

Sobre el uso de certificados digitales



Red IRIS

Grupos de Trabajo 2017. Madrid



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Miguel Macías Enguïdanos

Certificados **personales**

S/MIME

Firma/cifrado documentos

Autenticación

Grid

🛡️ REQUEST A CERTIFICATE

📊 DASHBOARD

🛡️ CERTIFICATES

Orders

Requests

Domains

Organizations

Orders Report

Expiring Certificates

👤 ACCOUNT

↔️ SAML

Request a Certificate

SSL Certificates

Client Certificates

Grid Certificates

Code Signing
Certificates

Document Signing
Certificates

Digital Signature Plus

Email Security Plus

Premium

Premium

A DigiCert Premium Certificate provides secure email services and client authentication. Enable your clients to encrypt and digitally sign email communications.

Note: This certificate does not include private key escrow and recovery.

- Client authentication
- Document signing (with programs that support digital signatures. For programs that use the Adobe Approved Trust List, please utilize a Document Signing product)
- Email encryption
- Email signing

Order Now



REQUEST A CERTIFICATE

DASHBOARD

CERTIFICATES

Orders

Requests

Domains

Organizations

Orders Report

Expiring Certificates

ACCOUNT

SAML

Request a Certificate

SSL Certificates

Client Certificates

Grid Certificates

Code Signing
Certificates

Document Signing
Certificates

Digital Signature Plus

Email Security Plus

Premium

Premium

A DigiCert Premium Certificate provides secure email services and client authentication. Enable your clients to encrypt and digitally sign email communications.

Note: This certificate does not include private key escrow and recovery.

- Client authentication
- Document signing (with programs that support digital signatures. For programs that use the Adobe Approved Trust List, please utilize a Document Signing product)
- Email encryption
- Email signing

Order Now



REQUEST A CERTIFICATE

DASHBOARD

CERTIFICATES

Orders

Requests

Domains

Organizations

Orders Report

Expiring Certificates

ACCOUNT

SAML

Request a Certificate



SSL Certificates

Client Certificates

Grid Certificates

Code Signing Certificates

Document Signing Certificates

Digital Signature Plus

Email Security Plus

Premium

Premium

A DigiCert Premium Certificate provides secure email services and client authentication. Enable your clients to encrypt and digitally sign email communications.

Note: This certificate does not include private key escrow and recovery.

- Client authentication
- Document signing (with programs that support digital signatures. For programs that use the Adobe Approved Trust List, please utilize a Document Signing product)
- Email encryption
- Email signing

Order Now



REQUEST A CERTIFICATE

DASHBOARD

CERTIFICATES

Orders

Requests

Domains

Organizations

Orders Report

Expiring Certificates

ACCOUNT

SAML

Request a Certificate



SSL Certificates

Client Certificates

Grid Certificates

Code Signing Certificates

Document Signing Certificates

Digital Signature Plus

Email Security Plus

Premium

Premium

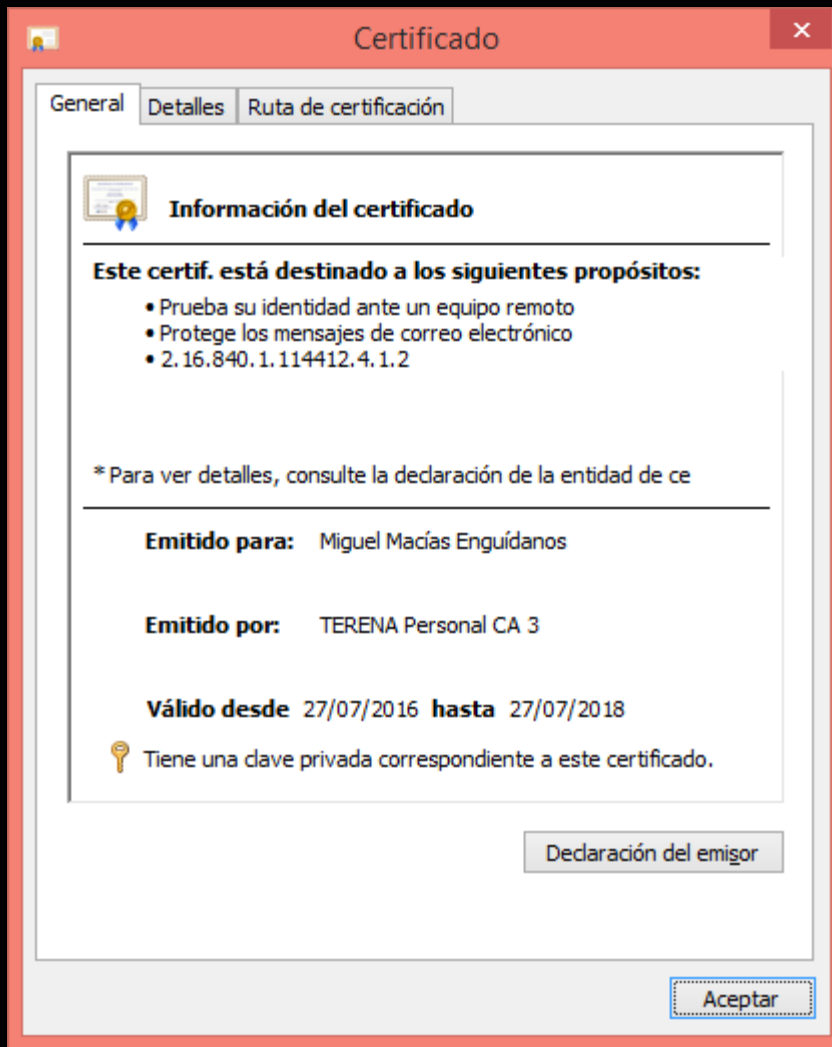
A DigiCert Premium Certificate provides secure email services and client authentication. Enable your clients to encrypt and digitally sign email communications.

Note: This certificate does not include private key escrow and recovery.

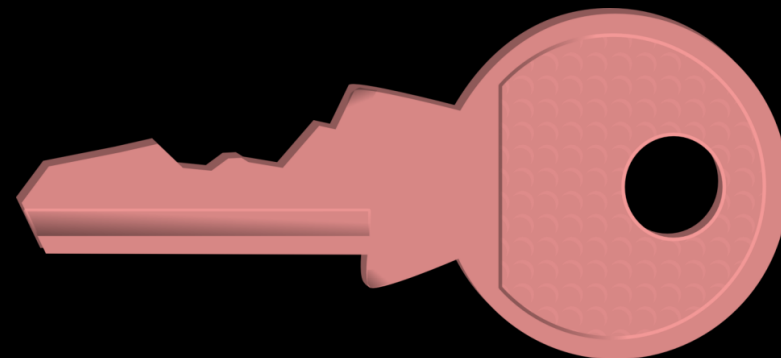
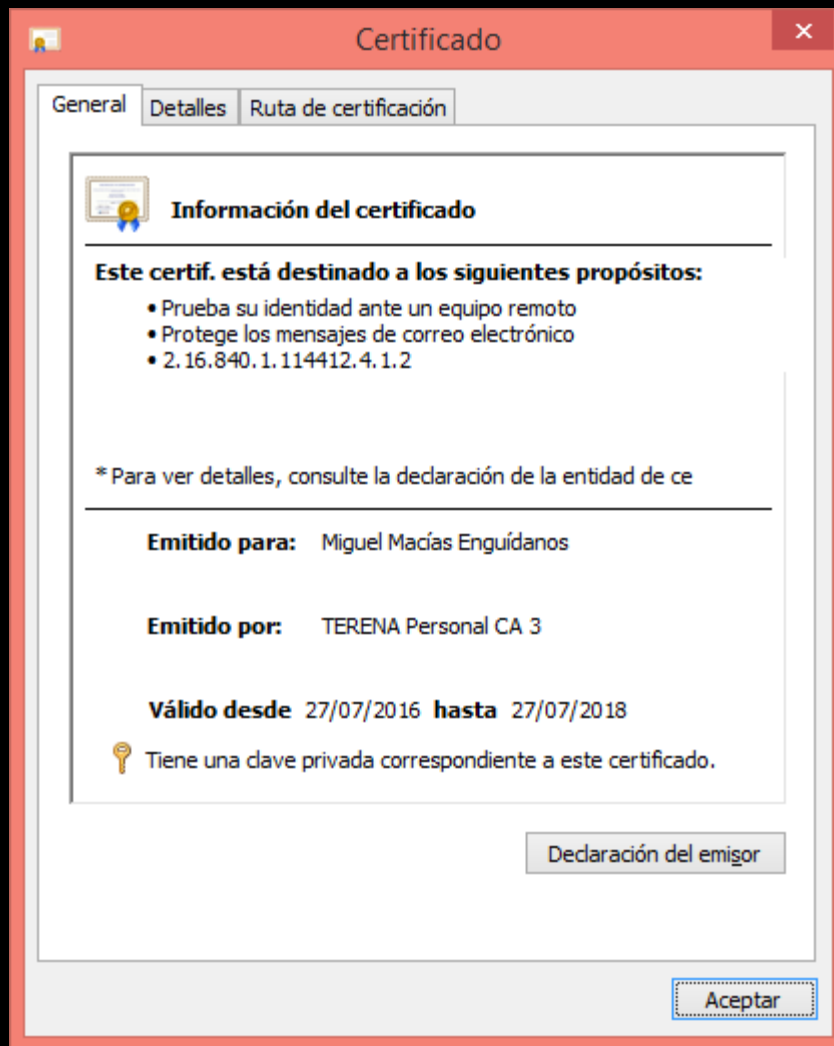
- Client authentication
- Document signing (with programs that support digital signatures. For programs that use the Adobe Approved Trust List, please utilize a Document Signing product)
- Email encryption
- Email signing

Order Now





¿confianza?



IDP Selection

Please enter the Identity Provider to authenticate with:

[Start single sign-on](#)





IDP Selection

Please enter the Identity Provider to authenticate with:

[Start single sign-on](#)

← InPrivate <https://www.digicert.com/secure/saml/discovery/?entityID=httj> DigiCert, Inc. [US]

IDP Selection :: DigiCert

digicert® | CERTCENTRAL®

IDP Selection

Please enter the Identity Provider to authenticate with:

Start single sign-on

¿IdP?

IDP Selection

Please enter the Identity Provider to authenticate with:

Start single sign-on



IDP Selection

Please enter the Identity Provider to authenticate with:

upv| - Universitat Politècnica de València



UPV - Universitat Politècnica de València



Identificación UPV. Accediendo a aplicación integrada en el SSO de la UPV

Una vez identificado, será redirigido a la aplicación.

como Alumno

DNI *

PIN *

Entrar

como Personal

DNI *

Clave UPVnet *

Entrar

como externo

ID *

Clave *

Entrar

Acceso con certificado

Acceso con certificado

Acceso con certificado

• ¿Ha olvidado su PIN?

- Los alumnos extranjeros consignarán el número de su pasaporte o NIE en lugar del DNI.
- En la casilla del PIN, se incluirá el número PIN de la automatrícula.
- Su identidad, así como los privilegios que lleva asociados, será recordada durante toda

• ¿Ha olvidado su clave?

- En la casilla de Clave de UPVnet, los usuarios introducirán su contraseña de usuario de UPVnet.
- Su identidad, así como los privilegios que lleva asociados, será recordada durante toda la sesión de trabajo. No olvide pues cerrar su sesión antes de abandonar el ordenador.

• ¿Ha olvidado su clave?

- Los usuarios españoles consignarán su DNI, mientras que los usuarios extranjeros introducirán su número de pasaporte o NIE.
- En la casilla de Clave, los usuarios introducirán su contraseña de usuario de extraNET.
- Su identidad, así como los privilegios que

IDP Selection

Please enter the Identity Provider to authenticate with:

[Start single sign-on](#)



[◀ Servicios](#) [◀ TCS](#) [◀ Acceso federado](#) [◀ Acceso WAYFless a SAML portal](#)

Acceso WAYFless a SAML portal

[Inicio TCS](#)

[Noticias](#)

[Características](#)

[Evolución histórica](#)

[Roles](#)

[Perfiles de certificado](#)

[Tarifas](#)

[Documentación](#)

[FAQ](#)

[CAs](#)

[CertCentral](#)

[ISC](#)

[Solicitar alta en TCS](#)

[Instituciones en TCS](#)

[Acceso federado](#)

[Estadísticas](#)

[Certificados/institución](#)

[Coordinación](#)

[Utilidades](#)

Usuarios del antiguo servicio pkIRISGrid

Mostramos a continuación una lista de los accesos WAYFless al SAML portal para las antiguas autoridades de registro de pkIRISGrid:

- [RA 1 - RedIRIS](#) - Red Académica y de Investigación Nacional
- [RA 2 - PIC - IFAE](#) - Instituto de Física de Altas Energías
- [RA 3 - DACYA - UCM](#) - Complutense University of Madrid
- [RA 4 - BSC](#) - Barcelona Supercomputing Center
- [RA 5 - UAM](#) - Universidad Autónoma de Madrid
- [RA 6 - BIFI - UNIZAR](#) - University of Zaragoza
- [RA 8 - CESGA](#) - Centro de Supercomputación de Galicia
- [RA 11 - IAA - CSIC](#) - Consejo Superior de Investigaciones Científicas
- [RA 12 - CIEMAT](#)
- [RA 13 - CETA-CIEMAT - CIEMAT](#)
- [RA 14 - UPV](#) - Universitat Politècnica de València
- [RA 19 - ECM - UB](#) - University of Barcelona
- [RA 20 - ARCOS - UC3M](#) - Universidad Carlos III de Madrid
- [RA 21 - DIPIC](#) - Donostia International Physics Center
- [RA 22 - CSIC](#) - Consejo Superior de Investigaciones Científicas
- [RA 23 - IFIC](#) - ([usuarios de UV](#)) ([usuarios del CSIC](#))
- [RA 25 - IFCA](#) - (usuarios de UNICAN) ([usuarios del CSIC](#))
- [RA 26 - CNB - CSIC](#) - Consejo Superior de Investigaciones Científicas
- [RA 29 - MAIA - UB](#) - University of Barcelona
- [RA 31 - UV](#) - Universitat de València
- [RA 32 - UAH](#) - University of Alcalá
- [RA 33 - EHU](#) - University of the Basque Country
- [RA 35 - UOC](#) - Universitat Oberta de Catalunya
- [RA 38 - BELLATERRA - CSIC](#) - Consejo Superior de Investigaciones Científicas
- [RA 40 - IAC](#) - Instituto de Astrofísica de Canarias

Portales de DigiCert

[CertCentral portal](#)
(certificados servidor,
código, documentos)

[SAML portal](#)
(certificados personales)



1.801.701.9600

My Account Live Chat English

Support

Your session has timed out. Please log back in to continue.

We've updated our [Privacy Policy](#)

DigiCert Account Login

Username:

Password:

[If you use SSO, click here to login](#)

LOGIN

Choose a product

Product:

Validity Period:

CSR:
(optional)

Common Name: Miguel Macías Enguádanos

Email: mimaen@upvnet.upv.es

Organization: Universitat Politècnica de València

[Request Certificate](#)

My Certificates

Order #	Date	Common Name	Status	Product	Expires	
	29 Nov 2017 00:39	Miguel Mac\u00edas Engu\u00eddanos	Not Submitted		29 Nov 2017 00:39	Place Order »





Generate your DigiCert Grid Premium Certificate

No se pudo completar la solicitud. Se ha generado un informa. Póngase en contacto con su administrador para recibir ayuda. X

For technical assistance or to make corrections, contact your administrator.

DigiCert Personal ID Details

Nombre: Miguel Subirats Sanjaume - 010110010 - 06070000000007000007@univ.es

Dirección Electrónica: msanjaum@upv.es

Organización: Universitat Politècnica de València

Acuerdo de Suscripción:

CERTIFICATE SERVICES AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGICERT DIGITAL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A DIGICERT DIGITAL CERTIFICATE OR BY CHECKING "I AGREE," YOU ACKNOWLEDGE THAT HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU AGREE TO IT, AND THAT YOU HAVE THE AUTHORITY TO OBTAIN THE DIGITAL EQUIVALENT OF A COMPANY STAMP, SEAL, OR OFFICER'S SIGNATURE TO ESTABLISH THE AUTHENTICITY OF CUSTOMER'S WEBSITE AND THAT CUSTOMER IS RESPONSIBLE FOR ALL USES OF THE CERTIFICATE. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A DIGICERT DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 1 año from the time it is issued. You have until November 24, 2017 to generate this certificate or you will need to contact your organization administrator to request a new email.

If your web server is configured to require "Client Authentication", you may need to configure it to allow client certs issued by DigiCert SHA2 Assured ID CA, as well as DigiCert Assured ID CA-1.

Due to new security standards, any client certificate expiring on or after January 1, 2020, will be issued using SHA-2

undefined...

Generating your DigiCert Personal ID...



DigiCert Personal ID Generated



2. Requisitos para el usuario solicitante

Tal y como se ha comentado en el punto 1.2, es necesario que desde el IdP de la institución se envíen una serie de atributos recomendados hacia DigiCert, entre ellos el atributo **eduPersonEntitlement** que debe contener, entre otros, **uno** de los valores siguientes:

- urn:mace:terena.org:tcs:**personal-user**
- urn:mace:terena.org:tcs:**escience-user**

Los dos valores dan acceso a solicitar certificados personales, sean de grid o no.

Request a Certificate

Choose a product

Product:

Premium

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Migue Tiene Un Nombre Demasiado Largo Pero Seguramente Se Acortará

Email:

migue.largo@upv.es

Organization:

Universitat Politècnica de València

Request Certificate

Request a Certificate

Choose a product

Product:

Grid Premium

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Migue Tiene Un Nombre Demasiado Largo Pero Seguramente Se
Acortara aab0e8fcd3edb4665b9caa5413030253@upv.es

Email:

migue.largo@upv.es

Organization:

Universitat Politecnica de Valencia

Request Certificate



Generate your DigiCert Grid Premium Certificate

No se pudo completar la solicitud. Se ha generado un informa. Póngase en contacto con su administrador para recibir ayuda. X

For technical assistance or to make corrections, contact your administrator.

DigiCert Personal ID Details

Nombre: Miguel Subirats Sanjaume - 010110010 - 06070000000007000007@univ.es

Dirección Electrónica: msanjaum@upv.es

Organización: Universitat Politècnica de València

Acuerdo de Suscripción:

CERTIFICATE SERVICES AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGICERT DIGITAL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A DIGICERT DIGITAL CERTIFICATE OR BY CHECKING "I AGREE," YOU ACKNOWLEDGE THAT HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU AGREE TO IT, AND THAT YOU HAVE THE AUTHORITY TO OBTAIN THE DIGITAL EQUIVALENT OF A COMPANY STAMP, SEAL, OR OFFICER'S SIGNATURE TO ESTABLISH THE AUTHENTICITY OF CUSTOMER'S WEBSITE AND THAT CUSTOMER IS RESPONSIBLE FOR ALL USES OF THE CERTIFICATE. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A DIGICERT DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 1 año from the time it is issued. You have until November 24, 2017 to generate this certificate or you will need to contact your organization administrator to request a new email.

If your web server is configured to require "Client Authentication", you may need to configure it to allow client certs issued by DigiCert SHA2 Assured ID CA, as well as DigiCert Assured ID CA-1.

Due to new security standards, any client certificate expiring on or after January 1, 2020, will be issued using SHA-2

DigiCert: nivel 1


making sure the user you're trying to request the certificate as has the correct permissions to allow that. In looking at the account roles I see that the product settings are configured to only allow Administrators to request that certificate

DigiCert: nivel 2

Looking into this I don't see xxxxx@upv.es as being a user on the account.

Maybe try adding them as a user with that email and have them try again?

Request a Certificate

 Common name must be less than 64 characters in order to be compliant with industry standards.

Choose a product

Product:

Choose a product

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Migue Tiene Un Nombre Demasiado Largo Pero Seguramente Se Acortará

Email:

migue.largo@upv.es

IdP

eduPersonEntitlement

displayName

eduPersonPrincipalName



IdP

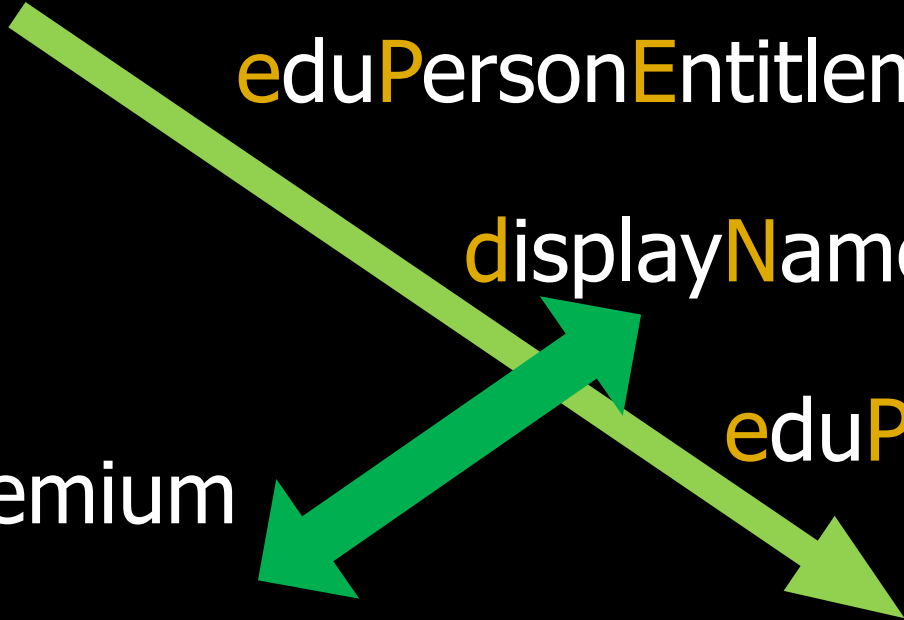
eduPersonEntitlement

displayName

eduPersonPrincipalName

Premium

Grid Premium



Request a Certificate

Choose a product

Product:

Choose a product

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Migue Tiene Ün NÓmbre Demásiado Largo Pero Seguramente Se Acortará

Email:

migue.largo@upv.es

Request a Certificate

Choose a product

Product:

Grid Premium

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Migue Tiene Uen Nombre Demasiado Largo Pero Seguramente Se
Acortara aab0e8fcd3edb4665b9caa5413030253@upv.es

Email:

migue.largo@upv.es

Request a Certificate

Choose a product

Product:

Choose a product



Validity Period:

1 Year



CSR:

(optional)

Common Name:

M. Lluïsa Ortola Yagüe

Email:

ml.ortya@upv.es

Request a Certificate

Choose a product

Product:

Choose a product

Validity Period:

1 Year

CSR:

(optional)

Common Name:

María Lluïsa Ortolà Yagüe

Email:

ml.ortya@upv.es

Request a Certificate

Choose a product

Product:

Grid Premium

Validity Period:

1 Year

CSR:


(optional)

Common Name:

Maria Lluisa Ortola Yaguee
9b1c0d460c0d321c1cabfb0f49806498@upv.es

Email:

ml.ortya@upv.es

 Common name must be less than 64 characters in order to be compliant with industry standards.

Choose a product

Product:

Grid Premium

Validity Period:

1 Year

CSR:

(optional)

Common Name:

Maria Lluisa Ortola Yaguee
9b1c0d460c0d321c1cabfb0f49806498@upv.es

Email:

ml.ortya@upv.es

CSR:

(optional)

CSR:

(optional)

```
[NewRequest]
Subject = "CN=upv.es"
Exportable = TRUE
KeyProtection = NCRYPT_UI_FORCE_HIGH_PROTECTION_FLAG
KeyLength = 2048
KeyUsage = 0xFF
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
Silent = false
RequestType = PKCS10
```

```
certreq -new certreq.inf certificado.csr
```

```
certreq -accept certificado.crt
```

2009



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

>> Intranet :: Consulta CFD

Cerrar sesión

Correos Oficiales de la UPV

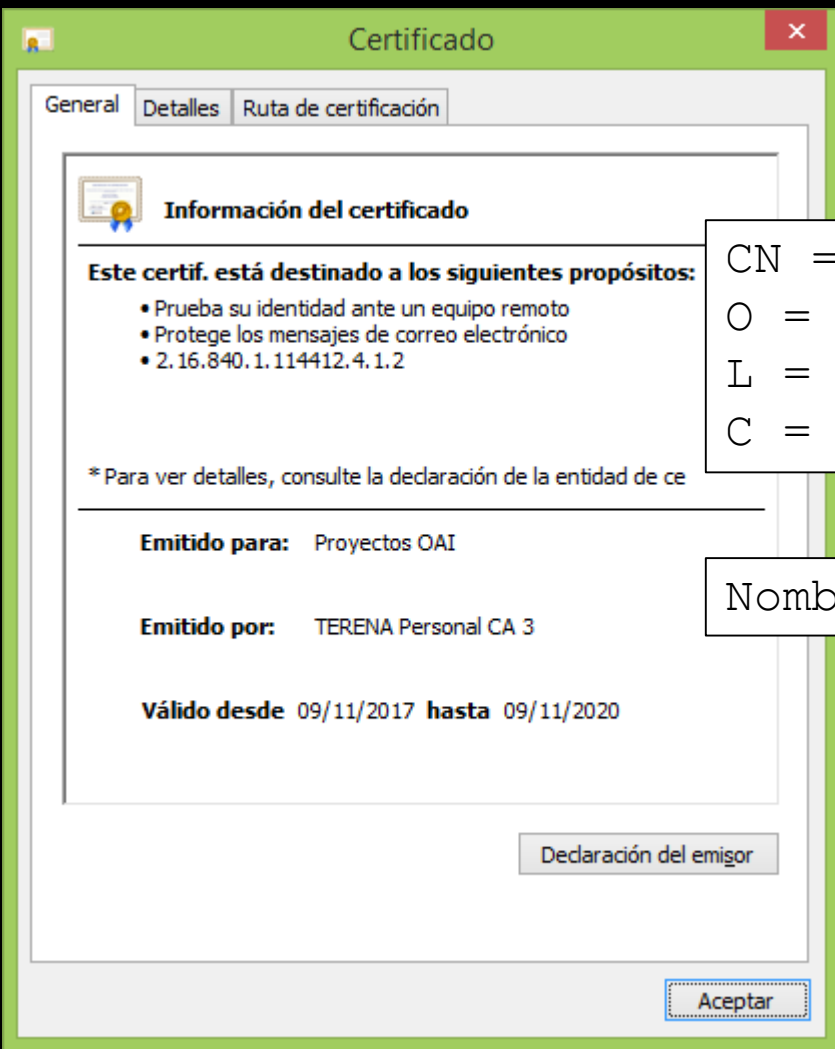
Correos Oficiales de la UPV

Para comprobar la autenticidad de los correos oficiales que ha recibido desde la UPV, puede consultar los últimos mensajes que se le han enviado en el siguiente listado.

Tenga en cuenta que estos correos también han sido firmados digitalmente, de manera que puede comprobar su autenticidad desde su cliente de correo habitual.

Panel de Entrada

#	Asunto	Remitente	Fecha	Adjunto/s
---	--------	-----------	-------	-----------



CN = Proyectos OAI

O = Universitat Politècnica de València

L = Valencia

C = ES

Nombre RFC822=proyectos.oai@upv.es

Certificado

General Detalles Ruta de certificación



Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Protege los mensajes de correo electrónico
- 1.3.6.1.4.1.6449.1.2.1.1.1

* Para ver detalles, consulte la declaración de la entidad de ce

Emitido para: scert@upv.es

Emitido por: COMODO RSA Client Authentication and Secure Email CA

Válido desde 20/11/2017 **hasta** 21/11/2018

Tiene una clave privada correspondiente a este certificado.

Declaración del emisor

Aceptar

E = scert@upv.es

Nombre RFC822=scert@upv.es

Instant SSL
by **COMODO**

Low Cost
High Assurance
SSL Certificates

- REQUEST A CERTIFICATE
- DASHBOARD
- CERTIFICATES
 - Orders
 - Requests
 - Domains
 - Organizations
 - Orders Report
 - Expiring Certificates
- ACCOUNT
- SAML

Request a Certificate

- SSL Certificates
- Client Certificates**
- Grid Certificates
- Code Signing Certificates
- Document Signing Certificates

- Digital Signature Plus
- Email Security Plus
- Premium**

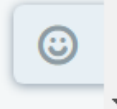
Premium

A DigiCert Premium Certificate provides secure email services and client authentication. Enable your clients to encrypt and digitally sign email communications.

Note: This certificate does not include private key escrow and recovery.

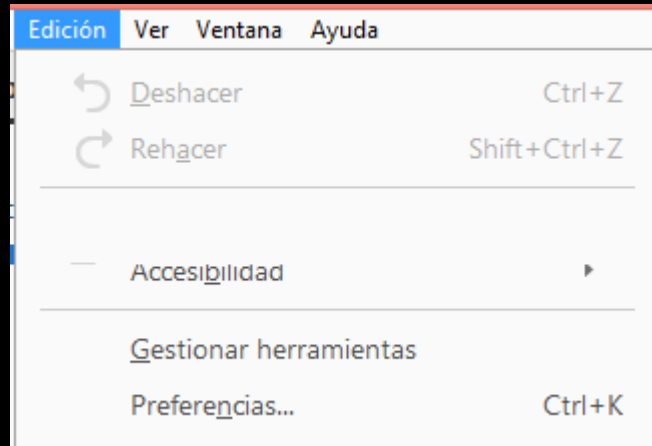
- Client authentication
- Document signing (with programs that support digital signatures. For programs that use the Adobe Approved Trust List, please utilize a Document Signing product)
- Email encryption
- Email signing

Order Now





Document Signing



revocación

revocación

CRL

revocación

CRL

OCSP

revocación

CRL

OCSP

OCSP Stapling

revocación

CRL

OCSP

OCSP Stapling

OCSP Must-Staple

OCSP Must-Staple

RFC 7633 (October 2015)

X.509v3 Transport Layer Security (TLS)

Feature Extension

OCSP Must-Staple

RFC 7633 (October 2015)

X.509v3 Transport Layer Security (TLS)

Feature Extension



OCSP Must-Staple

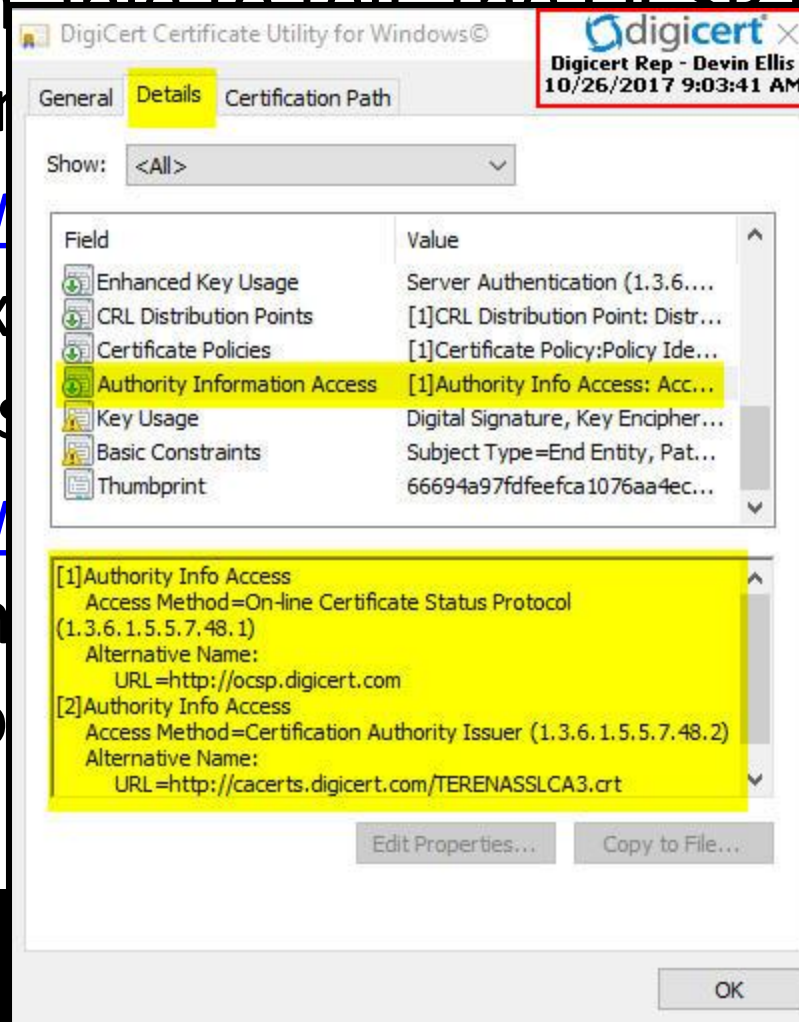


DigiCert: nivel 1

As far as I am able to tell, the OCSP is find and it does show on the certificate. First, if you go to <https://www.digicert.com/help/>, then enter in the domain xxxx.upv.es, you can see that the OCSP Staple status is good. 2nd, if you go to <https://www.digicert.com/util/> and download our Utility, then import your .pem certificate into the utility, you can view the certificate. While viewing ...

DigiCert: nivel 1

As far as I am able to tell, the OCSP is find and it does show on to <https://www.digicert.com> the domain x OCSP Staple s to <https://www.digicert.com> our Utility, th the utility, yo viewing ...



you go then enter in that the you go d download certificate into te. While

DigiCert: nivel 2

If does not look like we support that extension. Including it in the CSR is not an indicative way of getting it added with us. We do not rely on the CSR details when it comes to creating the certificate. We would rely on the account portal details and the extensions are not something that can be typically added or changed

DigiCert: nivel 3

As for knowing about OCSP Must Staple, yes we are aware of the feature and have decided not to include it at the moment. As for any future plans to include it, yes we currently do have plans for it to be made available for our customers.

Unfortunately with our current merger activities, it's not as high on the priority list as we'd like.

And unfortunately there is no deadline or ETA for this feature at this time.



Sobre el uso de certificados digitales



Red IRIS

Grupos de Trabajo 2017. Madrid



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Miguel Macías Enguïdanos