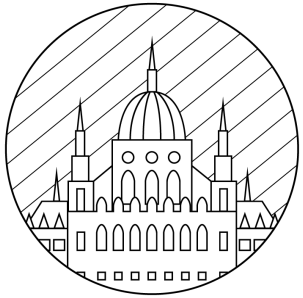
Security As A Service Leveraged by Apache Projects

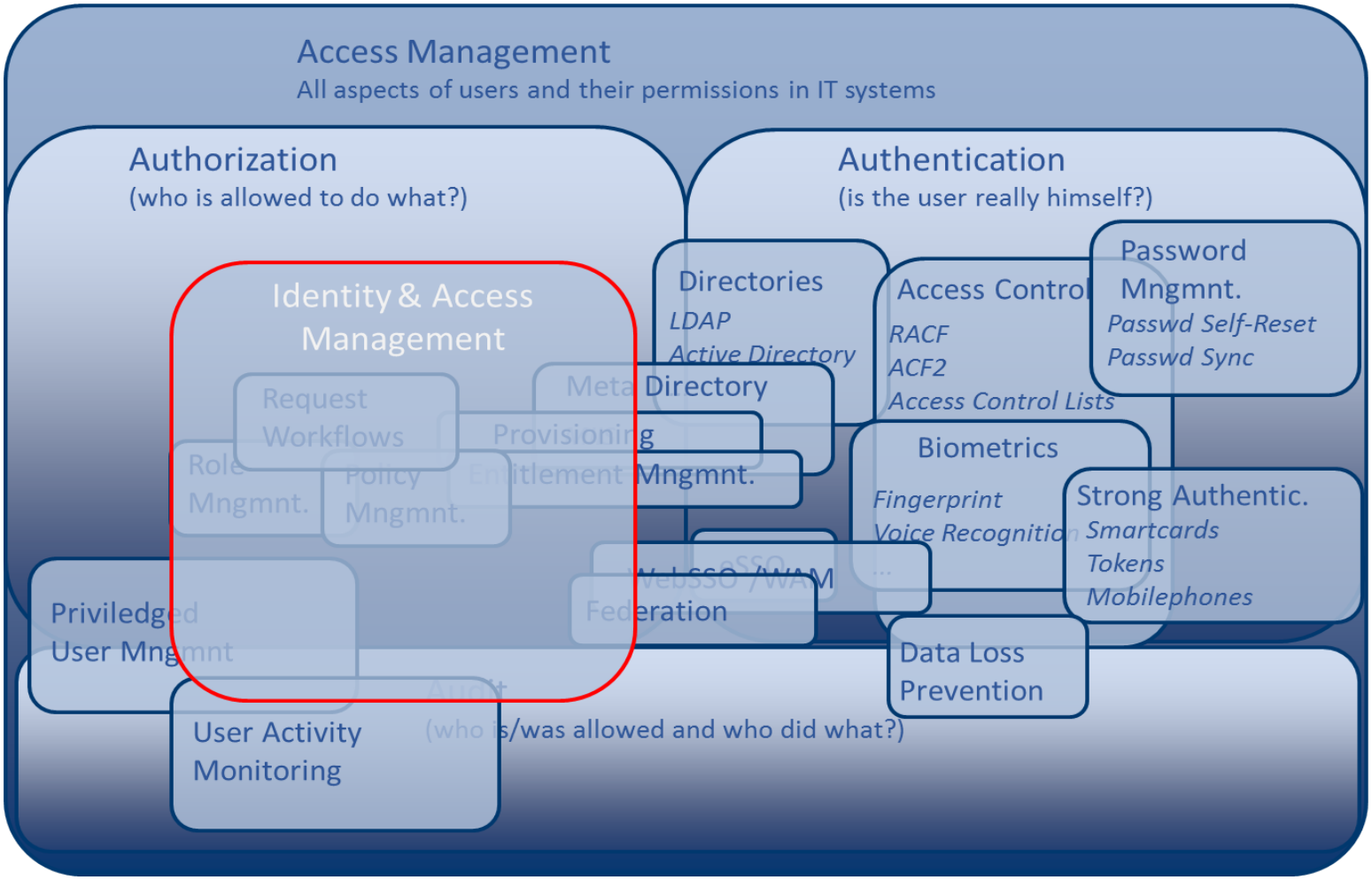
Oliver Wulff, Talend



APACHECON EUROPE

CORINTHIA HOTEL
BUDAPEST, HUNGARY
NOVEMBER 17-21, 2014

Application Security Landscape



Solution Building blocks

- Apache CXF Fediz
  - Single Sign On (WS-Federation)
  - Attribute Based Access Control (SAML AttributeStatement)
  - Identity Provider and Application Server Plugin
- Apache Syncope
  - IAM (User management, Attribute Management, Provisioning)
  - Connector LDAP
- Apache DS
  - LDAP Server
- PostgreSQL
  - Database for Syncope and Fediz IDP

Solution Building blocks

Demo

Federation/SSO with Apache Tomcat Application

Solution Building blocks

Apache CXF Fediz

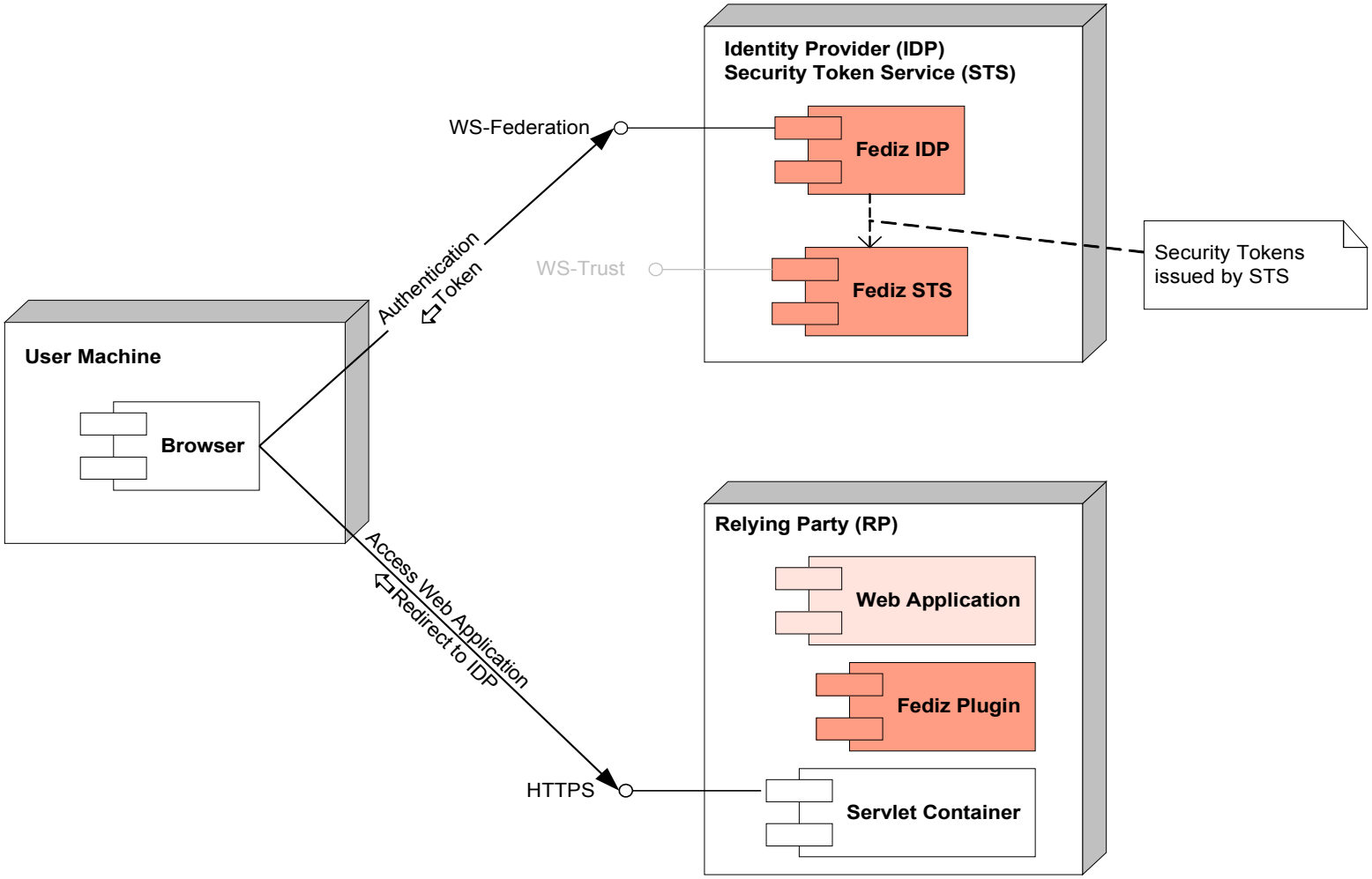
Apache CXF Fediz

- Sub-project of Apache CXF project
- Work started mid of 2011
- Community growing
- First release in June 2012
- Current release 1.1.2
- Finishing work for 1.2

OASIS WS-Federation 1.2

- OASIS Standard 2009
- Security Token agnostic (SAML 1.1/2.0, …)
- Extends OASIS WS-Trust
- Browser and Web Services SSO
- PRP adapts Browsers to WS-Trust
- No connectivity between Application and IDP required (Cloud)
- Claims/Attribute Based Access Control
- Supports several Authentication domains

WS-Federation



Fediz Plugin

- WS-Federation 1.0/1.1/1.2
- SAML 1.1 / 2.0 Tokens
- SAML-P support
- IDP trust types
  Chain Trust, Direct Trust
- Core Logic Container independent
- Supports Tomcat, Jetty, Karaf, Websphere and Spring Security
- WS-Federation Metadata
- Claims provided in FederationPrincipal

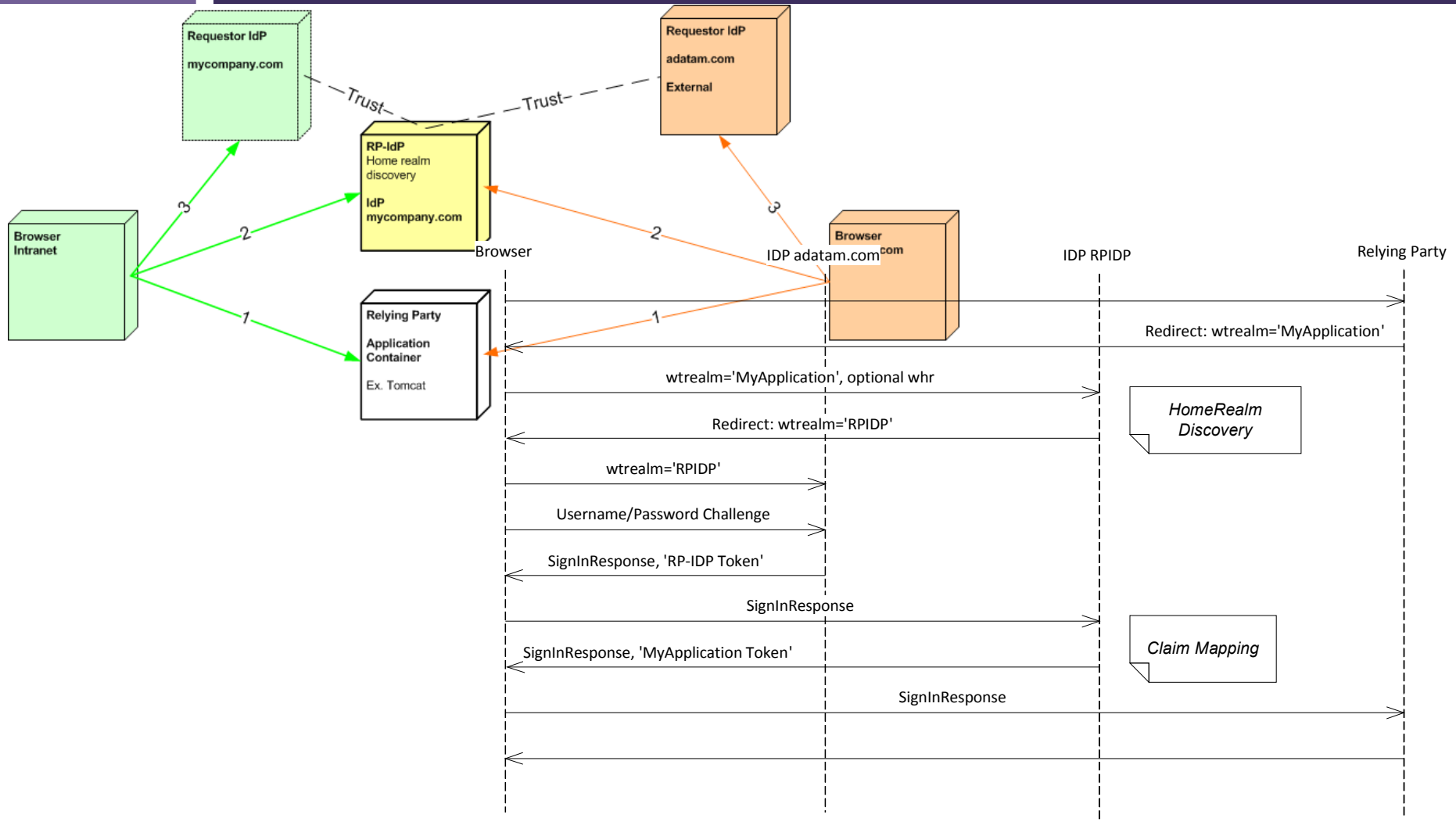
Fediz IDP/STS

- Authentication: Username/password, Kerberos, X509
- Spring Security (REST, Login)
- Spring Web Flow
- User Store:
  - File store (Mock testing)
  - LDAPLoginModule
  - Custom JAAS Login Module or custom WSS4J Validator
- Claims/Role store:
  - LdapClaimsHandler
  - FileClaimsHandler (Mock testing)
- SAML Token creation customizable

New Features in Fediz 1.1

- Fediz IDP refactored and leverages Spring Webflow
- WS-Federation support for RP-IDP
- HomeRealm Discovery
- Kerberos support
- Support encrypted SAML tokens
- SAML Holder-Of-Key
- New Containers supported: Karaf, Jetty, Spring Security and IBM Websphere
- Claim Mapping support with Apache Commons JEXL

Fediz IDP Relying Party Home Realm Discovery



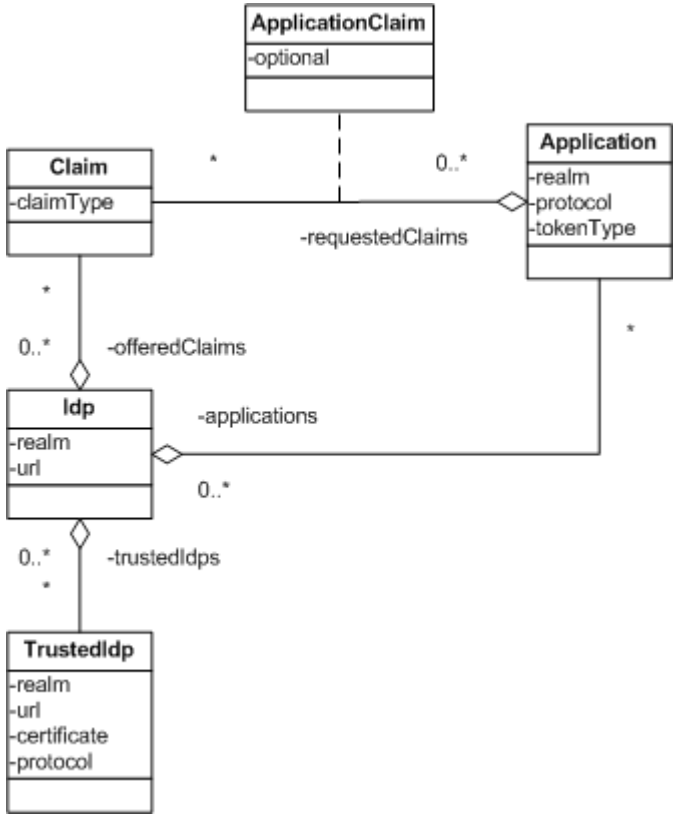
Fediz Roadmap

- Security Protocol pluggable in IDP (1.2)
  WS-Federation, SAML-P, Oauth2, ...
- IDP REST Interface (1.2)
  - Configure Claims, IDPs, Applications, Trusted IDPs
  - Fine grained security control
- SAML-P support in Fediz plugin (1.2)
- Fediz CXF Plugin (Security Protocols supported for JAX-RS)
- OAuth 2
- Launch Fediz IDP from Maven build (1.2)
- Single Logout (1.2)

REST Interface (1/3)

Resources

- Idp
  - `/idps`
- Claim
  - `/claims`
  - Many-to-many (requestedClaims, offeredClaims)
  - Attribute on Relation
- Application
  - `/applications`
  - many-to-many
- TrustedIdp
  - `/trustedIdps`
  - many-to-many



REST Interface (2/3)

- Many-To-May Relationship

```
/applications                                POST|GET
/applications/{realm}                        GET|PUT|DELETE
/applications/{realm}/claims                        POST
/applications/{realm}/claims/{claimType}    DELETE
```

- HTTP Error Codes (besides 200)
  - NoContent (204)
  - Error (500)
  - Created (201)
  - NotFound (404)
- Content Type
  - XML
  - JSON

REST Interface (3/3)

- HTTP Headers
  - Location (newly created resources)
  - X-Application-Error-Code, X-Application-Error-Info
- Query parameters (start, size, expand)
- Hypermedia support? (href Attribute, link Element)
- Security
  - Roles
  - Entitlements (CLAIM_LIST, CLAIM_CREATE, …, ROLE_CREATE, ...)

Solution Building blocks

Demo

Configure application using Fediz

Configure application in Fediz IDP (REST)

Federation/SSO with Apache Tomcat Application

Solution Building blocks

Apache Syncope

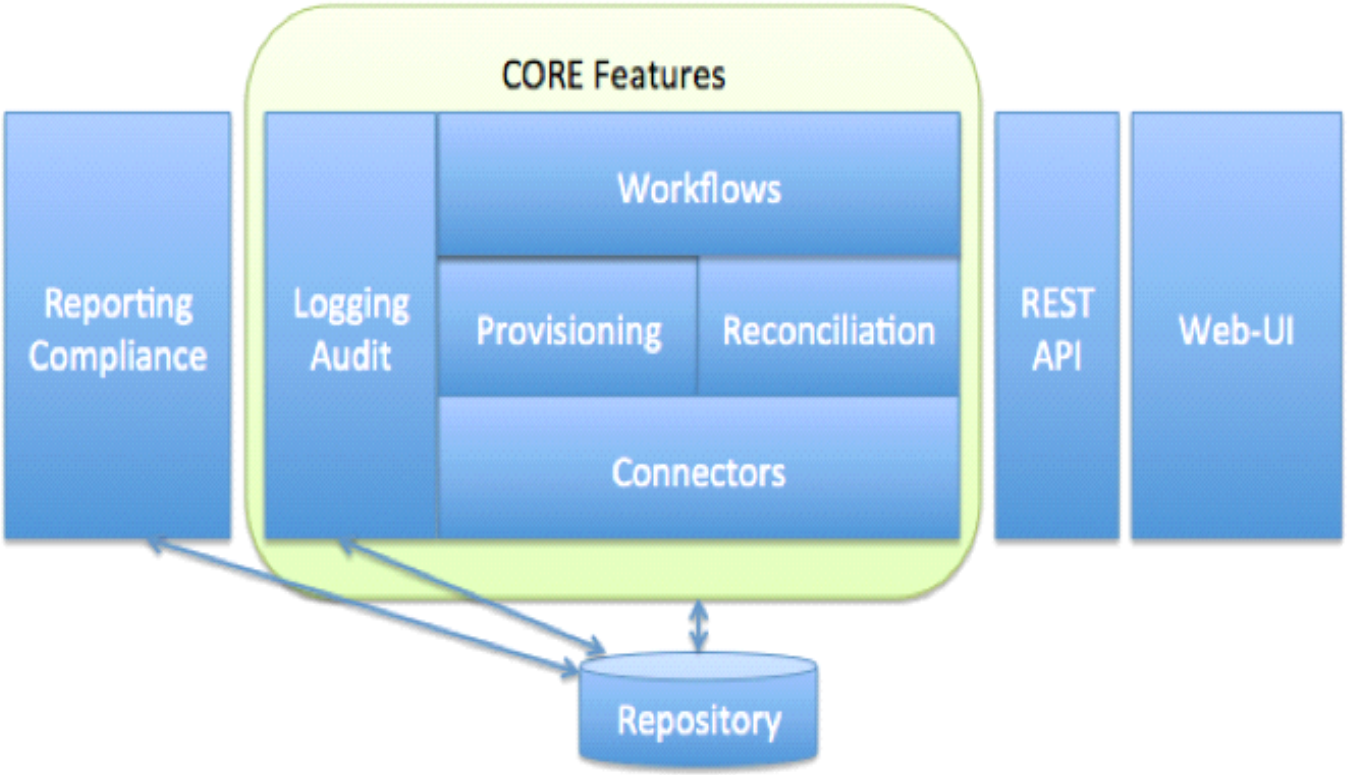
Identity Access Management

- Who has/had access to What, When, How, and Why?

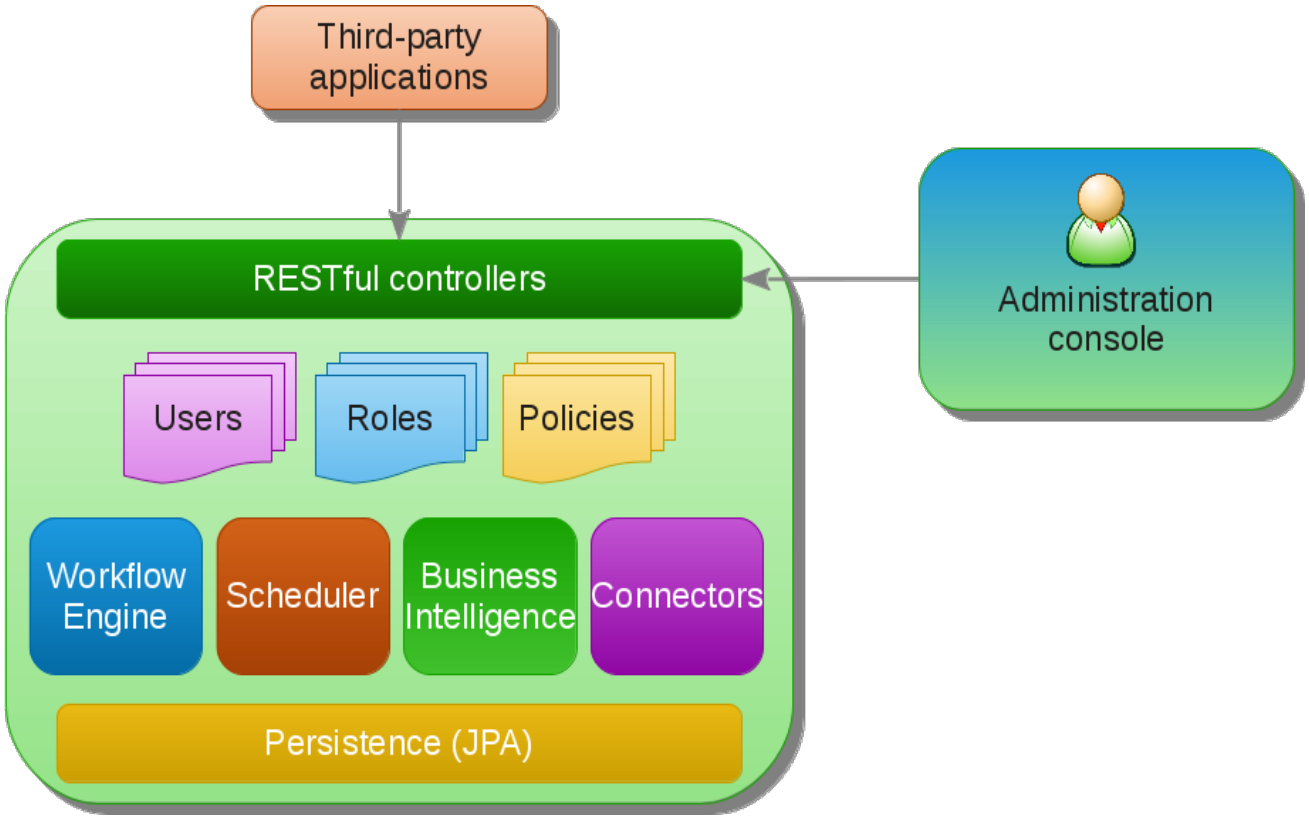
Identity & Access Management

- IAM is concerned with managing user data on systems and applications during the entire life cycle
- Involves user attributes, roles, resources, entitlements, etc.
- Provisioning / Reconciliation
  - Synchronize user (account) data across identity stores and a broad range of data sources, formats, meanings and purposes
  - Read user data from source systems
  - Write user data to target systems
- Reporting / Auditing
- Policy Enforcement (Segregation of Duty)

IAM Product Architecture



Apache Syncope Architecture (1/2)



Apache Syncope Architecture (2/2)

- Different Connector support (ConnId project)
- Workflow customizable (based on Activiti)
- User Schema definition
- Propagation/Synchronization
- Business Intelligence (Audit, Report)
- REST API

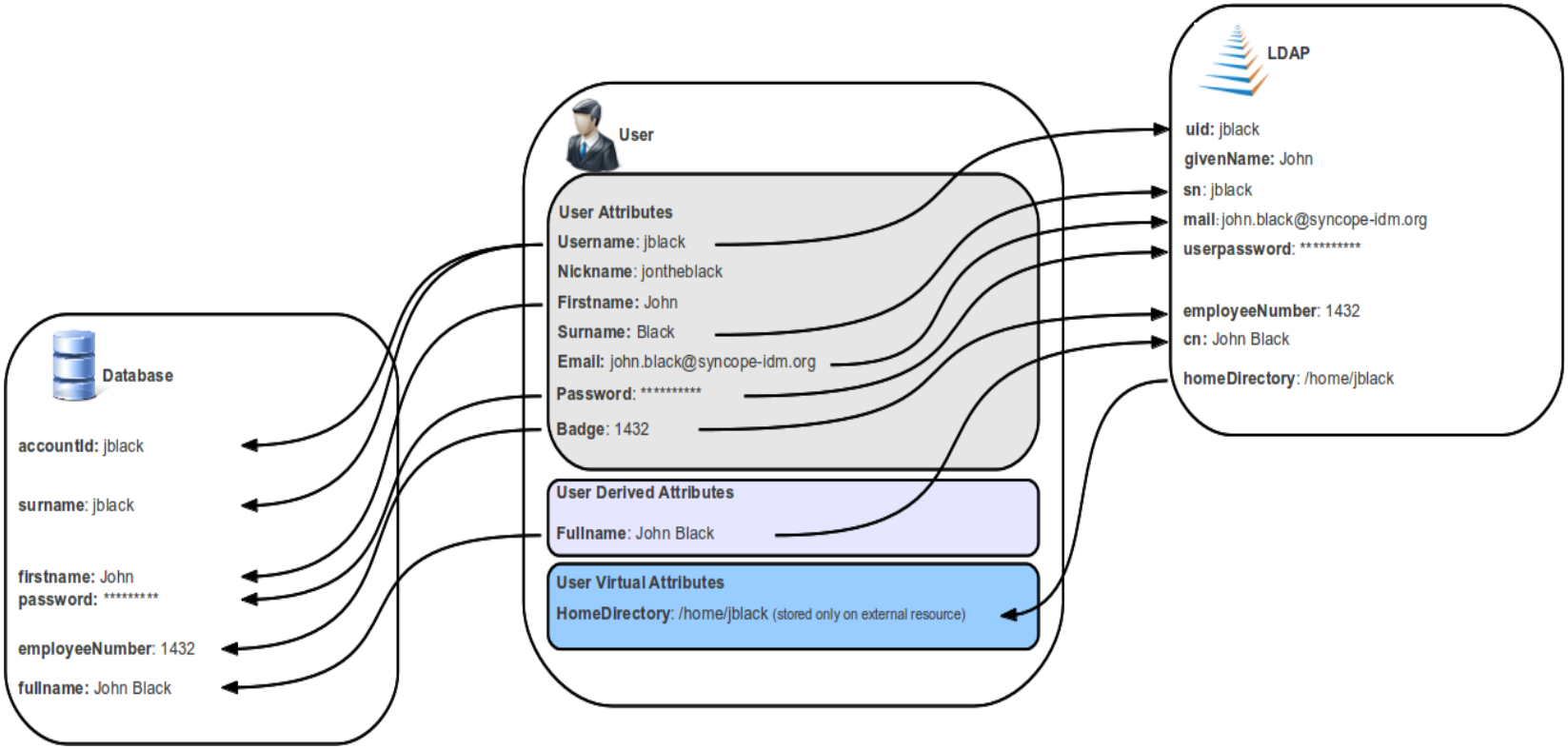
Apache Syncope - Schemas

- Apply for User and Roles
  - Normal Attributes
    - Stored in Syncope DB
    - Propagaded and synchronized when selected
  - Derived Attributes
    - Combination of Attributes
    - JEXL Expression Language
  - Virtual Attributes
    - Not stored in Syncope DB
    - Lookup from remote resource
  -

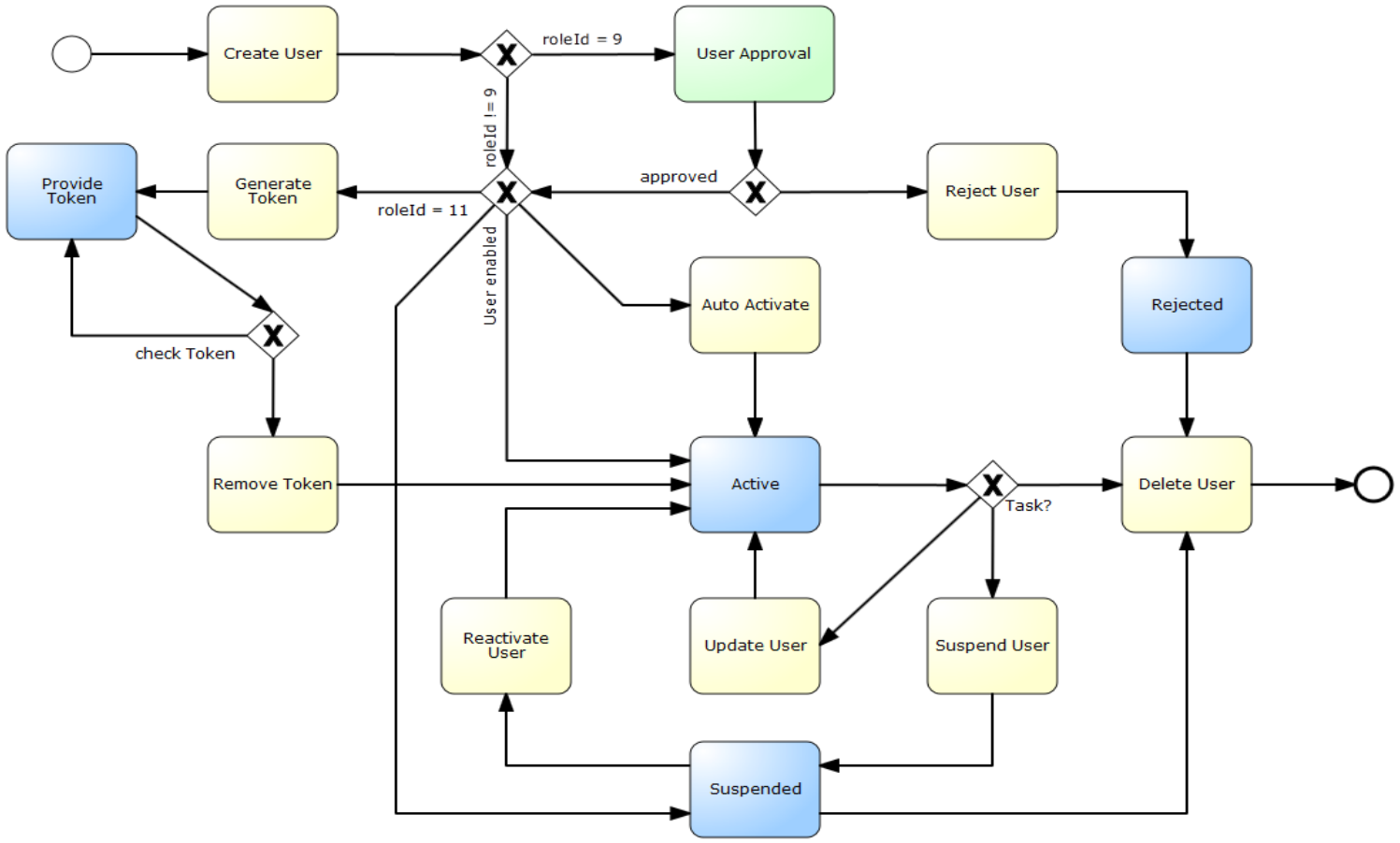
FirstName = John
LastName = Black

FullName = FirstName + LastName
FullName = John Black

Apache Syncope – Attribute Mapping



Apache Syncope - Workflow



Solution Building blocks

Demo

IAM Syncope

Federation/SSO with Apache Tomcat Application

More information

- Talend ‣ www.talend.com
- Apache Projects
  - Fediz ‣ http://cxf.apache.org/fediz.html
  - Syncope ‣ http://syncope.apache.org/
- Blogs
  - http://coheigea.blogspot.com
  - http://www.dankulp.com/blog/
  - http://sberyozkin.blogspot.com
  - http://owulff.blogspot.com


Thank You