RED HAT
OPEN SOURCE DAY
Europe, Middle East & Africa

ESERCITO

redhat.

Identità Digitale

Il caso d'uso di Esercito Italiano

Ten. Col. Fabio Ubaldi, Cap. Roberto Caramia - Comando C4 Esercito
Corelatori: Salvatore Incandela - Red Hat, Francesco Chicchiriccò - Tirasa
9 Novembre 2017

La soluzione di Identità digitale

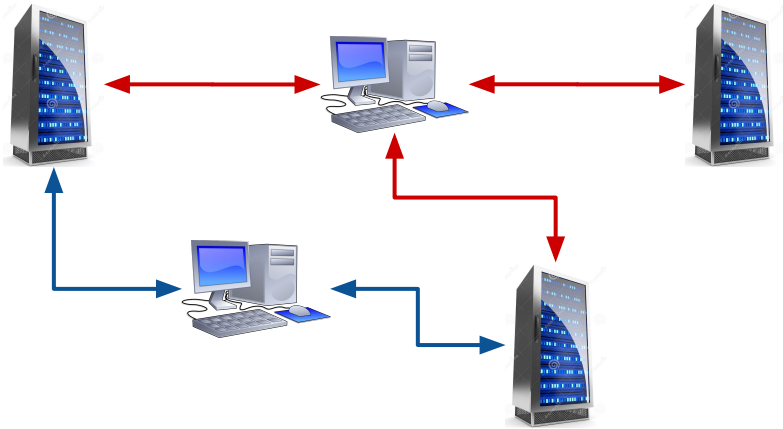
Implementata per l'Esercito Italiano

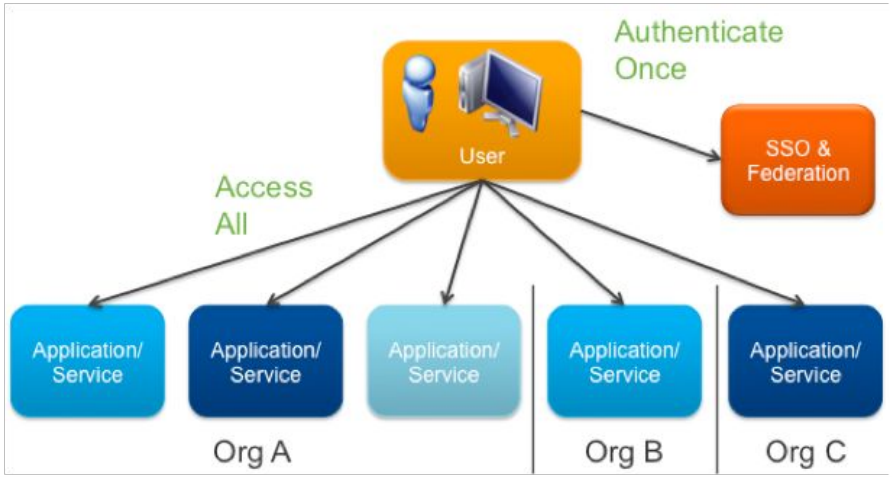
Realizzare un sistema di Identità Digitale completo per:

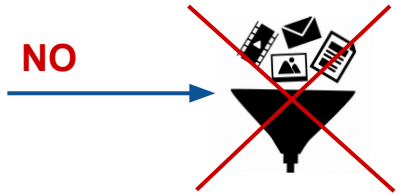
- Gestire il ciclo di vita dell'identità/credenziali/permessi
- Gestire SSO tra sistemi Open Source e Vendor Locked
- Gestire centralmente l'Audit di sicurezza
- Gestire l'accesso a vari sistemi di directory (SAMBA/MS Active Directory)

Esigenza


Carta Nazionale dei Servizi




Authenticate
Once
User
SSO &
Federation
Access
All
Application/
Service
Application/
Service
Application/
Service
Application/
Service
Application/
Service
Org A
Org B
Org C


NO

Check IN Fase 1

Inserimento dati a cura di SIGE

Nuovo utente

- Accademia Militare
- Scuola Applicazione
- Scuola Sottufficiali
- RAV

1

Inserimento dati sul SIGE

Nome: Mario
Cognome: Rossi
CF: RSSMRO80H02D810X
Reparto: RAV Capua
…

2

Calcolo e associazione attributi

Nome: Mario
Cognome: Rossi
CF: RSSMRO80H02D810X
Reparto: RAV Capua
…
Email: mario.rossi3@esercito.difesa.it
PSW 1° Accesso: Dj5lf46E49DfA4b9

3

Rilascio informazioni accesso ai sistemi

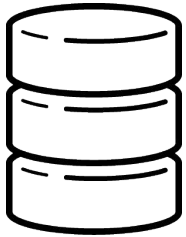
Account,
Procedure per attivazione,
Norme di utilizzo

Check IN Fase 2

Aggiornamento BDC

SIGE

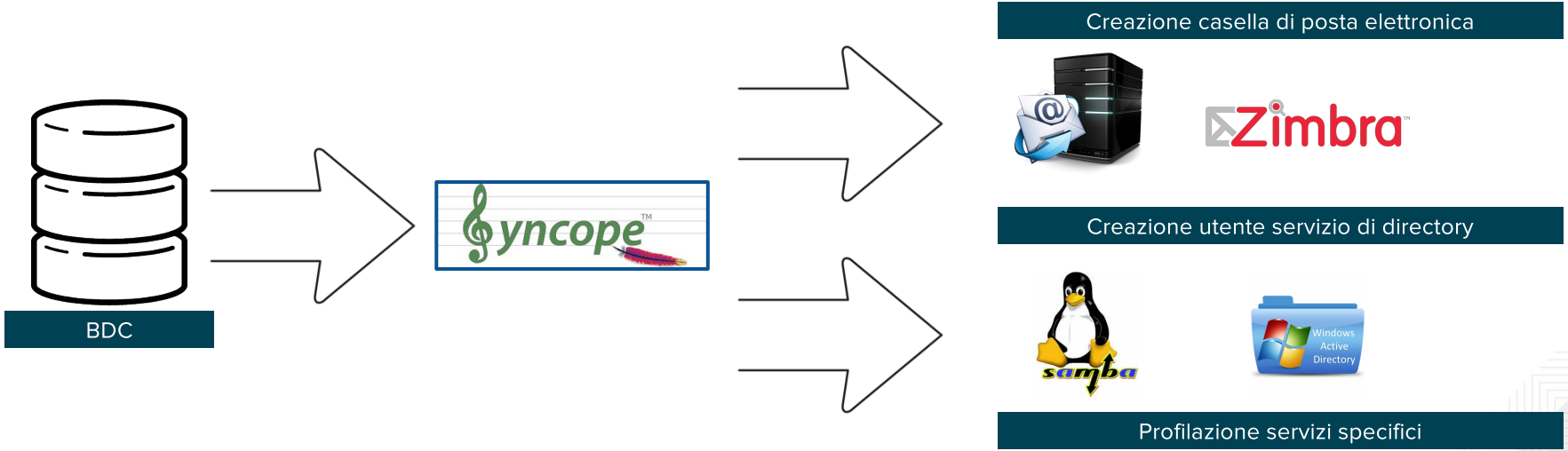
Nome: Mario
Cognome: Rossi
CF: RSSMRO80H02D810X
Reparto: RAV Capua
... ...
Email: mario.rossi3@esercito.difesa.it
PSW 1° Accesso: Dj5If46E49DfA4b9



BDC

Check IN Fase 3

Sincronizzazione Basi Dati



Check IN Fase 4

Comunicazione all'utente

Help Desk

E-mail contenente tutte le informazioni per l'accesso ai servizi abilitati/caratteristiche degli stessi/catalogo dei servizi richiedibili

Comunicazione di avvenuta attivazione

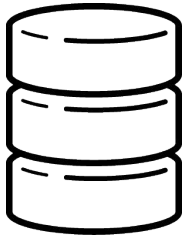
Utente

Check OUT Fase 1

Invio dati variazione posizione

SIGE

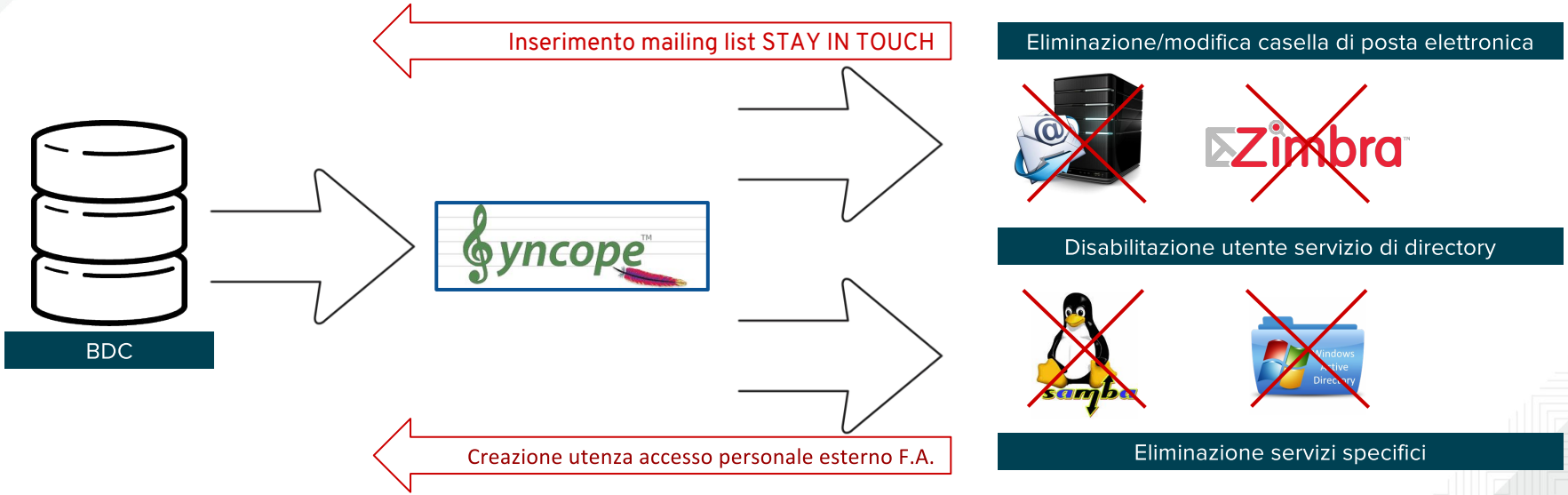
Nome: Mario
Cognome: Rossi
CF: RSSMRO80H02D810X
Reparto: RAV Capua
…: …
POSIZIONE:
PENSIONAMENTO/ARQ/CONGEDO/…
e-mail commerciale (STAY IN TOUCH)



BDC

Check OUT Fase 2

Sincronizzazione Basi Dati



Check OUT Fase 3

Comunicazione all'utente

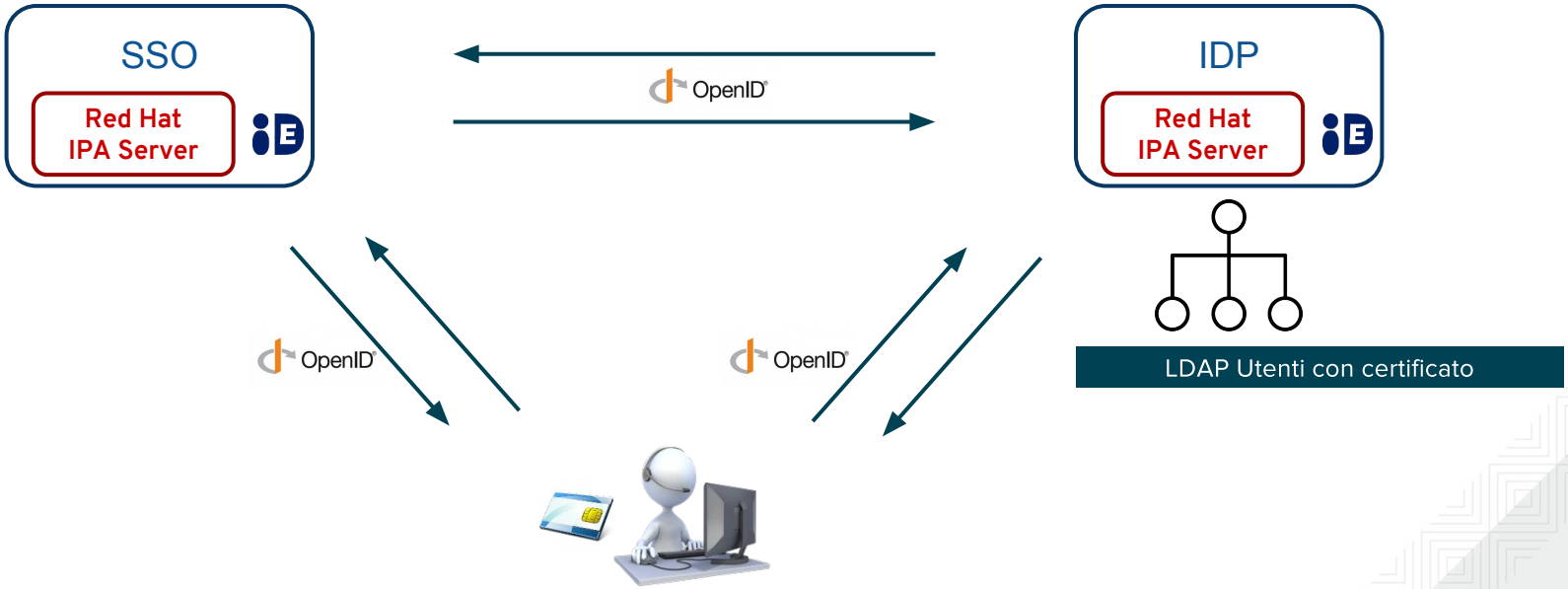
Help Desk

Comunicazione avvenuta disattivazione servizi **INTERNI** ed attivazione servizi per personale **ESTERNO**

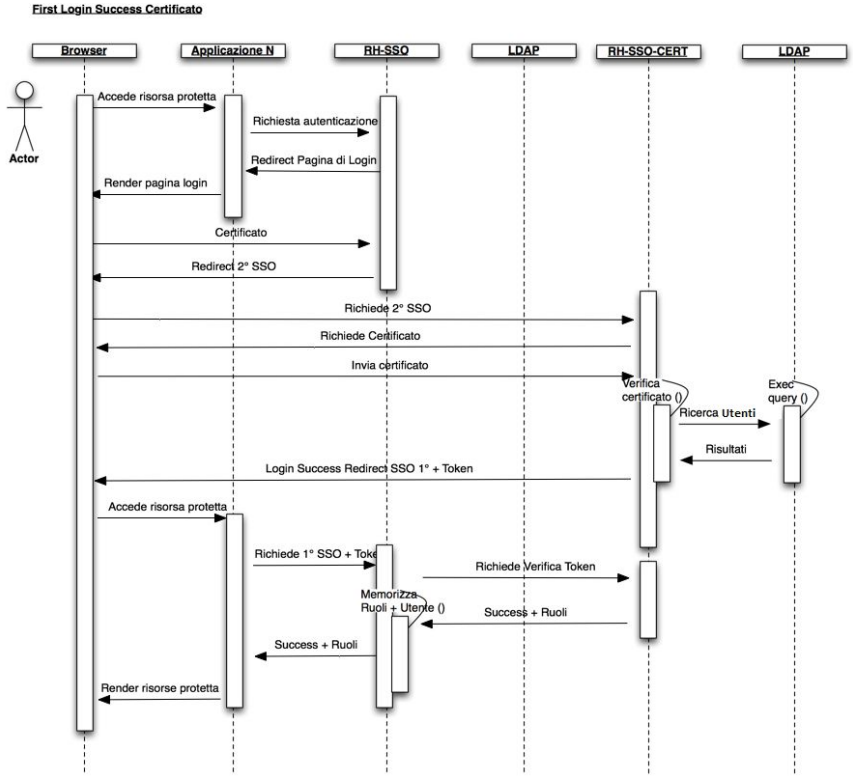
Comunicazione di avvenuta attivazione

Utente

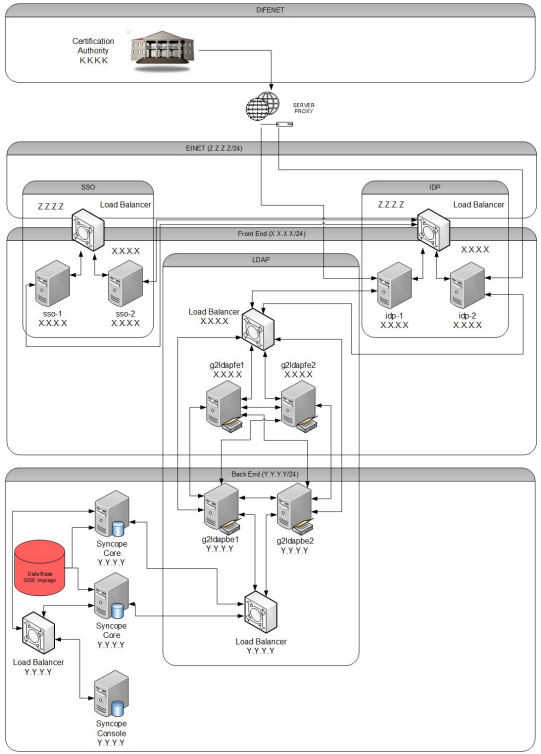
Struttura di Autenticazione



Flusso di Autenticazione



High level design

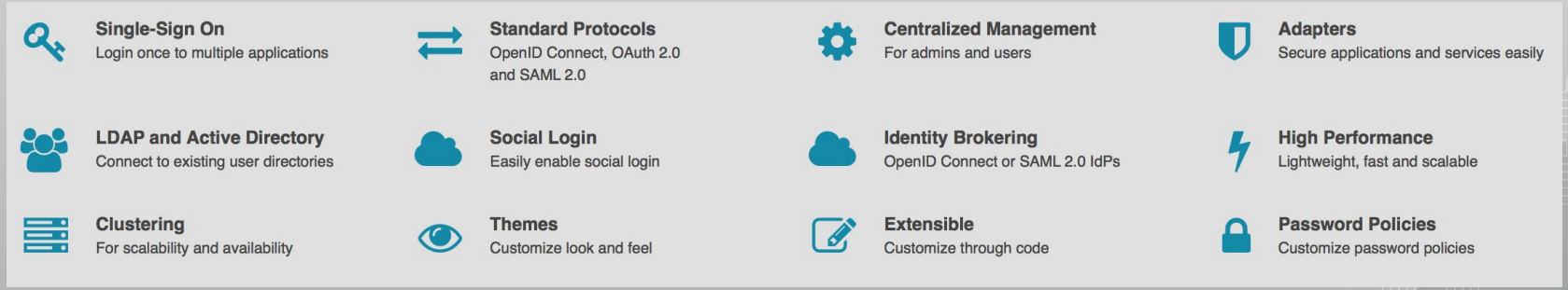


RED HAT SSO

RH SSO 7

Key Concepts

- Is a middleware security framework.
- Is the enterprise package of keyclock.org project.
- Is part of Core Services collection.
- Is included into JBoss MW subscription but… cores count.
- Is NOT an Identity Management Platform.



RH SSO 7

Key Features

- **SSO**

  Users authenticate with Keycloak rather than individual applications. So no need to deal with login forms, authenticating users, and storing users. Once logged-in to RHSSO, users don't have to login again to access a different application.

- **Kerberos**

  If your users authenticate to workstations with Kerberos they can also be automatically authenticated to RHSSO without having to authenticate again after they log on to the workstation (desktop SSO).

- **Social Login**

  Enabling login with social networks is easy to add through the admin console. It's just a matter of selecting the social network you want to add. No code or changes to your application is required.

- **Client Adapters (agents)**

  We have adapters available for a number of platforms and programming languages, but if there's not one available for your chosen platform don't worry. RHSSO is built on standard protocols so you can use any OpenID Connect Resource Library or SAML 2.0 Service Provider library out there. You can also opt **to use a proxy** to secure your applications which removes the need to modify your application at all.

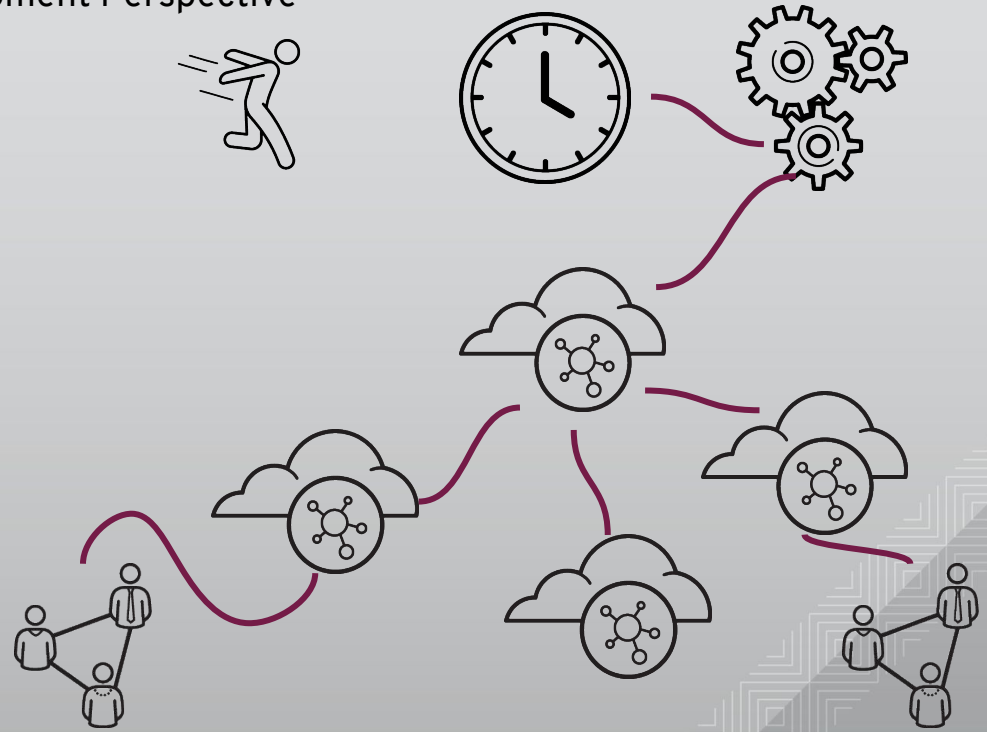
- **Admin and Account console**

  Through the account management console users can manage their own accounts. They can update the profile, change passwords, and setup two-factor authentication. Users can also manage sessions as well as view history for the account.

Being fit in modern days

Development Perspective

- Jogging session gets tracked on a smartwatch
- Route, pace, HR and etc. get uploaded automatically to the web portal
- Other social portals for runners automatically pull the data
- Everything gets automatically published on social media



Modern Token Based Security

Development Perspective

- Modern applications act on behalf of users and are interconnected
- All happening **AUTOMATICALLY** and **ON BEHALF** of a user
- Authorization and Delegation based on long living tokens
  - Granted once and valid for long time
  - Centrally managed active sessions
  - Possible to be revoked at any time by the user

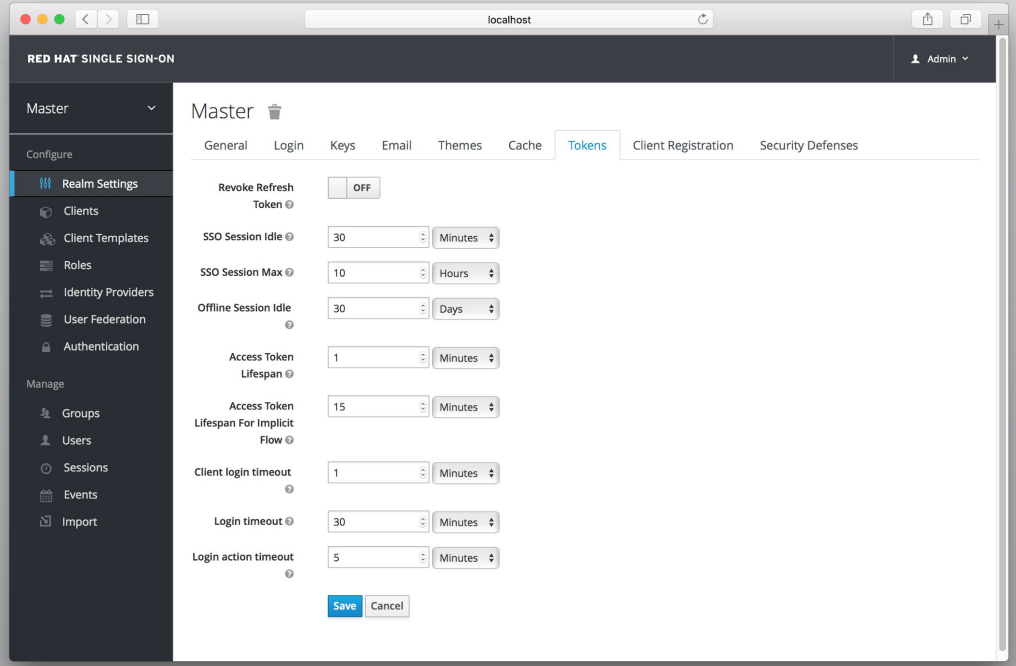
RH SSO 7 Provides

Development Perspective

- OpenID Connect / OAuth2 - Authorization Server implementation
  - Standards designed specifically for this use case
- Single place to define token configuration
  - Lifespan and etc.
  - Define included attributes, mappings and roles
- Centralized Session Management
  - Users able to review and invalidate active sessions
  - Admins able to revoke access to compromised clients/tokens

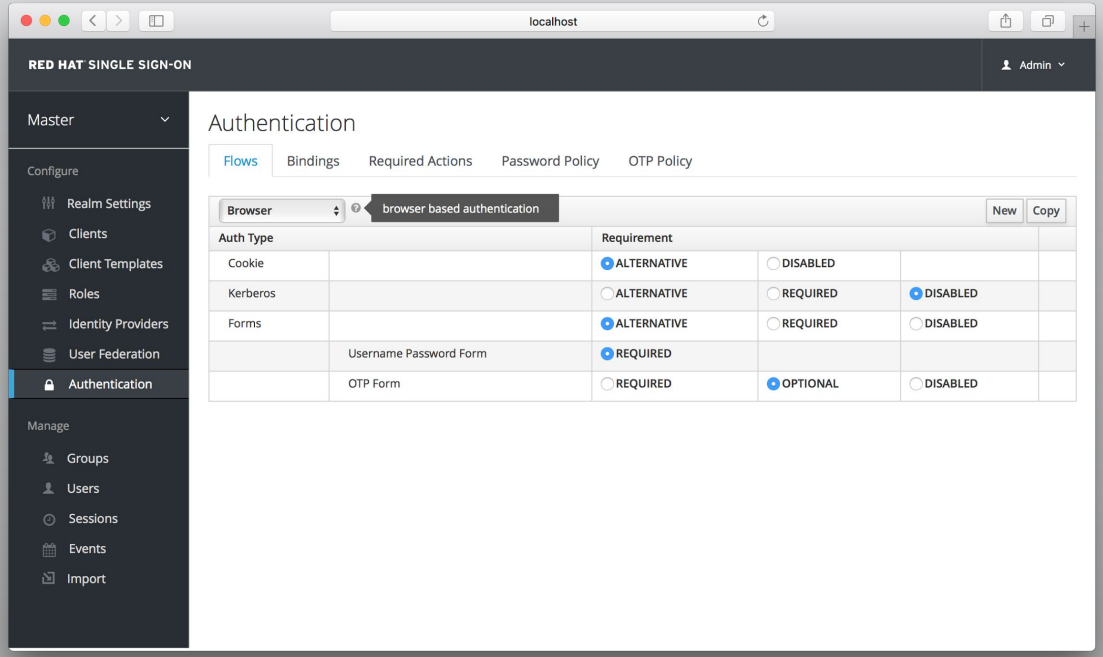
Token Management

Token configuration



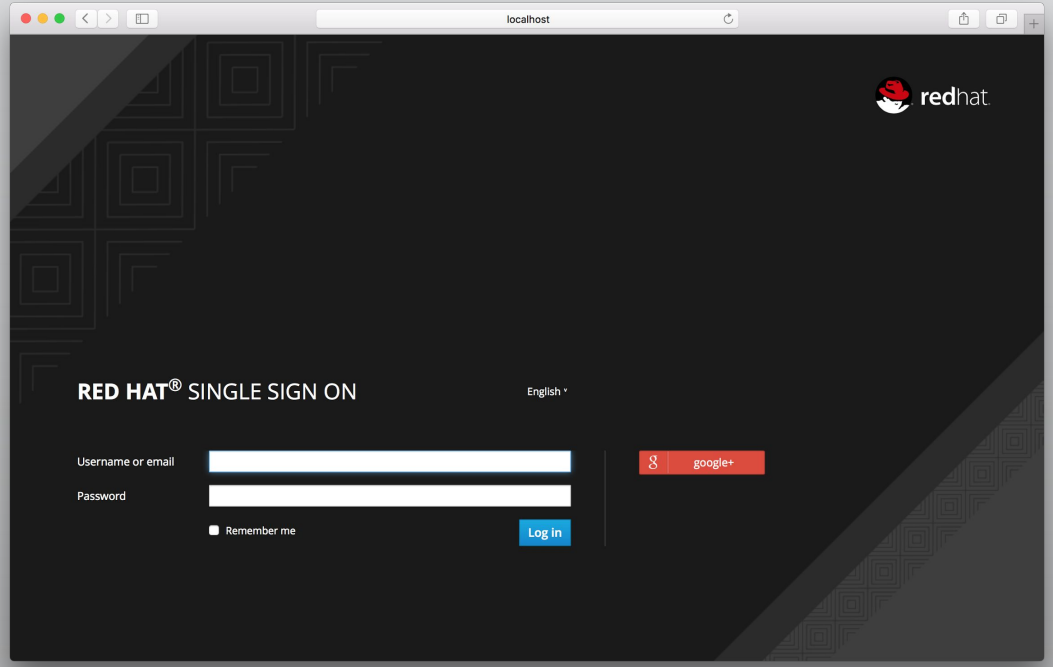
Browser flow

Flow configuration



External identity provider

Google example



Offloading the developer

Development Perspective

- Security concerns require high expertise
  - XSS, CSRF, SQL Injection…
  - Cryptography, Encryption, Hashing algorithms
  - Evolving best practices
- Every application shares same typical requirements
  - Login / Registration screen
  - User / Role management UIs
  - Password policies
  - Logging / Audit
- High risk of introducing vulnerabilities if every time implementing from scratch
- Keeping up with new security threats

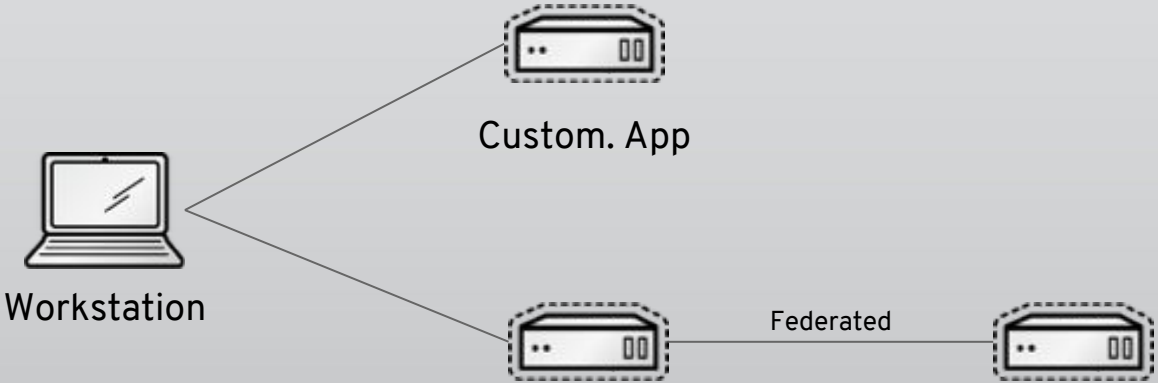
RH SSO 7 Provides

Development Perspective

- Easy to apply integration libraries and agents / adapters
  - Securing different applications and services within very few trivial steps
- Set of customizable and themable GUIs for
  - User, Role and Authorization Policies management
  - Authentication and Registration for end users
  - User self service
- Out of the box
  - Password policies & Two Factor Authentication
  - Session Management & Logging
  - Different Authentication flows & methods
  - Both RBAC and ABAC with flexible policies

RH SSO - Esercito

Big Picture



Login method choice
User and PWD
Utenti e ruoli
Federazione LDAP e AD

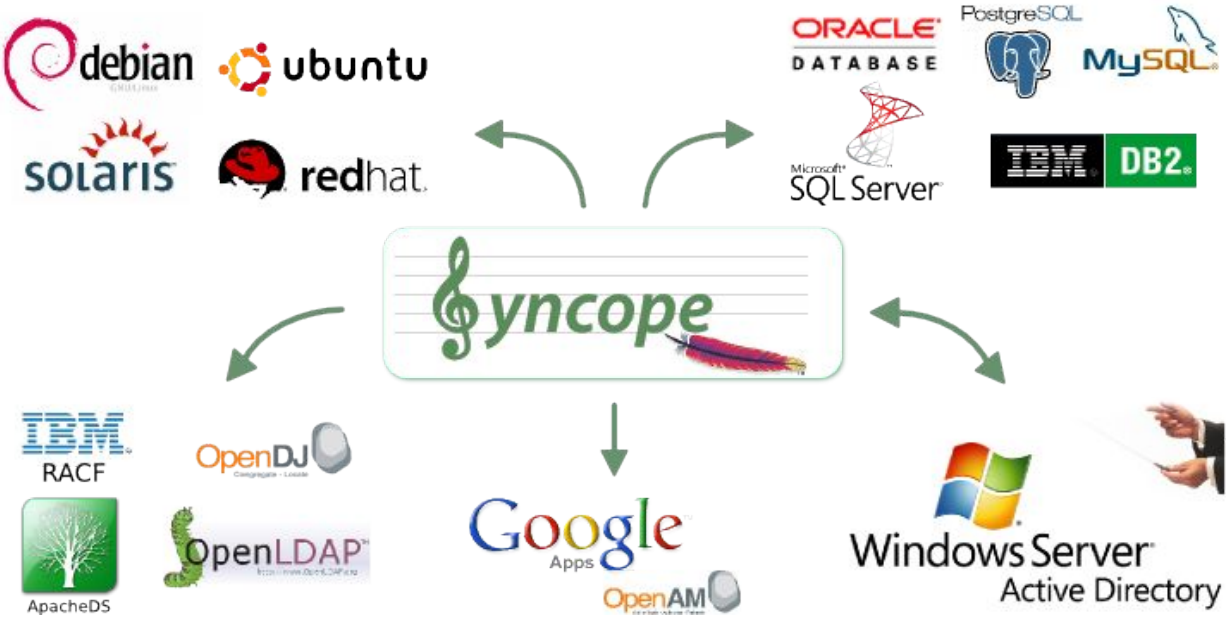
Login SmartCard
Verifica certificati
CRL List

Tirasa.net
ed il progetto Apache Syncope

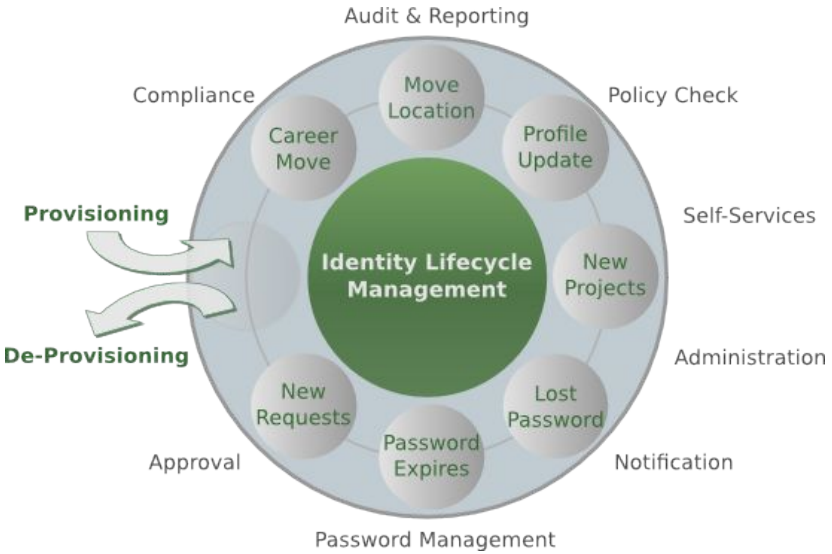
Identity & Access management

- **Identity Management**
  Strumenti e metodologie per gestire la sincronia e la consistenza dei dati relativi alle identità rispetto a repository, formati e modelli eterogenei
- **Access Management**
  Sistemi, protocolli e tecnologie a supporto dell'autenticazione (chi è l'Utente?) e l'autorizzazione (cosa può fare l'Utente?)

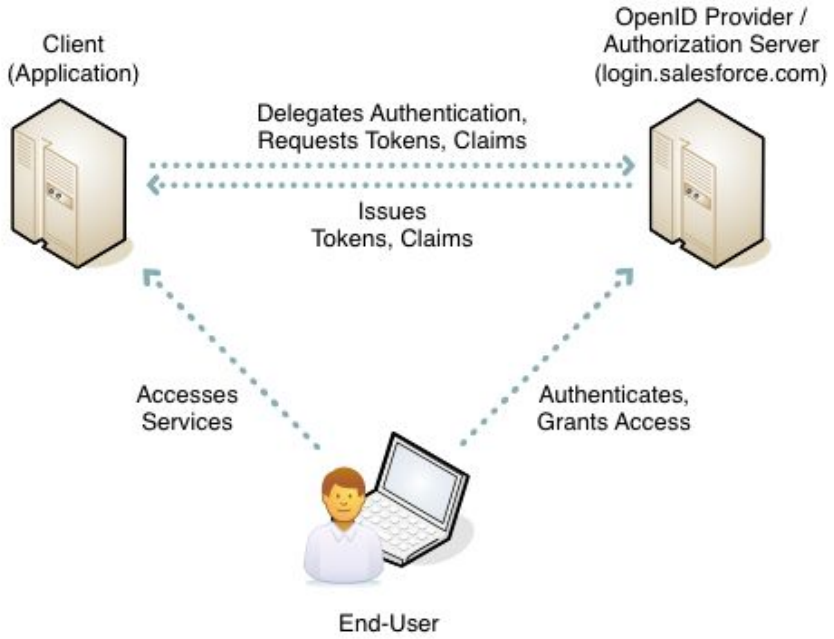
Tecnologie IAM - Identity Store



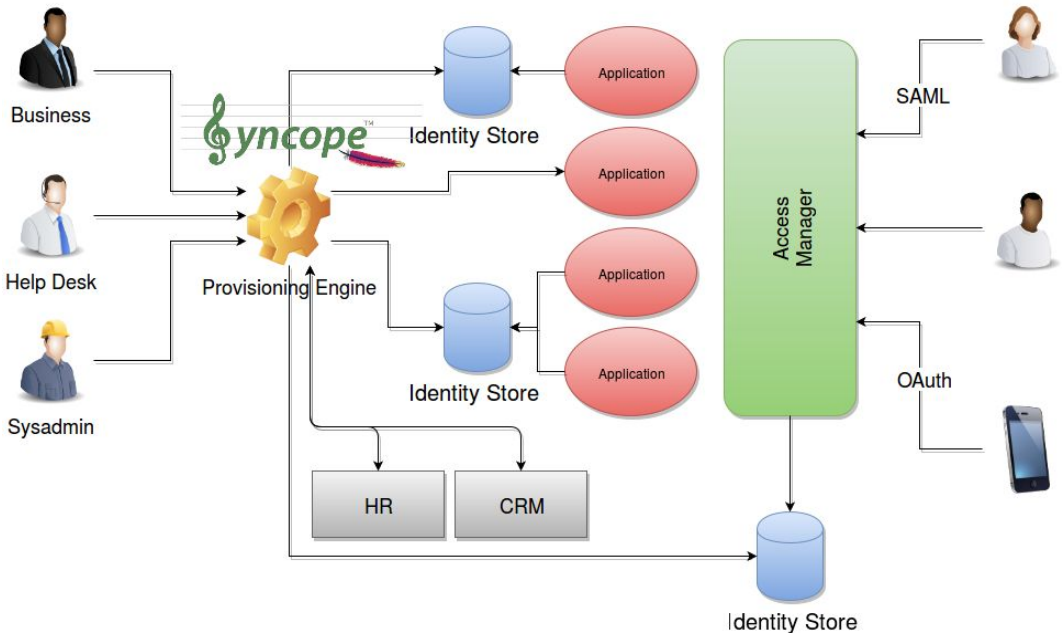
Tecnologie IAM - Provisioning Engine



Tecnologie IAM - Access Manager



IAM - Scenario di riferimento



Apache Syncope

Una attiva Comunità

Iniziato da Tirasa nel 2010

Entra nell'ASF incubator nel Febbraio 2012

Promosso TLP a Novembre 2012

Community attiva:

19 committer, 6 contributor

> 200 iscritti in ML

> 40 rilasci

Identità Digitali @ Esercito - Requisiti

- Importazione Utenti ed Enti da vista SQL Anagrafica
- Provisioning su:
  - Cluster RedHat 389 (LDAP)
  - Zimbra (SOAP)
- SSO KeyCloack (via SAML 2.0)
  - Console di Amministrazione
  - Reset password utente

Tirasa

- PMI Italiana
- Non molto numerosi ma con
- ottime referenze Open Source:
  - 1 ASF member
  - 5 PMC members
  - 2 ASF committer

Visit: http://www.tirasa.net

Referenze


ESERCITO


Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Ancona
Umberto I | G.M. Lancisi | G.Salesi


welcome


AZIENDA
ULSS 16
PADOVA


U.PORTO


plainID


SCIENTIA TICINEA STVDIVM


SWM
Stadtwerke München


HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

RED HAT
OPEN SOURCE DAY

Europe, Middle East & Africa

redhat®