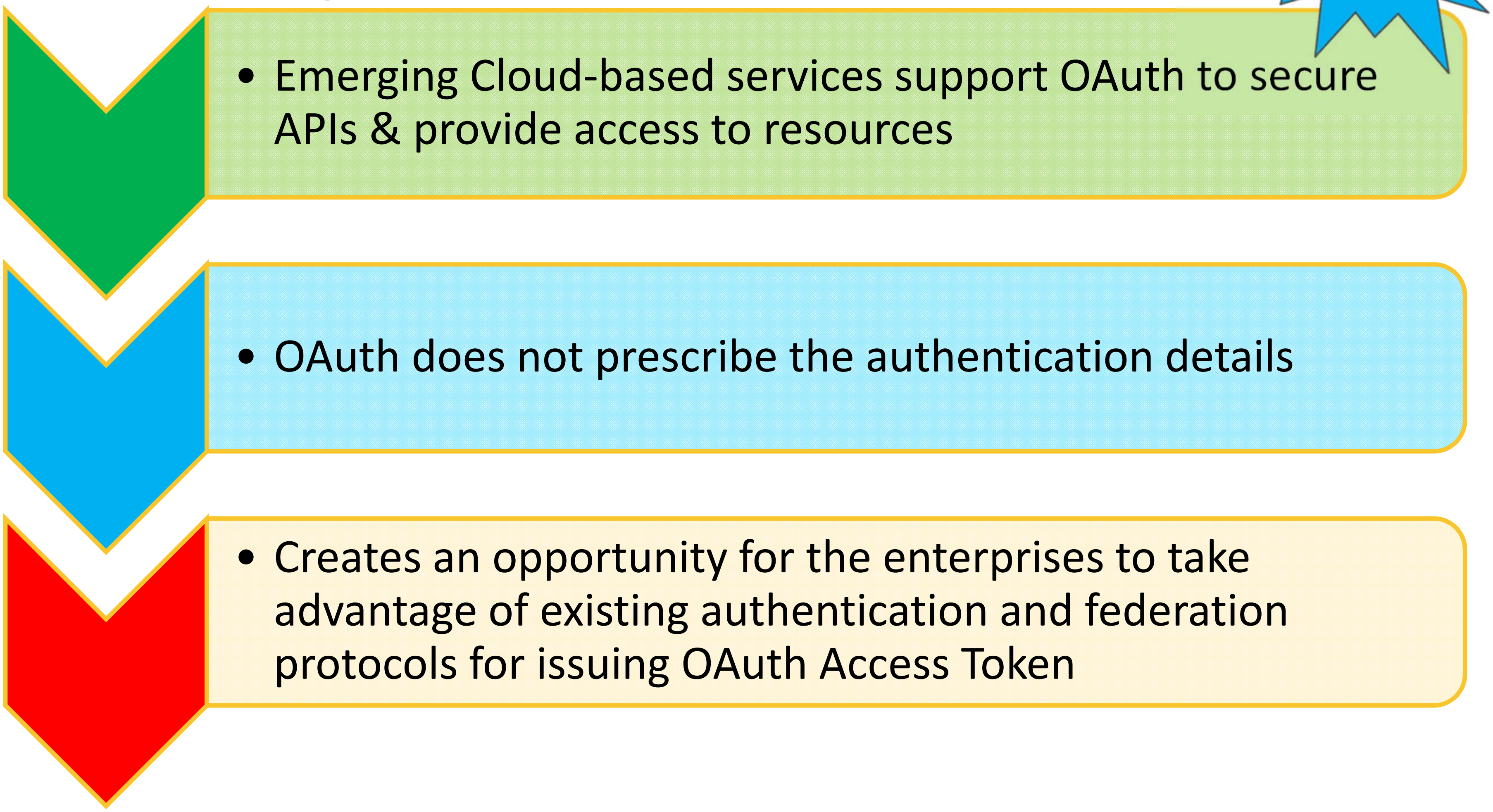
IS OAUTH RELEVANT TO ENTERPRISES?

Typical OAuth Use Cases	Typical Enterprise Use Case
User-centric	IT-centric
Simple authentication (focused on authorization)	Richer authentication
Low touch integration	High touch integration (e.g. with existing IAM)

Integration Use Cases

Business Perspective

WHAT ARE THE INTEGRATION USE CASES?

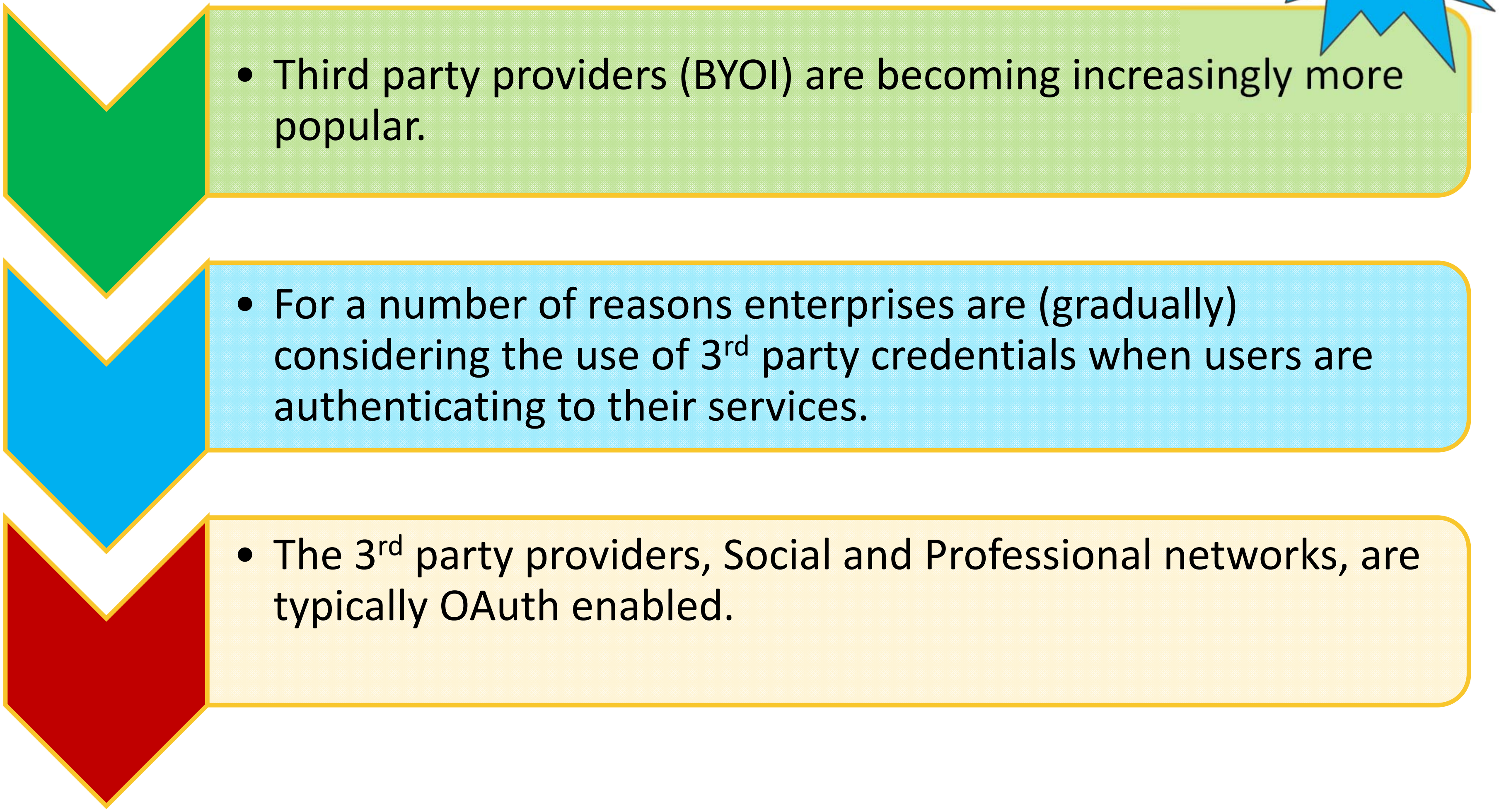


- Emerging Cloud-based services support OAuth to secure APIs & provide access to resources
- OAuth does not prescribe the authentication details
- Creates an opportunity for the enterprises to take advantage of existing authentication and federation protocols for issuing OAuth Access Token

Integration Use Cases

Business Perspective

WHAT ARE THE INTEGRATION USE CASES?

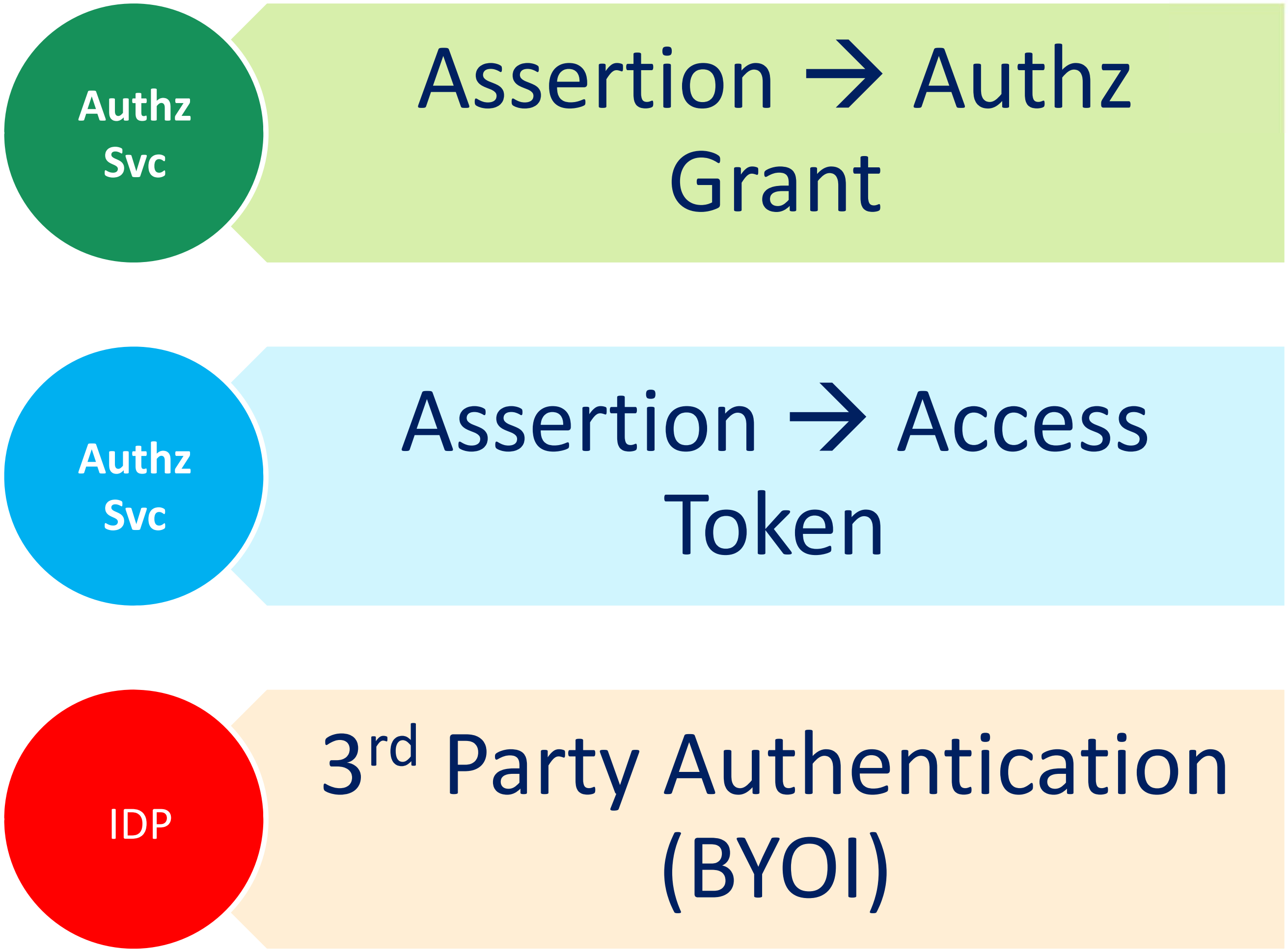


- Third party providers (BYOI) are becoming increasingly more popular.
- For a number of reasons enterprises are (gradually) considering the use of 3rd party credentials when users are authenticating to their services.
- The 3rd party providers, Social and Professional networks, are typically OAuth enabled.

Integration Use Cases

Technical Mapping

WHAT ARE THE INTEGRATION USE CASES?



Authz Svc

Assertion → Authz Grant

Authz Svc

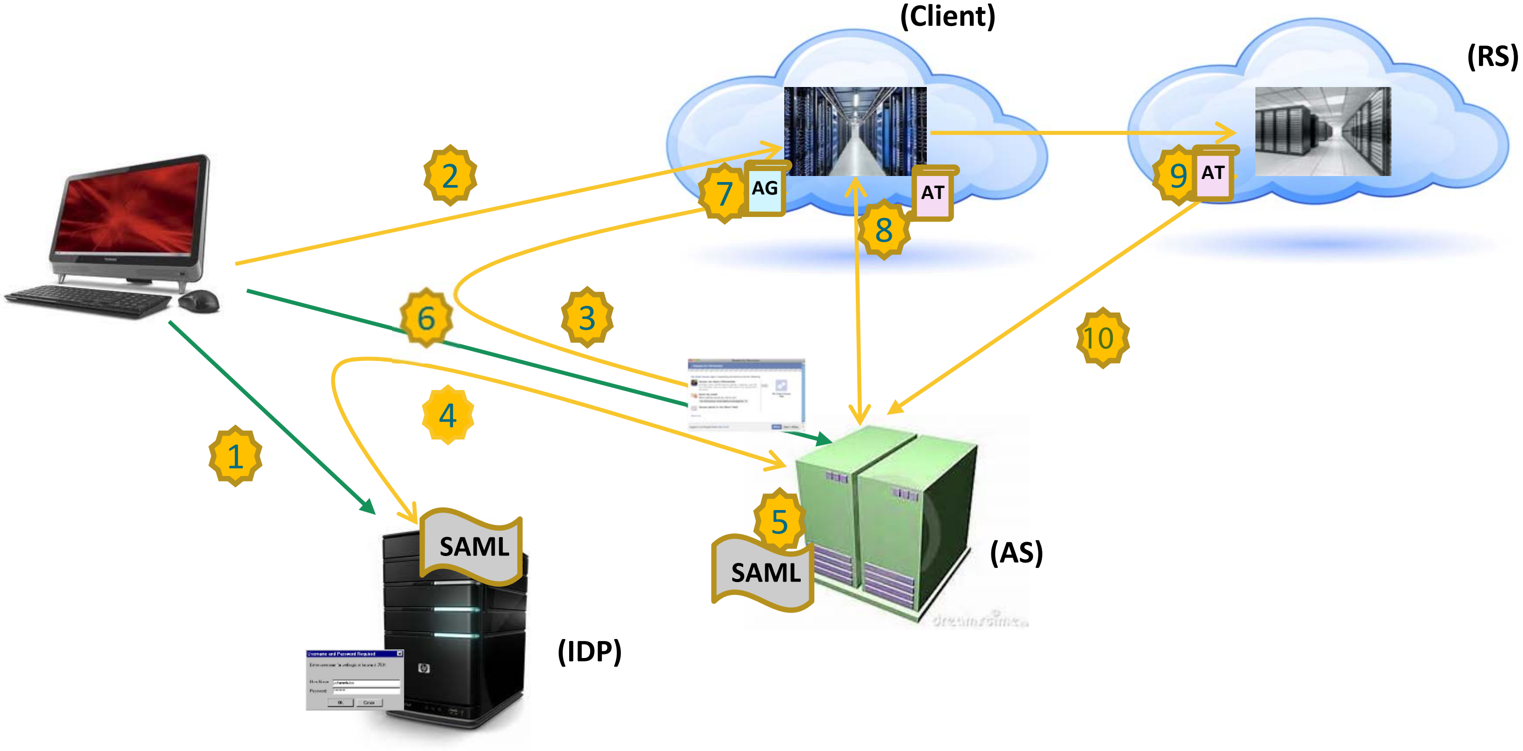
Assertion → Access Token

IDP

3rd Party Authentication (BYOI)

Integration Use Case

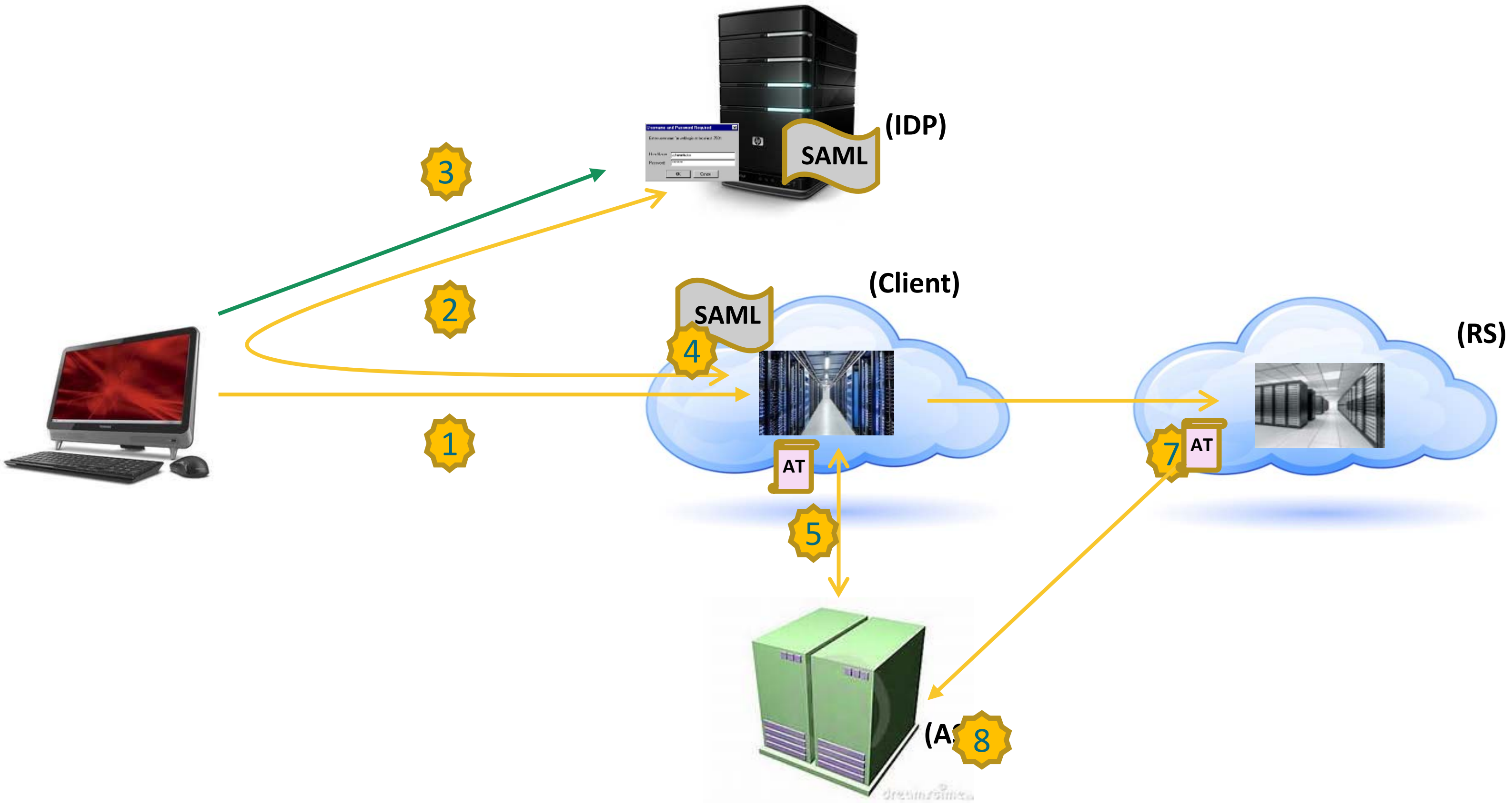
Requesting Authorization Grant using SAML Assertion



SAML
Assertion

Integration Use Case

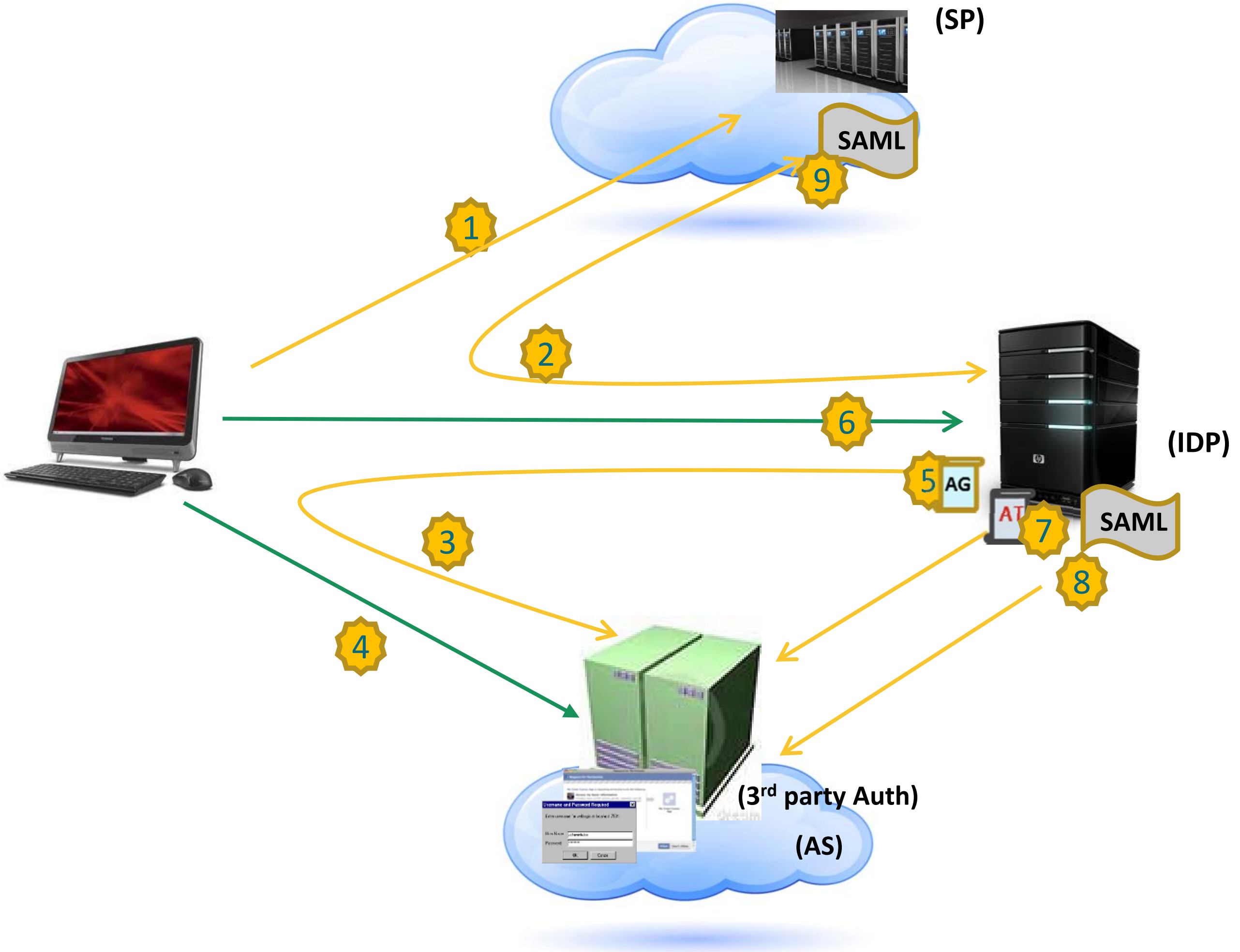
Requesting Access Token using SAML Assertion



Integration Use Case

3rd Party Authentication

HOW ARE THESE PROTOCOLS HELPING ME WITH BYOI?



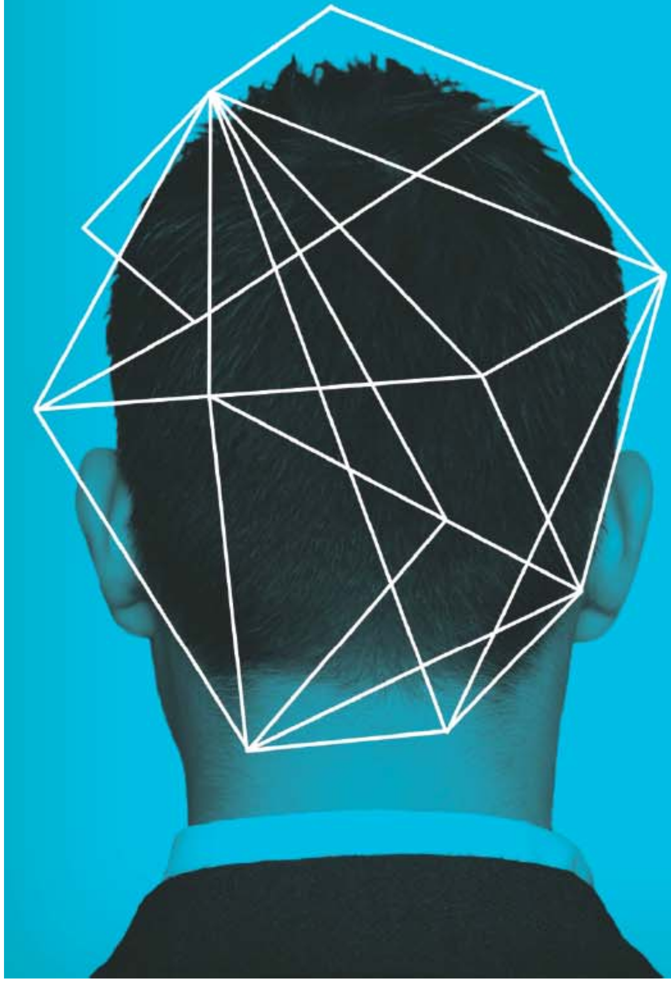
Conclusion

IS OAUTH REPLACING SAML?

- SAML and OAuth are complementary
- Enterprise investment in SAML is preserved
- Integrated use cases facilitate access to Could-based services
  - access to protected resources
  - external Identity Providers (BYOI)

References

- SAML Specifications
  http://saml.xml.org/saml-specifications
- The OAuth 2.0 Authorization Framework
  http://tools.ietf.org/html/rfc6749
- The OAuth 2.0 Authorization Framework: Bearer Token Usage
  http://tools.ietf.org/html/rfc6750
- SAML 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
  http://tools.ietf.org/html/draft-ietf-oauth-saml2-bearer-17



Thank you!

Riaz Zolfonoon

RSA, The Security Division of EMC

rzolfonoon@rsa.com

#RSAC

RSACONFERENCE EUROPE 2013