

# Meccanismi di Autenticazione e di Autorizzazione



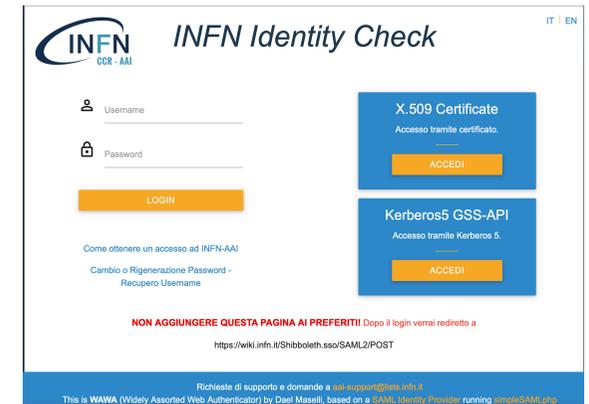
Tutorial days di CCR  
I Servizi Nazionali della CCR

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

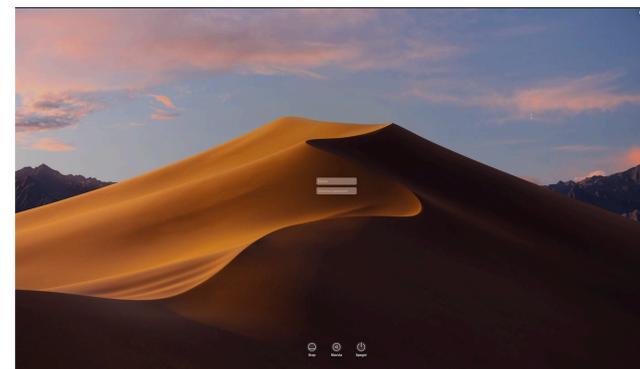
# Come autentico per un utente

- **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



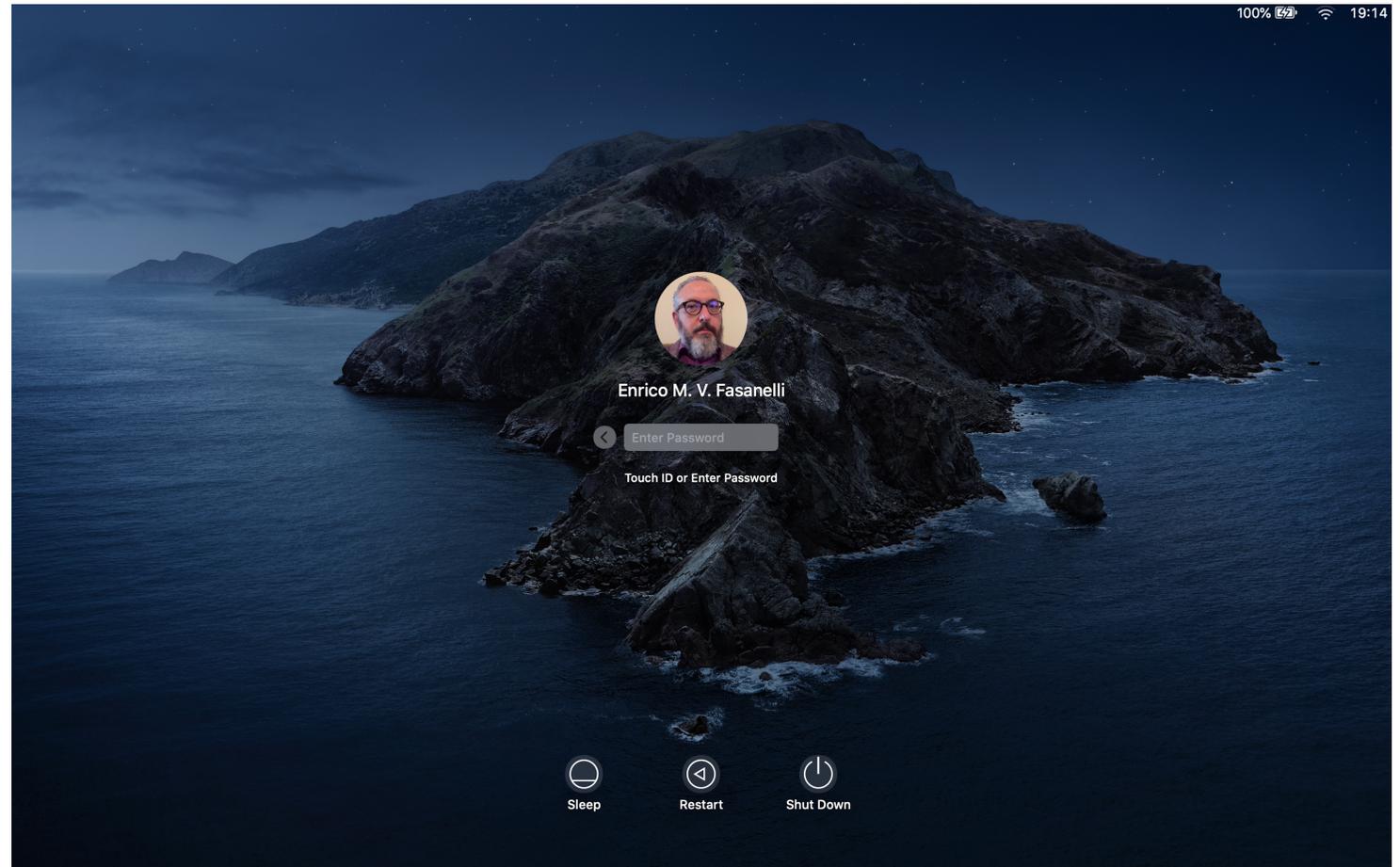
# Qualcosa che ho

- 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.



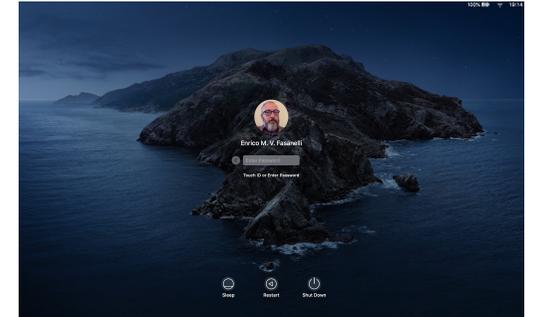
# Qualcosa che sono

- Impronte digitali
  - login PC



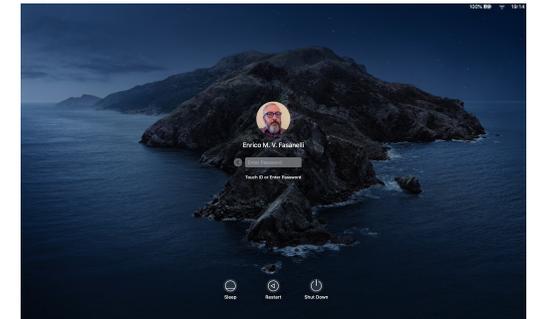
# Qualcosa che sono

- 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 ribattono completamente l'approccio alla scelta di una password

```

1 /var/log/secure:Oct 27 04:20:40 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
2 /var/log/secure:Oct 27 04:20:44 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
3 /var/log/secure:Oct 27 04:20:47 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
4 /var/log/secure:Oct 27 04:20:51 login sshd[25859]: Failed password for root from 222.186.169.194 port 53276 ssh2
5 /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
6 /var/log/secure:Oct 27 04:21:22 login sshd[26219]: Failed password for root from 122.4.241.6 port 10332 ssh2
7 /var/log/secure:Oct 27 04:21:34 login sshd[26230]: Failed password for root from 203.129.253.78 port 40010 ssh2
8 /var/log/secure:Oct 27 04:21:48 login sshd[26273]: Failed password for root from 81.12.159.146 port 47070 ssh2
9 /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
10 /var/log/secure:Oct 27 04:22:50 login sshd[26364]: Failed password for root from 117.50.95.121 port 57686 ssh2
11 /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
12 /var/log/secure:Oct 27 04:23:10 login sshd[26405]: Failed password for invalid user administrator from 162.243.50.8 port 45148 ssh2
13 /var/log/secure:Oct 27 04:23:14 login sshd[26437]: Failed password for root from 103.62.239.77 port 38856 ssh2
14 /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
15 /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
16 /var/log/secure:Oct 27 04:24:45 login sshd[26563]: Failed password for adm from 192.241.185.120 port 45074 ssh2
17 /var/log/secure:Oct 27 04:25:00 login sshd[26589]: Failed password for root from 104.40.0.120 port 7552 ssh2
18 /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
19 /var/log/secure:Oct 27 04:25:37 login sshd[26636]: Failed password for root from 122.4.241.6 port 36456 ssh2
20 /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
21 /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
22 /var/log/secure:Oct 27 04:27:30 login sshd[26803]: Failed password for root from 117.50.95.121 port 37456 ssh2
23 /var/log/secure:Oct 27 04:28:35 login sshd[26887]: Failed password for invalid user Password00 from 217.125.110.139 port 56484 ssh2
24 /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
25 /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
26 /var/log/secure:Oct 27 04:29:57 login sshd[27023]: Failed password for root from 122.4.241.6 port 56162 ssh2
27 /var/log/secure:Oct 27 04:30:02 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
28 /var/log/secure:Oct 27 04:30:06 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
29 /var/log/secure:Oct 27 04:30:10 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
30 /var/log/secure:Oct 27 04:30:13 login sshd[27026]: Failed password for root from 222.186.180.8 port 47406 ssh2
31 /var/log/secure:Oct 27 04:30:37 login sshd[27110]: Failed password for root from 139.59.5.65 port 40088 ssh2
32 /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
33 /var/log/secure:Oct 27 04:30:51 login sshd[27141]: Failed password for root from 192.241.185.120 port 35722 ssh2
34 /var/log/secure:Oct 27 04:31:08 login sshd[27169]: Failed password for root from 197.248.16.118 port 37218 ssh2
35 /var/log/secure:Oct 27 04:31:11 login sshd[27183]: Failed password for root from 82.238.107.124 port 55232 ssh2
36 /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
37 /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
38 /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
39 /var/log/secure:Oct 27 04:33:24 login sshd[27398]: Failed password for invalid user frederica123 from 106.52.35.207 port 58304 ssh2
40 /var/log/secure:Oct 27 04:33:37 login sshd[27415]: Failed password for root from 119.204.168.61 port 47614 ssh2
41 /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

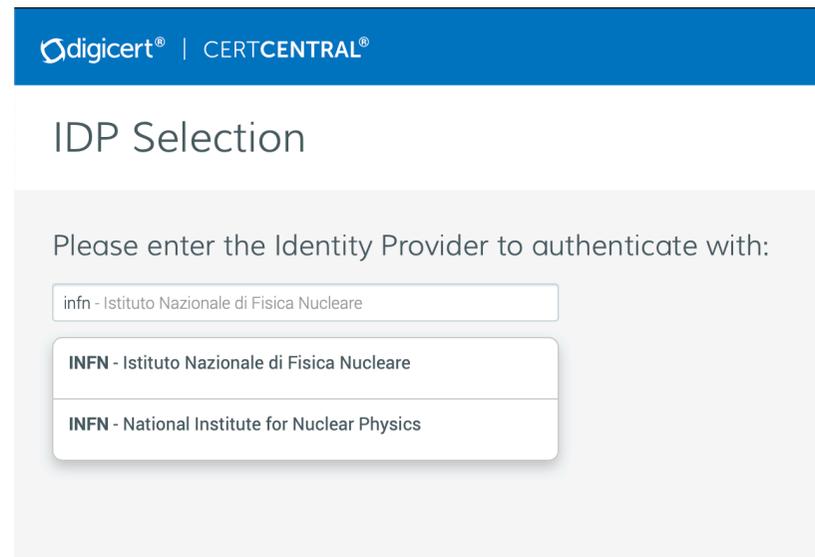
- La coppia di chiavi pubblica-privata è generata all'interno di un dispositivo (la SmartCard) e non è possibile estrarre la chiave privata dal dispositivo
- L'autorità di certificazione (PosteCert, InfoCamere, Aruba,...) legalmente riconosciuta in Italia, firma la chiave pubblica all'interno del dispositivo, **dopo aver effettuato il riconoscimento \*de visu\* 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



The screenshot shows the 'IDP Selection' page from digicert CERTCENTRAL. It features a blue header with the digicert and CERTCENTRAL logos. Below the header, the text 'IDP Selection' is displayed. A prompt asks the user to 'Please enter the Identity Provider to authenticate with:'. There are three input fields: the first contains 'inf - Istituto Nazionale di Fisica Nucleare', the second contains 'INFN - Istituto Nazionale di Fisica Nucleare', and the third contains 'INFN - National Institute for Nuclear Physics'.

# Premium vs GRID Premium

- Premium

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

- GRID Premium

- Validità 1 anno
- Premium + GRID

Request a Certificate

Choose a product

Product: Premium

Validity Period:
 

- ✓ 1 Year
- 2 Years
- 3 Years

CSR: (optional)

Common Name: Enrico Maria Vincenzo Fasanelli

Email: Enrico.M.V.Fasanelli@le.infn.it

Organization: Istituto Nazionale di Fisica Nucleare

Request Certificate

My Certificates

Request a Certificate

Choose a product

Product: Grid Premium

Validity Period:
 

- ✓ 1 Year

CSR: (optional)

Common Name: Enrico Maria Vincenzo Fasanelli enrco@infn.it

Email: Enrico.M.V.Fasanelli@le.infn.it

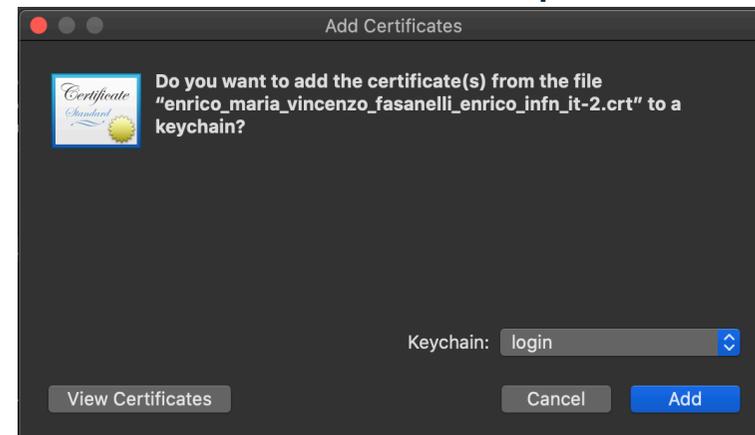
Organization: Istituto Nazionale di Fisica Nucleare

Request Certificate

My Certificates

# 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



Enrico Maria Vincenzo Fasanelli

**Enrico Maria Vincenzo Fasanelli**  
Issued by: TERENA Personal CA 3  
Expires: Thursday, 27 October 2022 at 14:00:00 Central European Summer Time  
This certificate is valid

Trust

Details

**Subject Name**

Country or Region IT  
Locality Frascati  
Organisation Istituto Nazionale di Fisica Nucleare  
Common Name Enrico Maria Vincenzo Fasanelli

**Issuer Name**

Country or Region NL  
County Noord-Holland  
Locality Amsterdam  
Organisation TERENA  
Common Name TERENA Personal CA 3

Serial Number 0B 48 1C EF 82 F1 57 DE BF 05 CD 9F 92 6F 0B AC  
Version 3  
Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.1 )  
Parameters None

Not Valid Before Sunday, 27 October 2019 at 02:00:00 Central European Summer Time  
Not Valid After Thursday, 27 October 2022 at 14:00:00 Central European Summer Time

**Public Key Info**

Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )  
Parameters None  
Public Key 256 bytes: D7 0F A5 32 26 75 3B 49 ...  
Exponent 65537  
Key Size 2,048 bits  
Key Usage Encrypt, Verify, Wrap, Derive  
Signature 256 bytes: A9 A0 24 14 E3 0F BD 8B ...

Extension Key Usage ( 2.5.29.15 )  
Critical YES  
Usage Digital Signature, Key Encipherment

Extension Basic Constraints ( 2.5.29.10 )  
Critical YES  
Certificate Authority NO

Extension Extended Key Usage ( 2.5.29.37 )  
Critical NO  
Purpose #1 Client Authentication ( 1.3.6.1.5.5.7.3.2 )  
Purpose #2 Email Protection ( 1.3.6.1.5.5.7.3.4 )

Extension Subject Key Identifier ( 2.5.29.14 )  
Critical NO  
Key ID 20 83 87 56 00 00 51 50 00 00 00 04 0F E7 DD E9 90 DD 98

Extension Authority Information Access ( 2.5.29.35 )  
Critical NO  
Key ID F0 21 E9 49 77 73 9F 85 AE 18 3B E8 52 70 14 06 EC 12 EE CA

Extension Subject Alternative Name ( 2.5.29.17 )  
Critical NO  
RFC 822 Name Enrico.M.V.Fasanelli@le.infn.it

Extension Certificate Policies ( 2.5.29.32 )  
Critical NO  
Policy ID #1 ( 2.16.840.1.114412.4.1.2 )  
Qualifier ID #1 Certification Practice Statement ( 1.3.6.1.5.5.7.2.1 )  
CPS URI <https://www.digicert.com/CPS>

Extension CRL Distribution Points ( 2.5.29.31 )  
Critical NO  
URI <http://crl3.digicert.com/TERENAPersonalCA3.crl>  
URI <http://crl4.digicert.com/TERENAPersonalCA3.crl>

Extension Certificate Authority Information Access ( 1.3.6.1.5.5.7.1.1 )  
Critical NO  
Method #1 Online Certificate Status Protocol ( 1.3.6.1.5.5.7.48.1 )  
URI <http://ocsp.digicert.com>  
Method #2 CA Issuers ( 1.3.6.1.5.5.7.48.2 )  
URI <http://cacerts.digicert.com/TERENAPersonalCA3.crl>

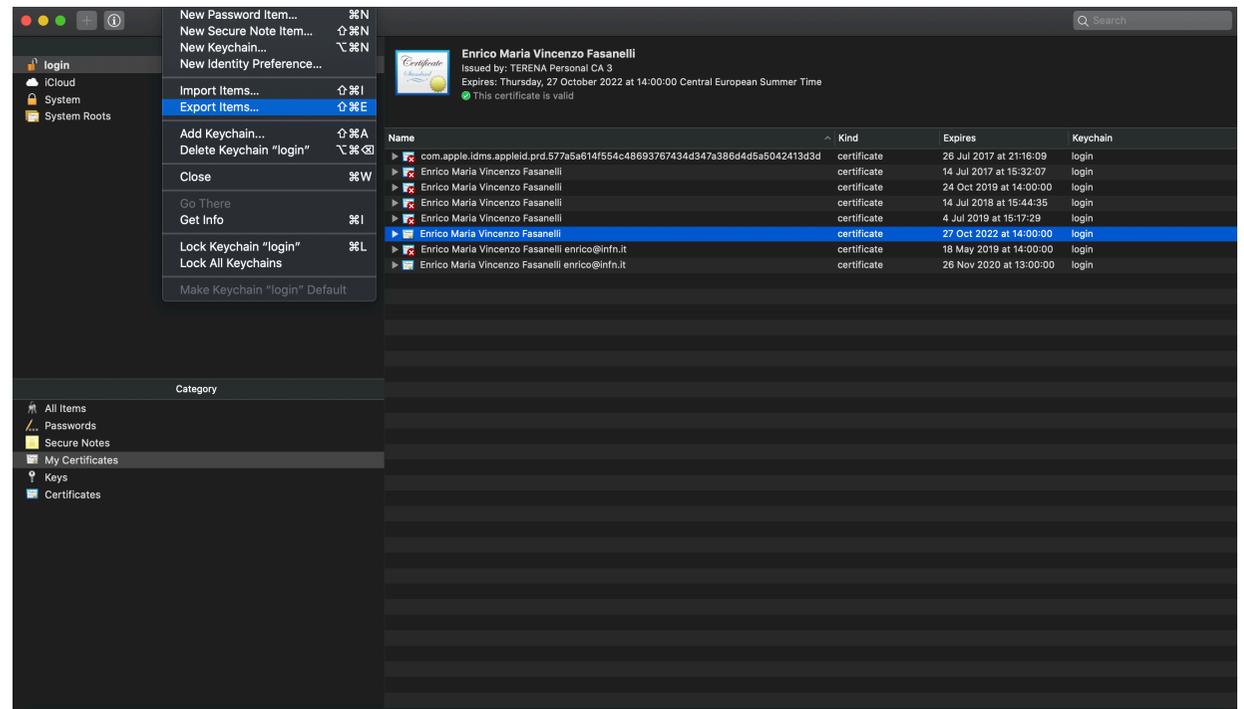
Fingerprints

SHA-256 F1 65 7F 9C 6E 05 11 C5 52 A8 66 97 96 A3 3C 85 8E F6 02 51 97 D8 E2 2E 5B EF A5 CA 58 81 30 F2  
SHA-1 D1 E0 10 8C 50 BD 33 0C 79 0E D7 4E A5 54 50 87 AA EB 73 83



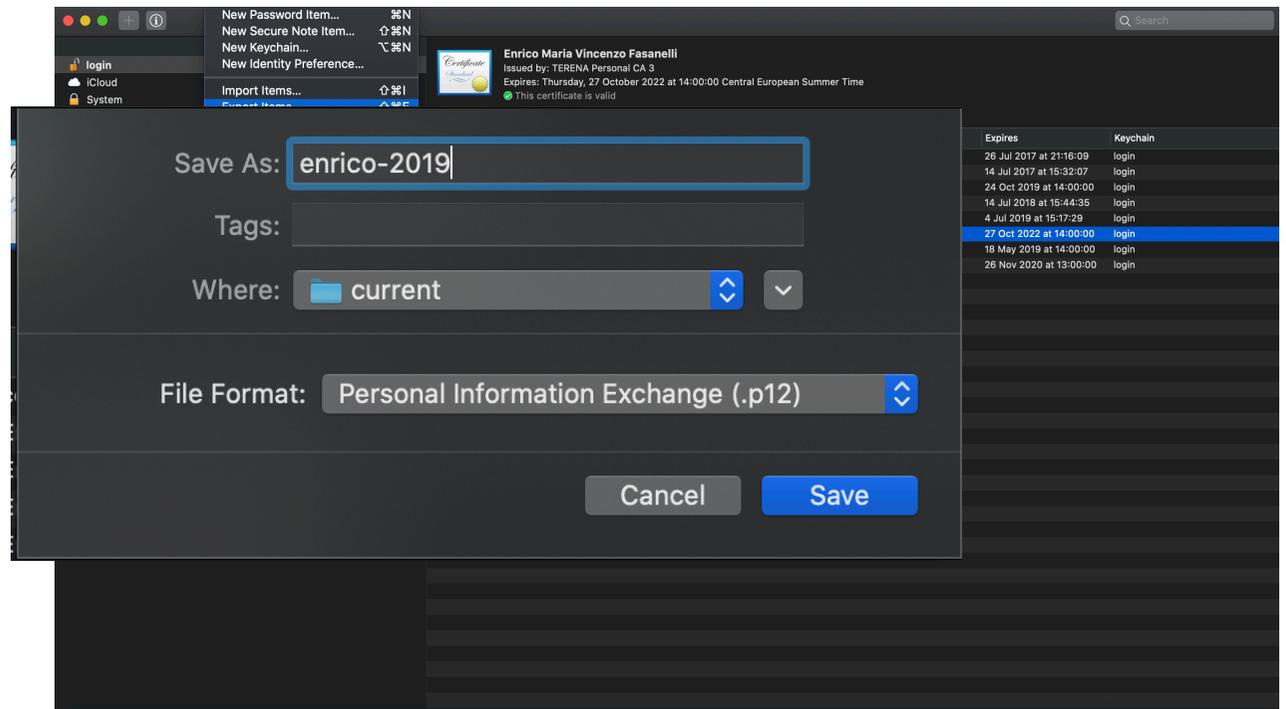
# Installare il certificato in altro browser

- Esportare il certificato



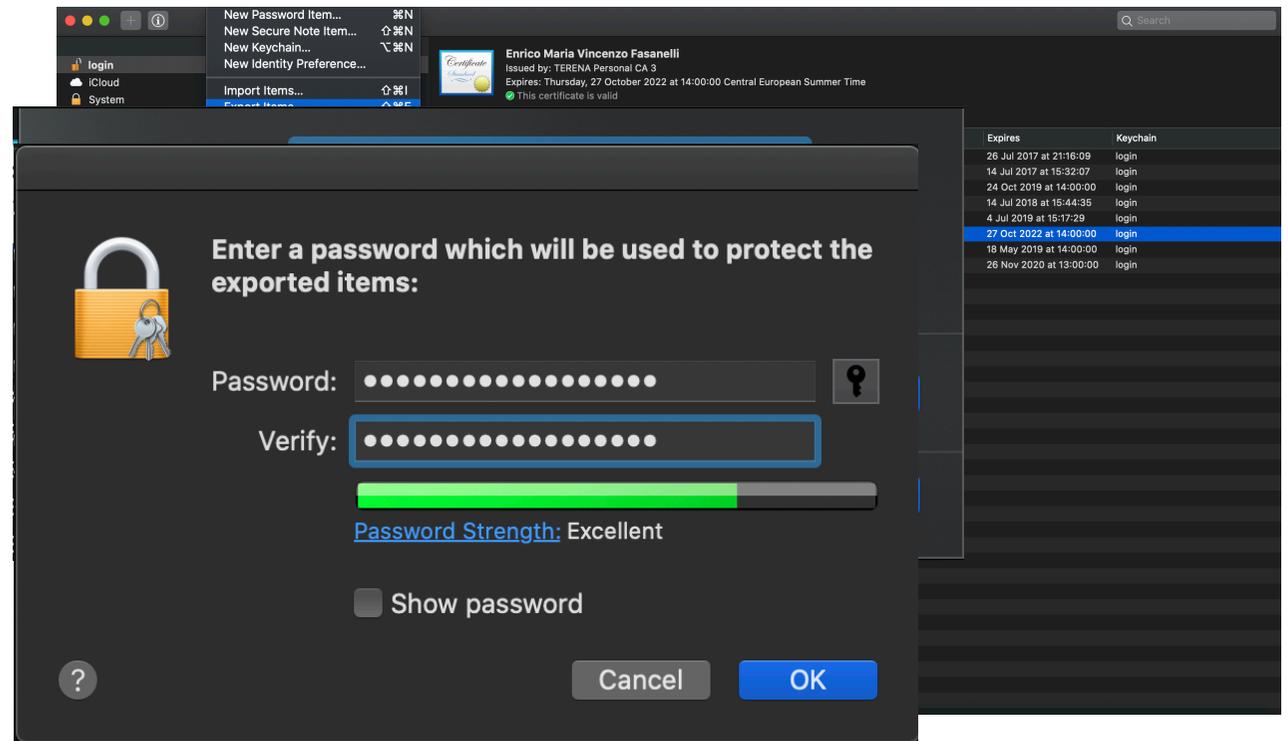
# Installare il certificato in altro browser

- Esportare il certificato
- Scegliere il nome del file



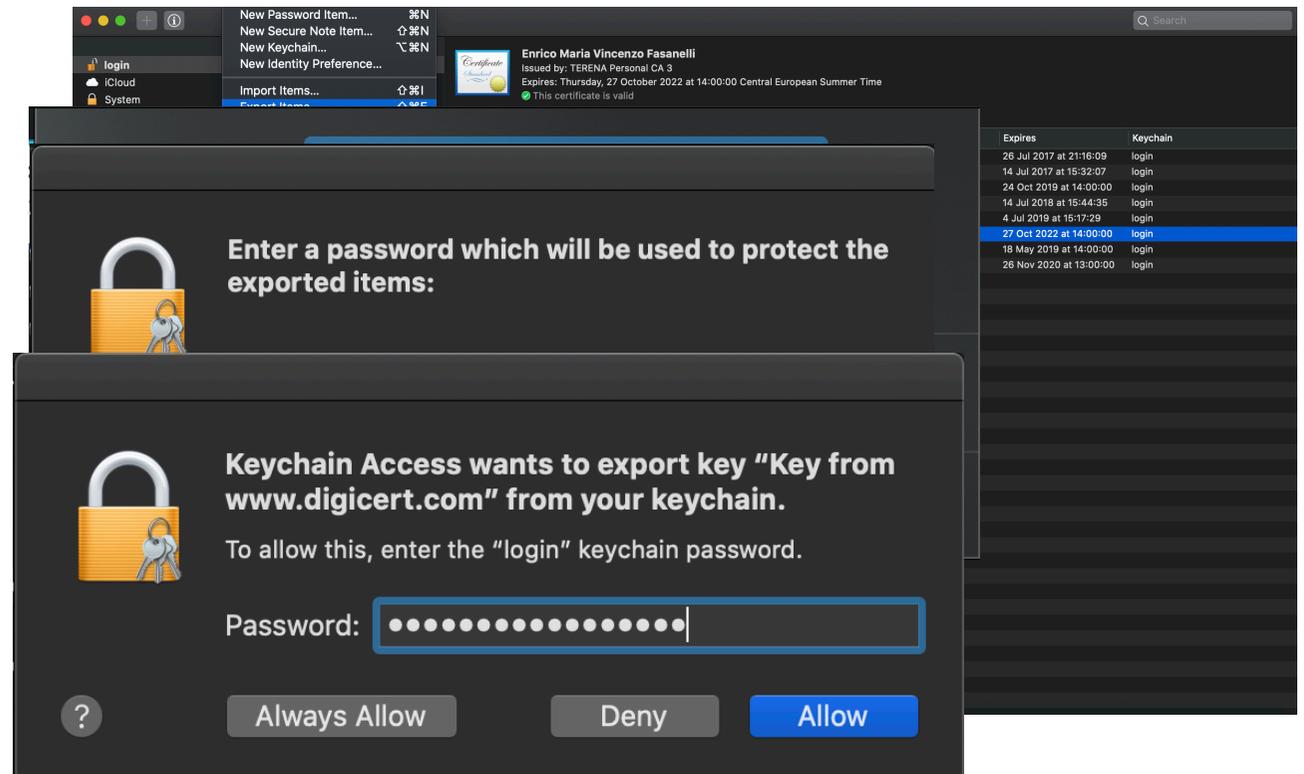
# Installare il certificato in altro browser

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



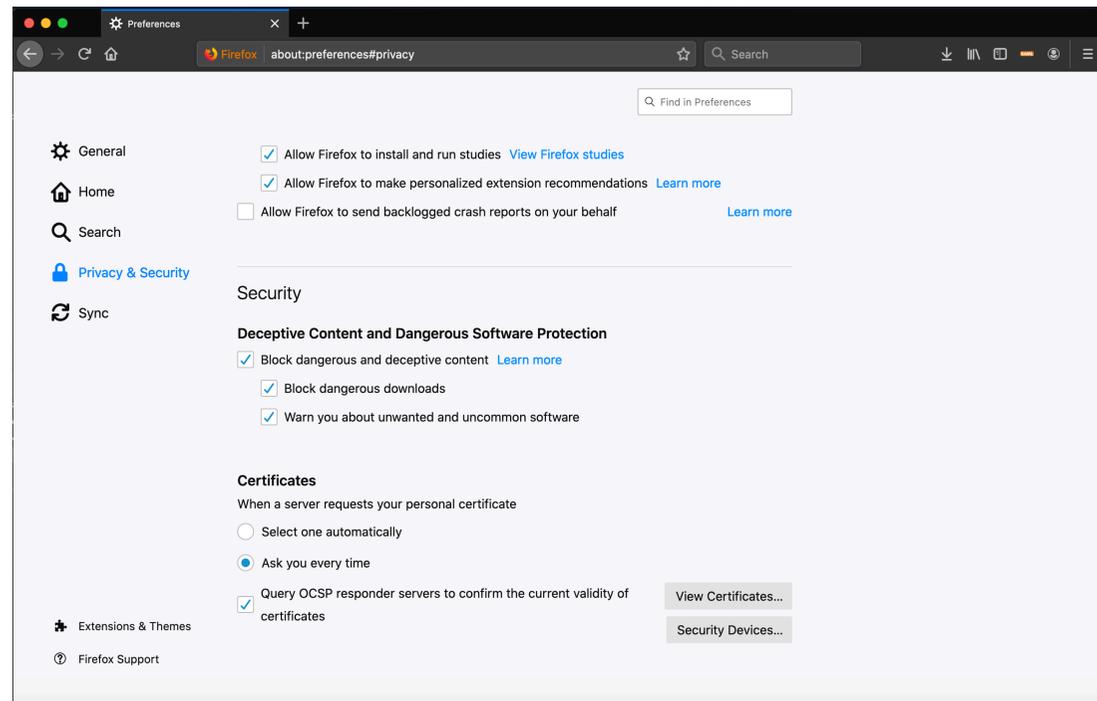
# Installare il certificato in altro browser

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



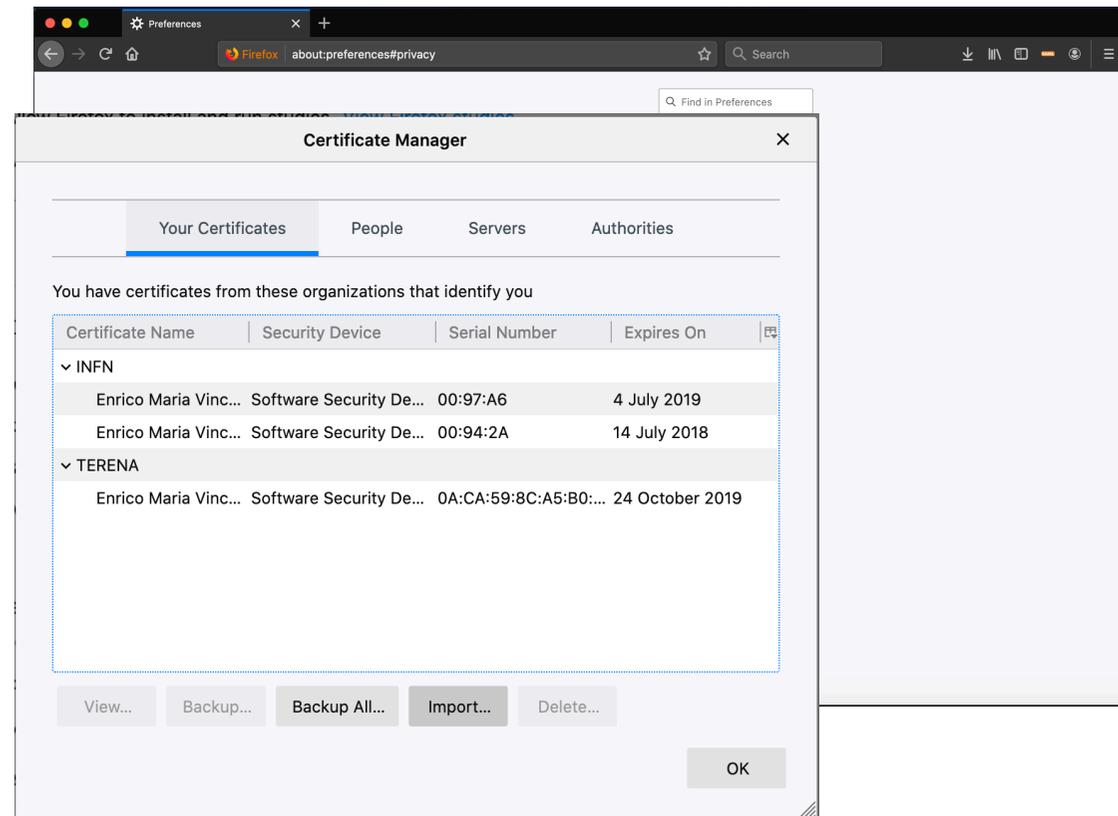
# Importare il certificato in Firefox

- Nelle impostazioni di Firefox
  - `about:preferences`



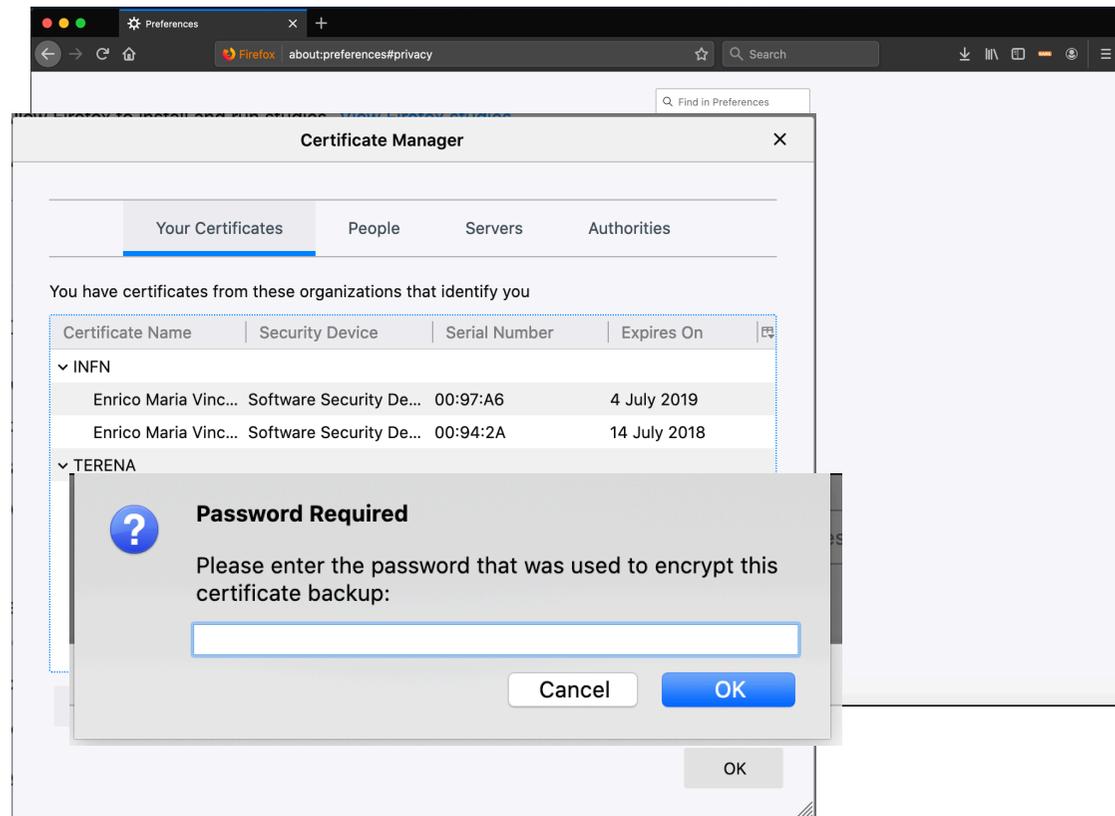
# Importare il certificato in Firefox

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



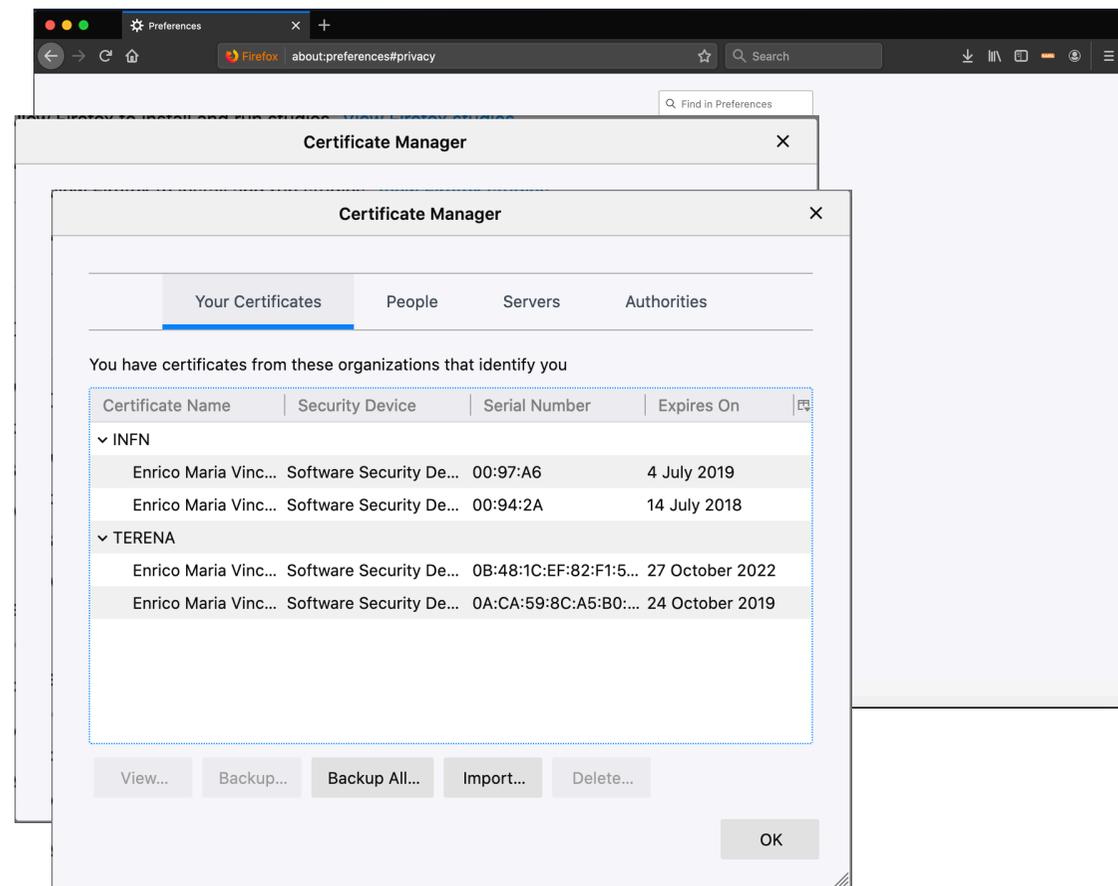
# Importare il certificato in Firefox

- 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

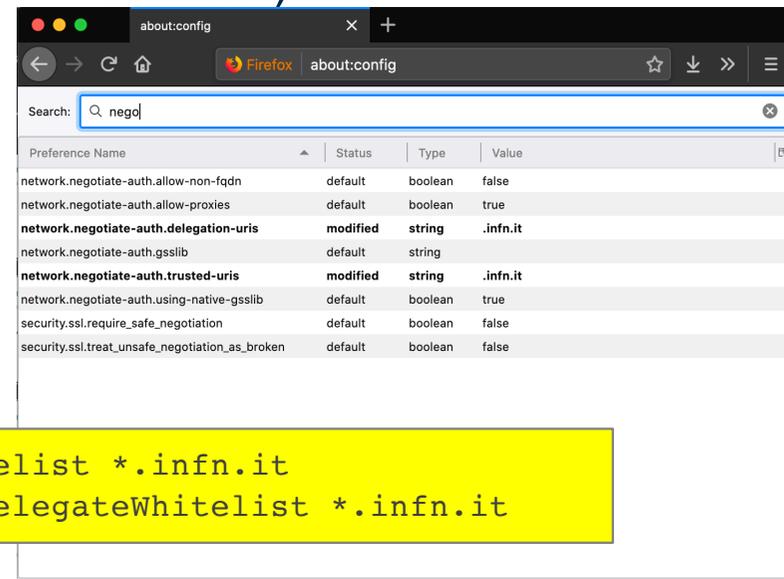
- Assomiglia a Username/Password ma è completamente differente
- A differenza dell'autenticazione Username/Password, con Kerberos la Password non viaggia in rete, ma serve ad aprire (decifrare) un «pacchetto» che viene chiuso (cifrato) con la password dell'utente dal server di autenticazione centrale (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)



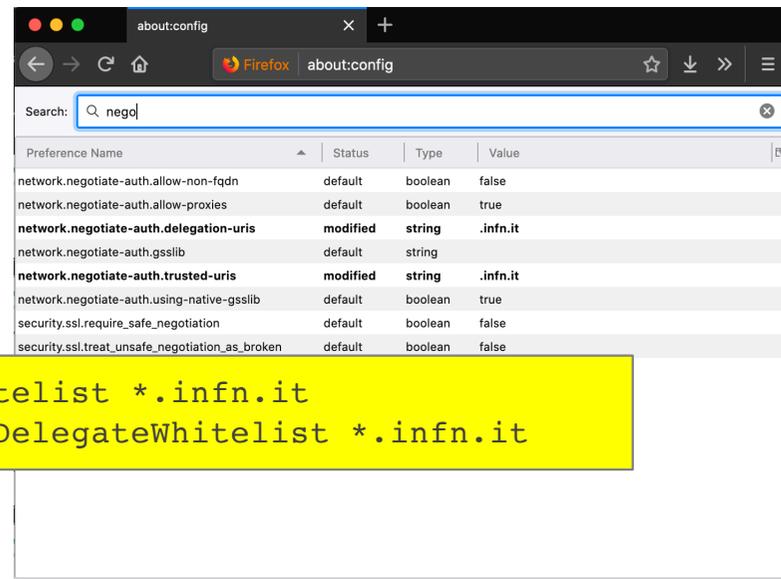
| Preference Name                                 | Status          | Type          | Value           |
|---|-----------------|---------------|-----------------|
| network.negotiate-auth.allow-non-fqdn           | default         | boolean       | false           |
| network.negotiate-auth.allow-proxies            | default         | boolean       | true            |
| <b>network.negotiate-auth.delegation-uris</b>   | <b>modified</b> | <b>string</b> | <b>.infn.it</b> |
| network.negotiate-auth.gsslib                   | default         | string        |                 |
| <b>network.negotiate-auth.trusted-uris</b>      | <b>modified</b> | <b>string</b> | <b>.infn.it</b> |
| network.negotiate-auth.using-native-gsslib      | default         | boolean       | true            |
| security.ssl.require_safe_negotiation           | default         | boolean       | false           |
| security.ssl.treat_unsafe_negotiation_as_broken | default         | boolean       | false           |

```
$ 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

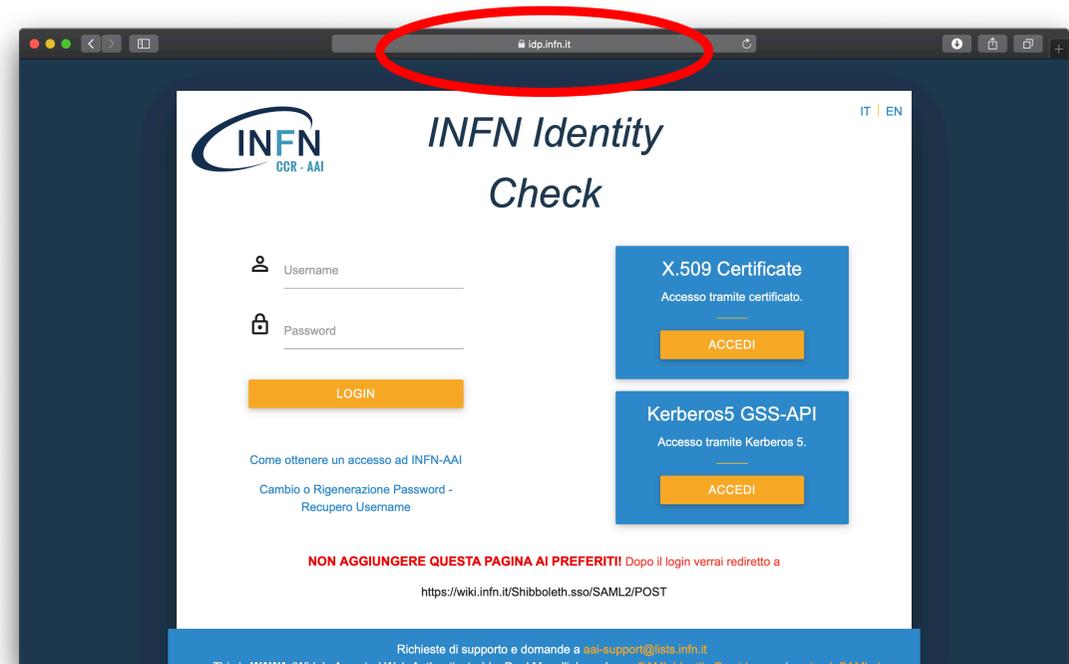
- Si definisce in **informatica** il processo tramite il quale un **sistema informatico**, un **computer**, un **software** o un **utente** verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole **comunicare** attraverso una **connessione**
- È il sistema 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)

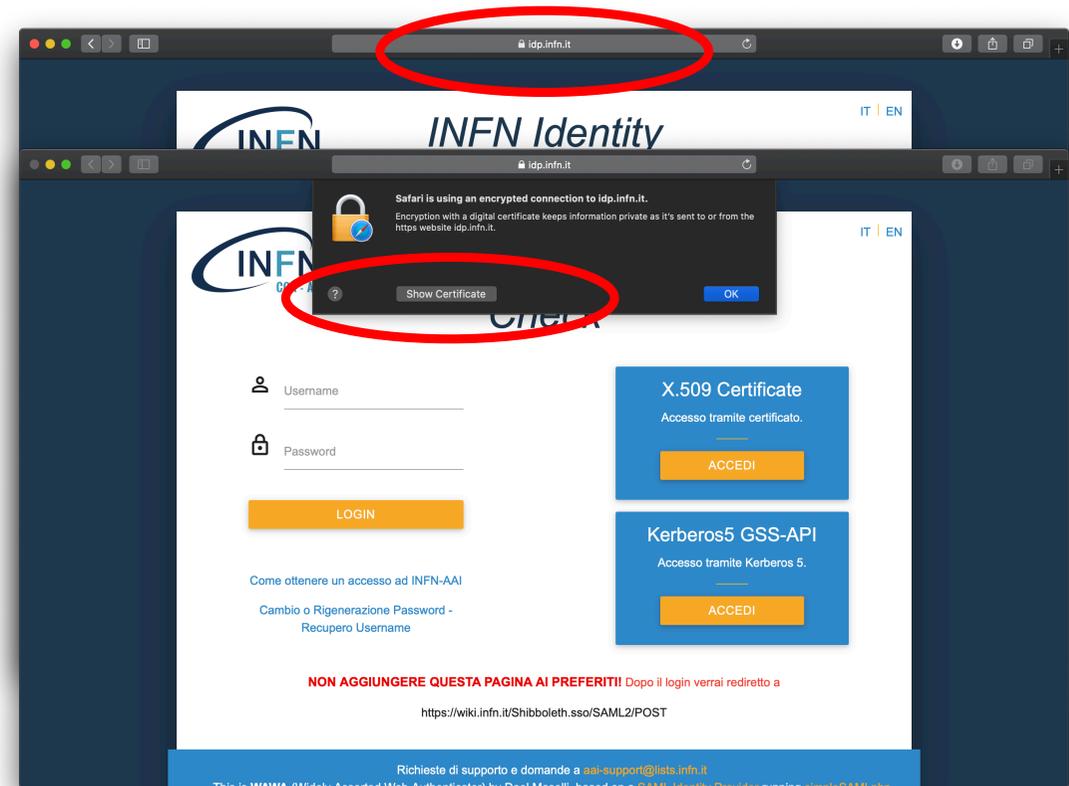
# SSL/TLS https://

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



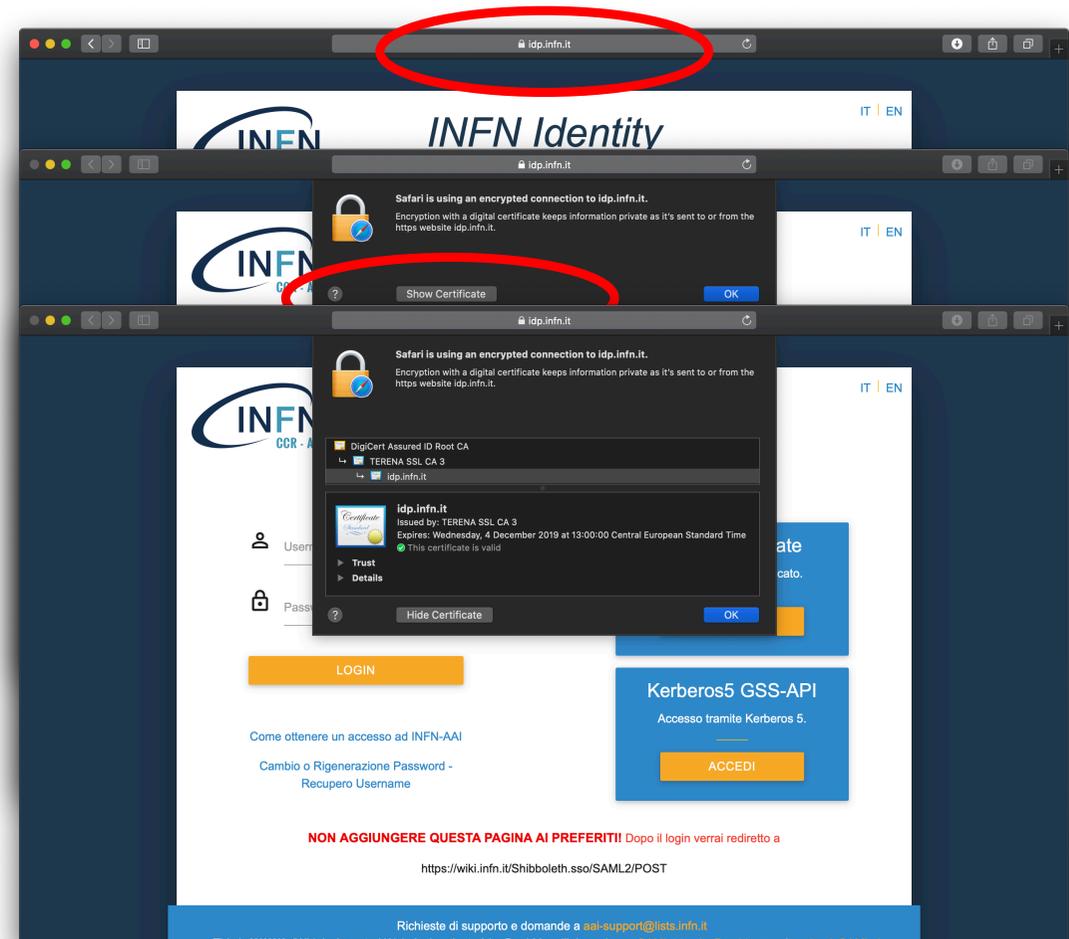
# SSL/TLS https://

- 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







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

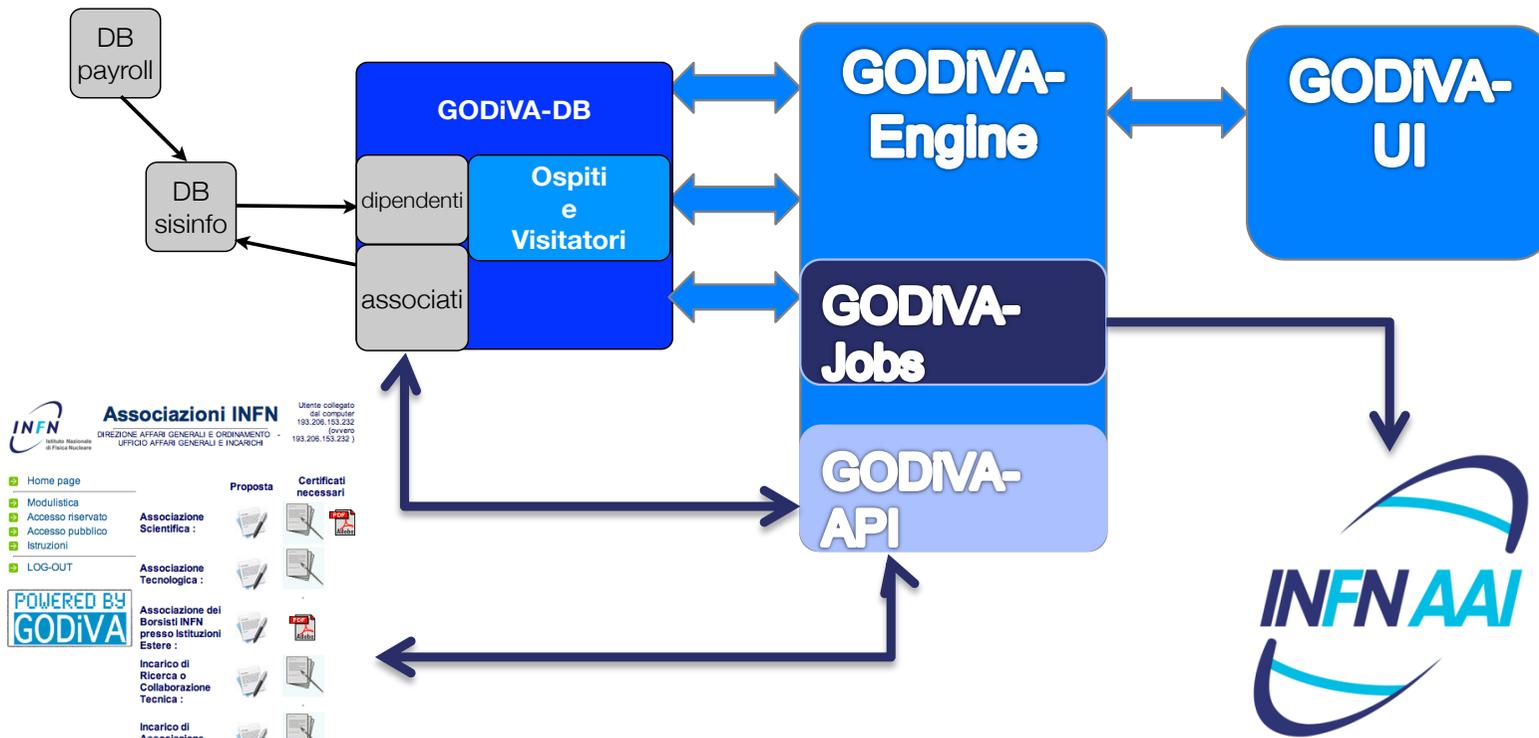
# GODiVA

- 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 al 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

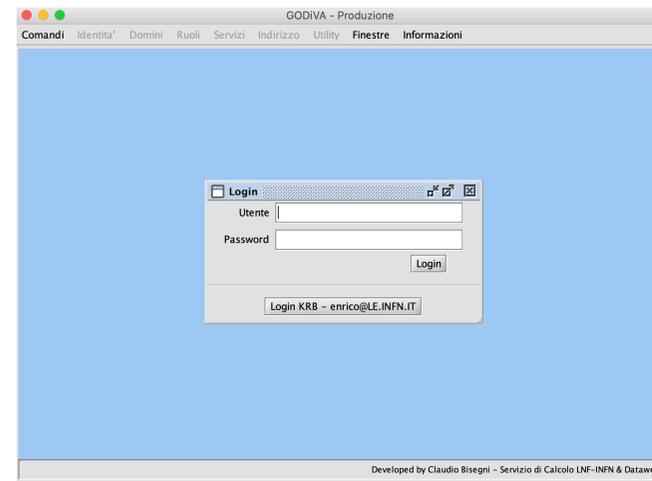


OU=People, DC=INFN, DC=IT



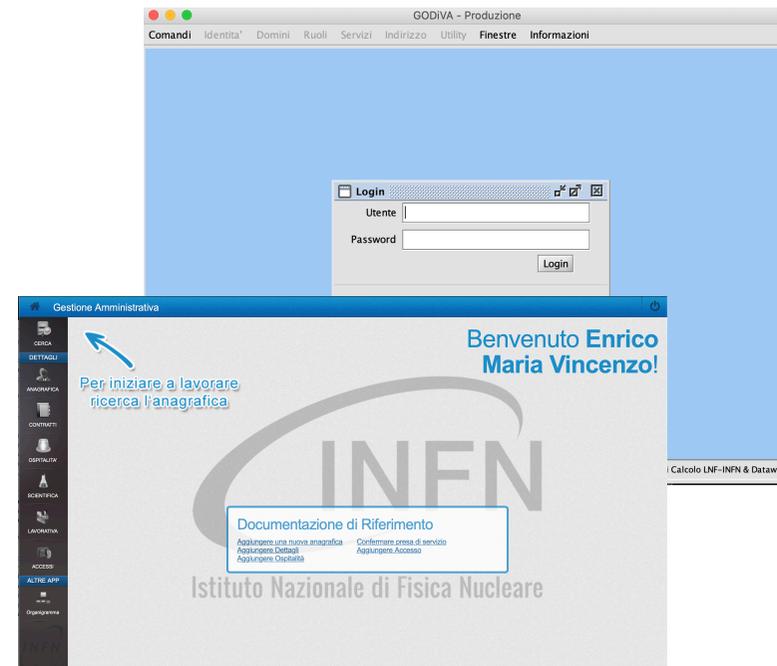
# GODiVA-UI

- 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
  - Gestione Amministrativa
- Interfaccia command-line
  - godivapy
  - <https://baltig.infn.it/infn-aai/godivapy>

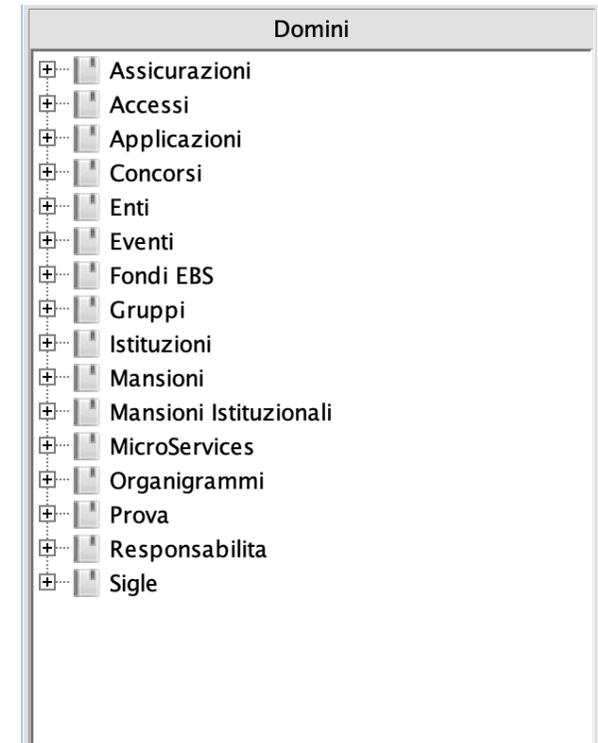


# GODiVA-DB & GODiVA-Engine

- 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

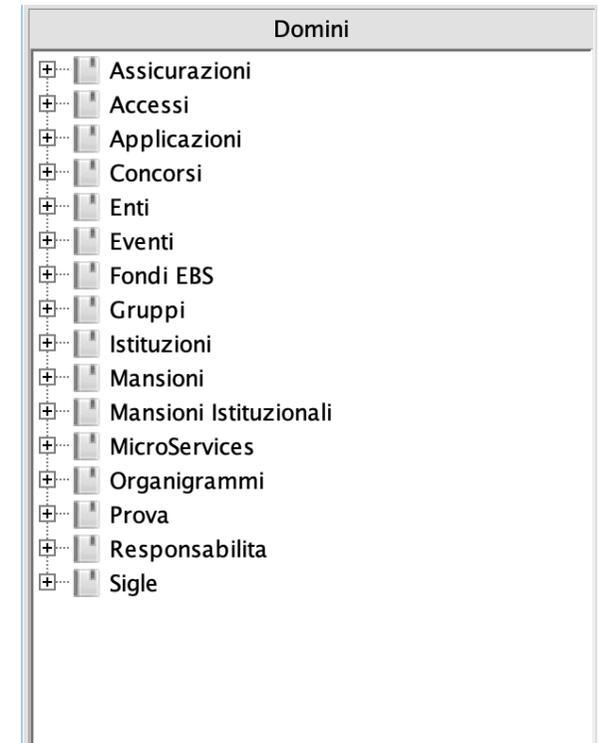
# Gestione delle Autorizzazioni

- 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-logicci>



# 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 []).

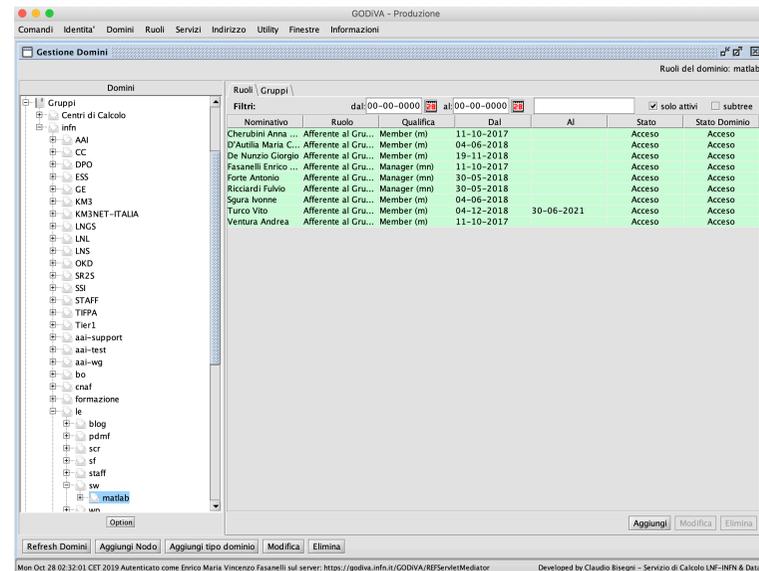
```
isMemberOf: accessi:inf:lnf:eps_tornello_stazione  
::acc_dip:acc_dip_norm@[i:inf:lnf::a:dottorando]
```

## 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:inf:le:sw:matlab) nel dominio dei Gruppi
  - Assegno al nodo finale le identità che voglio autorizzare
  - Definisco un filtro LDAP nella configurazione di sssd del server matlab in modo che permetta l'accesso agli utenti i cui attributi soddisfano la condizione (&(uid=\*)(isMemberOf=g:inf:le:sw:matlab::ag:m))

# Ruolo: Afferente al Gruppo

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



The screenshot shows the 'Gestione Domini' application window. The left pane shows a tree view of domains, with 'matlab' selected under the 'sw' group. The right pane displays a table of users and their roles in the 'matlab' group.

| Nominativo            | Ruolo               | Qualifica    | Dal        | Al         | Stato   | Stato Dominio |
|-----------------------|---------------------|--------------|------------|------------|---------|---------------|
| Cherubini Anna ...    | Afferente al Gru... | Member (m)   | 11-10-2017 |            | Accesso | Accesso       |
| D'Auria Maria C. ...  | Afferente al Gru... | Member (m)   | 04-06-2018 |            | Accesso | Accesso       |
| De Nunzio Giorgio ... | Afferente al Gru... | Member (m)   | 19-11-2018 |            | Accesso | Accesso       |
| Fasanelli Enrico ...  | Afferente al Gru... | Manager (mn) | 11-10-2017 |            | Accesso | Accesso       |
| Forte Antonio ...     | Afferente al Gru... | Manager (mn) | 30-05-2018 |            | Accesso | Accesso       |
| Ricciardi Fulvio ...  | Afferente al Gru... | Manager (mn) | 30-05-2018 |            | Accesso | Accesso       |
| Sgura Ivonne ...      | Afferente al Gru... | Member (m)   | 04-06-2018 |            | Accesso | Accesso       |
| Turco Vito ...        | Afferente al Gru... | Member (m)   | 04-12-2018 | 30-06-2021 | Accesso | Accesso       |
| Ventura Andrea ...    | Afferente al Gru... | Member (m)   | 11-10-2017 |            | Accesso | Accesso       |

# 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 Committee 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

**IDENTITY PROVIDER SETTINGS**

Set information relating to the IdP that will be connected with our WordPress. You can find these values at the Onelogin's platform inside WordPress on the Single Sign-On tab.

**IdP Entity Id \***   
*Identifier of the IdP entity. ("Issuer URL")*

**Single Sign On Service Uri \***   
*SSO endpoint info of the IdP. URL target of the IdP where the SP will send the Authentication Request. ("SAML 2.0 Endpoint (HTTP)")*

**Single Log Out Service Uri**   
*SLO endpoint info of the IdP. URL target of the IdP where the SP will send the SLO Request. ("SLO Endpoint (HTTP)")*

**X.509 Certificate**   
*Public x509 certificate of the IdP. ("X.509 certificate")*

# Caso d'uso: WordPress

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

### IDENTITY PROVIDER SETTINGS

Set information relating to the IdP that will be connected with our WordPress. You can find these values at the Onelogin's platform inside WordPress on the Single Sign-On tab.

#### ATTRIBUTE MAPPING

Sometimes the names of the attributes sent by the IdP do not match the names used by WordPress for the user accounts. In this section you can set the mapping between IdP fields and WordPress fields. Note: This mapping could be also set at Onelogin's IdP.

|                   |   |
|-------------------|---|
| <b>Username *</b> | <input type="text" value="uid"/>                  |
| <b>E-mail *</b>   | <input type="text" value="mail"/>                 |
| <b>First Name</b> | <input type="text" value="givenName"/>            |
| <b>Last Name</b>  | <input type="text" value="sn"/>                   |
| <b>Role</b>       | <input type="text" value="eduPersonEntitlement"/> |

*The attribute that contains the role of the user, For example 'memberOf'. If WordPress can't figure what role assign to the user, it will assign the default role defined at the general settings.*

```

oBwC0w6yVCLamL1U01vyytEtk1EY9vU/EEquV9CAChUMUv9yU19R1TzYV1KdYpC100yZOMHE41YU
sUoUBPhwXyCYJ2wAmi2VwIDAQABo4GnMIGkMB0GA1UdDg0WBBROEKiqRjIVFsHZKsnYbh+xPNmiLDB1B
gnVHSMebjBsgBROEKiqRjIVFsHZKsnYbh+xPNmiLKFJpEcwrTEUMBIGA1UEAxMLaWRwLmluZm4uaXQxET
APBgNVBAsTCeLORk4tQUFJMQU0wCwYDVQQKEwRJTzkzOMQswCQYDVQQGEwJVV1IJAOU290wo1W3MAWGA1U
dEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBALVvVWP9nrWlmu37KbTE3kuqJWptGmaDS2uuOg5RN5L
GevQvVu4cac23qaZZ+TN+b6WDxuhEfmVJzBYczxByVeGEvew0fHgRRMZLqST6j2gyb89qzNNFYTcyRZ/5
774Y84wDz2eQVxxx9hhTdcQ2E7EYi6dd4w2ebL0EhT4eG1EMU4Z8NUMeeY84ebhccyQYUud/

```

*Public x509 certificate of the IdP. ("X.509 certificate")*

# Caso d'uso: WordPress

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

**IDENTITY PROVIDER SETTINGS**

Set information relating to the IdP that will be connected with our WordPress. You can find these values at the Onelogin's platform inside WordPress on the Single Sign-On tab.

**ATTRIBUTE MAPPING**

Sometimes the names of the attributes sent by the IdP do not match the names used by WordPress for the user accounts. In this

**ROLE MAPPING**

The IdP can use its own roles. In this section, you can set the mapping between IdP and WordPress roles. Accepts comma separated values. Example: `admin, owner, superuser`

Administrator

Editor

Author

Contributor

Subscriber

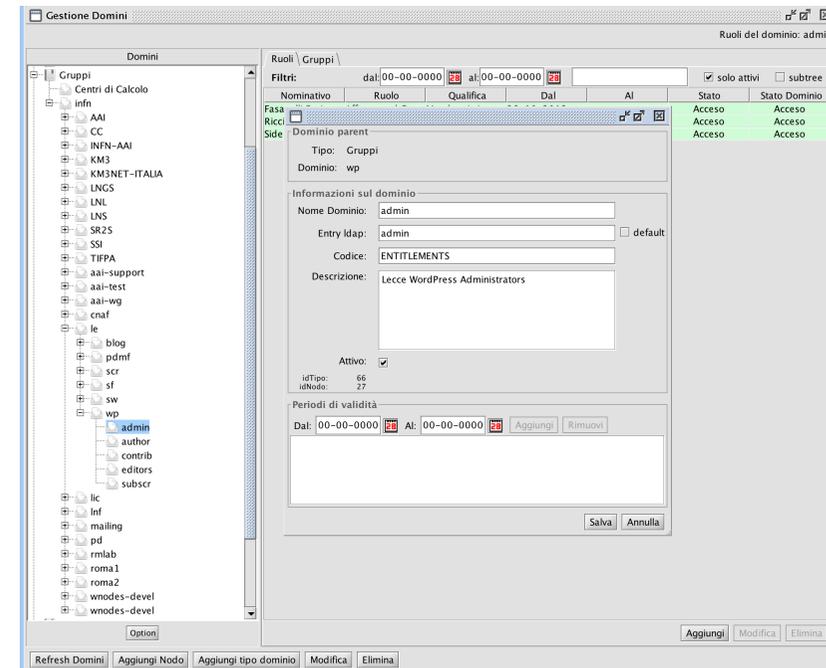
Multiple role values in

```
gNVHSMebjBsgBROEKigrjIVFsHZKsnYbh+xPNmilkFJpEcwrTEUMBIGAIUEAxMLaWrwLmluZm4uaXQxET
APBgNVBAsTCeLORk4tQUFJMq0wCwYDVQQKEwRJKzOMQswCQYDVQQGEwJVV1IJAOU290wo1W3MAWGA1U
dEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBALVvVvWP9nrWlmu37KbTE3kuqJWptGmaDS2uuOg5RN5L
GevQvVu4cac23qaZZ+TN+b6WDxuhEfmVJzBYczxByVeGEvew0fHgRRMZLqST6j2gyb89qzNNFyTcyRZ/5
774Y84wDz3eQVxxx0hhYdcQ2E7EYi6dd4w3ebL0Efi7e1u6M1EMLU4ZuNUMeeY84ebccvQYUud/
```

*Public x509 certificate of the IdP. ("X.509 certificate")*

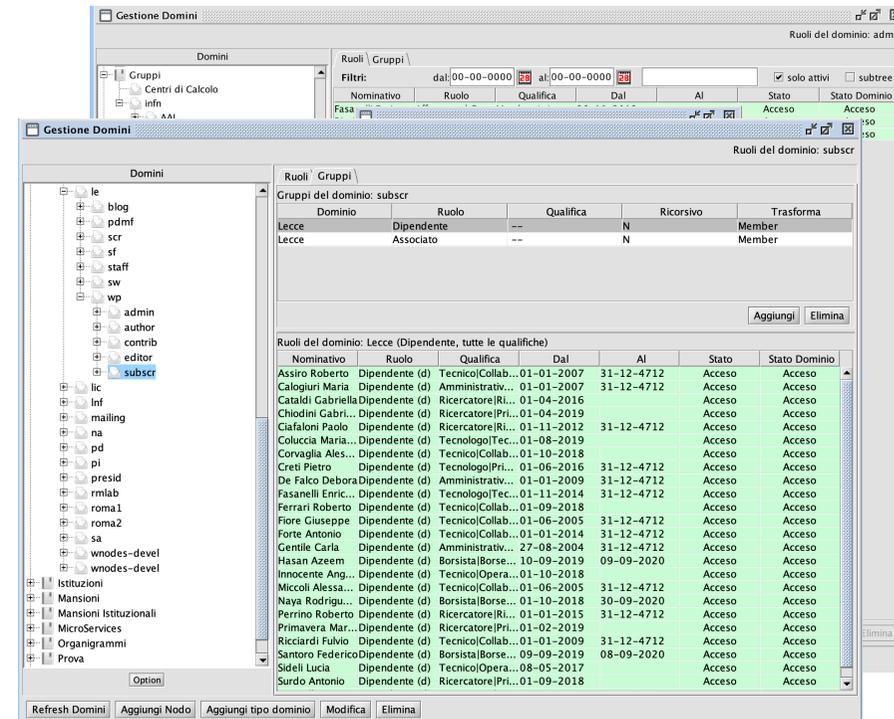
# Caso d'uso WordPress: GODiVA

- 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



The screenshot shows the 'Gestione Domini' (Domain Management) interface. The left pane shows a tree view of domains, with 'subscr' selected under the 'Lecce' domain. The right pane shows the 'Ruoli' (Roles) configuration for the 'subscr' group.

**Ruoli del dominio: subscr**

| Gruppi del dominio: subscr | Domino     | Ruolo | Qualifica | Ricorsivo | Trasforma |
|----------------------------|------------|-------|-----------|-----------|-----------|
| Lecce                      | Dipendente | --    | N         | Member    |           |
| Lecce                      | Associato  | --    | N         | Member    |           |

**Ruoli del dominio: Lecce (Dipendente, tutte le qualifiche)**

| Nominativo         | Ruolo          | Qualifica          | Dal        | Al         | Stato   | Stato Dominio |
|--------------------|----------------|--------------------|------------|------------|---------|---------------|
| Assiro Roberto     | Dipendente (d) | Tecnico Collab...  | 01-01-2007 | 31-12-4712 | Accesso | Accesso       |
| Caloguri Maria     | Dipendente (d) | Amministrativ...   | 01-01-2007 | 31-12-4712 | Accesso | Accesso       |
| Catadi Gabriella   | Dipendente (d) | Ricercatore Ri...  | 01-04-2016 |            | Accesso | Accesso       |
| Chiodini Gabri...  | Dipendente (d) | Ricercatore Pri... | 01-04-2019 |            | Accesso | Accesso       |
| Ciafaloni Paolo    | Dipendente (d) | Ricercatore Ri...  | 01-11-2012 | 31-12-4712 | Accesso | Accesso       |
| Coluccia Maria...  | Dipendente (d) | Tecnologo Tec...   | 01-08-2019 |            | Accesso | Accesso       |
| Corvaglia Ales...  | Dipendente (d) | Tecnico Collab...  | 01-10-2018 |            | Accesso | Accesso       |
| Creti Pietro       | Dipendente (d) | Tecnologo Pri...   | 01-06-2016 | 31-12-4712 | Accesso | Accesso       |
| De Falco Debora    | Dipendente (d) | Amministrativ...   | 01-01-2009 | 31-12-4712 | Accesso | Accesso       |
| Fasanelli Enric... | Dipendente (d) | Tecnologo Tec...   | 01-11-2014 | 31-12-4712 | Accesso | Accesso       |
| Ferrari Roberto    | Dipendente (d) | Tecnico Collab...  | 01-09-2018 |            | Accesso | Accesso       |
| Fiore Giuseppe     | Dipendente (d) | Tecnico Collab...  | 01-06-2005 | 31-12-4712 | Accesso | Accesso       |
| Forte Antonio      | Dipendente (d) | Tecnico Collab...  | 01-01-2014 | 31-12-4712 | Accesso | Accesso       |
| Gentile Carla      | Dipendente (d) | Amministrativ...   | 27-08-2004 | 31-12-4712 | Accesso | Accesso       |
| Hasan Azeem        | Dipendente (d) | Borsista Borse...  | 10-09-2019 | 09-09-2020 | Accesso | Accesso       |
| Innocente Ang...   | Dipendente (d) | Tecnico Opera...   | 01-10-2018 |            | Accesso | Accesso       |
| Miccoli Alessa...  | Dipendente (d) | Tecnico Collab...  | 01-06-2005 | 31-12-4712 | Accesso | Accesso       |
| Naya Rodrigu...    | Dipendente (d) | Borsista Borse...  | 01-10-2018 | 30-09-2020 | Accesso | Accesso       |
| Perrino Roberto    | Dipendente (d) | Ricercatore Ri...  | 01-01-2015 | 31-12-4712 | Accesso | Accesso       |
| Primavera Mar...   | Dipendente (d) | Ricercatore Pri... | 01-02-2019 |            | Accesso | Accesso       |
| Ricciardi Fulvio   | Dipendente (d) | Tecnico Collab...  | 01-01-2009 | 31-12-4712 | Accesso | Accesso       |
| Santoro Federico   | Dipendente (d) | Borsista Borse...  | 09-09-2019 | 08-09-2020 | Accesso | Accesso       |
| Sideli Lucia       | Dipendente (d) | Tecnico Opera...   | 08-05-2017 |            | Accesso | Accesso       |
| Surdo Antonio      | Dipendente (d) | Ricercatore Pri... | 01-09-2018 |            | Accesso | Accesso       |

# 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?

?

?

?



?