

## 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

#### 📌 REQUEST A CERTIFICATE

ALL PRODUCTS

Product Summary

SSL CERTIFICATES

Multi-Domain SSL

EV Multi-Domain

#### **GRID CERTIFICATES**

Grid Premium

Grid Robot Email

Grid Robot FQDN

Grid Robot Name

Grid Host Multi-Domain SSL

CODE SIGNING CERTIFICATES

Code Signing

EV Code Signing

- 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.

INAF



# **DigiCert CA: Utenti INAF**

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

Alessandro Tacchini Alessandro Costa Amedeo Petrella Andrea Di Dato **Chiara Giorgieri** Cristian Boso Danilo Selvestrel Federico Gasparo Francesco Tribioli Franco Tinarelli **Giacomo Fazio** Giuliano Taffoni Guido Buscema Massimiliano Lisi Massimo Sponza Massimo Quintini Mauro Nanni Piero Massimino **Robero Merighi** 

**IASE-BO** OACT OAPD **OA-Capodimonte** SEDE OATS OAPD OATS **OA-Arcetri** IRA IFC OATS **OA-Roma OA-Roma** OATS **OA-Teramo** IRA OACT OABO **IASF-MI** 



franco.tinarelli@inaf.it Giacomo.Fazio@ifc.inaf.it

#### nanni@ira.inaf.it

Roberto Regni Ponzeveroni



# **DigiCert CA: Utenti?**

Android

iOS

# 

## 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

Certificate Details		Information	
Common Name:	ldap.inaf.it	Now just copy and paste this command into a terminal	R
Organization:	INAF	session on your server. Your CSR will be written to dap_inaf_it.csr.	
Department:	CED	openssl reg -new -newkey rsa:2048 -nodes -	
City:	Roma	out ldap_inaf_it.csr -keyout ldap_inaf_it.key - subi	
State / Province:	Italy	"/C=IT/ST=Italy/L=Roma/O=INAF/OU=CED/ CN=Idap.inaf.it"	
Country:	Italy		
Key Size:	RSA 2048 (recommended)		
	Generate		

## 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;
- Idap\_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**

## Request Multi-Domain SSL Certificate

Paste your CSR	Click to upload a CSR or paste one b
BEOIN CERTIFICATE REQUEST	Anton SAMBagWaAgTBULI DYKASHQOACSYTD WijowCyt TOYOGLEMANISHQO HAT ANTON ANTON WIJOWCH AND ANTON
s&Lbwr/ymBh09msJfBcCAwEAAsAAAAGO h3xuGl-17qsVqSyDmm37e537+STCAN LJJVFV9aVG2Y7yJ4K1jv+v03HLAdb 2CMFMEZb7AO7lmug/2AFFboxTROIL SWUyzmy1+KrWAIT77/d1ZaB1fsp3fj AlDwV211jNuGPJxClewpUJNuuHfHDRr JaMyDPfDIB 	Cogotis Livopomorcula Hanogomorcular Barbon Hano Hanogo Hanogo Hanogo Hanogo Hanogo Longo NAVITA I INTERNASIA / Fana MARADA 42 Longo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Hanogo Ha
#8Lbwr./ymbh09ms/f8cCAwt2AaAAM00        b3x021-1/getVg5/bms7/65/-+8CAJB        xJJYTV9WL076/7/3/4L19/vc40301L4db        2CHTWEZb7A071mug/c2xfPboxTR001        bV0yamy/t4LVW1073/c1L8aBfep5jf        ALbwr.V1175/c1L8aBfep5jf        abvyDp4D12m	Credit III Journal (III Alledgelliou)Linn III Alledgelliou (III Alledgelliou)Linn III Alledgelliou (III Alledgelliou)Linn III Alledgelliou (III Alledgelliou)Linn IIII Alledgelliou (III Alledgelliou)Linn IIII Alledgelliou (III Alledgelliou)Linn - How do you generate a CSR?

+Show Submitt	ed Domains
Idan inaf it	

Other	Hostnames	(SANs)
-------	-----------	--------

ldap.ced.inaf.it	
radius.ced.inaf.it eduroam.ced.inaf.it	
courounideanante	
OPTIONAL	
Organization	
INAF (INAF Direzione)	
Organization Unit	
CED	
Validity Period	
validity renou	
1 Year	
2 Years	
3 Years	
Cignoture Heeb	
Signature Hash	
SHA-512	
Server Platform	
Anache	
Apaone	

- 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 "Idap\_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.

ICT 2016 Trieste

oad

Down

TrustedRoot

DigiCertCA

Idap inaf i



# **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)

ICT 2016 Trieste

Franco Tinarelli (IRA)



## **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

🖸 di	gi <mark>ce</mark>	ert   <	ERT <b>CEI</b>	NTR	AL∝			
IDP Selection								
Please enter the Identity Provider to authenticate with:								
National Institute for Astrophysics - INAF								
Start single sign-on								
Choose a prod	luct							
Product: CSR: (optional)	Choo Pren Grid	ose a product nium Premium Robot Name		Ð				
Common Name:	Franco	Tinarelli						
Email:	f.tinan	elli@ira.inaf.it						
Organization:	INAF							
	Requ	est Certificate						
My Certificate	S							
Order # Date		Common Name		Status	Product	Expires		
725670 2015	-07-22 14:20	Franco Tinarelli fra	nco.tinarelli@inaf.it	Issued	Grid Premium	2016-08-21 08:00	Download	Revoke
728100 2015	-07-27 12:56	Franco Tinarelli		Issued	Premium	2016-07-27 08:00	Download	Revoke
Per Page:	20 \$							1 to 2 of 2
	oose a	product						
Grid	d Prem	ium						
Grid	d Robo	t Name						ŧ

- 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
- Ia 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 <u>https://servizi.ced.inaf.it</u>



INAF

## H1 impostazione/cambio password



word nel menu di sinistra.

Se hai dimenticato la password usa il tasto Reset Password nel menu di sinis
(Ricorda che il tuo Nome utente e` nome.cognome)
Nome utente
Vecchia password
Nuova password
Reimmetti password*
FT Salva

'A'	Reimposta una password temporanea per permetterti di modificare e sincronizzare le password per accedere a H1/TNS. Le IDEM/eduRoam				
ambia Password	MPORTANTe de l'infrede l'occimentatione delle due email, una di conferma e l'altra contenete la password temporanea, devi impostare immediatamente la password definitiva. (Ricorda che il tuo Nome utente e' nome.cognome)				
	Salva				

https://servizi.ced.inaf.it (Portale H1);  $\succ$ 

Reset

Cambia

- Attivare il link Cambio Password a centro pagina;
- Se vi ricordate la vecchia fate comungue 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	
	SSL,S/MIME,JAR/XPI
DigiCert CA	СТ,,
Trusted Root	СТ,,
ldap.inaf.it	u,u,u

- 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
- 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
- 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/openIdap/cacerts\_2019
- 4. Rimuoviamo la password dal database (dopo l'inserimento della vecchia password premiamo ENTER alla richiesta della nuova)
  > certutil -d /etc/openIdap/cacerts 2019 –W
- 5. Importiamo i files della CA uno alla volta
  > certutil -A -d /etc/openIdap/cacerts\_2019 -n "DigiCert CA" -t CT,, -a -i DigiCertCA.crt
  > certutil -A -d /etc/openIdap/cacerts\_2019 -n "Trusted Root" -t CT,, -a -i TrustedRoot.crt
- Aggiungiamo la coppia certificato/chiave (ENTER a vuoto per non inserire la password)
  > pk12util -i ldap\_inaf\_it.p12 -d /etc/openldap/cacerts\_2019
- Controlliamo la riuscita dell'operazione richiedendo la lista dei certificati introdotti ← > certutil -d /etc/openIdap/cacerts\_2019 -L