Meccanismi di Autenticazione e di Autorizzazione

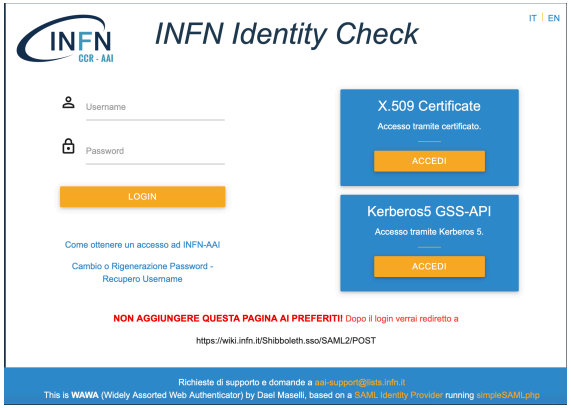
Tutorial days di CCR

I Servizi Nazionali della CCR

Enrico M.V. Fasanelli

Agenda

- Autenticazione
  - Brevissimo intermezzo sulla qualità delle password
  - Certificati X.509
  - Kerberos/GSSAPI
- Autorizzazione
  - Ruoli (Gruppi)
  - Attributi (Entitlements)
- Cos'è e come funziona GODiVA



Autenticazione

Autenticazione (diritto)

- Nel diritto **l'autenticazione** è, in generale, la certificazione **dell'autenticità** di un documento.
  - La specie più diffusa è l'autenticazione della firma, ossia l'attestazione rilasciata da organismo autorizzato e accreditato che un documento è stato sottoscritto da una determinata persona, avendolo sottoscritto alla presenza di chi certifica ed essendo questi **certo della sua identità**.

Autenticazione

- Liberamente adattato da https://it.wikipedia.org/wiki/Autenticazione
  - Si definisce in **informatica** il processo tramite il quale un **sistema informatico**, un **computer**, un **software** o un **utente** verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole **comunicare** attraverso una **connessione**
  - È il sistema che verifica, effettivamente, che **chi partecipa alla comunicazione** è chi sostiene di essere.
  - **L'autenticazione** è diversa **dall'identificazione** (la determinazione che un individuo sia conosciuto o meno dal sistema e **vice-versa**) e **dall'autorizzazione** (il conferimento ad un utente del diritto ad accedere a specifiche risorse del sistema, sulla base della sua identità)

Come autentico per un utente

- **Qualcosa che conosce**
  - In generale una «parola d'ordine»
  - In informatica una coppia username/password, un PIN
- **Qualcosa che ha**
  - In generale un documento di riconoscimento
  - In informatica un token, una smart-card
- **Qualcosa che è**
  - La mia faccia, la mia voce, le mie impronte digitali, l'impronta retinica, il DNA

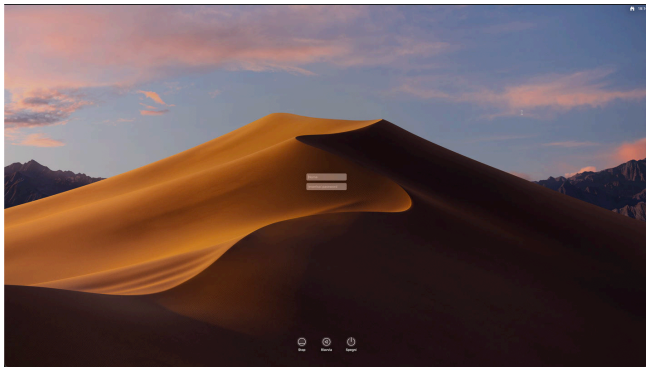
Come autentico per un utente

- **Qualcosa che conosce**
  - In generale una «parola d'ordine»
  - In informatica una coppia username/password, un PIN
- **Qualcosa che ha**
  - In generale un documento di riconoscimento
  - In informatica un token, una smart-card, un telefono
- **Qualcosa che è**
  - La mia faccia, la mia voce, le mie impronte digitali, l'impronta retinica, il DNA

Autenticazione a due fattori 2FA

Qualcosa che conosco

- Coppia Username/password
  - Le più comunemente usate
    - Accesso diretto ai PC o server
    - Accesso ai vari servizi
- PIN

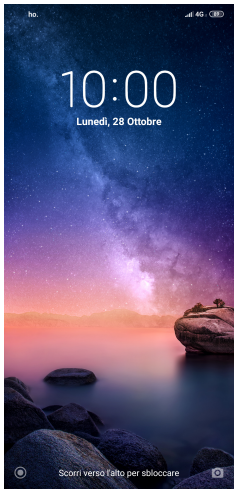


Qualcosa che ho

- Smart-card o token USB (esempio postecert)
  - In generale in questi casi è necessario conoscere anche un PIN e quindi è una 2FA

- Token RSA (generatore di numeri)

- Un telefono, il cui numero è registrato presso chi eroga il servizio, ed al quale viene inviato un codice usa e getta.

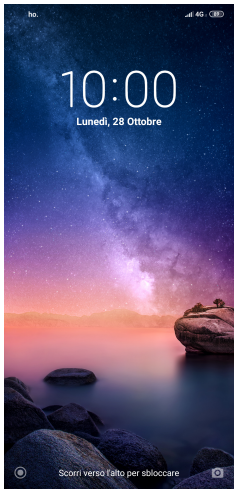


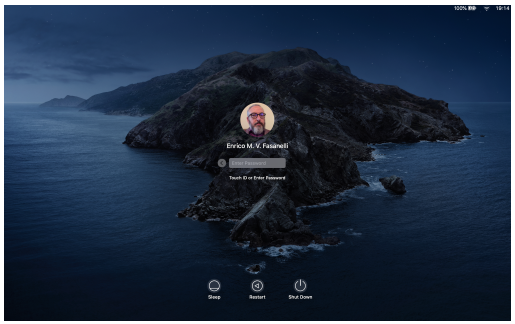
Qualcosa che sono

- Impronte digitali
  - login PC

Qualcosa che sono

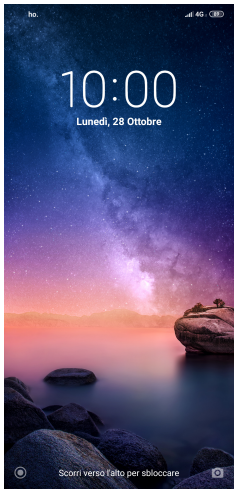
- Impronte digitali
  - login PC
  - accesso allo smartphone

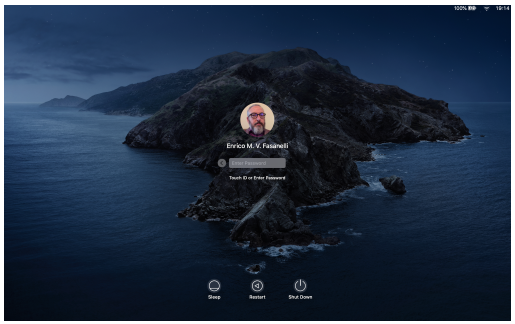


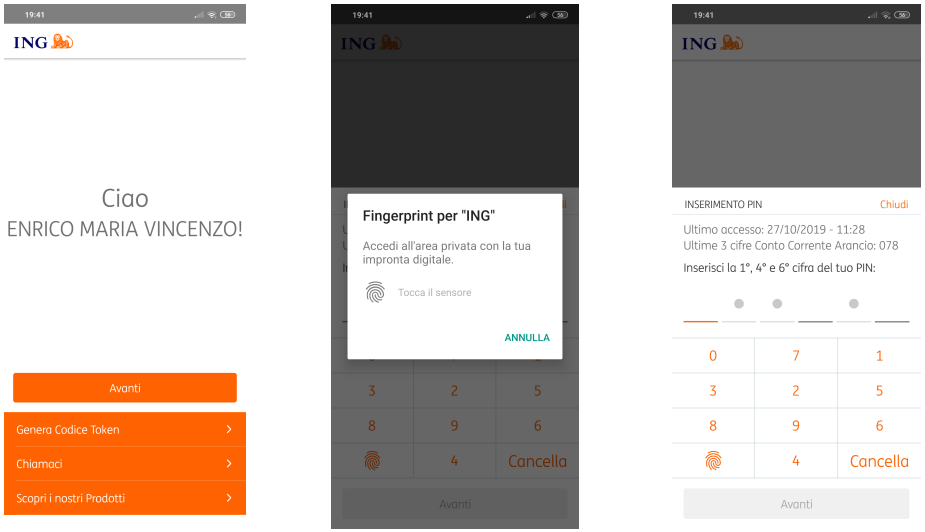


Qualcosa che sono

- Impronte digitali
  - login PC
  - accesso allo smartphone
  - accesso alle applicazioni (banche)







Username/password

- Le più usate e le più «pericolose»
  - migliaia di tentativi di accesso remoto ogni giorno, su tutti i servizi.
- NIST (National Institute of Standards and Technology) USA ha pubblicato negli anni una serie di raccomandazioni.
- Nel 2017 ha prodotto nuove raccomandazioni che ribaltano completamente l'approccio alla scelta di una password

```
/var/log/secure:Oct 27 04:20:40 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
/var/log/secure:Oct 27 04:20:44 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
/var/log/secure:Oct 27 04:20:47 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
/var/log/secure:Oct 27 04:20:51 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
/var/log/secure:Oct 27 04:21:16 login sshd[26193]: Failed password for invalid user foxi from 106.12.218.159 port 54168 ssh2
/var/log/secure:Oct 27 04:21:22 login sshd[26219]: Failed password for root from 122.4.241.6 port 10332 ssh2
/var/log/secure:Oct 27 04:21:34 login sshd[26230]: Failed password for root from 203.129.253.78 port 40010 ssh2
/var/log/secure:Oct 27 04:21:48 login sshd[26273]: Failed password for root from 81.12.159.146 port 47070 ssh2
/var/log/secure:Oct 27 04:22:17 login sshd[26316]: Failed password for invalid user service from 186.170.28.46 port 44018 ssh2
/var/log/secure:Oct 27 04:22:50 login sshd[26364]: Failed password for root from 117.50.95.121 port 57686 ssh2
/var/log/secure:Oct 27 04:22:50 login sshd[26367]: Failed password for invalid user trojans1 from 106.52.35.207 port 42632 ssh2
/var/log/secure:Oct 27 04:23:10 login sshd[26405]: Failed password for invalid user administrator from 162.243.50.8 port 45148 ss
/var/log/secure:Oct 27 04:23:14 login sshd[26437]: Failed password for root from 103.62.239.77 port 38856 ssh2
/var/log/secure:Oct 27 04:24:04 login sshd[26512]: Failed password for invalid user admin from 206.189.137.113 port 42950 ssh2
/var/log/secure:Oct 27 04:24:43 login sshd[26566]: Failed password for invalid user AOL from 217.125.110.139 port 46460 ssh2
/var/log/secure:Oct 27 04:24:45 login sshd[26563]: Failed password for adm from 192.241.185.120 port 45074 ssh2
/var/log/secure:Oct 27 04:25:00 login sshd[26589]: Failed password for root from 104.40.0.120 port 7552 ssh2
/var/log/secure:Oct 27 04:25:32 login sshd[26630]: Failed password for invalid user devop from 124.165.207.150 port 47406 ssh2
/var/log/secure:Oct 27 04:25:37 login sshd[26636]: Failed password for root from 122.4.241.6 port 36456 ssh2
/var/log/secure:Oct 27 04:26:21 login sshd[26719]: Failed password for invalid user ia from 139.59.5.65 port 58534 ssh2
/var/log/secure:Oct 27 04:26:55 login sshd[26756]: Failed password for invalid user nancy from 120.70.101.103 port 54686 ssh2
/var/log/secure:Oct 27 04:27:30 login sshd[26803]: Failed password for root from 117.50.95.121 port 37456 ssh2
/var/log/secure:Oct 27 04:28:35 login sshd[26887]: Failed password for invalid user Passw0rd00 from 217.125.110.139 port 56484 ss
/var/log/secure:Oct 27 04:29:13 login sshd[26956]: Failed password for invalid user Admin from 104.40.0.120 port 7552 ssh2
/var/log/secure:Oct 27 04:29:48 login sshd[27010]: Failed password for invalid user cellphone from 120.132.7.52 port 43168 ssh2
/var/log/secure:Oct 27 04:29:57 login sshd[27023]: Failed password for root from 122.4.241.6 port 56162 ssh2
/var/log/secure:Oct 27 04:30:02 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
/var/log/secure:Oct 27 04:30:06 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
/var/log/secure:Oct 27 04:30:10 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
/var/log/secure:Oct 27 04:30:13 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
/var/log/secure:Oct 27 04:30:37 login sshd[27110]: Failed password for root from 139.59.5.65 port 40088 ssh2
/var/log/secure:Oct 27 04:30:50 login sshd[27140]: Failed password for invalid user thebest from 110.45.155.101 port 56046 ssh2
/var/log/secure:Oct 27 04:30:51 login sshd[27141]: Failed password for root from 192.241.185.120 port 35722 ssh2
/var/log/secure:Oct 27 04:31:08 login sshd[27169]: Failed password for root from 197.248.16.118 port 37218 ssh2
/var/log/secure:Oct 27 04:31:11 login sshd[27183]: Failed password for root from 82.238.107.124 port 55232 ssh2
/var/log/secure:Oct 27 04:31:42 login sshd[27222]: Failed password for invalid user test from 120.70.101.103 port 44935 ssh2
/var/log/secure:Oct 27 04:32:06 login sshd[27265]: Failed password for invalid user th from 117.50.95.121 port 45460 ssh2
/var/log/secure:Oct 27 04:32:52 login sshd[27342]: Failed password for invalid user test from 203.129.253.78 port 34880 ssh2
/var/log/secure:Oct 27 04:33:24 login sshd[27398]: Failed password for invalid user frederica123 from 106.52.35.207 port 58304 ss
/var/log/secure:Oct 27 04:33:37 login sshd[27415]: Failed password for root from 119.204.168.61 port 47614 ssh2
```

Password sicure

- Vecchie raccomandazioni
  - Cambiare la password regolarmente (ogni 6 mesi)
  - Almeno 3 categorie di caratteri (maiuscolo, minuscolo, numeri, punteggiatura) almeno 8 caratteri
  - Questo ha portato di fatto a scegliere password con sostituzione lettera→numero
    - P4p3r0pol!
- Nuove raccomandazioni
  - Non ha senso cambiare regolarmente una buona password
  - Non ha senso la «danza dei caratteri» in quanto i computer sono più bravi degli umani ad effettuare le sostituzioni. Meglio una password lunga.
  - La password non deve essere nota **(verifica verso i vari dizionari)**

AgID & MM vs Password

- AgID (Agenzia per l'Italia Digitale della Presidenza del Consiglio dei Ministri) ha emanato nel 2017 una circolare per la definizione delle Misure Minime di sicurezza.
  - Viene richiesto (tra le altre cose) il cambio password periodico per gli amministratori di sistema.
  - Il resto del mondo si sta adeguando alle nuove direttive del NIST
  - Io spero che AgID si adegui in fretta

Qualcosa che ho (smartcard/certificato)

- X.509 si basa sulla tecnologia crittografica a coppia di chiavi asimmetriche
  - Due chiavi collegate, ma da una non si può ottenere l'altra.
  - Una chiave viene resa pubblica, l'altra deve essere tenuta segreta.
  - Quello che si cifra con una delle due chiavi può essere decifrato solo con l'altra
  - La chiave resa pubblica viene «certificata» da una autorità di certificazione che garantisce l'associazione di tale chiave pubblica certificata, con la persona a cui tale chiave appartiene.

SmartCard

- La coppia di chiavi pubblica-privata è generata all'interno di un dispositivo (la SmartCard) e non è possibile estrarre la chiave privata dal dispositivo
- L'autorità di certificazione (PosteCert, InfoCamere, Aruba,…) legalmente riconosciuta in Italia, firma la chiave pubblica all'interno del dispositivo, **dopo aver effettuato il riconoscimento *de vusu* dell'utente**
  - La chiave pubblica firmata è il certificato X.509
- L'accesso alle chiavi è protetto da PIN

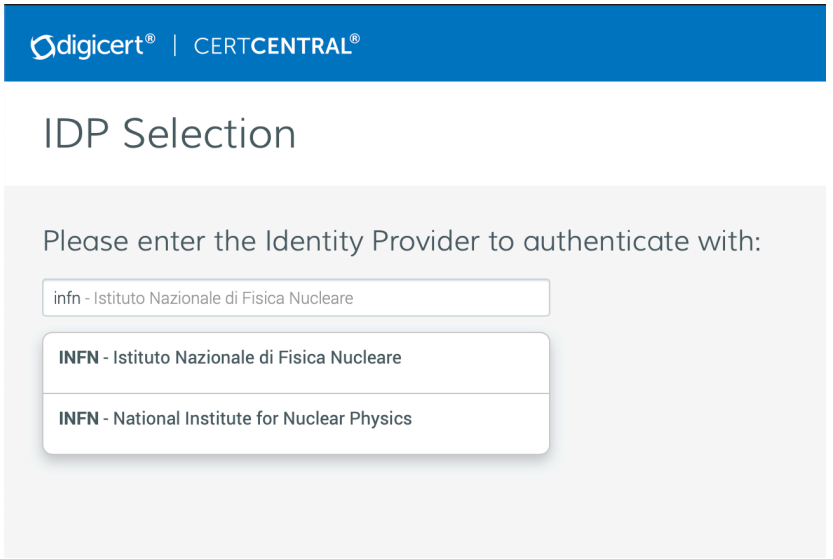
Certificato

- La coppia di chiavi pubblica-privata viene generata dal browser, che espone la chiave pubblica al servizio web (INFN-CA, GARR-CA, **TERENA-TCS**) per la firma.
- L'autorità di certificazione firma la chiave pubblica generando quindi il certificato X.509 dell'utente, che viene quindi acquisito dal browser
- Il browser collega il certificato alla chiave privata (che era nella memoria privata del browser)
- Chi effettua il riconoscimento *de visu* dell'utente?
  - INFN-CA e GARR-CA le Registration Authority (RA) in ogni struttura
  - TERENA-TCS le segreterie di direzione/personale

TERENA-TCS

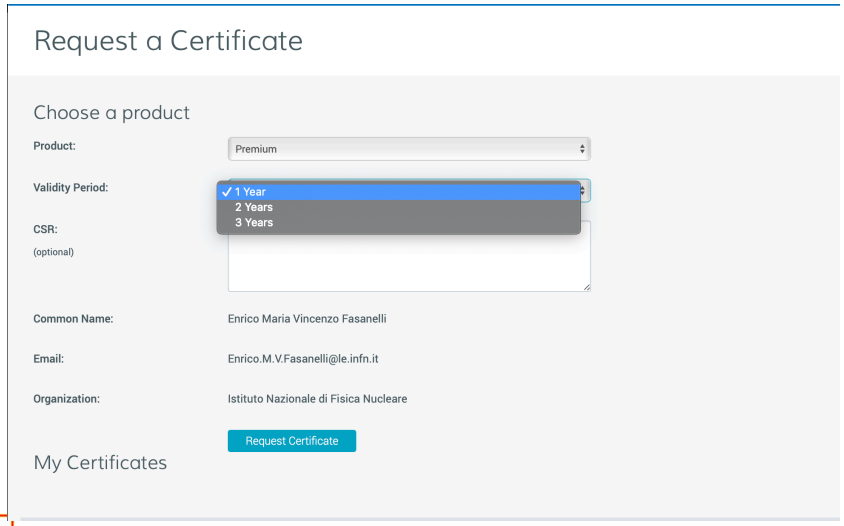
- Servizio di rilascio di certificati, accessibile attraverso federazione GARR-IDEM e quindi attraverso INFN-AAI
  - Utenti per i quali possiamo garantire l'avvenuta **identificazione** (dipendenti ed associati)
- https://www.digicert.com/sso

- Browser sono supportati
  - Safari
  - IE
  - Firefox-ESR
  - Firefox Portable

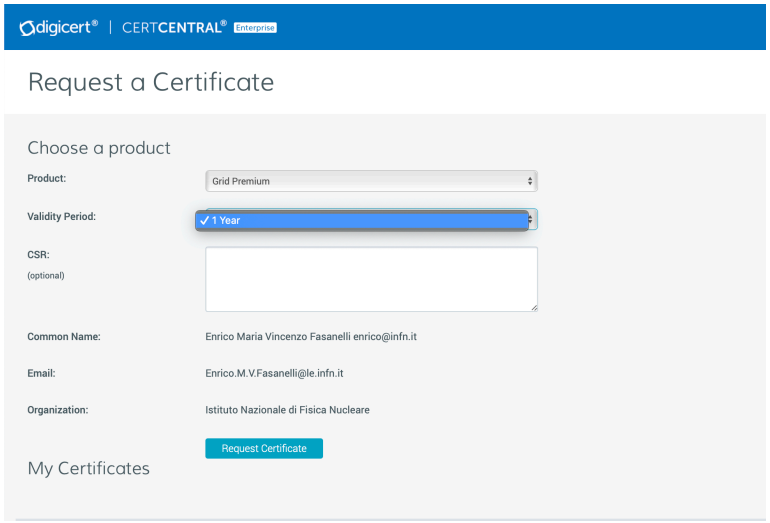


Premium vs GRID Premium

- Premium
  - Validità 1,2 o 3 anni
  - Client Authentication
  - Email protection

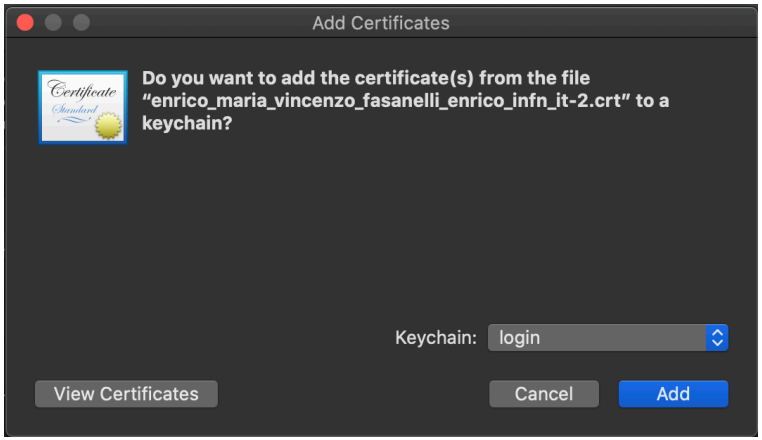


- GRID Premium
  - Validità 1 anno
  - Premium + GRID

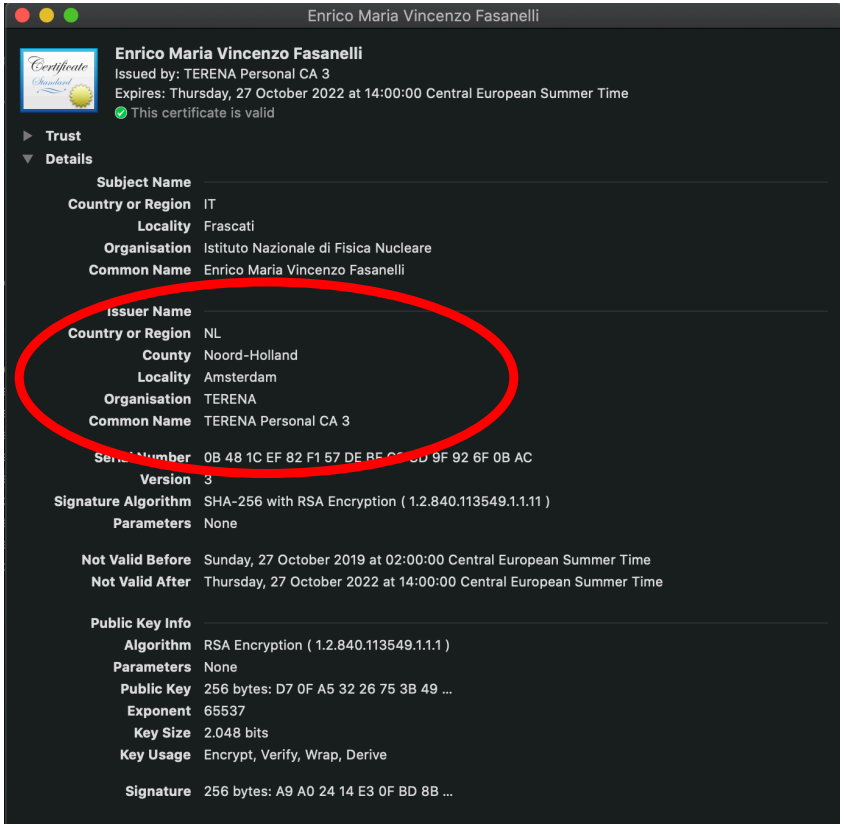


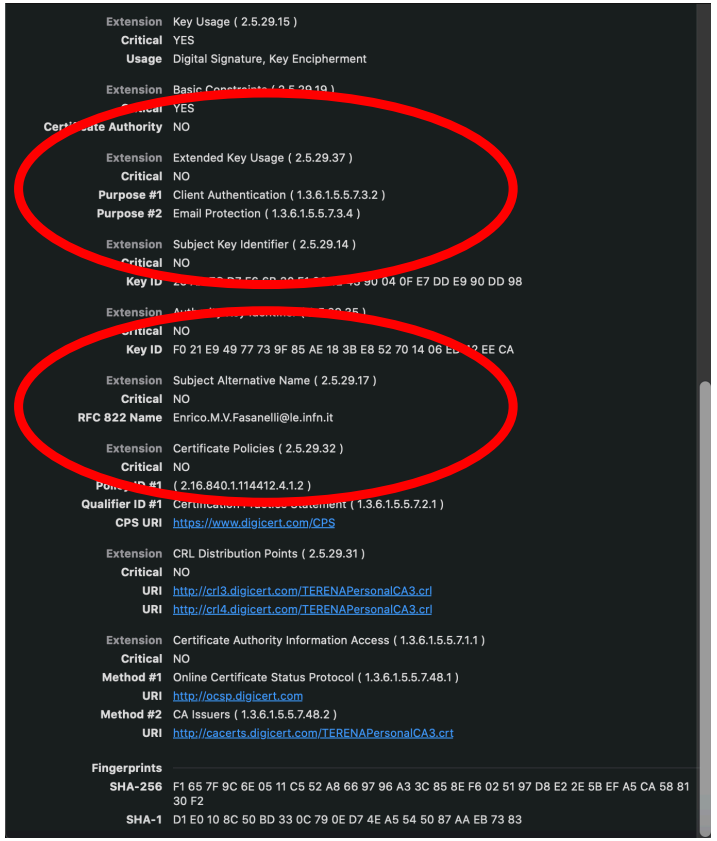
Rilascio automatico del certificato

- «Request Certificate» scatena la generazione della coppia di chiavi nel browser e l'invio al server web di Digicert della chiave pubblica per la firma.
- Il server web di Digicert firma la chiave generando il certificato che viene accoppiato alla chiave privata e salvato
  - Safari salva tutto su disco (poi importato automaticamente nel portachiavi)
  - Firefox salva tutto nel sul database



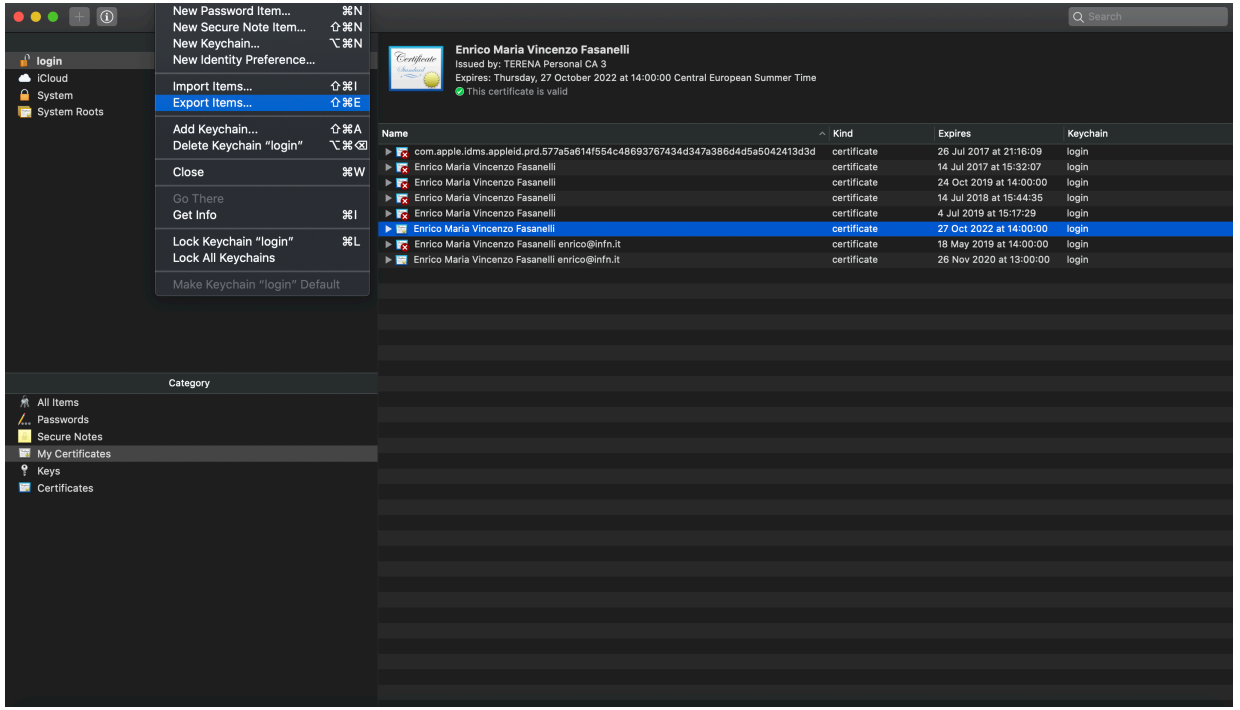
Il mio certificato





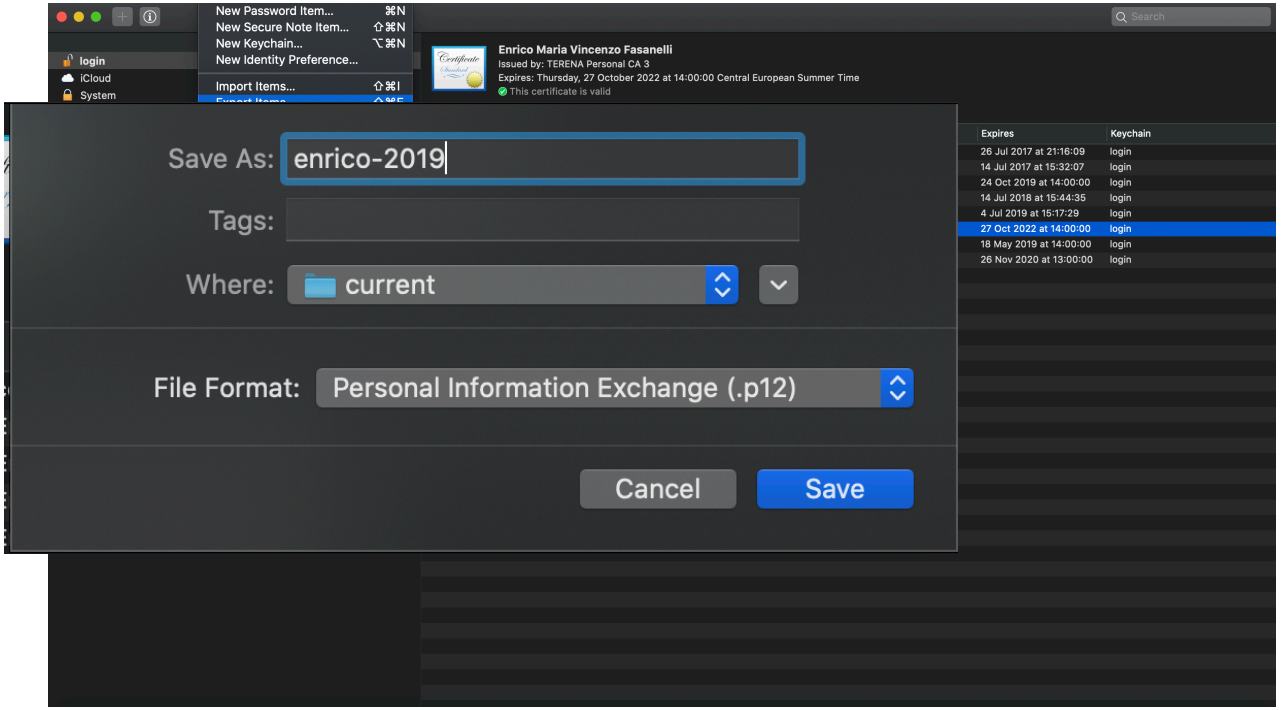
Installare il certificato in altro browser

- Esportare il certificato



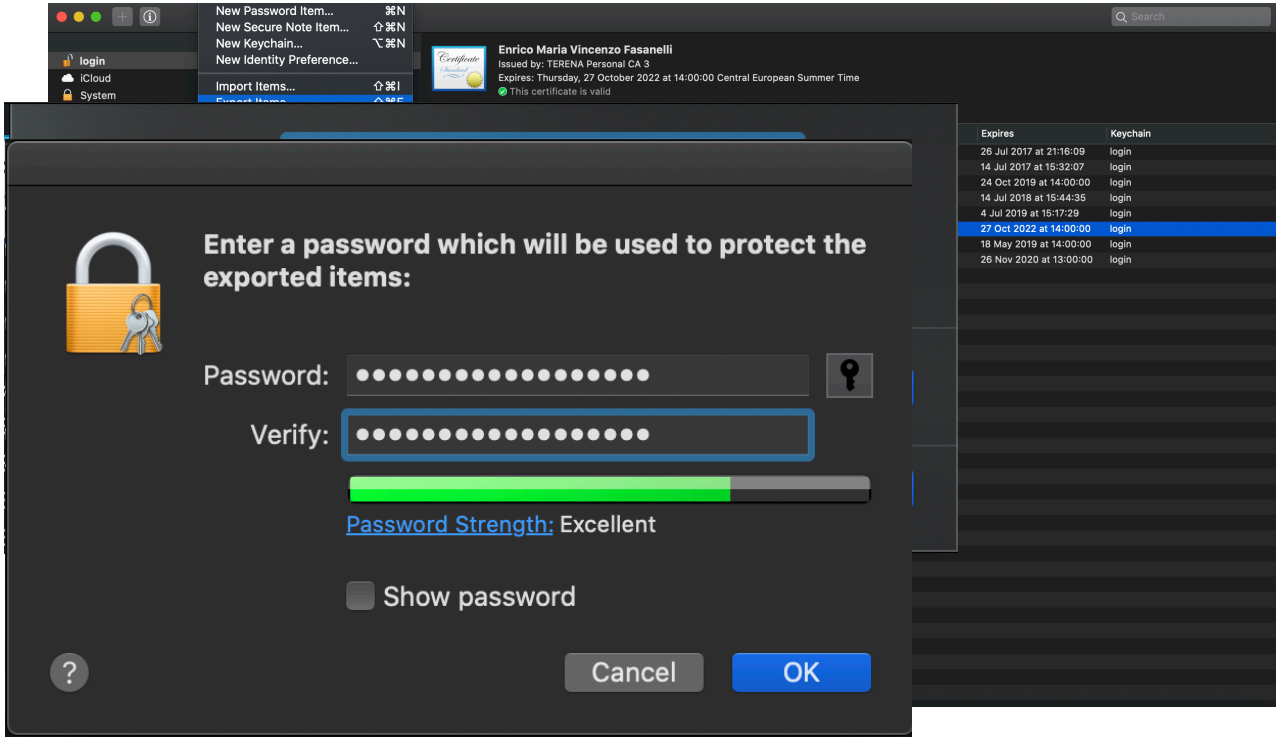
Installare il certificato in altro browser

- Esportare il certificato
- Scegliere il nome del file



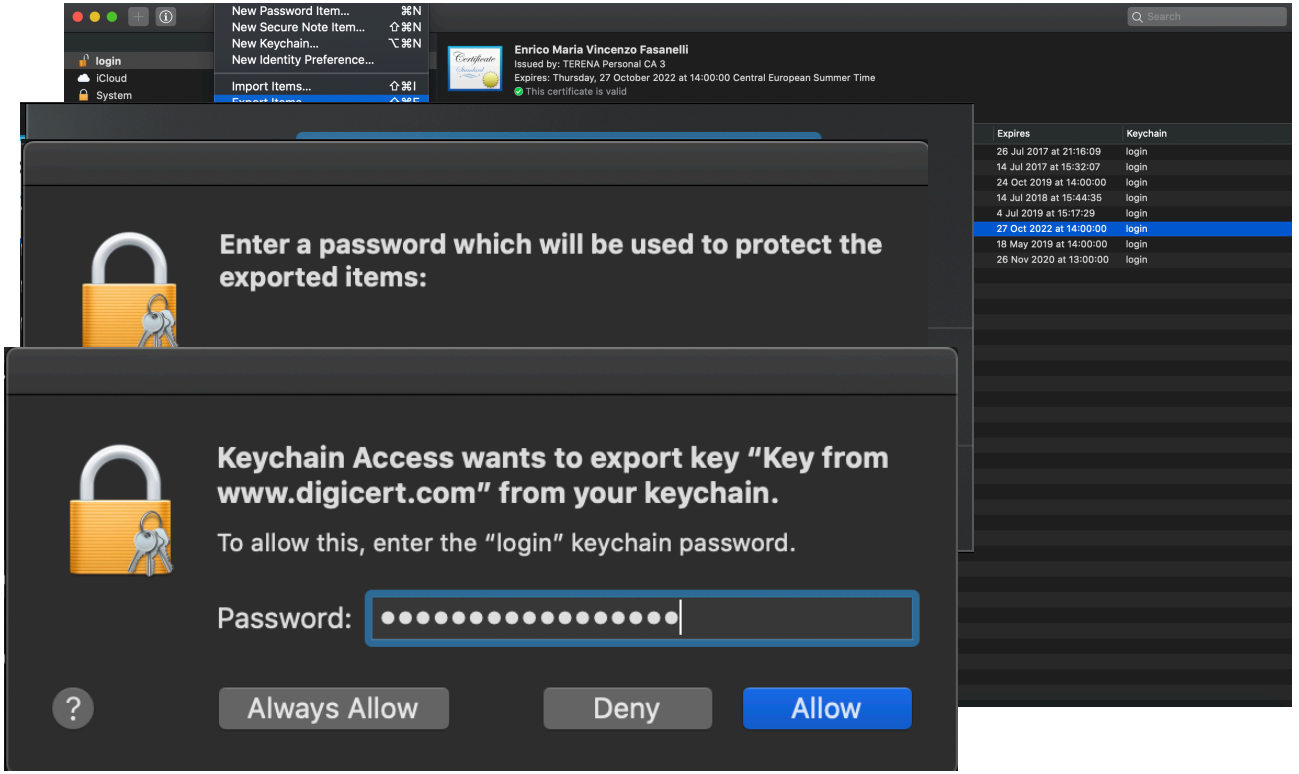
Installare il certificato in altro browser

- Esportare il certificato
- Scegliere il nome del file
- Scegliere una password per proteggere tale file



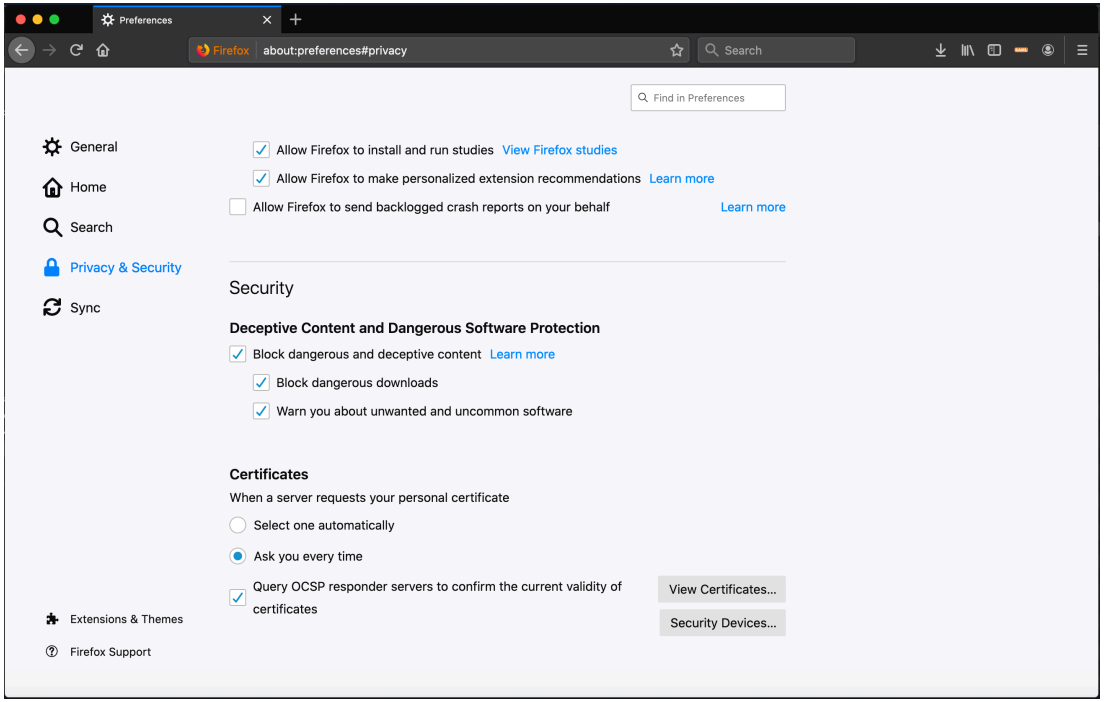
Installare il certificato in altro browser

- Esportare il certificato
- Scegliere il nome del file
- Scegliere una password per proteggere tale file
- Permettere l'export



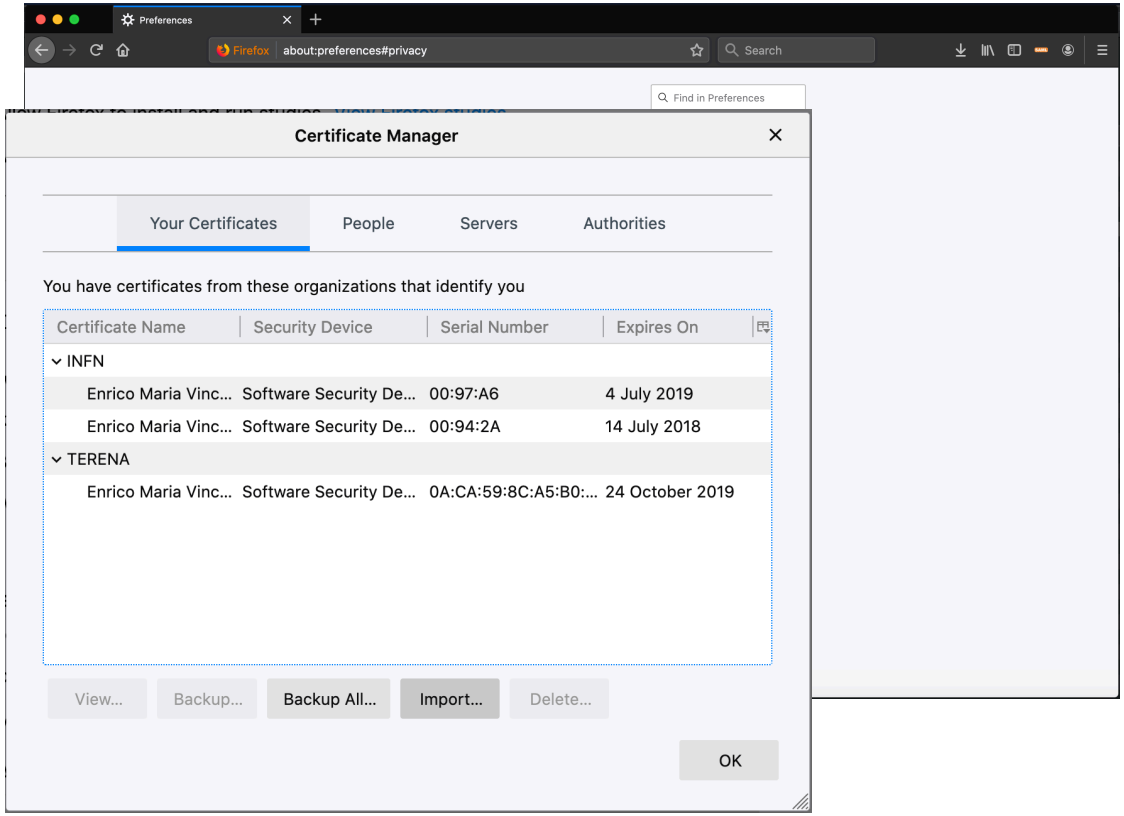
Importare il certificato in Firefox

- Nelle impostazioni di Firefox
  - about:preferences



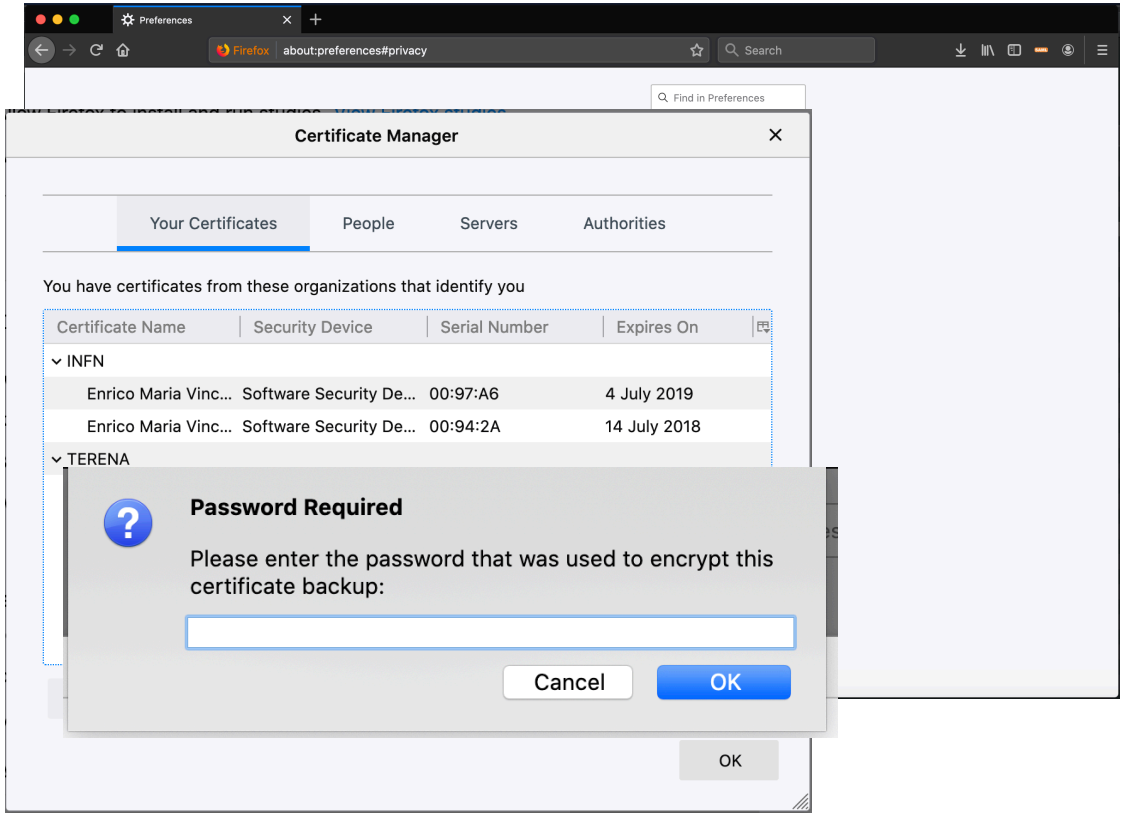
Importare il certificato in Firefox

- Nelle impostazioni di Firefox
  - about:preferences
- Selezionare «mostra certificati» e quindi «import»



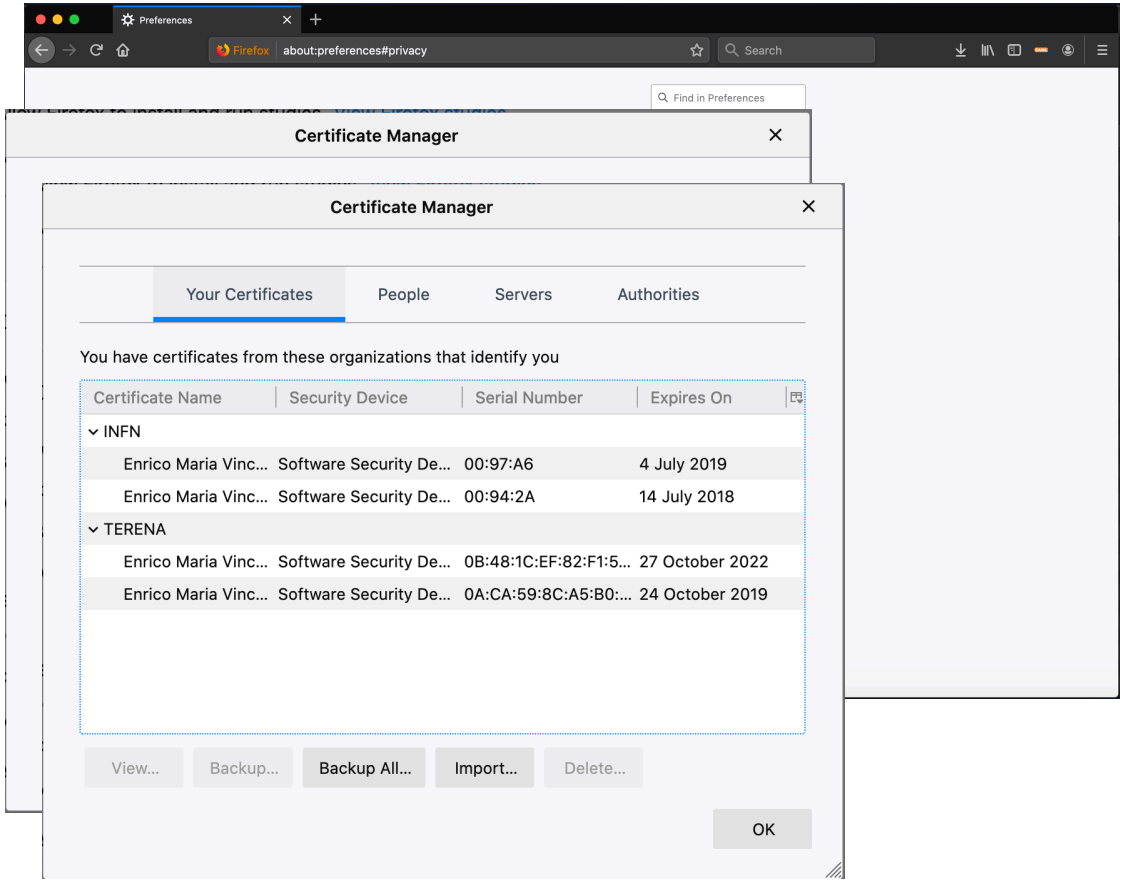
Importare il certificato in Firefox

- Nelle impostazioni di Firefox
  - about:preferences
- Selezionare «mostra certificati» e quindi «import»
- Firefox chiederà la password di protezione del file



Importare il certificato in Firefox

- Nelle impostazioni di Firefox
  - about:preferences
- Selezionare «mostra certificati» e quindi «import»
- Firefox chiederà la password di protezione del file
- Ed alla fine importerà il certificato e la chiave privata



Kerberos/GSSAPI

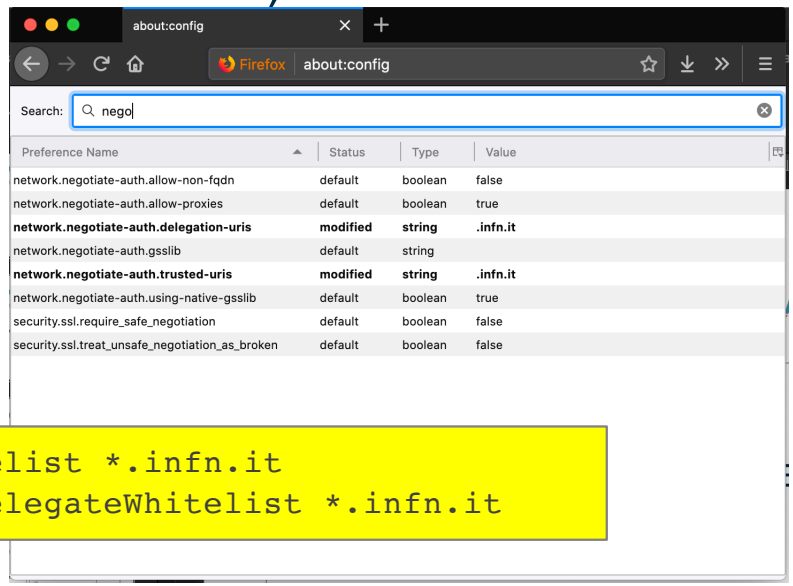
- Assomiglia a Username/Password ma è completamente differente
- A differenza dell'autenticazione Username/Password, con Kerberos la Password non viaggia in rete, ma serve ad aprire (decifrare) un «pacchetto» che viene chiuso (cifrato) con la password dell'utente dal server di autenticazione centrale (KDC) ed inviato all'utente.
- Se l'utente inserisce la password corretta, riesce ad aprire il pacchetto ed a estrarre i biglietti (ticket) con i quali accedere ai vari servizi o ottenere altri biglietti (ticket) per accedere ai servizi
- Single Sign-On senza mai dover far viaggiare la password in rete.

Usare Kerberos/GSSAPI

- Per ora gli utenti delle sedi che usano Kerberos (prevista l'estensione a tutti gli utenti INFN-AAI)
  - Roma1, Trieste, Bologna (INFN.IT cella AFS infn.it)
  - PI, LE, LNF, LNGS, MI, MIB, GE

Usare Kerberos/GSSAPI

- Per ora gli utenti delle sedi che usano Kerberos (prevista l'estensione a tutti gli utenti INFN-AAI)
  - Roma1, Trieste, Bologna (INFN.IT cella AFS infn.it)
  - PI, LE, LNF, LNGS, MI, MIB, GE

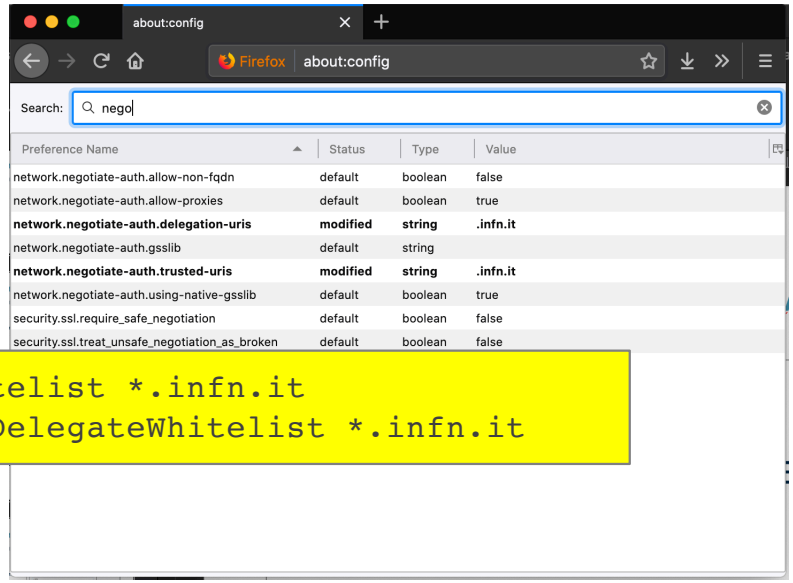


- Configurare il browser
  - Firefox
  - Chrome (MacOS)

```
$ defaults write com.google.Chrome AuthServerWhitelist *.infn.it
$ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist *.infn.it
```

Usare Kerberos/GSSAPI

- Per ora gli utenti delle sedi che usano Kerberos (prevista l'estensione a tutti gli utenti INFN-AAI)
  - Roma1, Trieste, Bologna (INFN.IT cella AFS infn.it)
  - PI, LE, LNF, LNGS, MI, MIB, GE
- Configurare il browser
  - Firefox
  - Chrome (MacOS)




```
$ defaults write com.google.Chrome AuthServerWhitelist *.infn.it
$ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist *.infn.it
```

- Acquisire il ticket
  - kinit

Mutua autenticazione

- Si definisce in **informatica** il processo tramite il quale un **sistema informatico**, un **computer**, un **software** o un **utente** verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole **comunicare** attraverso una **connessione**
- È il sistema che verifica, effettivamente, che **chi partecipa alla comunicazione** è chi sostiene di essere.
- **L'autenticazione** è diversa **dall'identificazione** (la determinazione che un individuo sia conosciuto o meno dal sistema e **vice-versa**) e **dall'autorizzazione** (il conferimento ad un utente del diritto ad accedere a specifiche risorse del sistema, sulla base della sua identità)

Mutua autenticazione

- Non è solo il sistema informatizzato a dover autenticare l'utente, ma deve essere anche l'utente ad autenticare il sistema o il servizio
- Con chi sto parlando?
- A chi sto inviando le mie credenziali?
- Posso stare tranquillo?

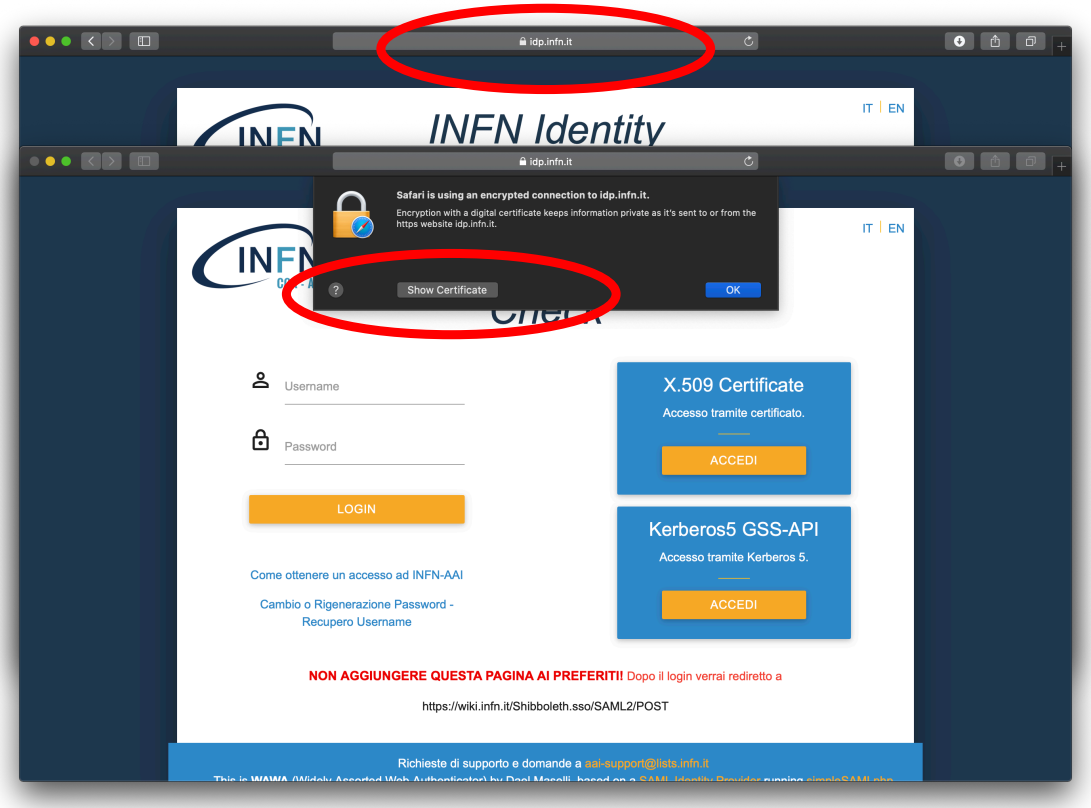
- Si definisce in **informatica** il processo tramite il quale un **sistema informatico**, un **computer**, un **software** o un **utente** verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole **comunicare** attraverso una **connessione**
- È il sistema che verifica, effettivamente, che **chi partecipa alla comunicazione** è chi sostiene di essere.
- **L'autenticazione** è diversa **dall'identificazione** (la determinazione che un individuo sia conosciuto o meno dal sistema e **vice-versa**) e **dall'autorizzazione** (il conferimento ad un utente del diritto ad accedere a specifiche risorse del sistema, sulla base della sua identità)

SSL/TLS https://

- Bastano pochi click per chiedere al browser informazioni sul certificato del server web

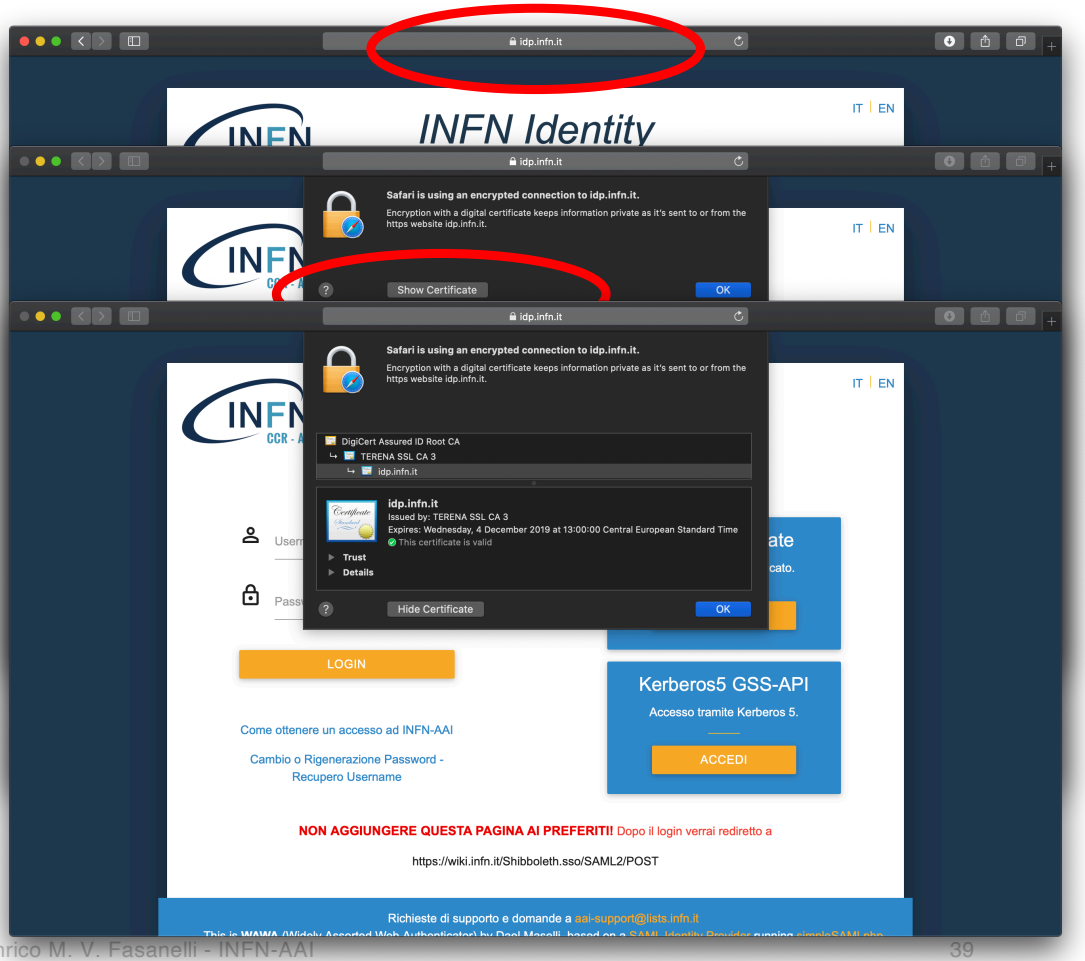
SSL/TLS https://

- Bastano pochi click per chiedere al browser informazioni sul certificato del server web
- Con il primo ho una prima informazione, ma «mascherata»



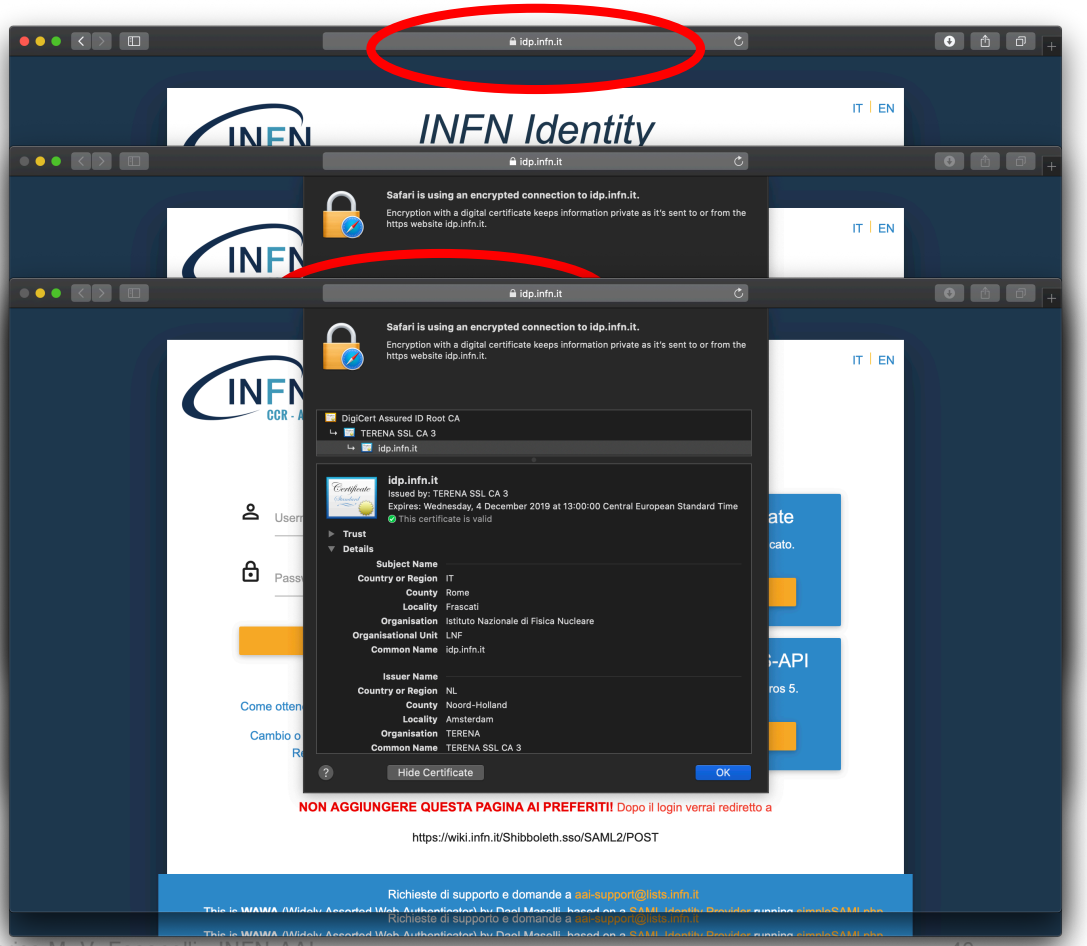
SSL/TLS https://

- Bastano pochi click per chiedere al browser informazioni sul certificato del server web
- Con il primo ho una prima informazione, ma «mascherata»
- Il secondo click mi fa vedere di più



SSL/TLS https://

- Bastano pochi click per chiedere al browser informazioni sul certificato del server web
- Con il primo ho una prima informazione, ma «mascherata»
- Il secondo click mi fa vedere di più
- Posso farmi mostrare ulteriori dettagli



Autorizzazione

Autorizzazione

- In informatica, l'**autorizzazione** è la funzione che specifica i privilegi di accesso alle risorse legate alla sicurezza delle informazioni, alla sicurezza informatica in generale e in particolare al controllo degli accessi.
- Più formalmente, autorizzare significa definire una politica di accesso.
- La politica di accesso può essere basata sull'assegnazione di privilegi in funzione di:
  - ruoli e quindi il modello è Role Based Access Control o RBAC
  - «corredo esplicito di autorizzazioni» memorizzate in appositi «attributi» ed in questo caso si parla di Attribute Based Access Control o ABAC

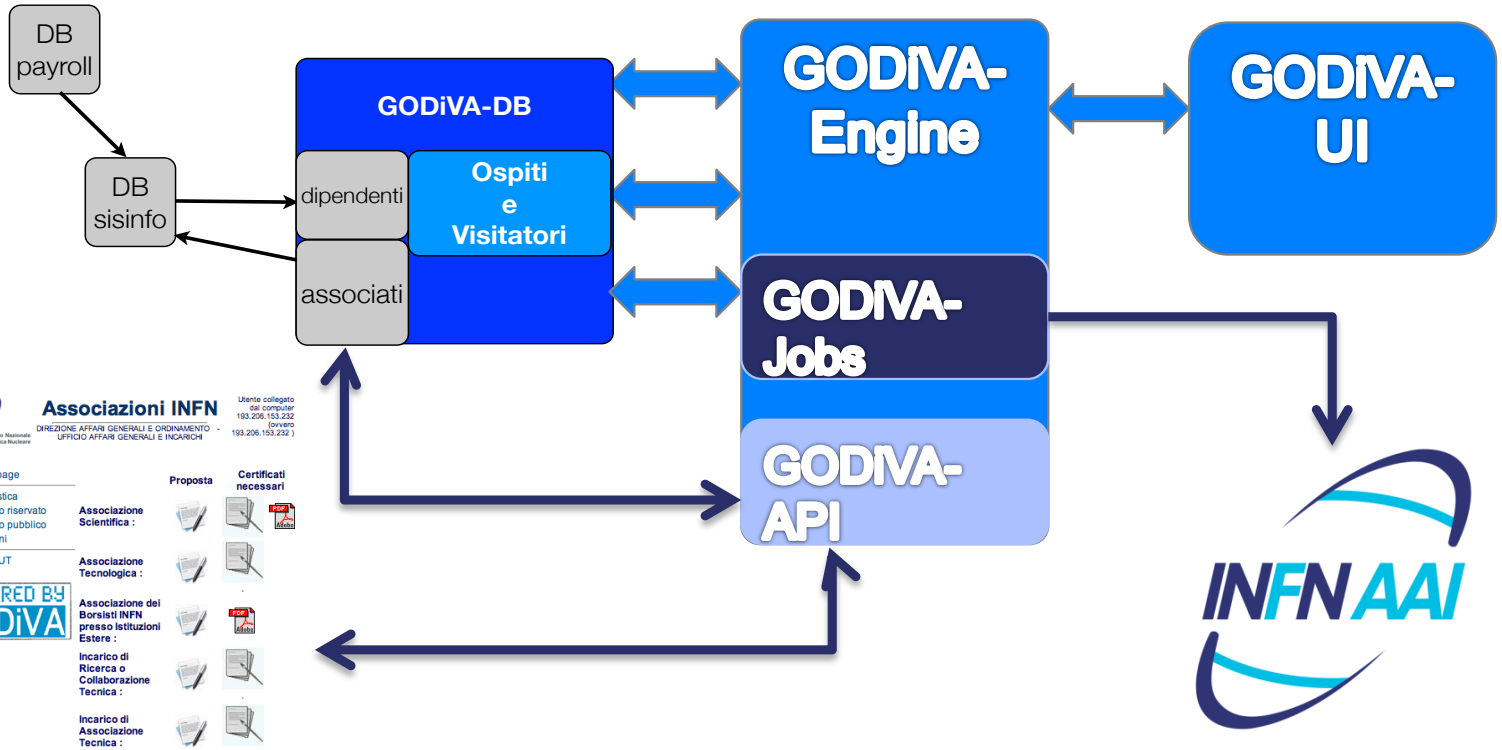
GODiVA

- Gestione Ospiti DIpendenti Visitatori ed Associati
  - 4 macro-categorie di ruoli «amministrativi»
- GODiVA è l'Identity and Access Management System (IAM) dell'INFN, ossia il sistema software per la gestione delle Identità e dei privilegi di accesso degli utenti INFN.
- E' stato disegnato per la gestione delle 4 macro-categorie ed, al loro interno, di tutti i ruoli funzionali/operativi
- Implementa il modello RBAC, cioè assegna permessi in funzione dei ruoli, ma supporta anche il modello ABAC in quanto permette di assegnare singoli attributi a gruppi di utenti (in una prossima versione anche sl singolo utente)

Identity and Access Management

- Il cuore è l'Identità Digitale
  - Registrare (auto-registrare) una Identità Digitale
  - Arricchire tale Identità Digitale assegnandole un ruolo

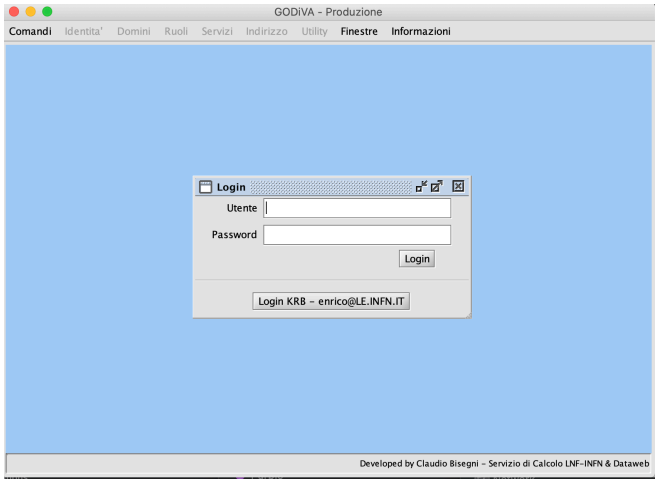
GODiVA




```
OU=People,DC=INFN,DC=IT
```

GODiVA-UI

- Interfaccia grafica Java (nerdissima)
  - https://godiva.infn.it/GODiVA/

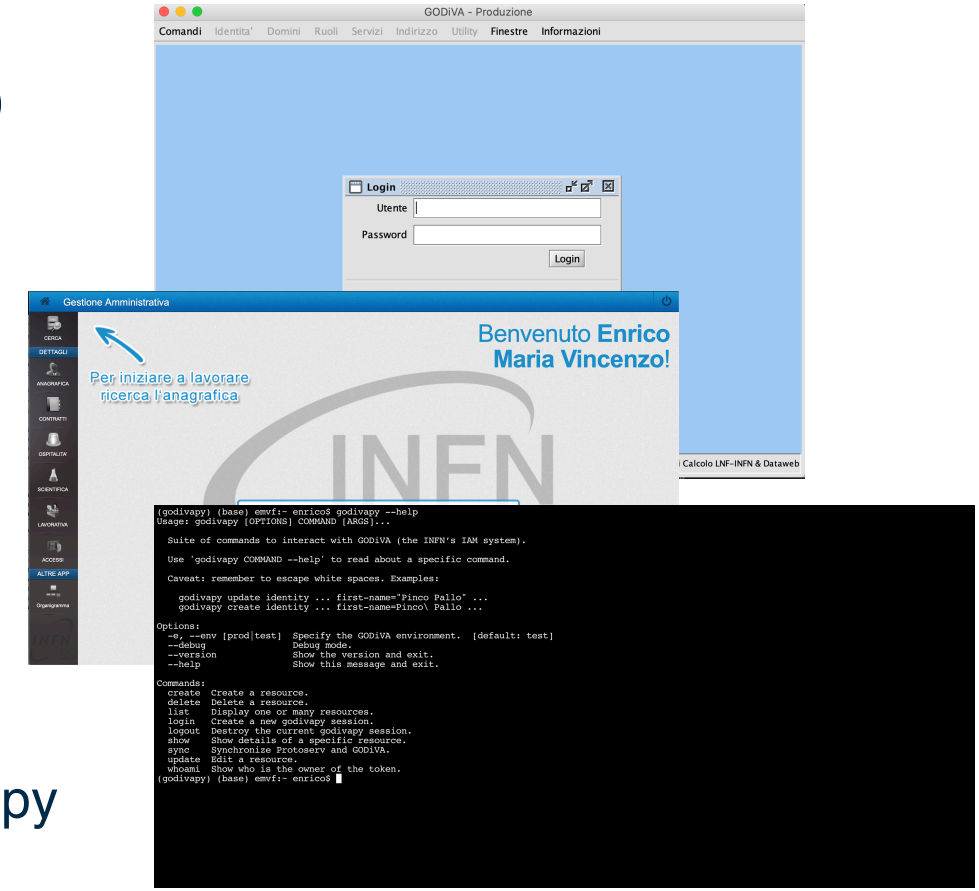


GODiVA-UI

- Interfaccia grafica Java (nerdissima)
  - https://godiva.infn.it/GODiVA/
- Interfaccia grafica web semplificata
  - GestioneAmministrativa

GODiVA-UI

- Interfaccia grafica Java (nerdissima)
  - https://godiva.infn.it/GODiVA/
- Interfaccia grafica web semplificata
  - GestioneAmministrativa
- Interfaccia command-line
  - godivapy
  - https://baltig.infn.it/infn-aai/godivapy



GODiVA-DB & GODiVA-Engine

- Multi-dominio
  - Alberi dei Ruoli
- Delega gestione sotto-albero dei Guppi
  - Struttura RBAC
  - Assegnazione automatica di Entitlement
- Ad ogni ruolo corrisponde un gruppo LDAP i cui membri sono le identità che sono nel ruolo

Gestione delle Autorizzazioni

- Ruoli Istituzionali
  - Dipendenti, Associati, Ospiti, Visitatori
  - Nomine, afferenze scientifiche, mansioni, organigramma, ecc. ecc.
  - Strutture ad albero gestite dagli uffici preposti

Gestione delle Autorizzazioni

- Ruoli Istituzionali
  - Dipendenti, Associati, Ospiti, Visitatori
  - Nomine, afferenze scientifiche, mansioni, organigramma, ecc. ecc.
  - Strutture ad albero gestite dagli uffici preposti
- Gruppi Logici (Gruppi)
  - Strutture ad albero con gestione delegabile
  - Raggruppamenti differenti da quelli «istituzionali»
  - https://wiki.infn.it/cn/ccr/aai/howto/authz/gruppi-logici

Gestione delle Autorizzazioni

- Ereditarietà
  - E' possibile associare una Identità Digitale ad un dominio (ovvero assegnare ad essa un ruolo) anche in modo indiretto, associando al dominio un gruppo di Identità Digitali opportunamente selezionate
  - Ad esempio è possibile associare tutte le Identità Digitali che hanno un ruolo attivo di «Dipendente in Amministrazione Centrale» al dominio

    Accessi –> INFN –> LNF –> EPS Tornello Stazione

Gestione delle Autorizzazioni

- isMemberOf
  - Qualunque Ruolo associato ad una Identità Digitale presente in GODiVA viene trasformato in un opportuno valore dell'attributo isMemberOf che può essere quindi utilizzato per gestire il processo di Autorizzazione.
  - Ad esempio il ruolo di responsabile nazionale del progetto AAI di Commissione Calcolo e Reti (Commissione Scientifica Nazionale 7) si traduce nel valore

`isMemberOf: s:csn7:ccr_aai::resp:nazionale`

Gestione Autorizzazioni

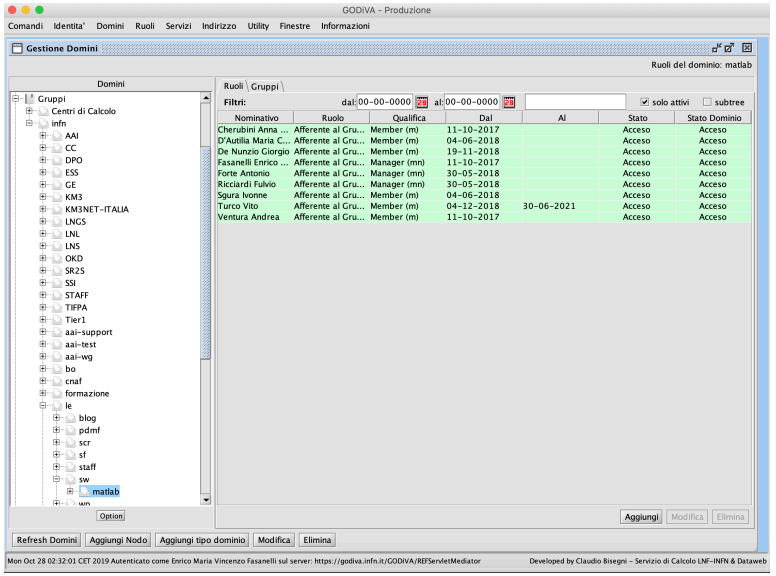
- Ereditarietà
  - Nel caso di ruoli ereditati, al relativo valore dell'attributo isMemberOf viene agganciato (@) anche l'origine del ruolo ereditato (inserito tra parentesi quadre []).

```
isMemberOf: accessi:infn:lnf:eps_tornello_stazione
::acc_dip:acc_dip_norm@[i:infn:lnf::a:dottorando]
```

Autorizzazione: caso d'uso

- Voglio permettere l'accesso ad un server che è abilitato a far girare matlab ad identità selezionate da me.
  - Creo l'albero (g:infn:le:sw:matlab) nel dominio dei Gruppi
  - Assegno al nodo finale le identità che voglio autorizzare
  - Definisco un filtro LDAP nellla configurazione di sssd del server matlab in modo che permetta l'accesso agli utenti i cui attributi soddisfano la condizione (&(uid=*)(isMemberOf=g:infn:le:sw:matlab::ag:m))

Ruolo: Afferente al Gruppo



- Gruppo
  - g:infn:le:sw:matlab
- Ruolo
  - Afferente al Gruppo
- Qualifiche
  - member
  - manager
- (&(uid=*)(isMemberOf=g:infn:le:sw:matlab::ag:m)) permette l'accesso solo a chi ha la qualifica «member»
- (&(uid=*)(isMemberOf=g:infn:le:sw:matlab::*)) permette l'accesso indipendentemente dalla qualifica

Considerazioni sul caso d'uso

- Caso facile
  - posso configurare il mio server con Autenticazione Kerberos ed Autorizzazione LDAP
  - sssd permette la definizione di filtri LDAP con *
- Che succede se non posso usare LDAP e non posso usare * come ad esempio nel caso di servizi web con autenticazione effettuata dall'IdP di INFN-AAI?

Entitlement (abilitazione) ovvero ABAC

- Nell'architettura di INFN-AAI sono utilizzati due attributi di tipo entitlement
  - schAcUserStatus (definito nello SCHema for ACademia SCHAC)
  - eduPersonEntitlement (definito nello schema eduPerson di Internet2)
- Per entrambi gli attributi è previsto un valore del tipo URN, con delega dello spazio dei nomi.

```
schacUserStatus: urn:schac:userStatus:it:infn.it:godiva-role:dipendente:attivo+ttl=nolimit
                                                ^
                                                |__  Delega implicita all'INFN
```

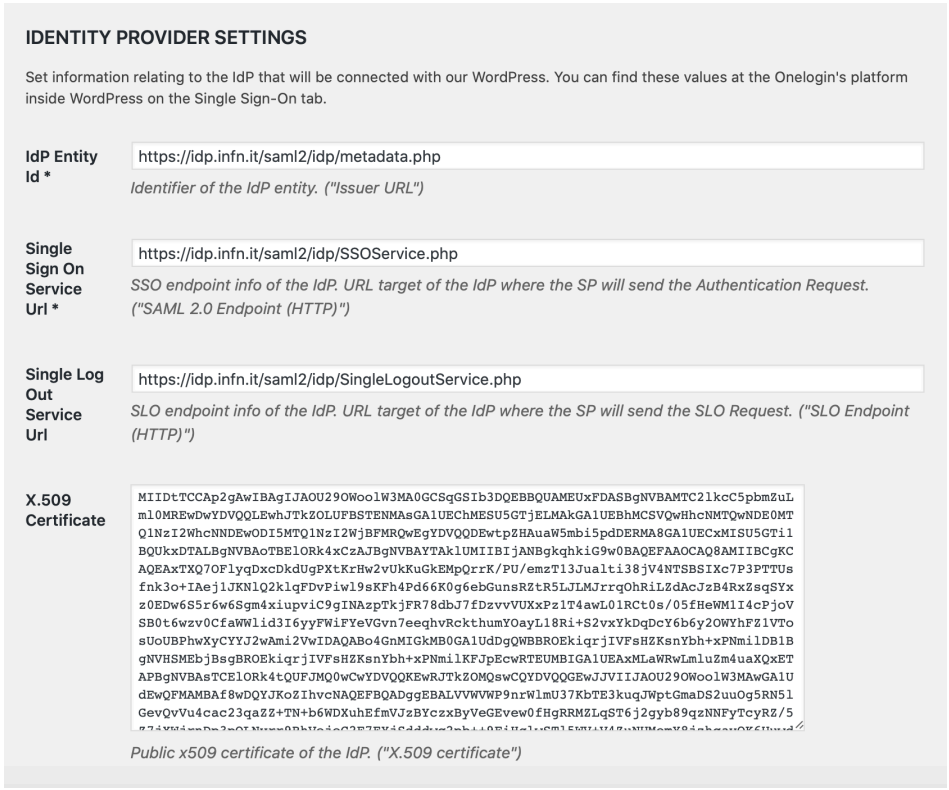
urn:mace:infn.it

- Il valore di URN da assegnare ad eduPersonEntitlement, come da specifiche di Internet2, deve essere un URN che dello spazio dei nomi definito da MACE (Middleware Architecture Commitee for Education)
- INFN-AAI ha la delega alla gestione dello spazio dei nomi definito a partire da urn:mace:infn.it
- Registro dei nomi allocati https://wiki.infn.it/cn/ccr/aai/en/tech/namespace segue la struttura ad albero dei gruppi logici.

```
eduPersonEntitlement: urn:mace:infn.it:g:infn:le:wp:admin
```

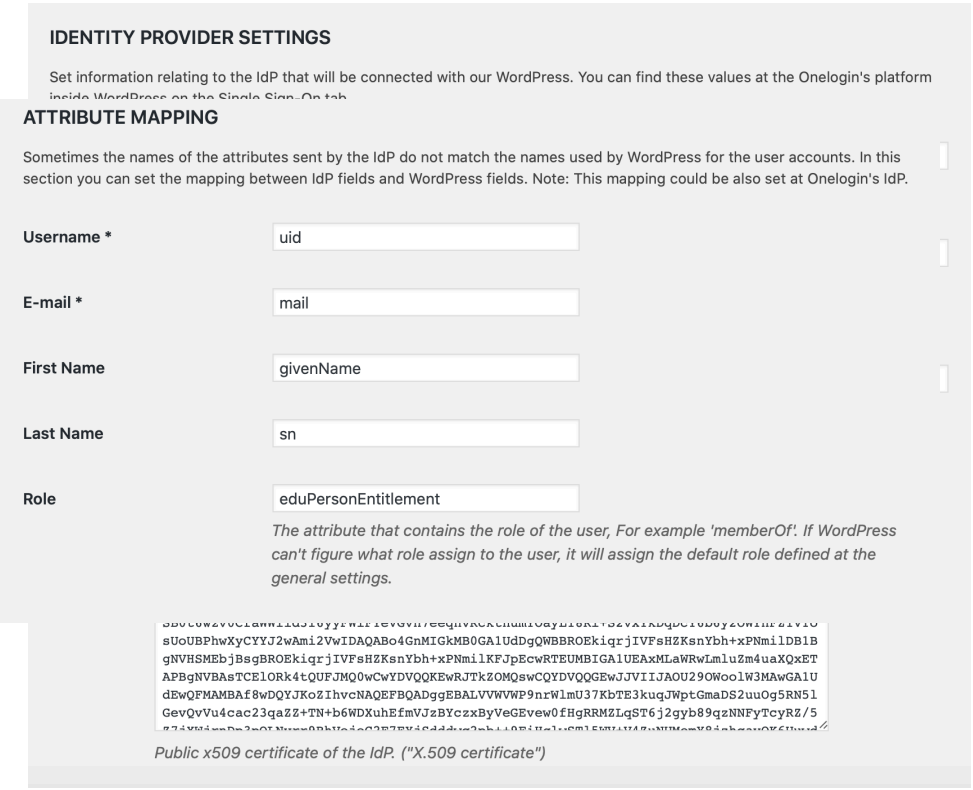
Caso d’uso: WordPress

- Configuro WordPress come Service Provider di INFN-AAI



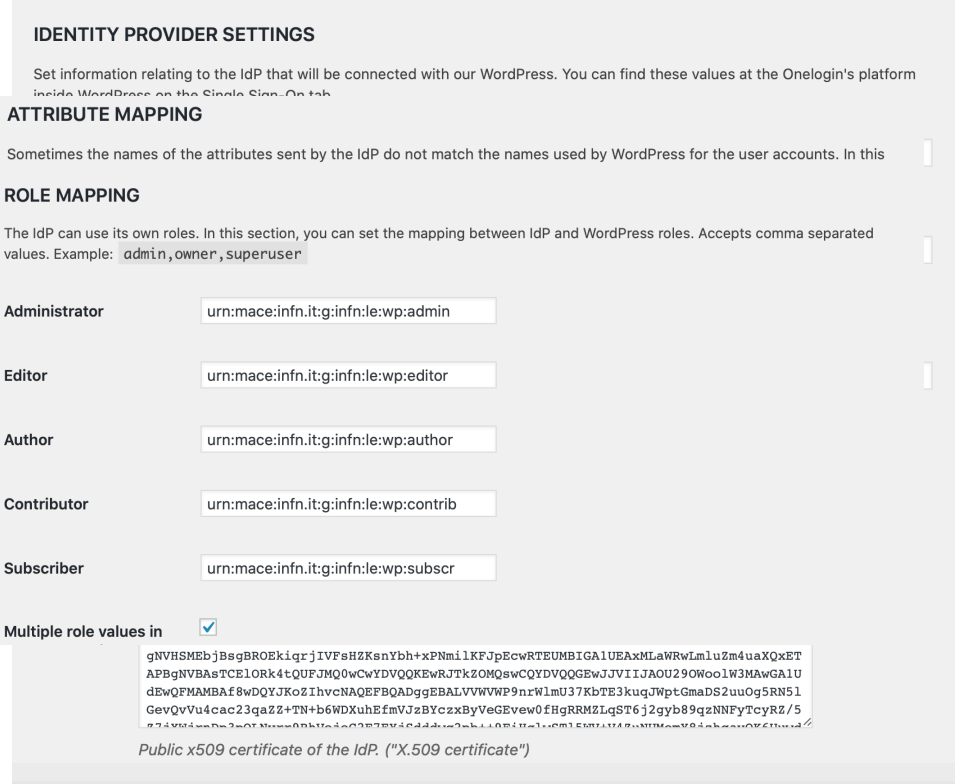
Caso d’uso: WordPress

- Configuro WordPress come Service Provider di INFN-AAI
- Corrispondenza tra attributi



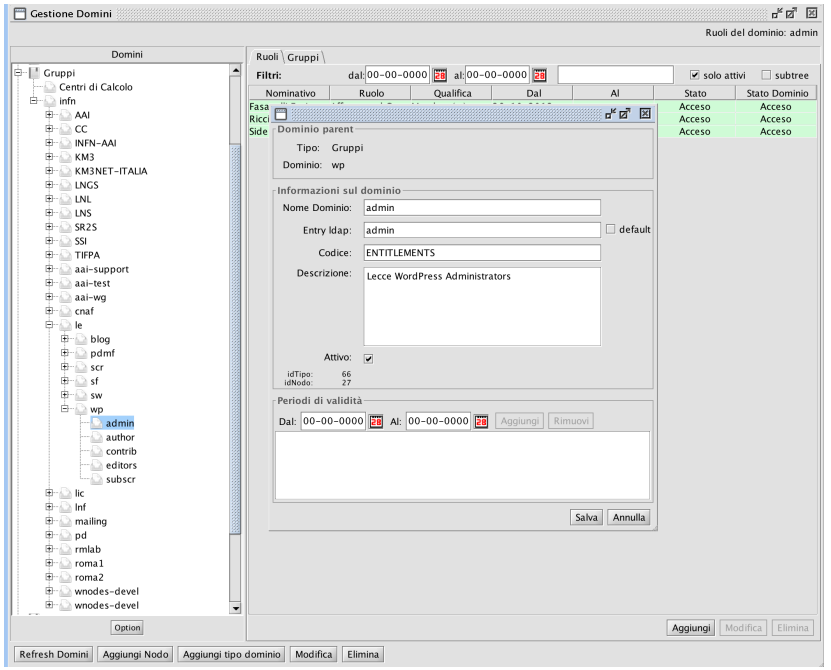
Caso d’uso: WordPress

- Configuro WordPress come Service Provider di INFN-AAI
- Corrispondenza tra attributi
- Corrispondenza tra ruoli in WordPress e valori degli attributi



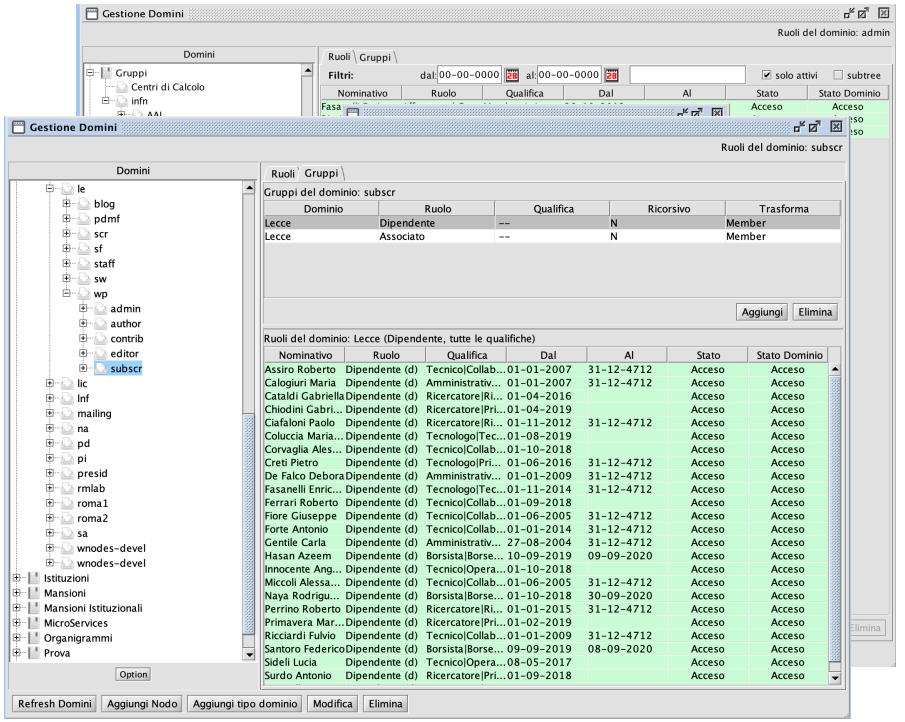
Caso d'uso WordPress: GODiVA

- Definisco la struttura ad albero relativa a WrdPress a Lecce



Caso d'uso WordPress: GODiVA

- Definisco la struttura ad albero relativa a WrdPress a Lecce
- Assegno al ruolo «subscr» tutti i dipendenti ed associati della sezione di Lecce



RBAC: provisioning e de-provisioning

- Nel modello RBAC quando una identità non è in un ruolo, ad essa non verranno associati gli entitlements relativi a quel ruolo
  - Se ho autorizzato tutti gli associati della sezione di Lecce ad utilizzare un servizio web, alla scadenza dell'associazione l'autorizzazione sarà automaticamente revocata.
- Ogni ruolo è definito con un periodo di validità (inizio e fine) ma possono esserci proroghe o interruzioni anticipate
- E' di cruciale importanza che gli uffici che hanno la responsabilità di aggiornare lo stato dei ruoli istituzionali relativi alle Identità Digitali lo facciano tempestivamente.

The End

Grazie

Domande?