

Certificad0s Digital3s

F.N.M.T.

Universidad de Oviedo
Seguridad de Sistemas Informáticos

Mayo, 2017

Guillermo Facundo Colunga, Samuel Fernández Cabello,
Katia Fernández Fernández, Daniel González García y
Rubén Gutiérrez Guerrero

Contenidos

Introducción

Clave pública y privada

Certificados

- Anulación

- Renovación

Autoridades certificadoras

FNMT

- Certificados expedidos por la FNMT

Caso práctico

Introducción: certificados F.N.M.T.

Fábrica Nacional de Moneda y Timbre es Prestador de Servicios de Certificación.
Es capaz de expedir certificados.

Clave pública y privada

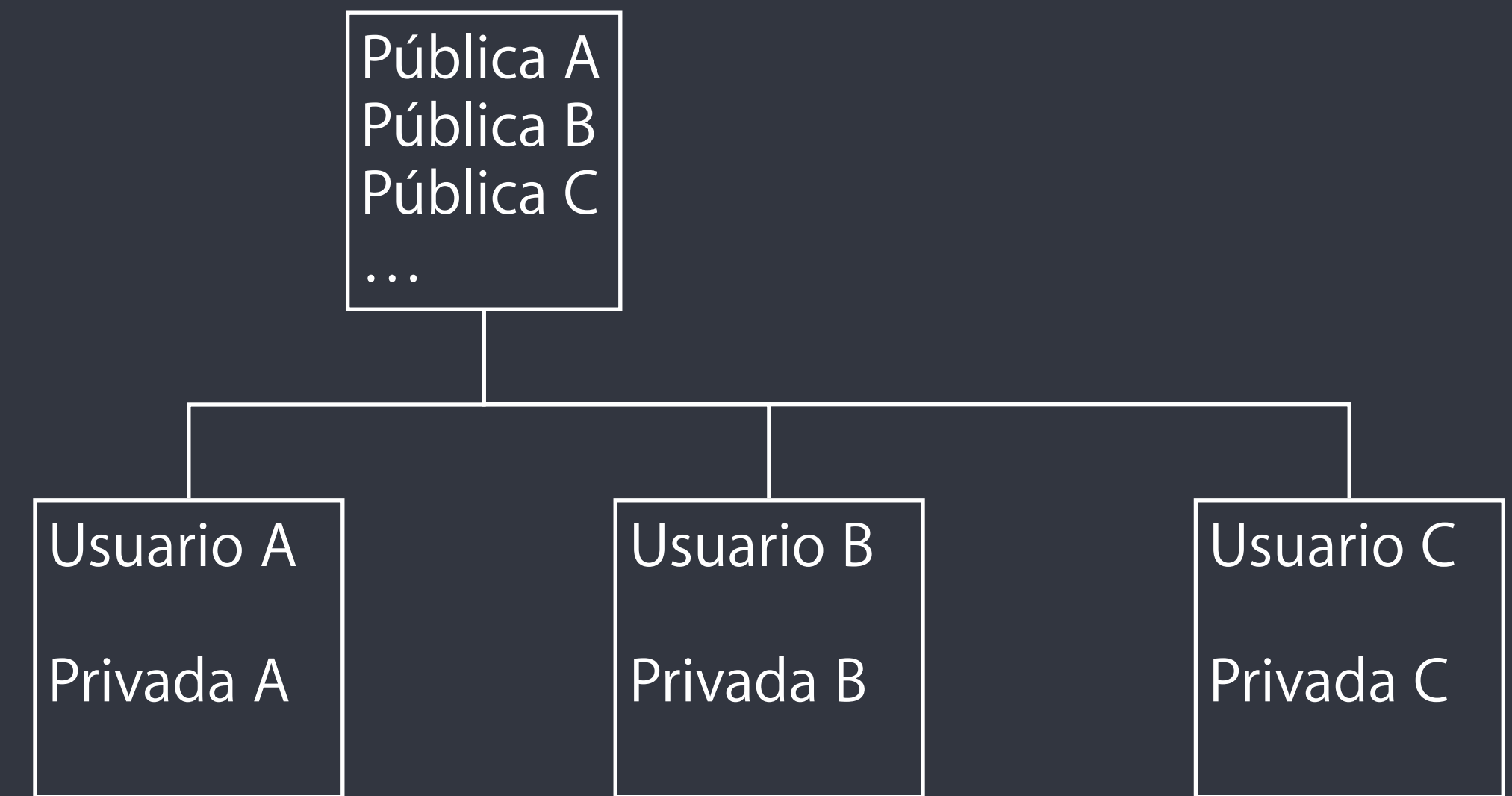
Envío de un mensaje desde A hasta C.

UsuarioA:

$C = \text{Cifrar}(M, \text{PúblicaC})$

UsuarioC:

$M = \text{Descifrar}(C, \text{PrivadaC})$



Caso práctico, ejemplo con RSA

1. Multiplicar dos números primos p y q : " $n=p*q$ ", así obtenemos n
2. Calculamos $\text{funcionEuler}(n)$ (Cálculo: $(p-1)(q-1)$) y buscamos un número e tal que:
 - 2.1. menor que $\text{funcionEuler}(n)$ y coprimo con $\text{funcionEuler}(n)$
 - 2.2. e será el exponente clave pública
3. Buscamos una d que satisfaga: $e*d \equiv 1 \pmod{\text{funcionEuler}(n)}$.
 - 3.1. d será el exponente de la clave privada.

Caso práctico, ejemplo con RSA

Siendo m un valor numérico:

Cifrado: $c = m^e \bmod(n)$

Descifrado: $m = c^d \bmod(n)$

Certificados, firmas, otros usos

Certificado: fichero que asegura que el contenido de un fichero es verídico. Consiste en una "firma" realizada por la unidad certificadora al fichero a certificar

Firma: Asegurar que nosotros hemos enviado el fichero -> encriptamos con la clave privada ya que SÓLO nosotros tenemos acceso a ella.

Envío pequeños por canales inseguros (Claves para encriptado simétrico, resúmenes [Hash's]...).

Anulación de certificados

El certificado tiene un período de validez

FNTM Usuarios, validez de 4 años

FNMT Clase 2, validez de 3 años

La autoridad certificadora conserva información

Estado de anulación

Condiciones para la anulación

Certificado dentro del período de validez

Persona con suficientes facultades de representación

Políticas y Prácticas de Certificación Particulares

Posee el certificado

Internet

No posee certificado

Oficina de Acreditación

Motivos de anulación de certificados

Recogidos en la "Declaración de Prácticas de Certificación":

- Defunción del suscriptor.

- Petición voluntaria.

- Cambios en los datos del suscriptor.

- Pérdida o daños en el soporte del certificado digital.

Autoridades certificadoras

Entidad de confianza

Verifica la identidad del solicitante

Verifica la validez de certificados

Autoridades certificadoras

Fábrica Nacional de Moneda y Timbre (FNMT)

Agencia Notarial de Certificación (ANCERT)

Autoridad de Certificación de la Abogacía (ACA)

Camerfirma

¿Qué es la F.N.M.T.?

Origen: Fusión de la Fábrica de Moneda y la Fábrica del Sello(1893)

Carácter: Servicio público. Colabora con entidades privadas en su seguridad y control de su producción.

Actividades de la F.N.M.T.

Fabrica: Monedas (circulantes y de colección), billetes de banco, papel de seguridad, documentos de identificación, productos gráficos, tarjetas, medallas...

Seguridad: aplicada en los procesos de producción, en los productos, en el tratamiento de la información, en las instalaciones...

CERES (CERTificación ESpañola)

Certificados que expide la F.N.M.T.

Persona física: Permite a un ciudadano realizar trámites de manera segura, a través de Internet.

Certificado de representante: Para relacionarse con entidades u organismos públicos bajo términos legales.

- Para administrador único o solidario

- Para persona jurídica

- Para Entidad sin Personalidad Jurídica

Certificados que expide la F.N.M.T. (II)

Administración pública: Certificado regulador de la administración pública

Certificado de componente: Da la confianza que acredita el certificado

- De servidor SSL/TLS, wildcard y SAN multidominio

- De sello de entidad

- Para firma de código

- De sede y sello para la administración pública

Obtener Certificado Personal



Guillermo Facundo Colunga



Guillermo Facundo Colunga

Consideraciones Previas

Todo el proceso desde mismo equipo

No formatear el ordenador

No actualizar durante el proceso

Internet Explorer o Firefox

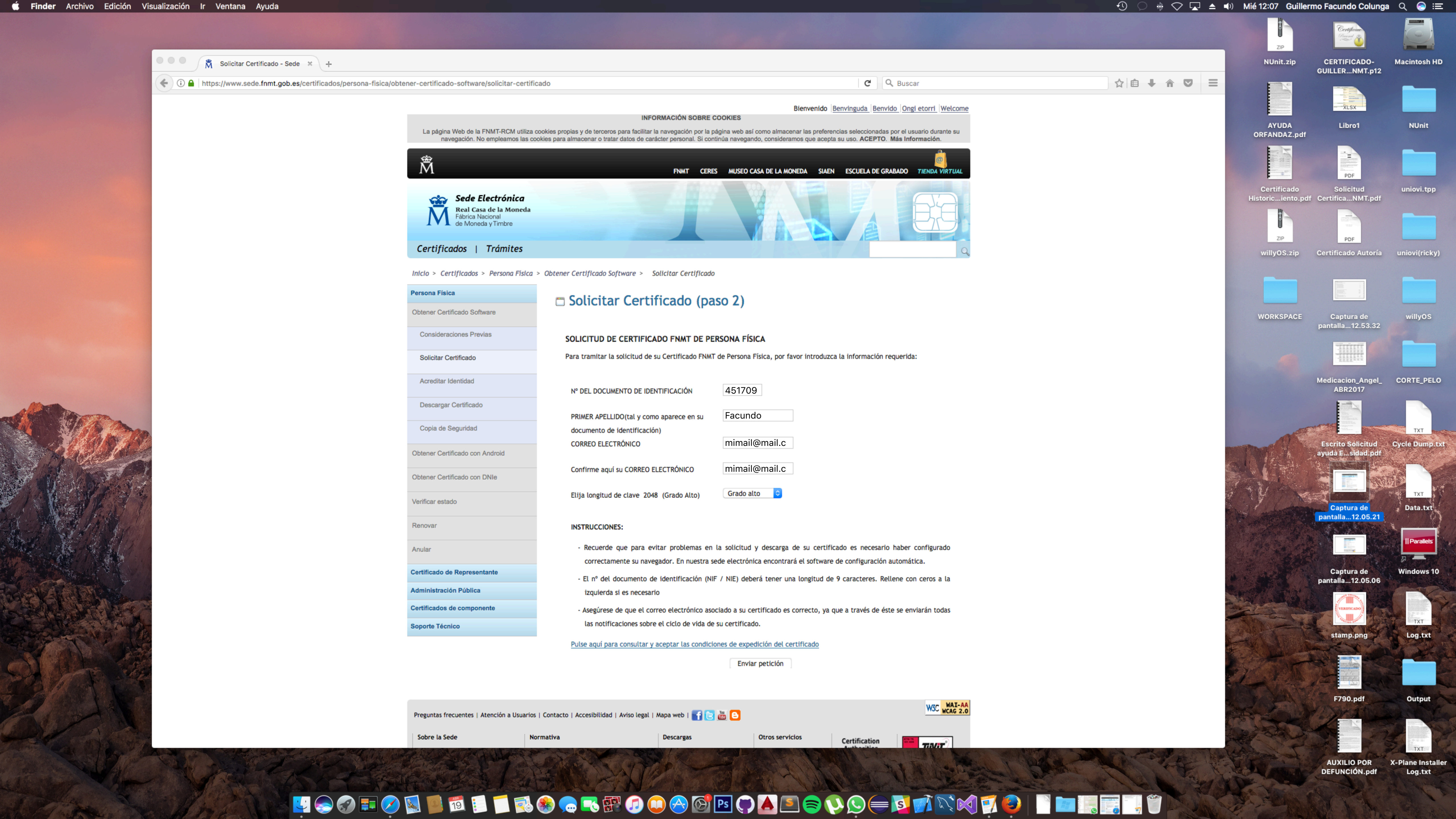
Añadir confianza en certificados de la FNMT

AC Raíz FNMT-RCM

FNMT Clase 2 CA

AC FNMT Usuarios

AC Componentes Informáticos





Guillermo Facundo Colunga

Estimado/a Sr/a Facundo

A continuación le facilitamos el CÓDIGO DE SOLICITUD del Certificado FNMT de Persona Física que nos ha solicitado:

918273465

NIF asociado a la solicitud:

45170929X

Con este Código de Solicitud y la documentación de su identidad requerida, deberá personarse en cualquiera de las Oficinas de Registro Autorizadas por la FNMT-RCM para acreditar su identidad. Para su comodidad, puede usted hacer uso de nuestro servicio de localización de las Oficinas más cercanas, que encontrará en nuestra Sede Electrónica en ACREDITAR SU IDENTIDAD.

Por favor verifique que los datos que introdujo en la fase de solicitud (nº de documento de identificación y primer apellido), se corresponden exactamente con los que figuran en el documento de identidad que utilizará para acreditarse en una de nuestras Oficinas de Registro. Si detecta cualquier error en los mismos, deberá generar una nueva solicitud.

Así mismo le recordamos que con la emisión de su nuevo certificado FNMT de Persona Física, el solicitante autoriza a la FNMT-RCM a revocar y dejar sin efecto cualquier certificado del mismo tipo que la FNMT-RCM le haya emitido con carácter previo e idénticos nombre, apellidos y NIF/NIE.

Agradecemos sinceramente su interés por nuestros certificados.



Guillermo Facundo Colunga

Acreditar Identidad

Personarse en oficinas más cercanas

Presentar Código de Solicitud + DNI



Guillermo Facundo Colunga

Acreditar Identidad


Personarse en oficinas más cercanas
Presentar Código de Solicitud + DNI

Descargar Certificado

Disponible en 1h
Avisan por email y SMS



Guillermo Facundo Colunga



FACUNDO COLUNGA GUILLERMO - 45170929X
Emitido por: AC FNMT Usuarios
Caduca: lunes, 5 de abril de 2021, 13:36:13 (hora de verano de Europa central)
✖ Este certificado ha sido firmado por un emisor no fiable

► Confiar

▼ Detalles

Nombre del sujeto

País ES

Número de serie IDCES-45170929X

Nombre de pila GUILLERMO

Apellidos FACUNDO COLUNGA

Nombre común FACUNDO COLUNGA GUILLERMO - 45170929X

Nombre del emisor

País ES

Empresa FNMT-RCM

Unidad organizativa Ceres

Nombre común AC FNMT Usuarios

Número de serie

Versión 3

Algoritmo de firma SHA-256 con encriptación RSA (1.2.840.113549.1.1.1)

Parámetros ninguno/a

No válido antes de

No válido después de

miércoles, 5 de abril de 2017, 13:36:13 (hora de verano de Europa central)

lunes, 5 de abril de 2021, 13:36:13 (hora de verano de Europa central)

Información de la clave pública

Algoritmo Encriptación RSA (1.2.840.113549.1.1.1)

Parámetros ninguno/a

Clave pública 256 bytes: CC 26 09 E8 D2 44 AF ED ...

Exponente

Tamaño de la clave 2048 bits

Uso de la clave Encriptar, Verificar, Ajustar, Derivar

Firma

Extensión

Crítico

Uso

Uso de la clave (2.5.29.15)

Sí

Firma digital, Sin rechazo, Encriptación de la clave

Extensión

Crítico

Entidad de certificación

Restricciones básicas (2.5.29.19)

Sí

NO

Casos Prácticos

Certificad0s Digital3s

F.N.M.T.

Universidad de Oviedo
Seguridad de Sistemas Informáticos

Mayo, 2017

Guillermo Facundo Colunga, Samuel Fernández Cabello,
Katia Fernández Fernández, Daniel González García y
Rubén Gutiérrez Guerrero