



Keycloak: Autenticazione SPID con strumenti Open Source

Christian Simonelli – Responsabile Area Application Security
@TaiSolutions



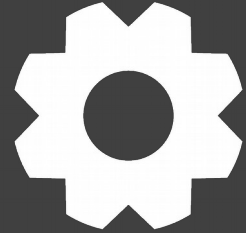
#RedHatOSD

Tai Solutions



- ❖ Dal 1987 sul mercato italiano
- ❖ Advanced Business Partner RedHat
- ❖ > 12 Anni di esperienza in progetti di Access e Identity Management (IAM)

Identity Access Manager



- Gestione dinamica identità
- Autenticazione Centralizzata
- Password Policy
- Autorizzazione Accesso Servizi

UC : Indice

- ✓ Keycloak
- ✓ SPID
- ✓ UC integrazione



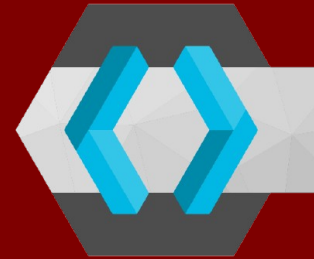
Keycloak : Progetto

- Open Source Access e Identity Manager
- Licenza Apache
- Versione attuale 4.5 (prima versione 2014)
- Community supportata da RedHat
- Disponibile supporto commerciale (Redhat SSO)

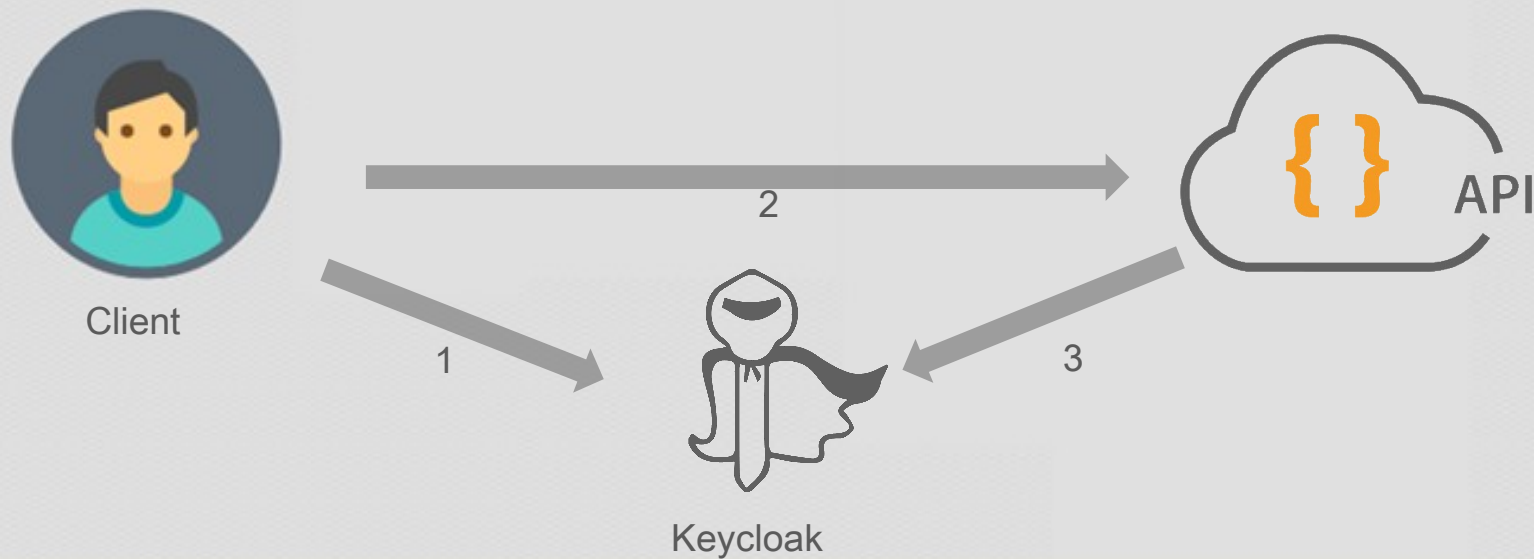


Keycloak : Funzioni

- ❖ Single Sign-on / Single Sign-out
- ❖ Gestione utente centralizzata
- ❖ Autenticazione Locale, Ldap, X 509, Kerberos, OTP, Remember Me
- ❖ Autorizzazione HRBAC, ABAC, ...
- ❖ Protocolli standard Oauth2, Saml2, OpenId Connect
- ❖ Social Login (Facebook, Google, Twitter,)



Keycloak : Accesso API



SPID : Sistema Pubblico di Identità Digitale

- Credenziali uniche per Servizi PA
- Basato su Standard Saml2
- Differenti Identity Provider
- Tre livelli di sicurezza



AgID Agenzia per
l'Italia Digitale



ENTRA CON SPID

SPID : Livelli di Sicurezza



Identità SPID di primo livello

Permette l'accesso ai servizi
con nome utente e password
stabiliti dall'utente

Corrisponde al Level of
Assurance LoA2 dello
standard ISO/IEC DIS 29115



Identità SPID di secondo livello

Permette l'accesso ai servizi
con nome utente e
generazione di una One Time
Password inviata all'utente

Corrisponde al Level of
Assurance LoA3 dello standard
ISO/IEC DIS 29115



Identità SPID di terzo livello

Permette l'accesso ai servizi
con nome utente e password
e dispositivi fisici (Smart
Card, Token fisici)

Corrisponde al Level of
Assurance LoA4 dello
standard ISO/IEC DIS 29115

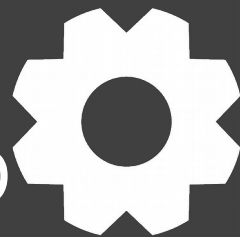
SPID : Processo Accreditamento

- ✓ Stipula convenzione con Agid
- ✓ Scambio Metadati Saml2
- ✓ Conservazione accessi
- ✓ Test integrazione

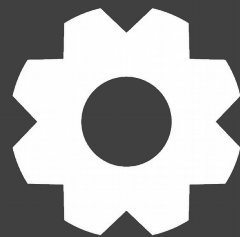


UC: Progetto

- Realizzazione Service Provider SPID
- Gui amministrativa e utente
- Supporto Docker
- Fase 2 : Supporto Livelli Spid

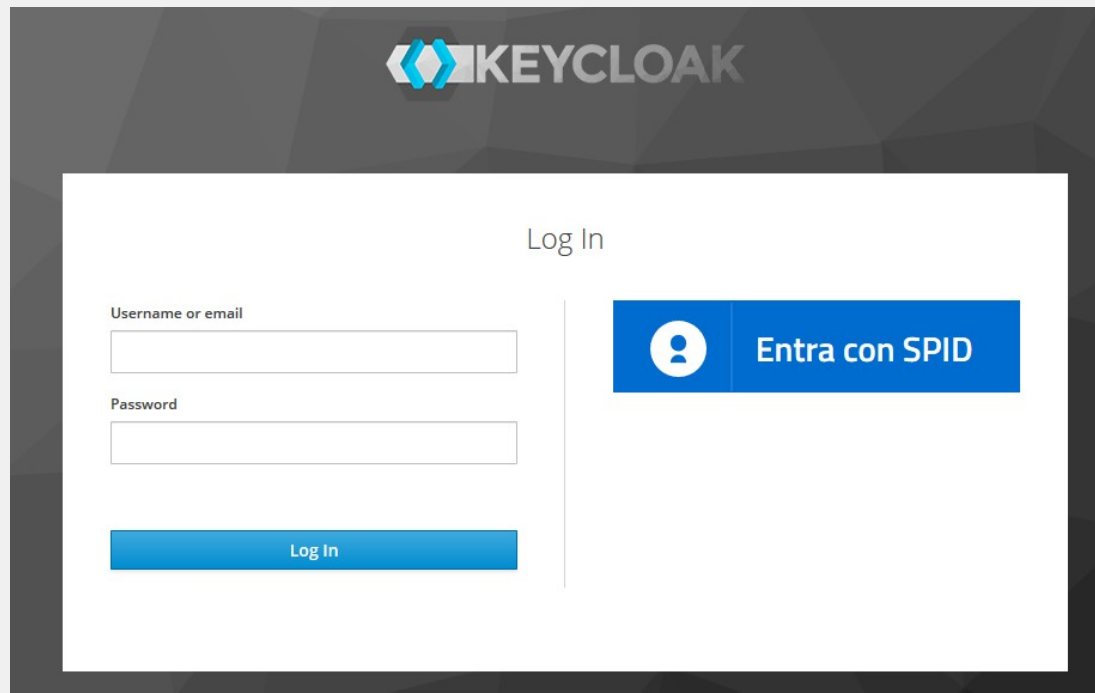


UC : Service Provider



- Basato su Identity Provider Saml2
- Gestione molteplici Idp SPID
- Mapping attributi SPID in KeyCloak
- Supporto Base Livelli Spid

UC : Gui Utente



The image shows the Keycloak login interface. At the top, the Keycloak logo is displayed. Below it, the text "Log In" is centered. On the left side, there are two input fields: "Username or email" and "Password". Below these fields is a blue "Log In" button. On the right side, there is a blue button with a user icon and the text "Entra con SPID".

KEYCLOAK

Log In

Username or email

Password

Log In

Entra con SPID

UC : Gui Amministratore

* Single Sign-On Service URL ?	
Single Logout Service URL ?	
Backchannel Logout ?	☐ OFF
NameID Policy Format ?	Transient
HTTP-POST Binding Response ?	☐ OFF
HTTP-POST Binding for AuthnRequest ?	☐ OFF
HTTP-POST Binding Logout ?	☐ OFF
Want AuthnRequests Signed ?	☐ OFF
Want Assertions Signed ?	☐ OFF
Want Assertions Encrypted ?	☐ OFF
Force Authentication ?	☐ OFF
Validate Signature ?	☐ OFF
v Import External IDP Config ?	
Import from URL ?	
Import from file	Select file



UC : Supporto Docker

- Libreria classi
- Html, js, png
- Configurazioni
- Docker

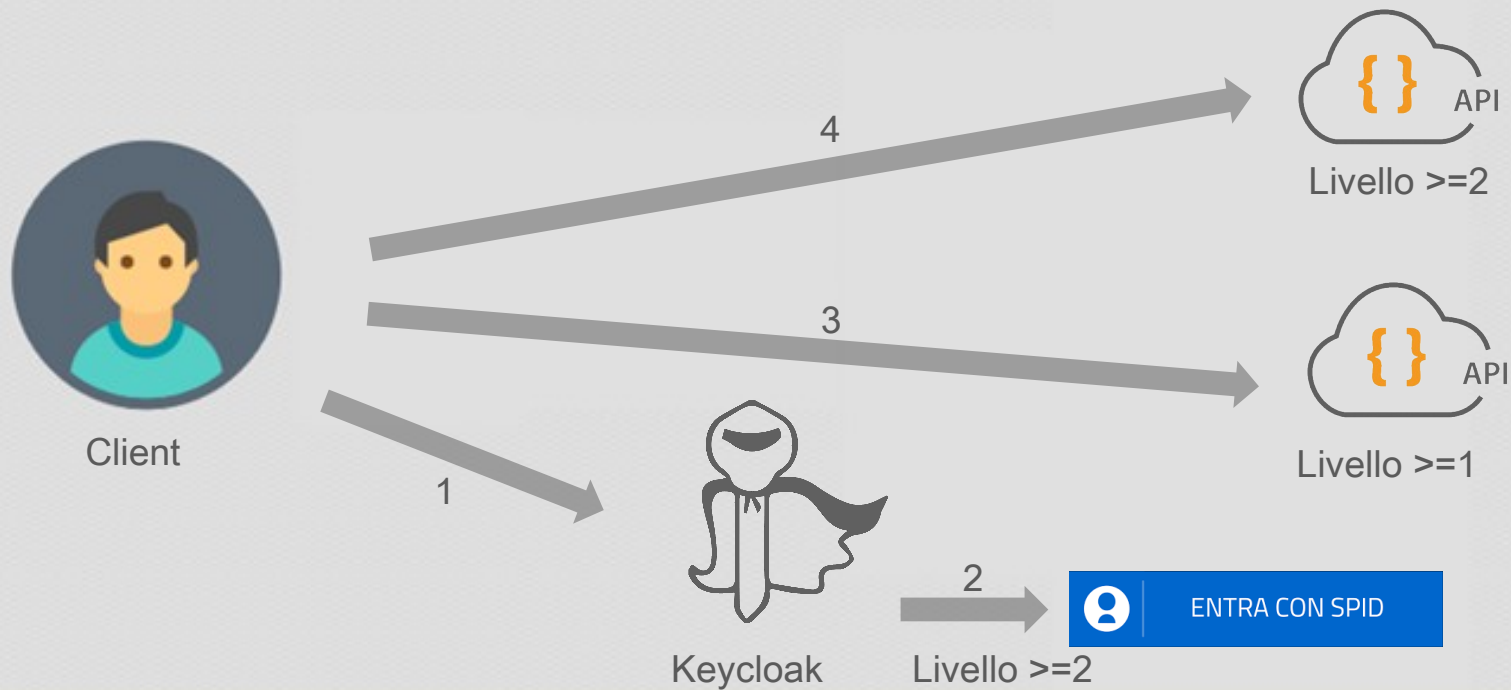
The screenshot shows the GitHub repository for 'Keycloak Maven SDK for managing the entire lifecycle of your extensions with Docker'. The repository is on the 'master' branch and has 4 commits, 1 branch, 0 releases, and 1 contributor. The file list includes:

File	Commit	Time
keycloak-assembly	first commit	21 days ago
keycloak-identity-providers	first commit	21 days ago
keycloak-integration-tests	first commit	21 days ago
keycloak-theme	first commit	21 days ago
src/main	first commit	21 days ago
.dockerignore	first commit	21 days ago
.gitignore	first commit	21 days ago
.maven-dockerignore	first commit	21 days ago
Dockerfile	first commit	21 days ago
LICENSE.txt	first commit	21 days ago
README.md	Update README.md	21 days ago
pom.xml	first commit	21 days ago

The 'README.md' file is selected, showing the 'Keycloak Docker Quickstart' section. The text states: 'This project is aimed to manage Keycloak extensions using a fully Maven lifecycle. The current supported component are the following:'

- keycloak-assembly
- keycloak-identity-providers
- keycloak-integration-tests
- keycloak-theme

UC : Supporto Livelli SPID



Riferimenti



- **Keycloak** <https://www.keycloak.org/>
- **Keycloak docker quickstart** <https://github.com/OpenPj/keycloak-docker-quickstart>
- **Specifiche tecniche Spid** <https://www.agid.gov.it/>



GRAZIE PER L'ATTENZIONE

Christian Simonelli – Responsabile Area Application
Security presso
@Tai Solutions



#RedHatOSD