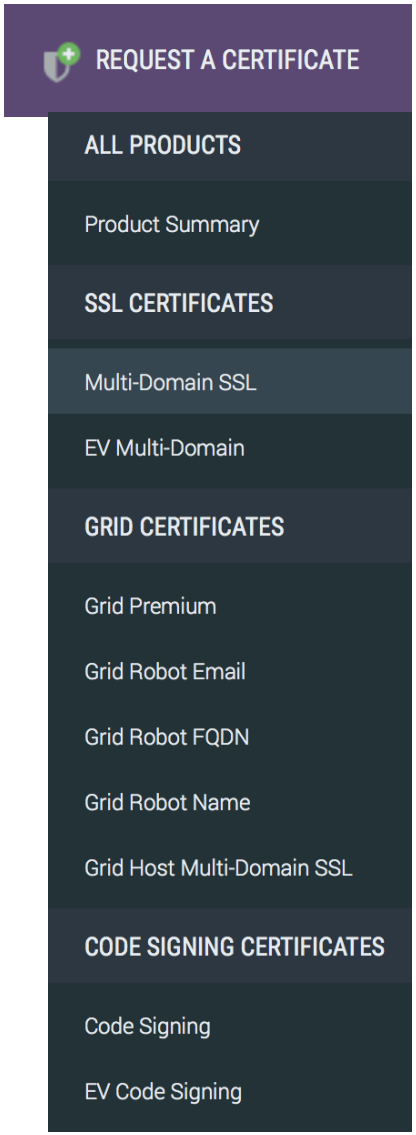
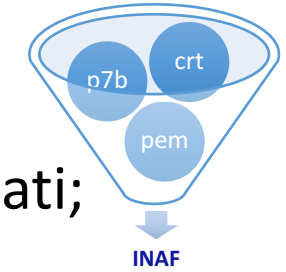
Certificazione e nuove credenziali utente: impatto sulle applicazioni

- DigiCert CA
- Certificati Server
- Certificati GRID
- Certificati Personali
- Nuova anagrafica e credenziali utente
- Cosa cambia e quali problemi

DigiCert CA: https://www.digicert.com



- Terena ha un contratto per la fornitura gratuita a tutte le NREN europee di certificati server e personali con la CA DigiCert;

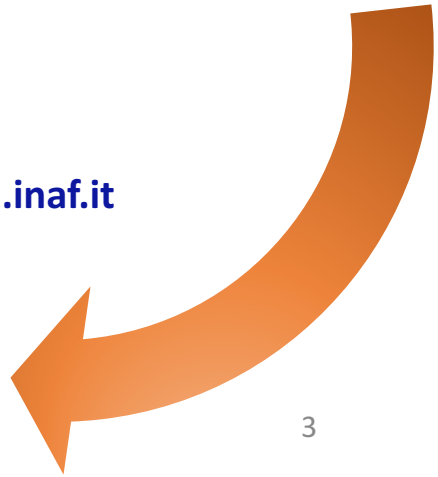


- INAF è accreditata per richiedere certificati;
- È possibile richiedere di essere registrati come utenti abilitati alla richiesta di certificati Server/GRID;
- Tutti i dipendenti INAF possono richiedere un certificato personale utilizzando le proprie credenziali IDEM.

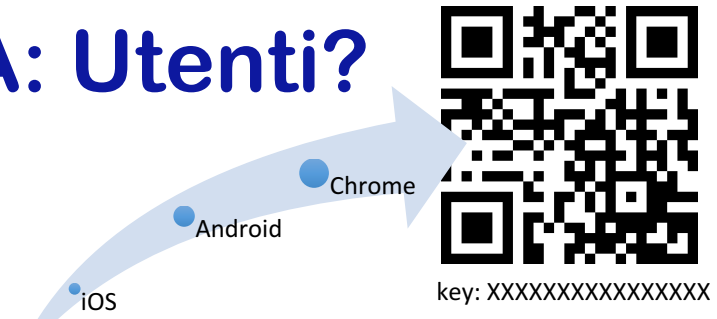
DigiCert CA: Utenti INAF

In blu gli amministratori di INAF, possono aggiungere utenti, approvare e revocare i certificati.

Alessandro Tacchini	IASF-BO	
Alessandro Costa	OACT	
Amedeo Petrella	OAPD	
Andrea Di Dato	OA-Capodimonte	
Chiara Giorgieri	**SEDE**	**giorgieri@inaf.it**
Cristian Boso	OATS	
Danilo Selvestrel	OAPD	
Federico Gasparo	OATS	
Francesco Tribioli	OA-Arcetri	
Franco Tinarelli	**IRA**	**franco.tinarelli@inaf.it**
Giacomo Fazio	**IFC**	**Giacomo.Fazio@ifc.inaf.it**
Giuliano Taffoni	OATS	
Guido Buscema	OA-Roma	
Massimiliano Lisi	OA-Roma	
Massimo Sponza	OATS	
Massimo Quintini	OA-Teramo	
Mauro Nanni	**IRA**	**nanni@ira.inaf.it**
Piero Massimino	OACT	
Robero Merighi	OABO	
Roberto Regni Ponzeveroni	IASF-MI	



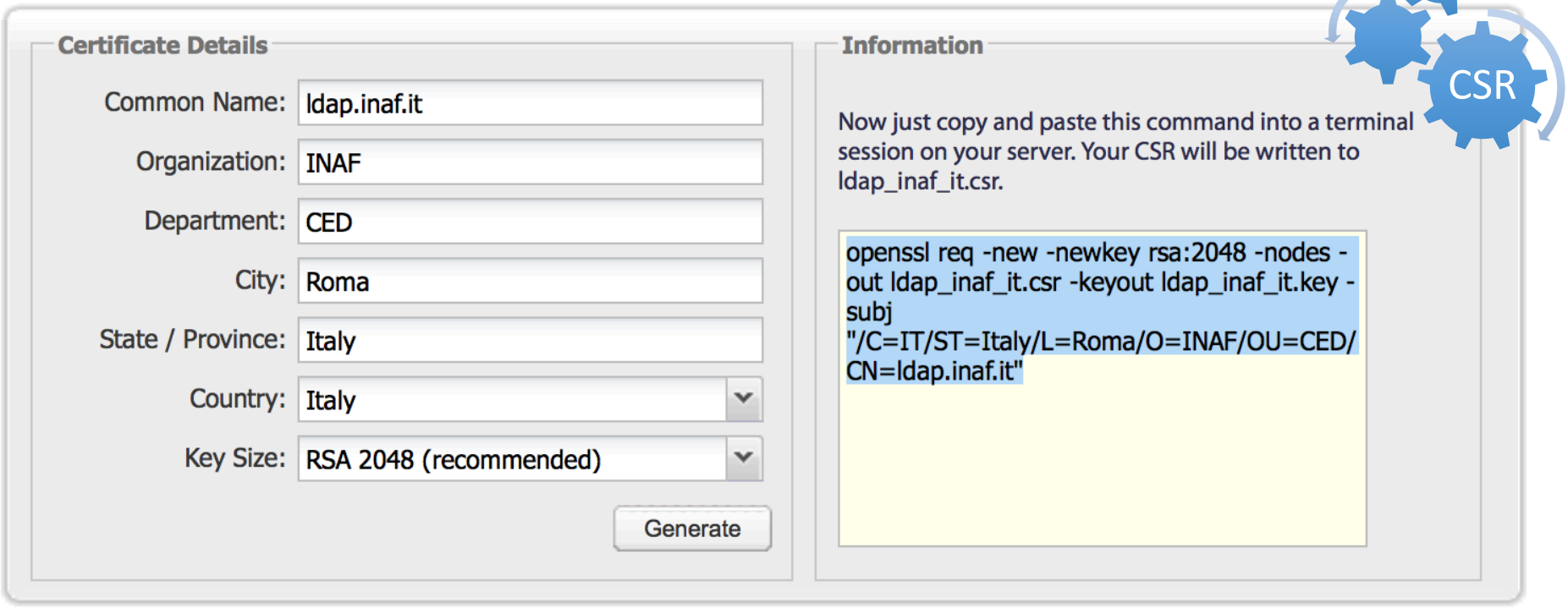
DigiCert CA: Utenti?



Per poter richiedere certificati server dovete essere accreditati:

- Inviate una mail ad un amministratore DigiCert di INAF contenente Nome, Cognome e indirizzo Email dove ricevere le comunicazioni di DigiCert;
- Seguire le istruzioni contenute nella mail d'invito di DigiCert;
- Registrare il QR Code o Key Code, contenuti nella pagina web di configurazione, sul proprio Smart Phone/Tablet/Mac/Chrome
- **SALVARE il QR Code e il Key Code!** Prima o poi si cambia telefono e si reinstalla il browser!
- Visto che non seguirete l'indicazione del punto precedente inviate una mail a **support@digicert.com** richiedendo un nuovo codice!

Certificati Server: creare il CSR

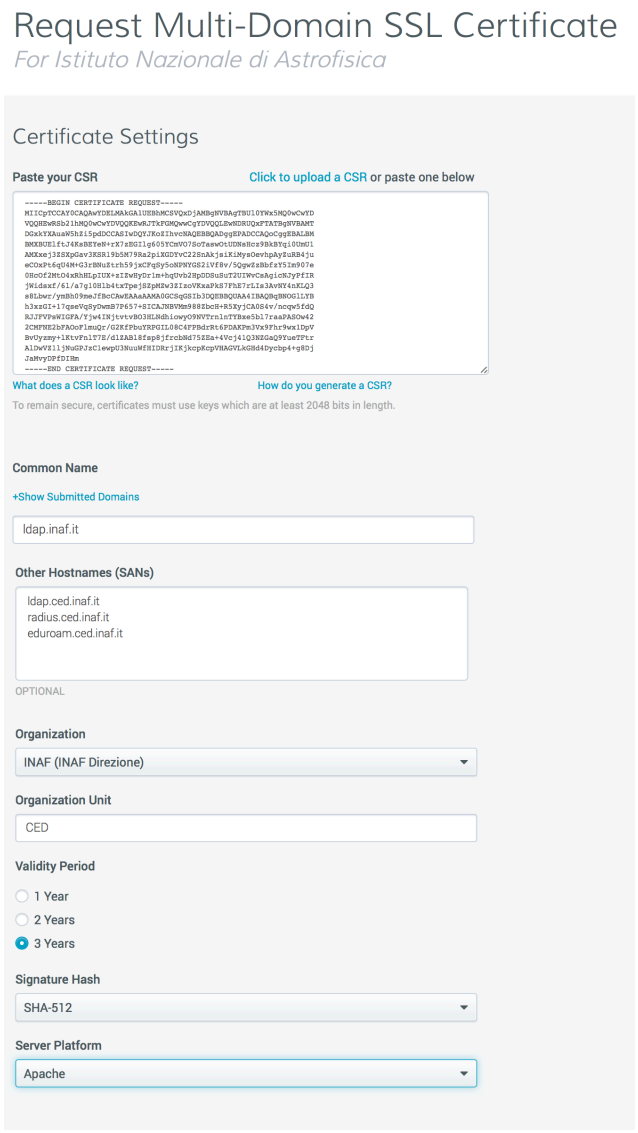


https://www.digicert.com/easy-csr/openssl.htm

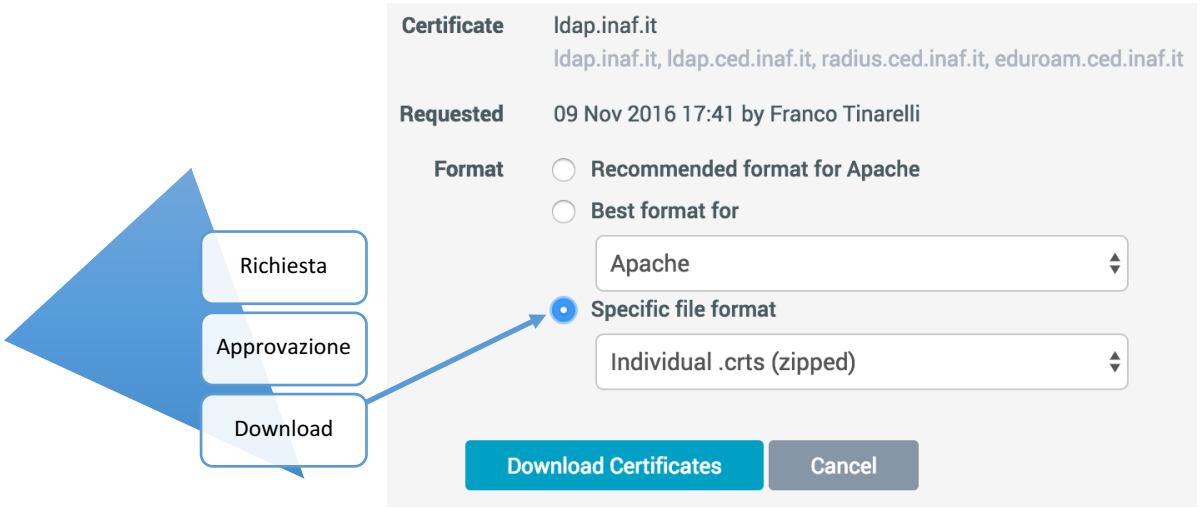
Usando il comando in un terminale vengono generati 2 files:

1. **ldap_inaf_it.csr -** contiene i dati per la creazione del certificato e verrà inserito nell'apposito spazio della pagina web di richiesta;
2. **ldap_inaf_it.key** – è la chiave privata del certificato; cambiatene immediatamente gli attributi (0600) e **conservatelo!!** Il certificato non vale nulla senza questo file;

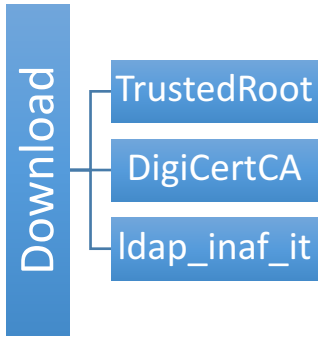
Certificati Server: la richiesta



- Si possono richiedere certificati Multi-Domain SSL;
- Si incolla il contenuto del file CSR generato;
- Si inseriscono tutti i nomi alternativi (SANs) associati al nome principale, devono essere registrati (CNAME);
- Si sceglie il periodo di validità, il tipo di hash, il tipo di piattaforma, il rinnovo automatico etc.;
- Una mail per l'approvazione arriverà automaticamente agli amministratori di INAF;
- Dopo l'approvazione l'utente riceverà una mail con le istruzioni per il download del certificato.



Certificati Server: Installazione



Il download/unzip genera una directory che contiene:

- Il certificato stesso, nel nostro esempio "**ldap_inaf_it.crt**";
- Il certificato della CA intermedia "**DigiCertCA.crt**";
- Il certificato della CA principale "**TrustedRoot.crt**";
- Files d'istruzione in diverse lingue, quello italiano "INSTALL_INSTRUCTIONS.it.txt", contenente le indicazioni per la configurazione SSL di apache.

Windows Server e **OSX Server** usano programmi dedicati per l'installazione dei propri certificati e richiedono che il file da importare sia l'insieme del certificato pubblico e della chiave privata, criptato e protetto da password nel formato **PKCS#12 / PFX**

Per convertire I file PEM nel formato PFX (estensione .p12 o .pfx) usate il comando:

```
openssl pkcs12 -export -out ldap_inaf_it.pfx \
               -inkey ldap_inaf_it.key \
               -in ldap_inaf_it.crt -certfile DigiCertCA.crt
```

Vi verrà richiesto di inserire una password per proteggere il file in quanto contiene anche la chiave privata.

Certificati Server: Installazione

Linux usa principalmente i certificati in formato **PEM**, files ASCII in codifica Base64 e con estensioni .pem, .crt, (.cer). I certificati host, CA e la chiave privata vengono salvati in directories di sistema:

Debian e derivati in **/etc/ssl/certs** i certificati e **/etc/ssl/private** la chiave privata

Red Hat e derivati in **/etc/pki/TLS/certs** i certificati e **/etc/pki/TLS/private** la chiave privata

RICORDATEVI di modificare gli attributi della chiave privata in 0600 (leggibile e scrivibile al solo proprietario, tipicamente root).

Apache, dovecot e altri daemon che usano SSL o TLS usano i certificati direttamente in formato PEM es.:

SSLCertificateFile /etc/pki/tls/certs/**ldap_inaf_it.crt**
SSLCertificateKeyFile /etc/pki/tls/private/**ldap_inaf_it.key**
SSLCertificateChainFile /etc/pki/tls/certs/**DigiCertCA.crt**

"Giusto per renderci comoda la vita!!!" OpenLDAP Server dalla versione 2.4 in poi usa il Netscape Communicator **cert8.db** and **key3.db** database!

(Trovate in Appendice 1 le istruzioni per popolare il database con i certificati PEM)

Certificati GRID Server

La richiesta di certificati GRID è identica a quella dei certificati Pubblici, cambiano l'Issuer, le Extensions e le Policies interne al certificato:

Server Pubblico

Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 CRL Distribution Points:

URI:http://crl3.digicert.com/TERENASSLCA3.crl

URI:http://crl4.digicert.com/TERENASSLCA3.crl

X509v3 Certificate Policies:

Policy: 2.16.840.1.114412.1.1

CPS: https://www.digicert.com/CPS

Policy: 2.23.140.1.2.2

Server GRID

Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, **CN=TERENA eScience SSL CA 3**

X509v3 Key Usage: critical

Digital Signature, Key Encipherment, **Data Encipherment**

X509v3 CRL Distribution Points:

URI:http://crl3.digicert.com/**TERENAeScienceSSLCA3.crl**

URI:http://crl4.digicert.com/**TERENAeScienceSSLCA3.crl**

X509v3 Certificate Policies:

Policy: 1.2.840.113612.5.2.2.1

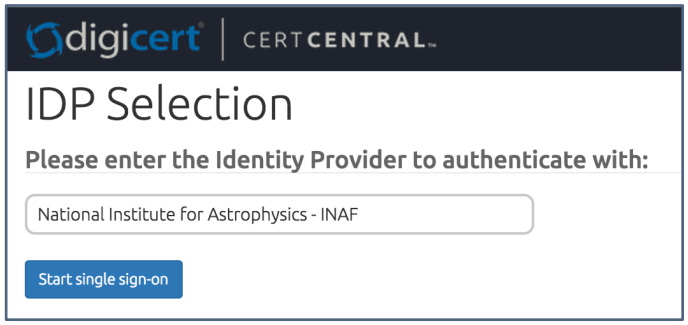
Policy: 2.16.840.1.114412.1.31.1

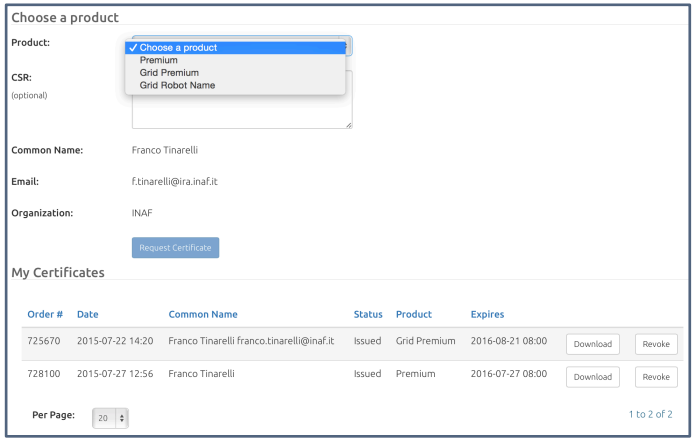
Policy: 1.2.840.113612.5.2.3.3.2

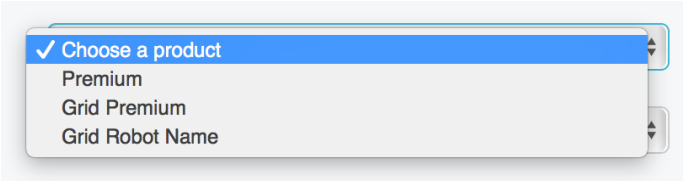
Policy: 2.23.140.1.2.2

Certificati Personali

https://www.digicert.com/sso



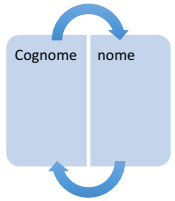




- Con le credenziali IDEM potete richiedere certificati personali **Premium**, **Grid Premium** e **Grid Robot Name**;
- **Premium** Common Name: **nome.cognome;**
- **Grid** Premium CN: **nome.cognome@inaf.it;**
- Questi certificati **sostituiscono** i certificati **GARR** e **INFN**. Il GARR chiuderà la propria CA;
- Dopo aver importato il certificato nel Browser con cui lo avete richiesto e dove la chiave privata è stata registrata, ricordatevi di **esportare immediatamente** il certificato in formato **PKCS#12;**

- **Il file esportato contiene sia il certificato che la chiave privata, proteggetelo con una password. È il vostro backup e può essere importato in diversi browser e programmi in grado di utilizzarlo;**

nome.cognome

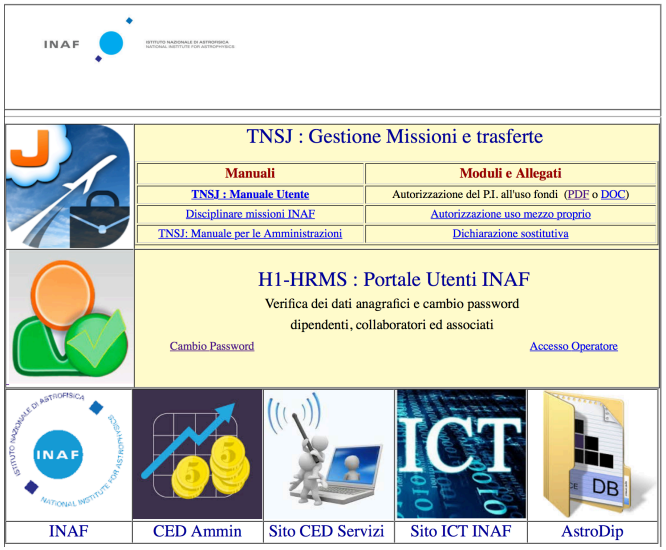


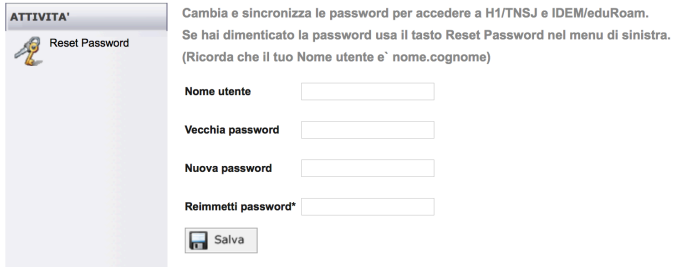
- Con l'utilizzo del nuovo programma per la gestione dell'anagrafica dell'Ente le credenziali utente cambiano da cognome.nome a nome.cognome **uid: franco.tinarelli**
- Le informazioni che popolano il server LDAP non vengono più ricavate da CSA ma dal nuovo programma **H1**, come **uid** viene ora usata la **username** creata evitando le omonimie
- la **uidNumber: 10XXX** diventa personale e non duplicabile per poter essere accreditati alle risorse di calcolo GRID, HPC, etc.
- Viene introdotta la **eduPersonOrcid: http://orcid.org/0000-0002-3161-182X**
- Da **eduPersonPrincipalName: franco.tinarelli@inaf.it** viene ricavato L'alias/indirizzo di posta elettronica, essendo formato da uid@dominio non può avere omonimie
- L'account rimane attivo per sei mesi dalla cessazione del rapporto di lavoro
- Cambia la procedura per la modifica delle password personali, raggiungibile ora sulla pagina https://servizi.ced.inaf.it

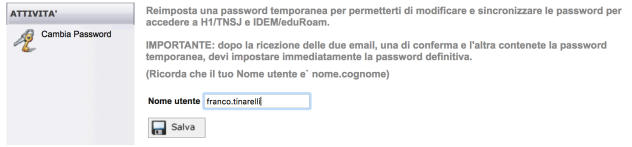
H1 impostazione/cambio password

Cambia

Reset





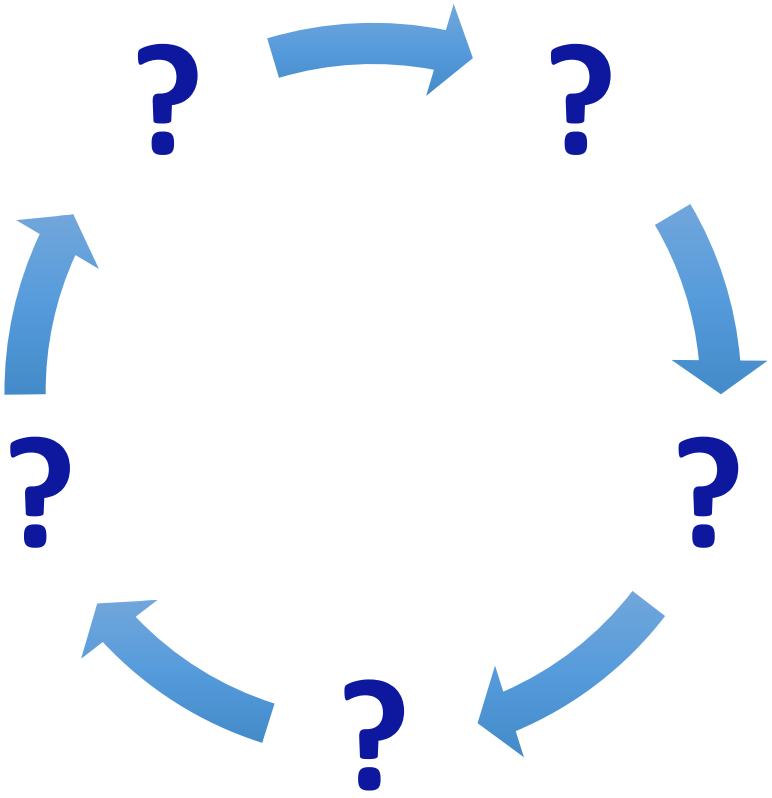


- **https://servizi.ced.inaf.it** (Portale H1);
- Attivare il link **Cambio Password** a centro pagina;
- Se vi ricordate la vecchia fate comunque un cambio inserendo sempre la stessa password, questo sincronizza le password Unix (IDEM) e Windows (eduROAM) sul server LDAP;
- Se non ricordate la vecchia usate il pulsante **Reset Password** nel menu di sinistra e usate come nome utente sempre **nome.cognome**;
- Riceverete due mail, la prima contiene il link per confermare l'operazione, la seconda una password temporanea per permettervi di impostare quella definitiva, **FATELO IMMEDIATAMENTE**, la password temporanea è quella Unix, non modifica quelle Windows e ha validità limitata;
- Se quando cambiate password dopo un reset ricevete come errore **La vecchia password non è valida**, controllate di non averla precedente **salvata nel browser**, in caso affermativo **cancellatela**.

nome.cognome: Problemi?!

- I server **WEB di ICT e CED** sono basati sul CMS Joomla e usano il server LDAP per autenticare gli utenti e registrarli nel proprio DB per l'assegnazione di gruppi e autorizzazioni.
  - **Problema**: il passaggio da cognome.nome a nome.cognome comporta la registrazione di un nuovo utente, l'operazione fallisce perché la email è identica e genera un errore.
  - **Soluzione**: in via d'investigazione
- **OwnCloud** non ha il problema descritto per Jomla e registra l'utente come nuovo.
  - **Problema**: come nuovo utente non possedete più files e condivisioni.
  - **Soluzione**: Chiedete al gestore di copiare i files dal vecchio account al nuovo. Oppure aprite due connessioni con vecchio e nuovo account e copiate voi i files.
- **NILDE** cerca di registrarvi come nuovo utente inviando la richiesta di registrazione al gestore del servizio.
  - **Problema**: se venite registrati come nuovo utente perdete lo storico delle precedenti richieste documentali.
  - **Soluzione**: Autenticatevi in IDEM e approvate l'invio dei parametri ma non la nuova registrazione richiesta dal servizio NILDE. Mandatemi una mail chiedendo il ripristino dello storico (franco.tinarelli@inaf.it)

Grazie per l'attenzione!



Appendice 1: da PEM a NSS

Certificate Nickname	Trust Attributes
	SSL,S/MIME,JAR/XPI
DigiCert CA	CT,,
Trusted Root	CT,,
ldap.inaf.it	u,u,u

1. Decrittiamo la chiave privata ldap_inaf_it.key generando il file ldap_inaf_it.crtkey
   > openssl rsa -in ldap_inaf_it.key -out ldap_inaf_it.crtkey
2. Convertiamo la coppia certificato/chiave in formato PKCS#12 (ENTER alla richiesta password per non bloccare con una password il file generato)
   > openssl pkcs12 -export -inkey ldap_inaf_it.crtkey -in ldap_inaf_it.crt \
   -out ldap_inaf_it.p12 -nodes -name ldap.inaf.it
3. Creiamo un nuovo database per i certificati usando la l'anno di scadenza del certificato (inseriamo una password o il comando non funziona)
   > certutil -N -d /etc/openldap/cacerts_2019
4. Rimuoviamo la password dal database (dopo l'inserimento della vecchia password premiamo ENTER alla richiesta della nuova)
   > certutil -d /etc/openldap/cacerts_2019 –W
5. Importiamo i files della CA uno alla volta
   > certutil -A -d /etc/openldap/cacerts_2019 -n "DigiCert CA" -t CT,, -a -i DigiCertCA.crt
   > certutil -A -d /etc/openldap/cacerts_2019 -n "Trusted Root" -t CT,, -a -i TrustedRoot.crt
6. Aggiungiamo la coppia certificato/chiave (ENTER a vuoto per non inserire la password)
   > pk12util -i ldap_inaf_it.p12 -d /etc/openldap/cacerts_2019
7. Controlliamo la riuscita dell'operazione richiedendo la lista dei certificati introdotti
   > certutil -d /etc/openldap/cacerts_2019 -L