WSO2 Identity Management

Panagiotis Kranidiotis
panagiotis.kranidiotis@gmail.com

4 Νοεμβρίου 2017

WSO2 Identity Server

Few things about me

- First engagement with open source technologies in 1995
- Open source consultant and systems engineer since 2004
- VC of Hellug 2008 , 2009
- Member scientific advisory team of GFOSS (Open Technologies Alliance) 2009 - present
- Member of the board of GFOSS (Open Technologies Alliance) 2015-present

About this presentation

- WSO2 and WSO2 products
- Identity Management and definitions
- WSO2 Identity Server
- Installation
- Examples - Hands-on
- How to contribute

WSO2

- Open source platform for APIs, applications, and web services
- Founded by Sanjiva Weerawarana and Paul Fremantle in August, 2005, and has been backed by investment from Intel Capital
- WSO2 products are released under the Apache License Version 2.
- Sanjiva Weerawaranaformer IBM researcher creator of IBM SOAP4J, which later became Apache SOAP, architect of Apache Axis, Apache WSIF, the IBM Web Services Gateway and IBM BPWS4J
- Full open source products.

WSO2 Products

- WSO2 API Manager
- WSO2 Enterprise Intergrator (Former WSO2 Enterprise Service Bus , WSO2 Message Broker , WSO2 Data Services Server and WSO2 Business Process Server)
- WSO2 Identity Server
- WSO2 Analytics Server
- WSO2 IoT Server (Former Enterprise Mobility Manager)

Why to use SSO platform

- Security
- Reuse
- Easy role management
- APIs
- Combine multiple user stores

WSO2 Identity Server

Identity Management Definition

Identity management, also known as identity and access management (IAM) is, in computer security, the security and business discipline that ”enables the right individuals to access the right resources at the right times and for the right reasons”. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements

Definitions

- **Authentication :** Verification that an entity is who/what it claims to be using a password, biometrics such as a fingerprint, or distinctive behavior such as a gesture pattern on a touchscreen.
- **Federated Authentication :** The ability to use 3rd party Identity providers to authendicate localy
- **Authorization :** Managing authorization information that defines what operations an entity can perform in the context of a specific application.
- **Roles :** Roles are groups of operations and/or other roles. Users are granted roles often related to a particular job or job function.
- **Attributes ή Claims :** A claim is a statement that one subject, such as a person or organization, makes about itself or another subject.

WSO2 Identity Server

Identity Management Architecture

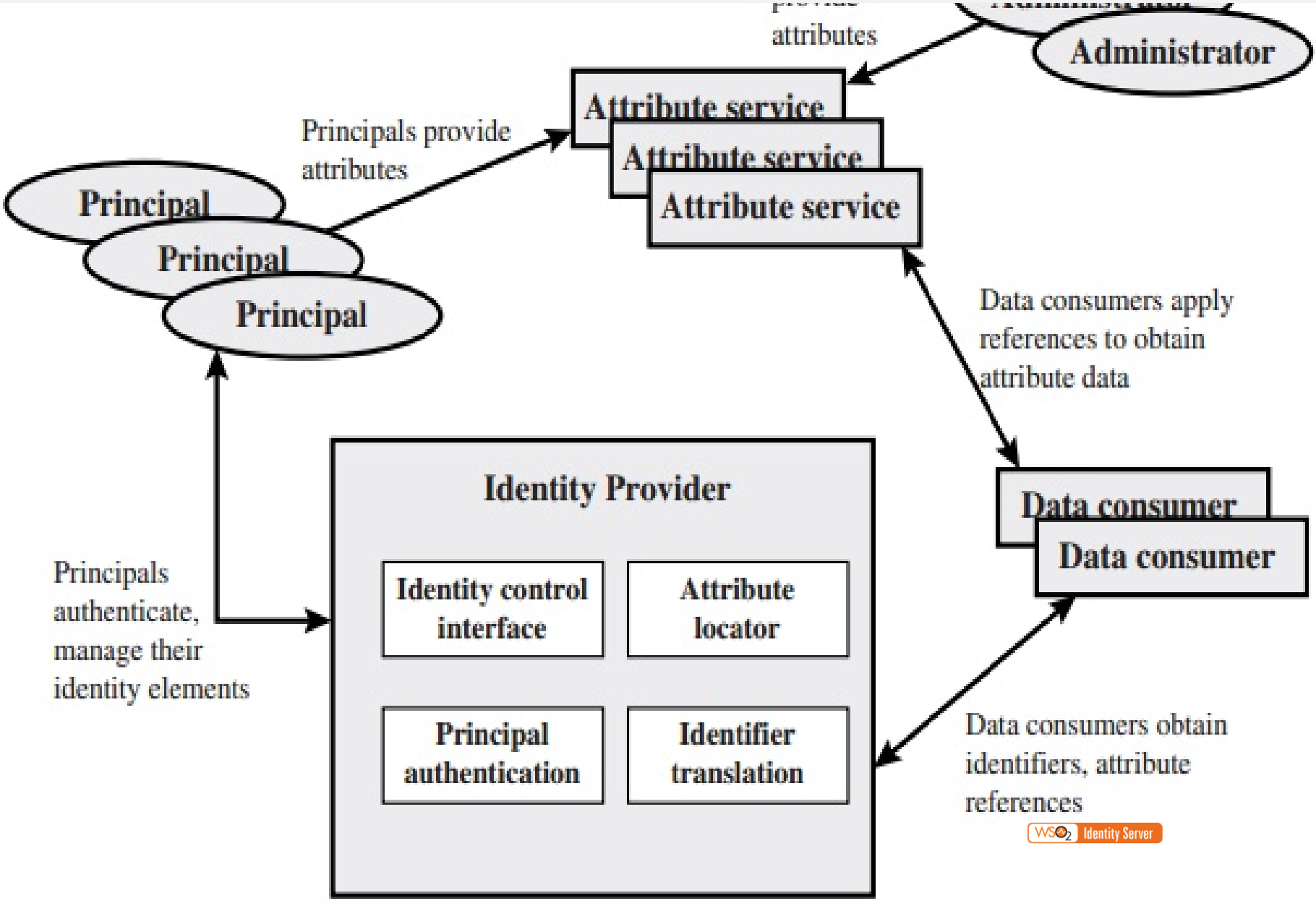


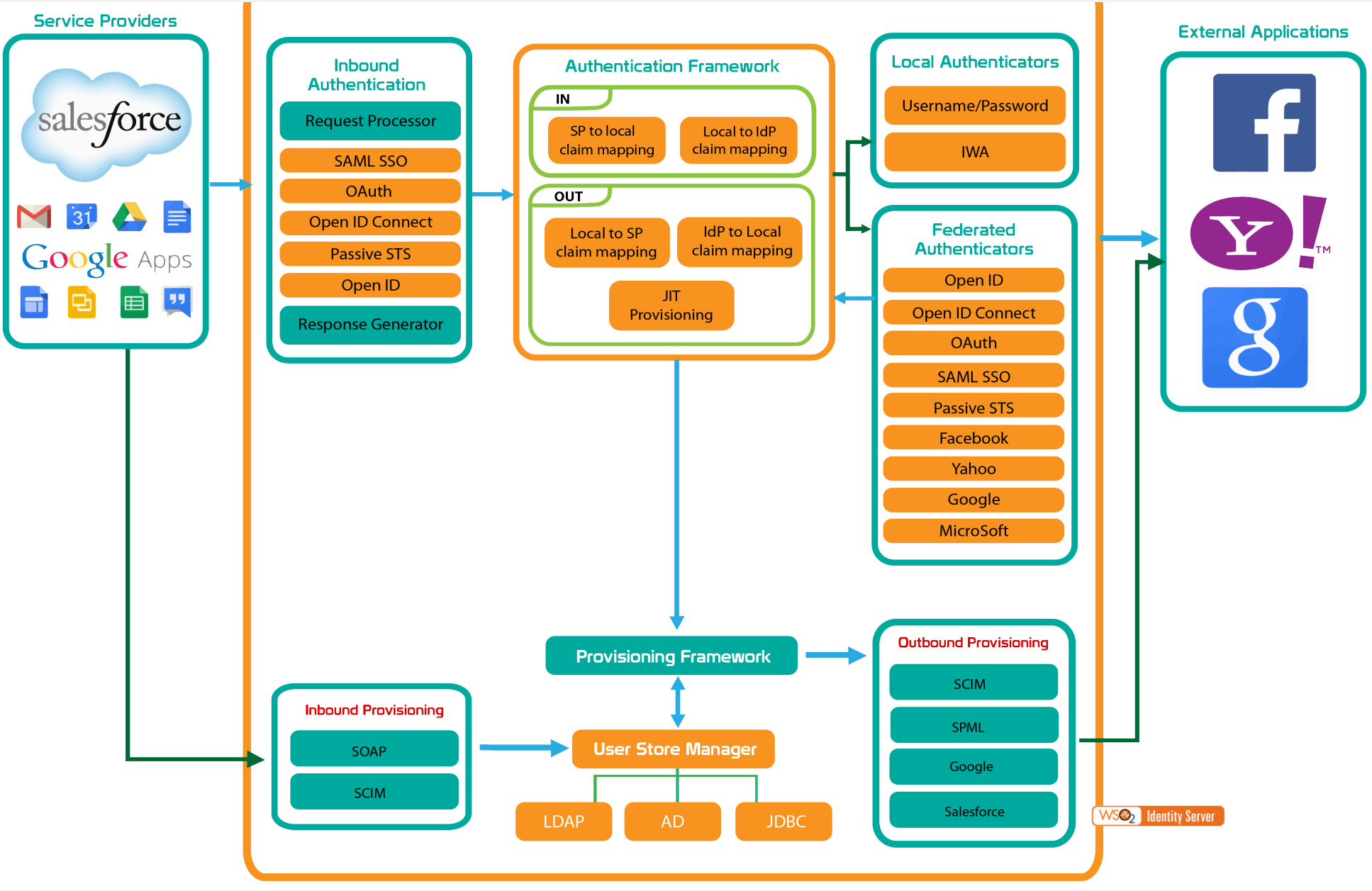
Figure 15.3 Generic Identity Management Architecture

Some more definitions

- **Userstore** : the system where information about the users and user roles is stored, including log-in name, password, first name, last name, and e-mail address. Usualy a DB or an LDAP
- **Identity Provider** : An Identity Provider (IdP) is responsible for issuing identification information and authenticating users by using security tokens like SAML 2.0, OpenID Connect, OAuth 2.0 and WS-Trust.
- **Federated IdP :** A 3rd party IdP that it can be consumed localy.
- **Service Provider :** A Service Provider (SP) is an entity that provides Web services.
- **Inbound Provisioning :** Inbound provisioning focuses on how to provision users to the Identity Server and it’s userstores
- **Outbound Provisiong :** Outbound provisioning talks about provisioning users to external systems.

WSO2 Identity Server

WSO2 Identity Server Architecture



WSO2 IdS Features - SSO

- Security Assertion Markup Language 2 (SAML2) and OpenID connect support
- Single logout
- SSO between on-premise applications and cloud applications
- Simple service provider and identity provider ecosystem management

WSO2 IdS Features - Identity Federation

- Federated SSO with external identity providers
- Support for Facebook, Google, Microsoft Windows Live and more
- User claims and roles transformation

WSO2 Identity Server

WSO2 IdS Features - Strong Authentication

- Multi-option and multi-factor authentication support
- Kerberos and X.509 support
- 2-factor authentication including FIDO, SMS/Email OTP, MePin and more

WSO2 IdS Features - Identity Governance and Administration

- User and group management
- User self service features (account recovery, self registration, account locking, etc.)
- Provisioning based on standards such as SCIM (System for Cross-domain Identity Management) and SPML (Service Provisioning Markup Language)
- On the fly and rule-based provisioning
- Workflows to user and role management and approval driven by templates
- HTML and multi-language email template support

WSO2 Identity Server

WSO2 IdS Features - Entitlement and Access Control

- Fine-grained authorization with eXtensible Access Control Markup Language (XACML) policies
- API security with delegated access control using OAuth2 and support for SAML2 bearer, JSON Web Token (JWT) assertion and Integrated Windows Authentication with NT LAN Manager (NTLM-IWA) grant types

Installation

- Download the latest built zip file
- Install the Oracle JDK
- Download the myslq or postgresql JDBC driver
- Prepare the database or the external ldap
- Create a valid SSL certificate and add it to Java Keystore. Use ie LetsEncrypt
- Change the hostname to the FQND
- Open the right ports on firewall (by default 9443)

Applications that can use IdS

- Any custom web app through protocols like SAML2, OAUTH2, OpenId
- Mobile apps usually with OAUTH2
- Web Services
- Standard web cms (drupal, wordpress etc)have plugins for SSO
- Windows shares, email accounts and legacy apps if you are using LDAP as user store

How to contribute

- Read the documentation https://docs.wso2.com/display/IS530/
- Check Stackoverflow for answers in your questions
- Learn the correct wso2 repositories for each product
- Need to know to build maven projects
- Better to use an IDE (ie Eclipse)
- https://wso2.github.io/