“Nuove funzionalità in Shibboleth 3”

ed accenni sulla migrazione da versioni precedenti

Daniele Albrizio
albrizio@units.it
CTS Idem

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Nota che

- Sono un sistemista linux, network oriented un po' prevenuto sulle webapp java e i loro contenitori
- Il punto di vista è un po' spostato verso il fornire/gestire agevolmente un servizio sufficientemente stabile in produzione.

Indice

- Nuove funzionalità
- Requisiti di sistema
  - Preparazione dell'ambiente
- Migrazione
  - Consent

Obbiettivi

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Come installo shibboleth?
  - Che versione installo?
  - Con che Servlet Container?
- Aggiorno shibboleth?
  - E' necessario?
  - A cosa vado incontro?

Deadline

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Shibboleth 2.x
  - End of Life 31 luglio 2016
    - Inizio dismissione dal febbraio 2016

New in IdPv3

New in IdPv3

- Sessioni built-in client-side tramite l'uso di cookies criptati e firmati per chi è sufficientemente saggio da lasciar perdere il single logout (SLO)
- Spring Web Flow viene usato per risolvere i problemi correlati a richieste multiple sovrapposte da più finestre o tab del browser.

New in IdPv3

- memcache e Hibernate (database) opzionali per lo storage delle sessioni lato server (disattivato di default)
- Login: il vecchio JAAS (Java Authentication and Authorization Service) viene affiancato da autenticazioni native (Spring) LDAP, Kerberos e X.509
- Supporto per i client ECP (non-browser) abilitato di default

New in IdPv3

- Supporto profili per i relying parties (individuati in gruppi, tag, ecc.) a cui poter applicare override di tipo pluggable (SAML1,2, SLO, artifact resolution, consent, ecc.)
- Implementazione del protocollo CAS da parte di uno sviluppatore del progetto (CAS login, CAS proxy, rilascio attributi)

New in IdPv3

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Security
  - Algoritmi di crittografia selezionabili basandosi sui metadati o sulla configurazione dei relying party.
  - Supporto per blacklists e whitelist di algoritmi di firma e crittografia (Poodle docet)
  - GCM encryption per gli SP che la supportano

Rispetto alla ver. 2.x

- Attribute Resolver
  - In caso di mancata connessione ai db di backend, il lookup non fallisce, ma si comporta come se la query avesse dato 0 risultati (opz.)
  - Aggiunte le dipendenze di attributi <Dependency> in modo da fare il merge di attributi con id sorgenti differenti:
    - Creare un singolo attributo con un valore composito costruito da due datasources diversi
    - Usare il valore di un attributo per comporre una query SQL per valorizzarne un altro

Rispetto alla ver. 2.x

- idp-process.log: Messaggi di warning molto più chiari
- Condizioni di errore user-facing maggiormente gestite (user experience più confortevole)
- APIs non backward-compatibili: estensioni personalizzate dovranno molto probabilmente essere aggiornate per funzionare con la versione 3

Rispetto alla ver. 2.x

- Attribute Filtering Changes
  - L'attributo ID è ora obbligatorio per tutte le policy (era opzionale).
- Autenticazione
  - Tipo di autenticazione selezionabile per SP
  - SSO disabilitabile per IP o con checkbox sulla pagina di login

Rispetto alla ver. 2.x

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Consent
  - Funzionalità uApprove inclusa col nome di consent
  - Consenso al rilascio degli attributi una volta eseguito il login
  - Disattivabile globalmente o per SP
  - Approvazione di Condizioni d'Uso generali (ToU) dell'IdP e le privacy policy degli SP (se puntate nei metadati) prima di esservi rediretti

Rispetto alla ver. 2.x

- Consent
  - Gli attributi da approvare vengono visualizzati con nome e descrizione valorizzati da attribute-resolver.xml
  - Consenso per singolo attributo (opz.)
    - **!!!** Solitmente non ben gestito dagli SP
  - Chiedi il consenso:
    - Sempre
    - Se gli attributi (id/valore) cambiano (default)
    - Mai più

Rispetto alla ver. 2.x

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

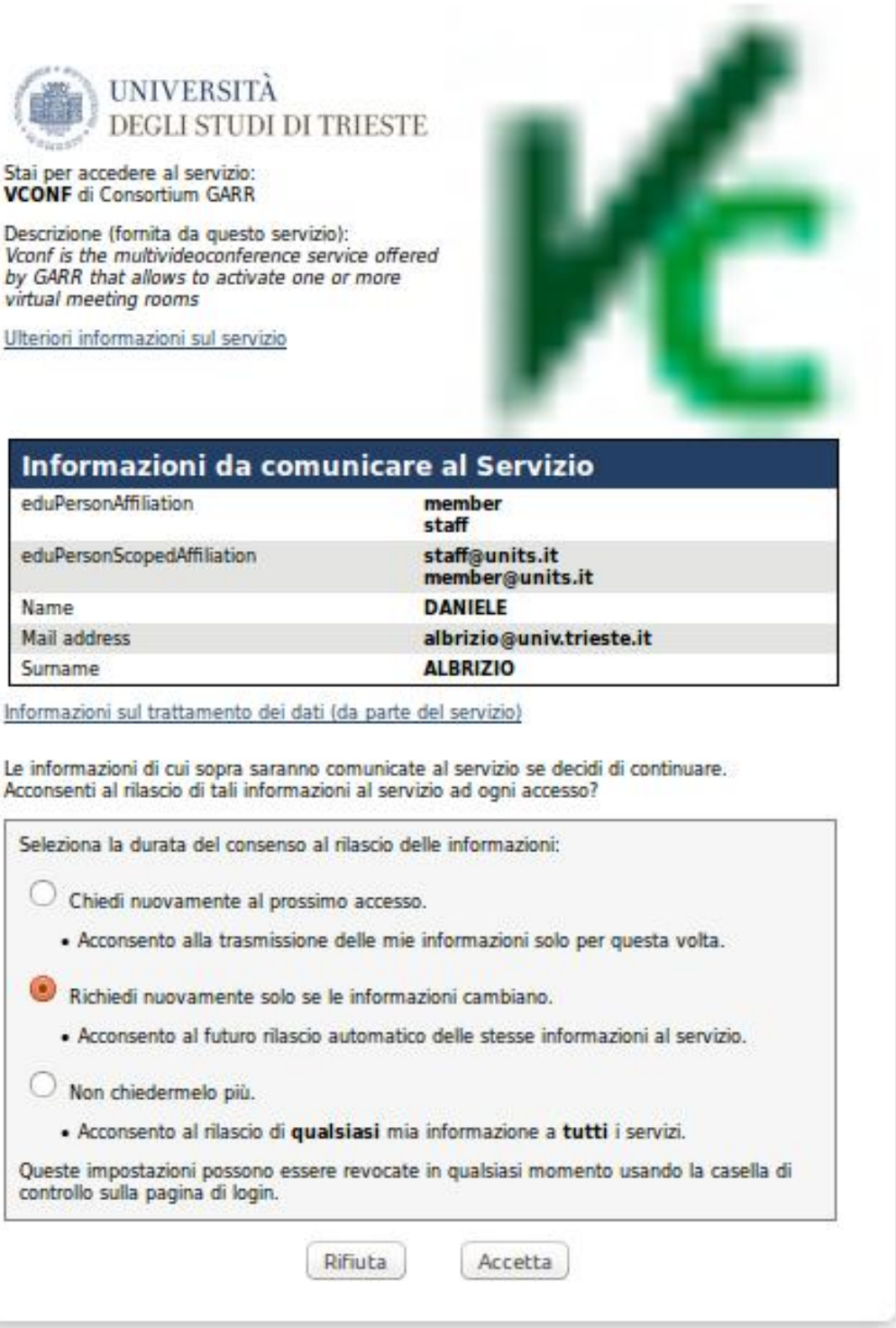
- Consent
  - Possibilità di **nascondere** alcuni Attributi e di **ordinare** la visualizzazione dei restanti
  - Nome e descrizione e logo dell'SP presi dai metadati dello stesso
  - Tutti i nomi e le descrizioni supportano l'internazionalizzazione

Parentesi i18n

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Apache Velocity template engine
  consent-messages_en.properties
  consent-messages_it.properties
  consent-messages.properties
- attribute-resolver.xml

```
<resolver:DisplayDescription xml:lang="it">
  Indirizzo
  </resolver:DisplayDescription>
  <resolver:DisplayDescription xml:lang="en">
  Address
  </resolver:DisplayDescription>
```


UNIVERSITÀ
DEGLI STUDI DI TRIESTE
Stai per accedere al servizio:
VCONF di Consortium GARR
Descrizione (fornita da questo servizio):
Vconf is the multivideoconference service offered by GARR that allows to activate one or more virtual meeting rooms
Ulteriori informazioni sul servizio
Informazioni da comunicare al Servizio
eduPersonAffiliation
member
staff
eduPersonScopedAffiliation
staff@units.it
member@units.it
Name
DANIELE
Mail address
albrizio@univ.trieste.it
Surname
ALBRIZIO
Informazioni sul trattamento dei dati (da parte del servizio)
Le informazioni di cui sopra saranno comunicate al servizio se decidi di continuare.
Acconsenti al rilascio di tali informazioni al servizio ad ogni accesso?
Seleziona la durata del consenso al rilascio delle informazioni:
Chiedi nuovamente al prossimo accesso.
• Acconsento alla trasmissione delle mie informazioni solo per questa volta.
Richiedi nuovamente solo se le informazioni cambiano.
• Acconsento al futuro rilascio automatico delle stesse informazioni al servizio.
Non chiedermelo più.
• Acconsento al rilascio di qualsiasi mia informazione a tutti i servizi.
Queste impostazioni possono essere revocate in qualsiasi momento usando la casella di controllo sulla pagina di login.
Rifiuta
Accetta

Rispetto alla ver. 2.x

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Consent
  - logging del consenso al rilascio degli attributi nell'audit log (memorizzazione nei cookie client side)
  - Consent non è disponibile nel backchannel (ECP)
  - Abilitato di default durante l'installazione “fresh”
  - Disabilitato di default durante l'upgrade

Rispetto alla ver. 2.x

- Metadata Provider
  - Merge dei metadata provider di tipo HTTP e File-backed in un unico tipo: FileBackedHTTPMetadataProvider
  - Struttura leggermente semplificata
- Nuovo metadata provider che “risolve” i metadati "just-in-time" usando il profilo SAML del MD Query protocol.

Rispetto alla ver. 2.x

- Il filtro EntityRoleWhitelist supporta il white/blacklisting delle entities e la rimozione di organization e contact person

Rispetto alla ver. 2.x

- Single Logout se richiesto avviene tramite l'uso di Hibernate (database per le sessioni)
- IdP 2.4 SLO
  - Supporto limitato al SLO che non propagava il logout sugli altri SP con sessione attiva. Ciò a causa di problemi di design della cache di sessione.

Rispetto alla ver. 2.x

- IdP 3 SLO
  - Il supporto iniziale al SLO permette all'SP di iniziare una richiesta di SLO o dal front-channel o dal back-channel, ma limita la propagazione della richiesta ad altri SP solo sul back-channel.
  - Le applicazioni protette dall'SP devono quindi usare esclusivamente la sessione dell'SP o alternativamente accoppiare la sessione dell'applicazione a quella dell'SP cosicché una non possa essere usata senza l'altra.

Rispetto alla ver. 2.x

- Molti (ma non tutti) i file di configurazione possono essere ricaricati periodicamente (1 min.)
  - Attribute Filter
  - Attribute Resolver
  - Credentials
  - Metadata Providers
  - UI properties

Rispetto alla ver. 2.x

- Modificato e ordinato il layout del Configuration Tree in modo da adattarsi ad ...
- Apache Velocity template engine per tutte le pagine user-facing, dove possibile.
- Supporto iniziale al clustering

Clustering

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Clustering

- Terracotta non è più supportato (era usato in qualche implementazione con Tomcat)
- Storage service
  - in-memory via hashtable → WebFlows
  - client-side via secured cookies → sessione e consent
  - relational database via Hibernate → sessione, SLO, consent server-side
  - Memcached → sessione, fase di login

Clustering

- Per
  - Implementare l'HA
  - Implementare il SLO (non supportato nel secure cookie storage client-side)
- Necessito di
  - DB (JPA+connection pooling+postgres/mysql)
    - .jar diver necessari per connection pooling e db engine
  - Memcached ...

Clustering

  - Front node: stateful director cluster o linux HA (che tenga traccia della sessione) è ancora necessario

- Limitazioni
  - SAML 1 artifacts solo mono-nodo

Logging

- Logging avanzato tramite le librerie logback
  - Mail alert degli errori
  - Rotazione e compressione dei log
  - Cancellazione automatica vecchi file
  - Ri-caricamento automatico della configurazione
  - Recovery da situazioni di I/O failure

Belle novità, quindi?

Requisiti

- S.O. raccomandati genericamente: Linux, OS X e Windows
- Oracle Java (o OpenJDK) versioni 7 e 8
  - **NO** Java6 e precedenti
  - **NO** GNU Java compiler and VM (gcj)
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files OBBLIGATORIO per l'uso di chiavi a AES a 256 bit

Requisiti

- L'uso di OpenJDK implica quantomeno la modifica della configurazione riguardo all'implementazione del Security Manager
- Servlet containters
  - che implementino Servlet API 3.0
  - Tomcat ≥ 7 o Jetty ≥ 8
  - Consigliati e supportati ufficialmente solo Tomcat 8 e Jetty 9.2

Jetty

- Eclipse Jetty vs. ApacheTomcat
  - Jetty si focalizza su
    - HTTP connection multiplexing
    - (WebSockets) e SPDY
    - HTTP/2.0 ready
  - Impronta in memoria ridotta (scalabilità e performance)
  - Jetty 9 è stato riarchitettato
    9.1 è il 30% più veloce di jetty 8

Jetty

- Configurazione iniziale semplificata (su un IdP in produzione generalmente gira solo la servlet di Shibboleth)
- “Don’t put your application into Jetty, put Jetty into your application.”
- Usato nell'installer windows come bundled servlet container
- Maggiormente documentato per il deployment di Shibboleth 3

Migrazione

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Snow Goose Migration CC-BY 2.0 USFWS Mountain-Prairie

Migrazione

- Nuovo sistema o copia del sistema
- Installazione, configurazione e test di Jetty (opzionale)
- Copia della directory di installazione di Shibboleth 2.x (attenzione ai log voluminosi, uApprove dismesso)
- Installazione del nuovo shibboleth in-place
- Aggiustamenti della configurazione secondo la documentazione di upgrade

Migrazione

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Run e aggiustamenti successivi della configurazione secondo i warning molto esaustivi dell'idp-process.log
- Configurazione ex novo del meccanismo di consent (opzionale)
- Configurazione manuale dell'autenticazione (riscritta) se non va al primo colpo

Migrazione

- Backward compatibility e file immutati.
  - Backward compatibility della configurazione almeno per una major release
  - Vengono mantenuti i vecchi
    - Attribute Resolver
    - Attribute Filter
- Metadata Provider va modificato secondo gli upgrade tasks o secondo quanto segnalato nell'idp-process.log (opzionale)

Migrazione - Consent

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Relying Party: relying-party.xml viene copiato in metadata-providers.xml
  - gli upgrade tasks si riducono parecchio se non è necessaria la compatibilità con SAML 1 (opz.)
  - Una volta compliant col nuovo formato è possibile modificare in services.properties
    - idp.service.relyingparty.resources
      da shibboleth.**Legacy**RelyingPartyResolverResources
      a shibboleth.RelyingPartyResolverResources
  - Questa modifica abilita automaticamente il parsing nativo v3 e il meccanismo di **consent** altrimenti non disponibile

Secure coockies

- L'IdP V3, al contrario del V2, salva le informazioni di stato in un cookie client-side
- Il cookie viene criptato dal componente "DataSealer" con delle chiavi apposite
- Per limitare il tempo in cui tale chiave è valida, è opportuno rigenerarla periodicamente (quotidianamente a cron) con l'utility seckeygen

Secure coockies

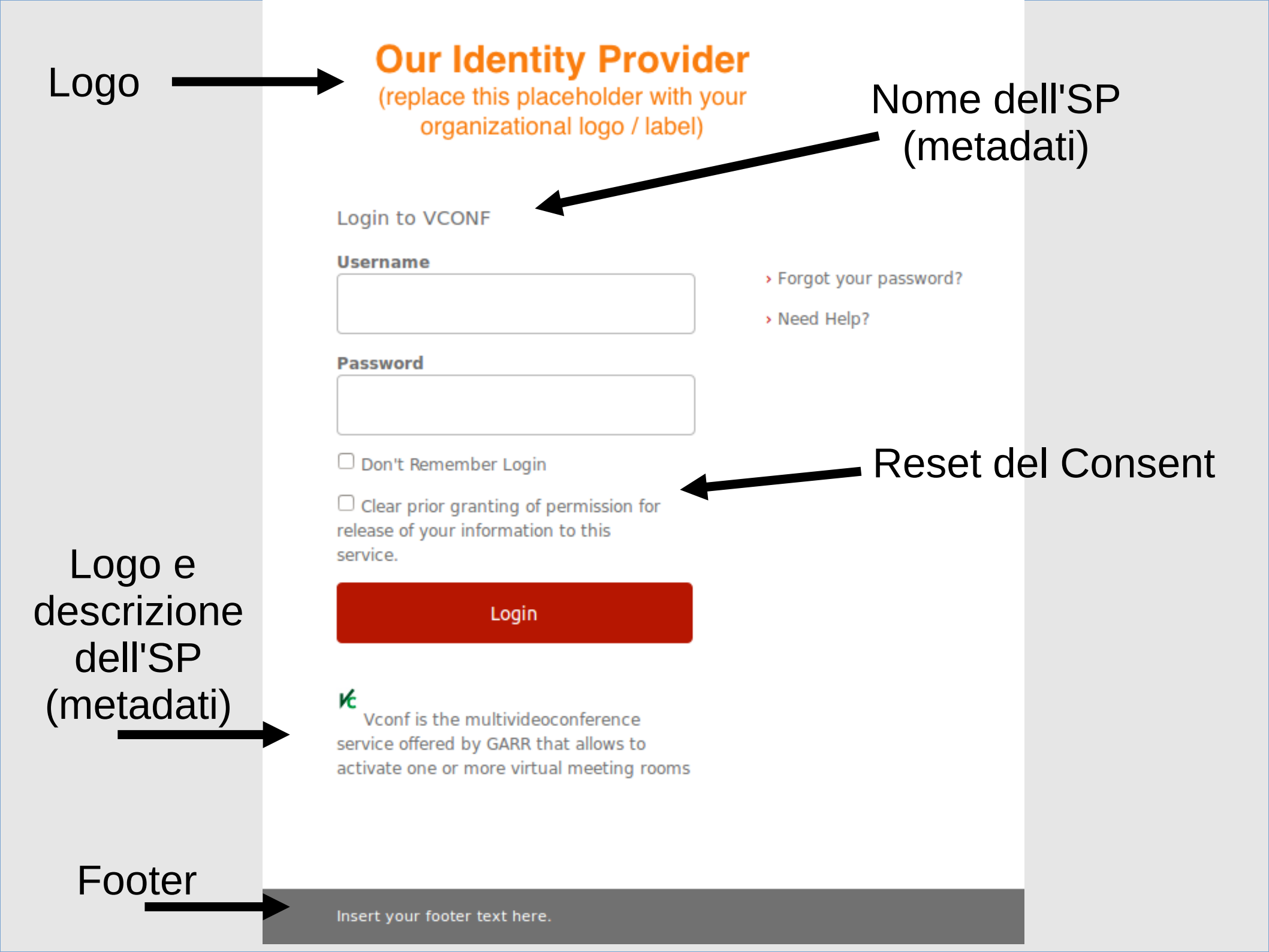
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Seckeygen memorizza la chiave in un keystore che ne mantiene le ultime (30)
- Questo keystore deve essere copiato su ogni nodo del cluster di IdP

Interfaccia

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Igor Stepanov and Oculus Rift
CC-BY-SA 2.0 Sergey Galyonkin


Logo
Our Identity Provider
(replace this placeholder with your organizational logo / label)
Nome dell'SP (metadati)
Login to VCONF
Username
Password
› Forgot your password?
› Need Help?
Don't Remember Login
Reset del Consent
Clear prior granting of permission for release of your information to this service.
Login
Logo e descrizione dell'SP (metadati)
Vconf is the multivideoconference service offered by GARR that allows to activate one or more virtual meeting rooms
Footer
Insert your footer text here.

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Login to VCONF

Username

Password

Non ricordare il login

Cancella le autorizzazioni precedenti per il rilascio di informazioni a questo servizio.

Login

› Dimenticata la tua password?

› Hai bisogno di aiuto?

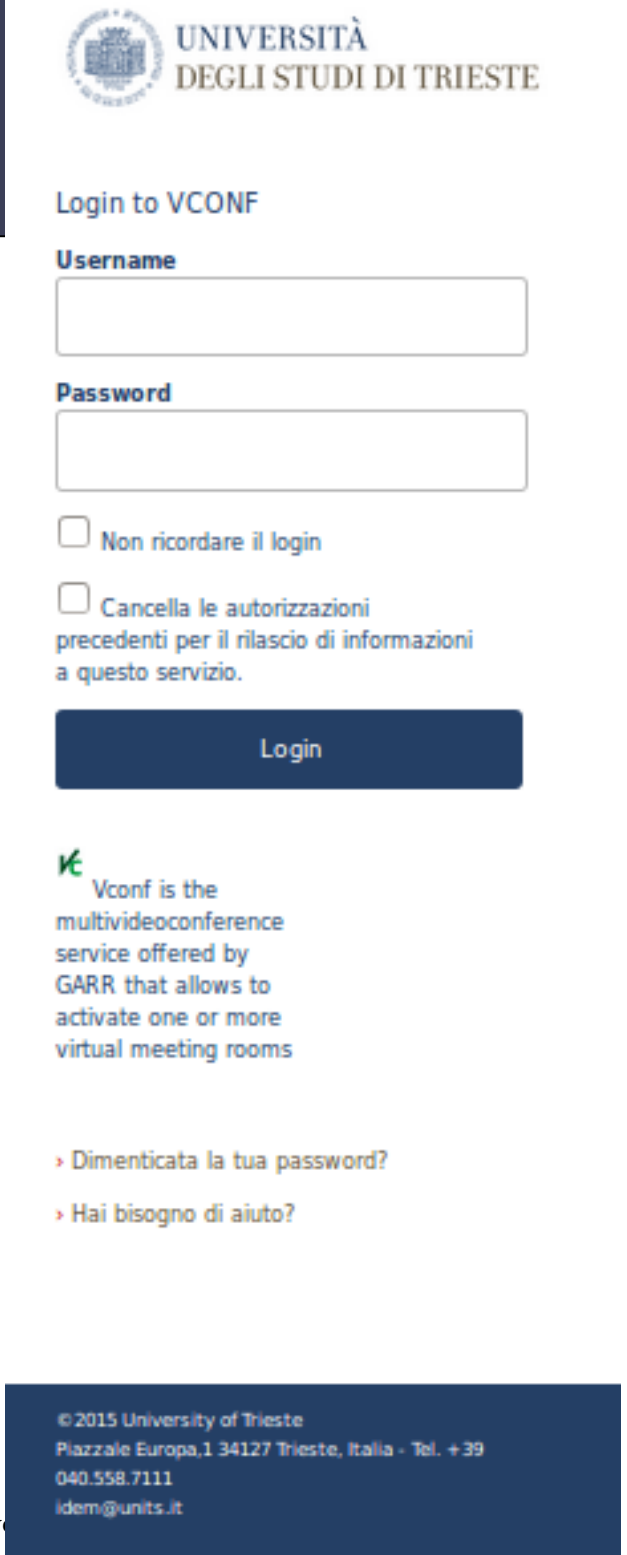
Vconf is the multivideoconference service offered by GARR that allows to activate one or more virtual meeting rooms

Tutto il testo può essere personalizzato in messages/authn-messages.properties

Piazzale Europa,1 34127 Trieste, Italia - Tel. +39 040.558.7111
idem@units.it

Mobile

- CSS pensato
  per dispositivi mobili



What's next

- Ottimizzazioni Kerberos
- Ordine di visualizzazione degli attributi in consent
- UTF-8 nel parsing dei files *.properties

Obbiettivi

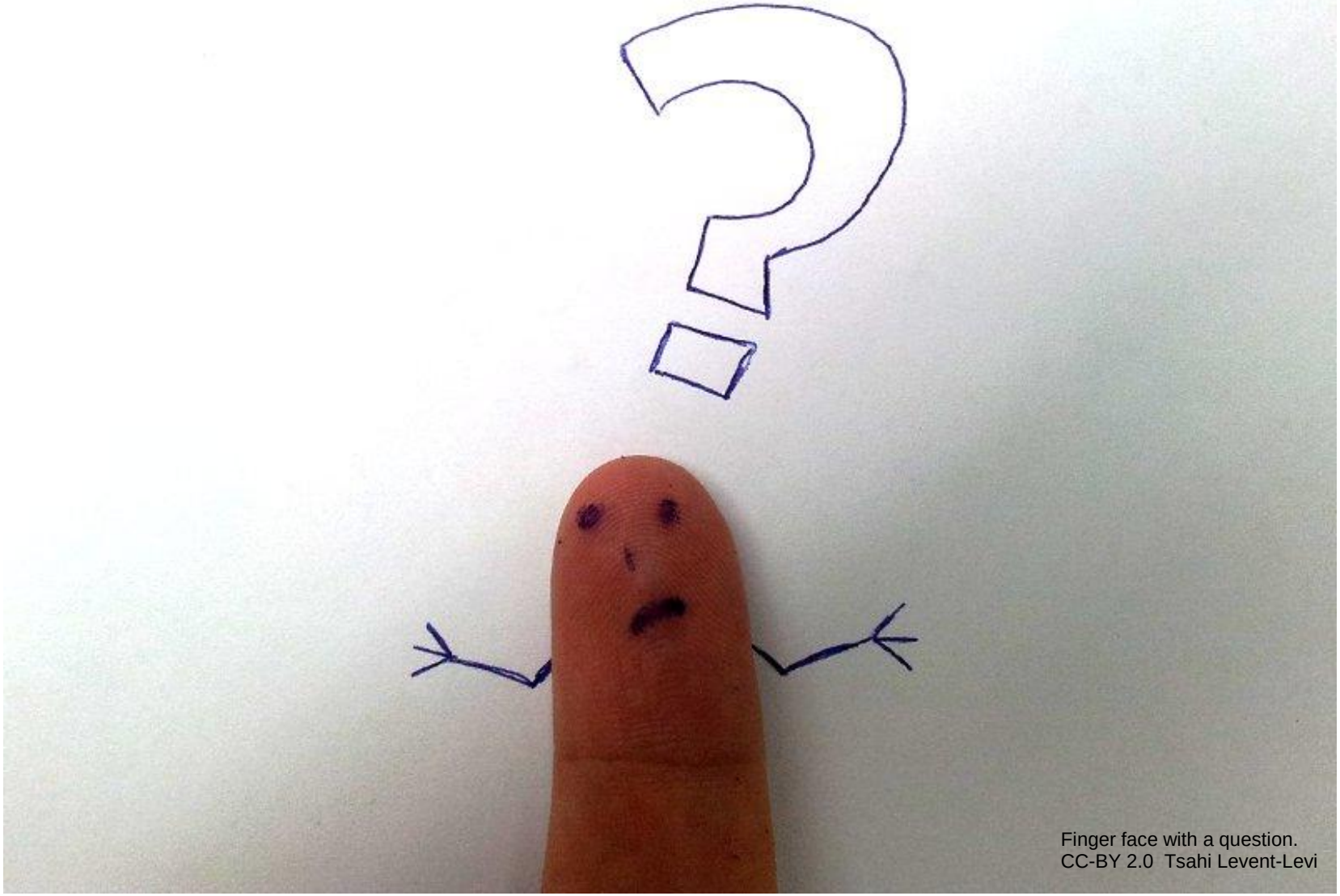
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Come installo shibboleth.
  - Che versione installo.
  - Con che Servlet Container.
- Aggiorno shibboleth.
  - A cosa vado in contro.

Ma....

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Domande?



Finger face with a question.
CC-BY 2.0 Tsahi Levent-Levi

Grazie

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Per l'attenzione e la pazienza

Thank You
CC-BY-NC-ND 2.0 Avard Woolaver

Links

- http://en.wikipedia.org/wiki/Spring_Framework
- http://en.wikipedia.org/wiki/Java_Persistence_API
- https://www.switch.ch/aai/support/presentations/techupdate-2014/06_IdPv3.pdf
- https://wiki.shibboleth.net/confluence/display/CONCEPT/IdPSkills
- https://wiki.shibboleth.net/confluence/display/CONCEPT/ECP
- http://docs.oasis-open.org/security/saml/Post2.0/saml-ecp/v2.0/cs01/
- https://wiki.shibboleth.net/confluence/display/DEV/IdP3Details
- http://www.slideshare.net/Codemotion/jetty-9-the-next-generation-servlet-container

Licenza

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Alcuni contentuti, come specificato sugli stessi, sottostanno ad una diversa licenza d'uso Creative Commons