RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Conceptos Básicos PKI

Maria Paula Encinas Zevallos
Analista de Servicios PKI

GERENCIA DE CERTIFICACIÓN Y REGISTRO DIGITAL
SUB GERENCIA DE CERTIFICACIÓN E IDENTIDAD DIGITAL

MARZO 2018

Contenido

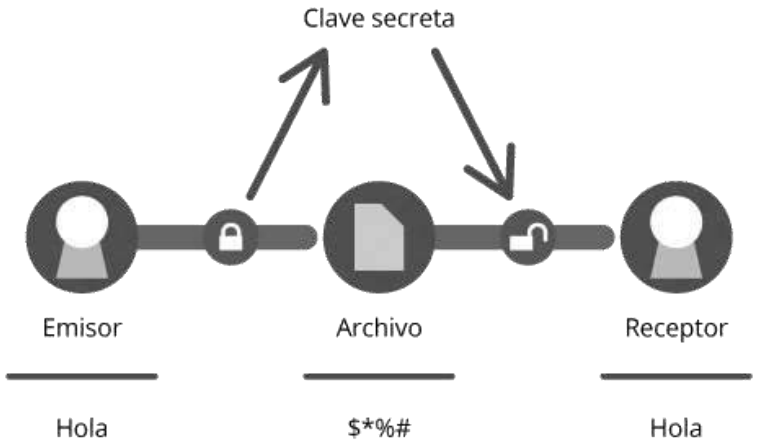
1. Criptografía simétrica y asimétrica
2. Par de llaves y certificado digital
3. Firma Digital
4. Cifrado con llave pública
5. Validación: CRL y OCSP
6. Jerarquías PKI del RENIEC
7. Autoridades PKI
8. Object Identifier (OID)

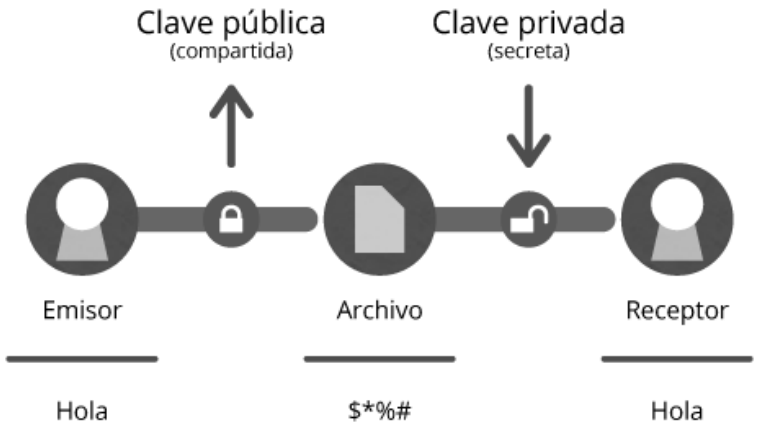
Criptografía

criptografía

Del gr. κρυπτός *kryptós* 'oculto' y *-grafía*.

1. f. Arte de escribir con clave secreta o de un modo enigmático.

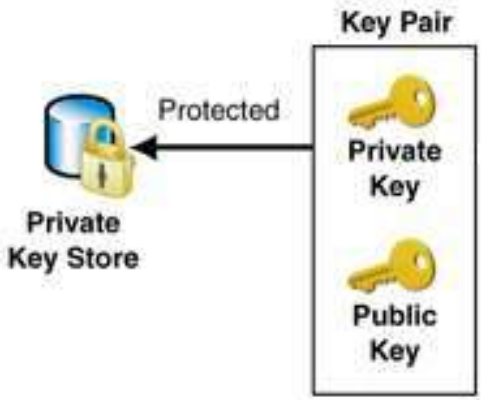




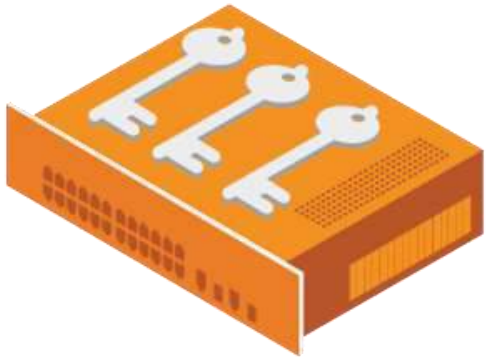
Algoritmos de generación de llaves

a) **Criptografía Simétrica**
   - AES (Rijndael): 128 bits
   - DES: 56 bits
   - 3DES: 168 bits
   - Blowfish: 64 bits
b) **Criptografía ASimétricas**
   - RSA: 1024, 2048, 4096 bits
   - ECC: 256, 512 bits

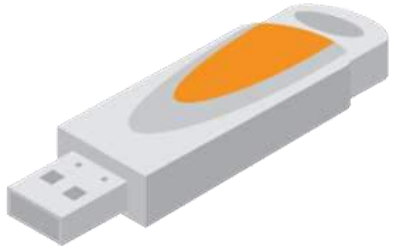
Par de llaves asimétricas: contenedores



HSM



Token



Smartcard

SO Windows

Keystore

CSR: Certificate Signing Request (RFC 2986)

RFC2986: PKCS#10 Synxtax

```
CertificationRequest ::= SEQUENCE {
     certificationRequestInfo CertificationRequestInfo,
     signatureAlgorithm AlgorithmIdentifier{{ SignatureAlgorithms }},
     signature          BIT STRING
}
```

```
CertificationRequestInfo ::= SEQUENCE {
     version       INTEGER { v1(0) } (v1,...),
     subject       Name,
     subjectPKInfo SubjectPublicKeyInfo{{ PKInfoAlgorithms }},
     attributes    [0] Attributes{{ CRIAttributes }}
}

SubjectPublicKeyInfo { ALGORITHM : IOSet} ::= SEQUENCE {
     algorithm        AlgorithmIdentifier {{IOSet}},
     subjectPublicKey BIT STRING
}
```

reniec1.csr

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEYzCCAksCAQAwHjELMAkGA1UEBhMCUEUxDzANBgNVBAMMBlJlbmllYzCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBAJiwLILP1G4He5Y9mKBorQwHo7v8hhceW/8KiI2kNgcxWQaB9WZY
9THbzcDiqg7LAZsfGVL1Iy/YEGlAfOciPukPx3J/tMQmfqt7Gre0oghZMNxgly/gxgiK6CiSfcn8
bWjmYzuvQLeDZ728ePBZ1+8HlfmzWfOpFNlFT/VRSMTP8dQIYWpann4avUYpeS6Tf46YAniI2K31
NqM/vzcz2G50bdKHez/I2xWS/s6yOvN0s0IKH82uX0+xnG5emuUzWLp+wjBpHS7YAtsjg/9d/62A
PIkm4fWpDGPzOUwgBHpYa1r1dLV+MQjlEmdg5XcgeQQ3xOjt9mDrMbsEEIrrDDQz60QWQCuCooQ6
2U2UmtjpP5X+OEkHFj2N38IQRlHM5G66EHnwKjdvtGQaYucbfSplRrcbF51NMIrxfS5g2qhSyeEp
QLORUq32yC1G24Oxu9iJMn4DSoL7/3EIm6ZFVjtA0jXVa6JPRj5bm9datJQJ8Bnb00Rty5aU2DLh
K9+N7XSeMoICKpyXxH9jzuc7aOW3bw1GCtzBR7PgpbJA5hvWU8VjCzduRbPIAA9YgUlN7UjNWLGS
vd1JCStE0JxkcgX3Ygan6nLVoiRDk/FvPkcRCGv8K8M38Yhf47tsQTJSrW2CudfGwvD2rMhB5cEM
lSnDQETVDdJAewiw7L/wWJrrAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAgEATjXss5/9LOvGXZag
Xl1BwkpimAYieM/O3o2FIg7oRD80xi3vaH32S+PpN11gbCN1p7UVU2atkOo5zQfUtliSvIKgClP2
DJfjGyuUDvyqHDAS0aQsZ3FhQjEZj9xEVPdD3M13v4WIG9J90WtZzgToRuK9pzcSV+kFna8mCB20
CrdBhsnuADTErGqbHf/ttTzj5yvGYnWolpFTbh4UvaQtO2qBwKk6RyLNizwbWiFXCU773My/MqzB
0Z7pucvmigBY2Iw9yGjqq1iPlojmedsAQhj0WqdkZ490xRlv2xTDEatQNMtexVlLBra201V6CjXH
62jKZqNC/jJY1oFvV+bW5QmjLYRZNWFnlp0j+Ii/10ItV1dnP0n6rXlkTkCvljQ4n0W+jZacZN82
gLb8MlhRrW2jsevyTO+7SkDhayTfUqikHonTpaywB5NQrw6Zxv2CExqLcmxpRJ9i56nEZWDTVXLm
X529//sqEsZ/aVTeU8ZEEY915xPwtSPXr1GZ3fxkxR1dN+lpe2osgtQ3+AFXyQm5l0cjJmehryoW
9ZE3JvWBUj81//VvlpH97Ex1kOBtN6+rQ6qzSZSsQvo8HpzuFVFFAcVJlX02nOrMlcfUMY6X8tOH
EhCwt2+9TtzKlRHHGrhJTrQO5kkZJ3aKL94eu+qXlrp67+VFjOpSq8g5/j0=
-----END CERTIFICATE REQUEST-----
```

Algoritmo de firma

- Rsa-with-sha-1
- Familia rsa-with-sha2 → rsa-with-sha256, rsa-with-sha384, rsa-with-sha512

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3TCCAcUCAQAwgZcxCzAJBgNVBAYTAlBFMRIwEAYDVQQIDAlMaW1hLUxpbWExDTALBgNVBAcM
BExpbWExDzANBgNVBAoMBlJFTklFQzEOMAwGA1UECwwFU0dDSUQxDTALBgNVBAsMBEdSQ0QxNTAz
BgNVBAMMLEFnZW50ZSBBdXRvbWF0aXphZG8gLSBEb21pY2lsaW8gRWxlY3Ryw7NuaWNvMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqvgV3wQaHdfcmyVcQX+4EUVu4FP8n11tslB6o0m1
AniOTrEDFjll1kYwBpi1T6gYCwMISm1TMWUE6v5QYRJD4N2Jnm9XsX9l0WBGYTZu6C6fPzOhfk1n
U0Mb22rXN6r6EO2vl7oEWAyeVDqehvQu2nkJusC25a76BDs8Y9oi8pN3N3q7DRvp/bZPVYyvollm
GMvUXuk8YcBPBv+aD4H54DwHQMEQT/TCVQJXXLYxEcmkXSSOg1Y5STmhYTKqZcfTR0EkTD7C3BKo
YuUQfPxFhuvGXPICWrQ0LjxMQaOG5BKgQ4H9sN2t0D66JF4D4mVnuywS9Hv4OGOBelgWgcH22QID
AQABoAAwDQYJKoZIhvcNAQELBQADggEBAKD0SzW0lE9vUr9qba3eA7bhWH2E2jC1ulkVHaa7bNS1
gNq+heTX3TowtTGwn8EZ1bWulXvV0lCW5waCsgvnm9p3Dhs1xtRzsdakfWjqOJ/jcDfWc7rgvzkE
FdKj2Kcpk/AK1BmTmu76ZTGhIpamT2tSiB1gwkvbWTUdyogqYCkmvlBdYaSolE0+8ZNEhe2T8A/V
jBGwq/At8XojD2P1Vc6zfcBl05IRJfi3WlyfhNvA4J9kjvYWSdcnyODMpRMmmHq+R7myuW6djjr+
Yvc7Bd1hJup+leBrduqplrbHXu86OO4kssdgElBKuga3EVuqrOAaTGXlsXJMulACkG8vl7M=
-----END CERTIFICATE REQUEST-----
```

CSR Contents

CSR Checks

Signature:	✔ Signature is valid.
Debian Weak Key:	✔ No Debian weak key detected.

Subject

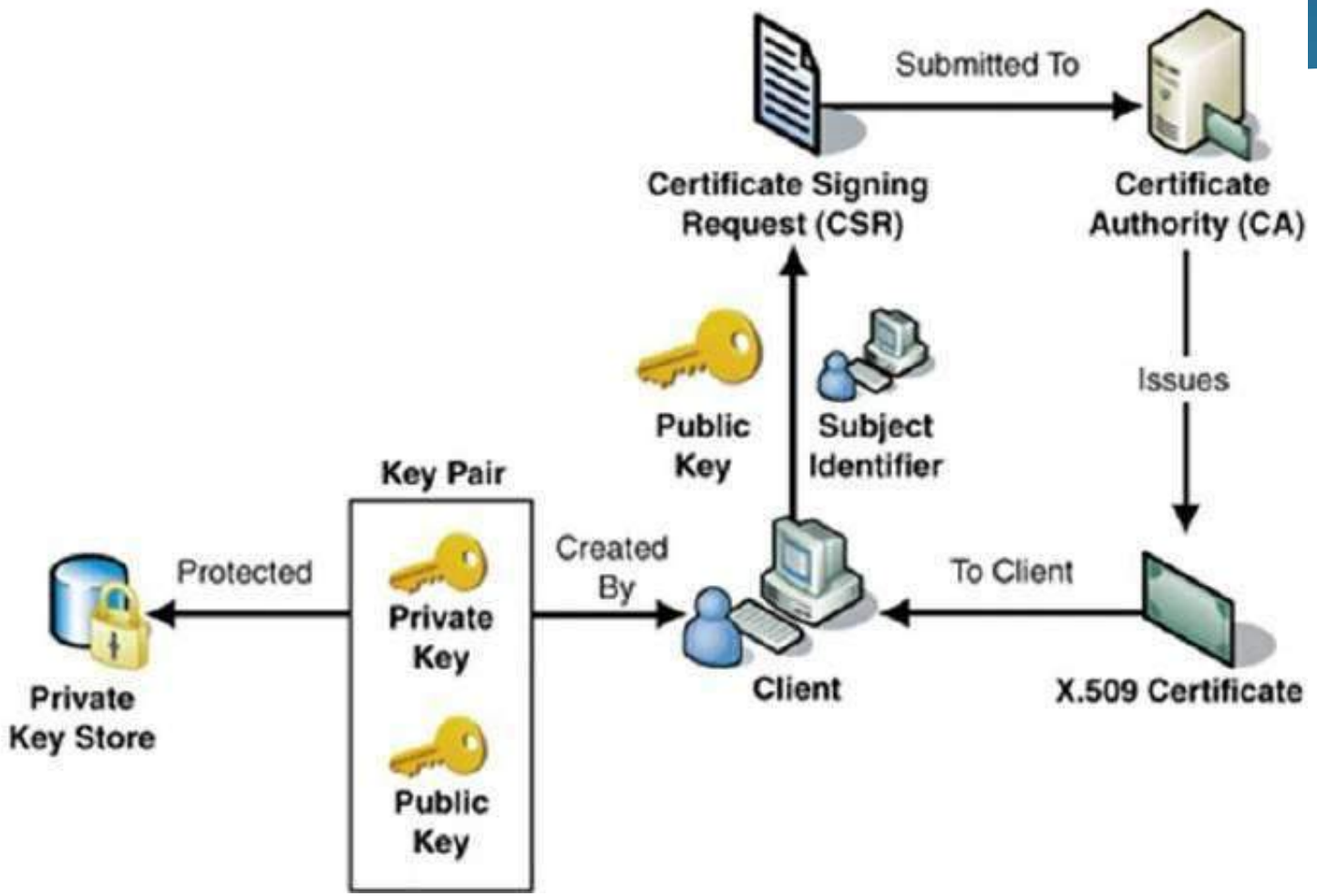
Common Name:	Agente Automatizado - Domicilio Electrónico
Organizational Unit:	SGCID
Organization:	RENIEC
Locality:	Lima
State:	Lima-Lima
Country:	PE

Properties

Key Type:	RSA
Key Size:	2048
Signature Type:	sha256WithRSAEncryption

http://www.entrust.net/ssl-technical/csr-viewer.cfm

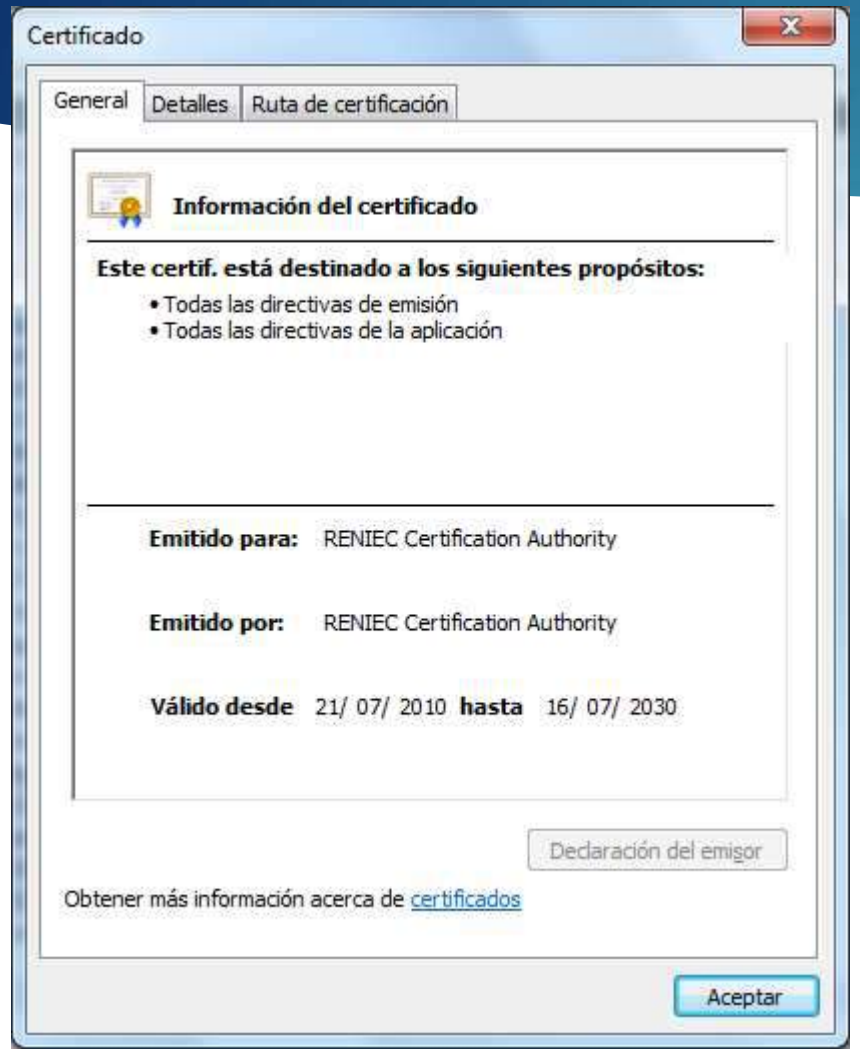
Certificado digital

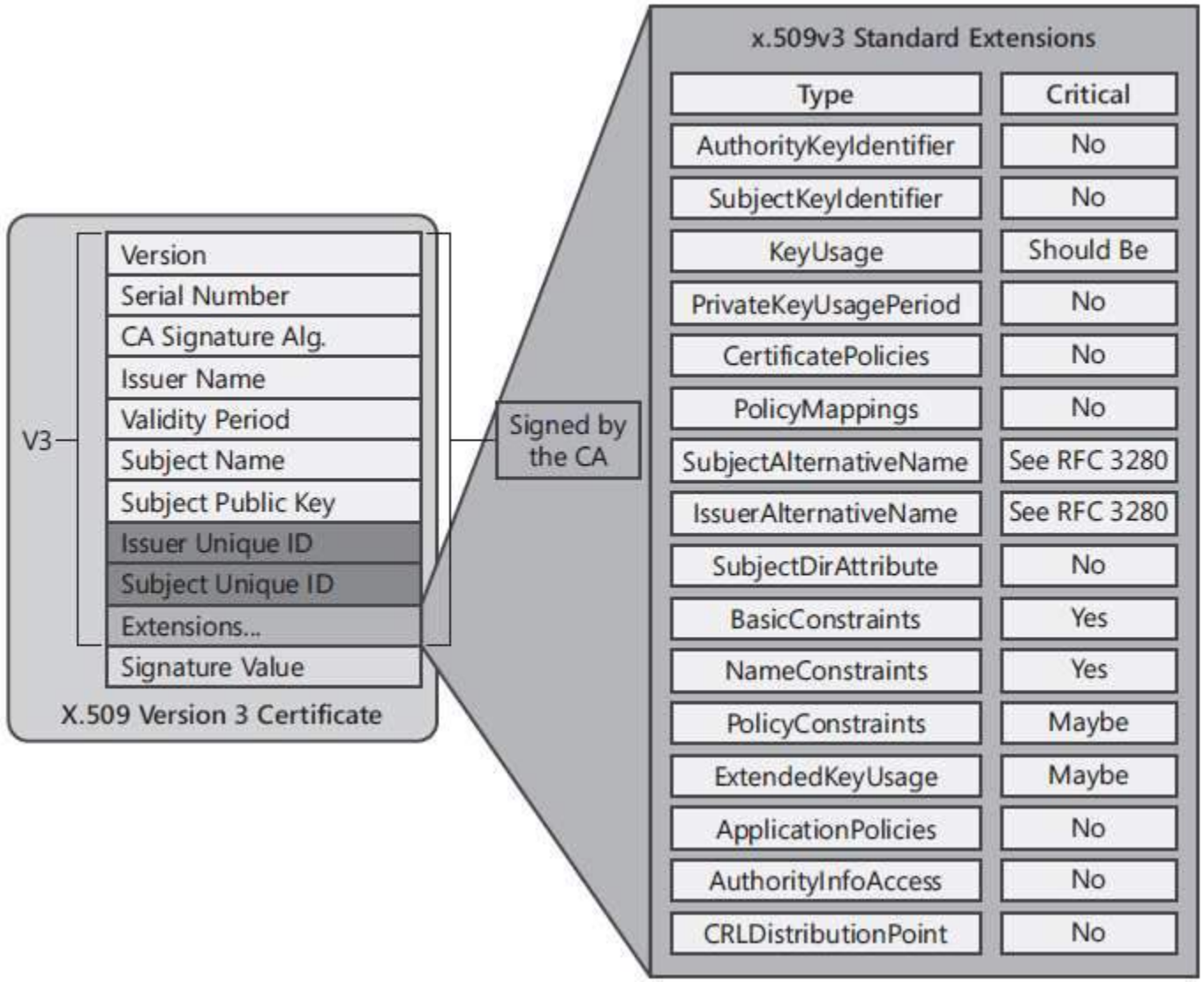


Algoritmo de firma

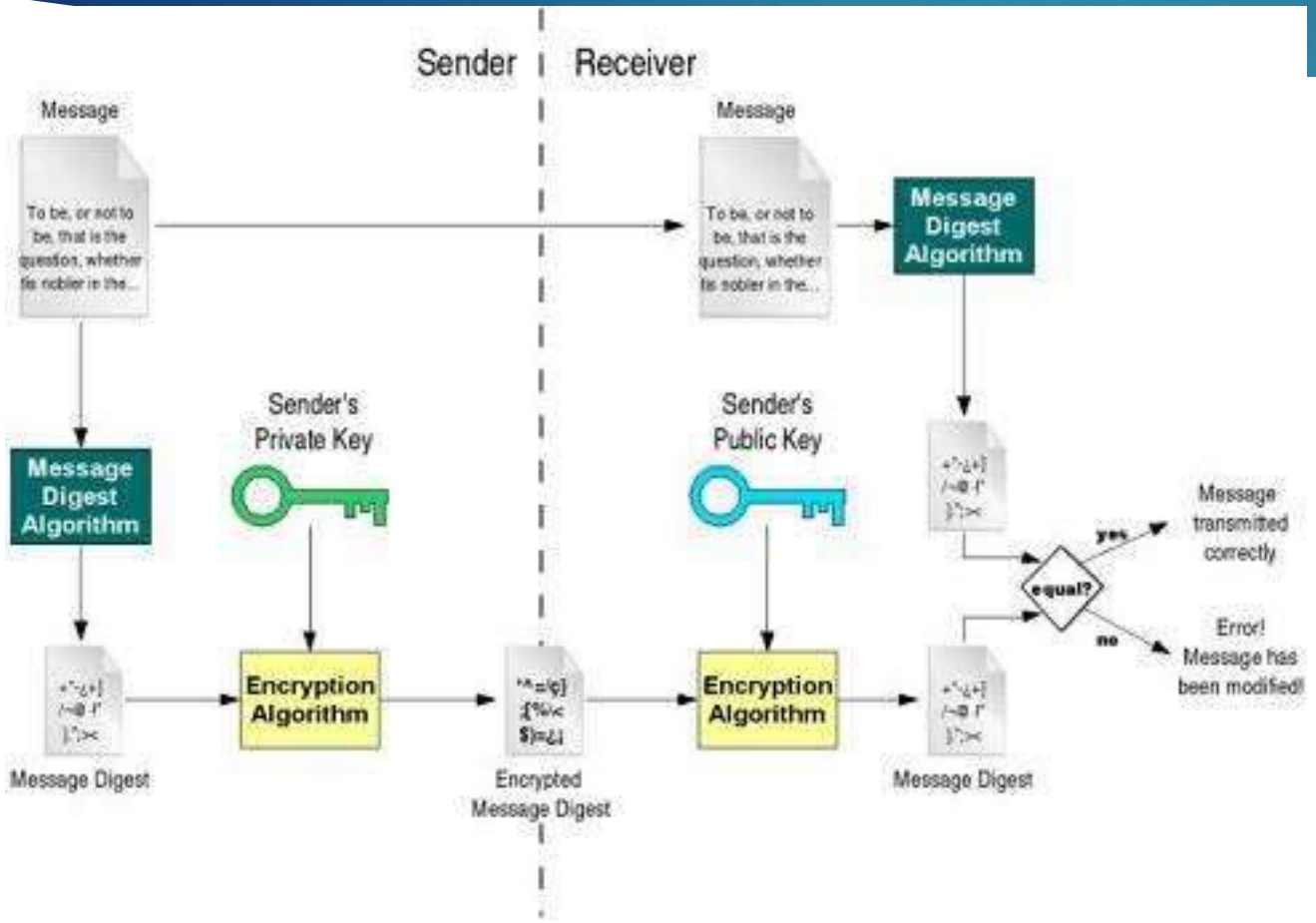
- Rsa-with-sha-1
- Familia rsa-with-sha2

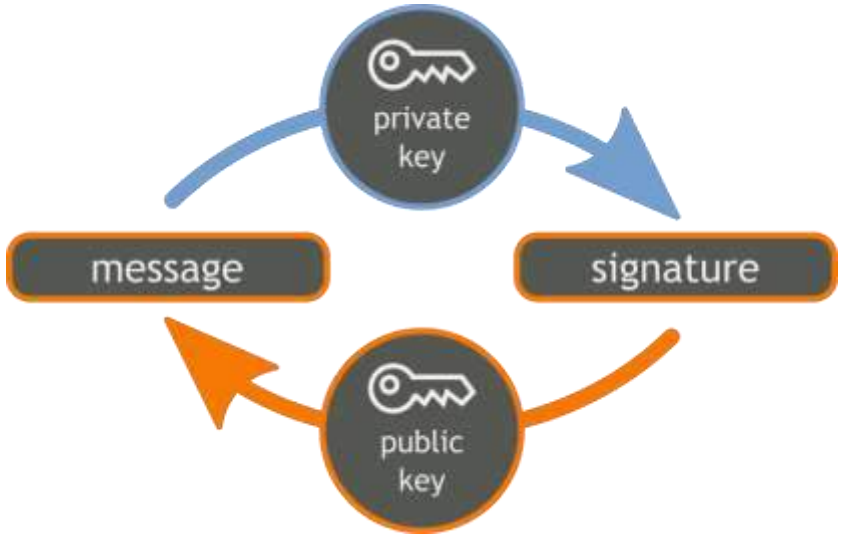
Certificado Digital X.509 versión 3 (RFC 5280) / ITU-T X.509



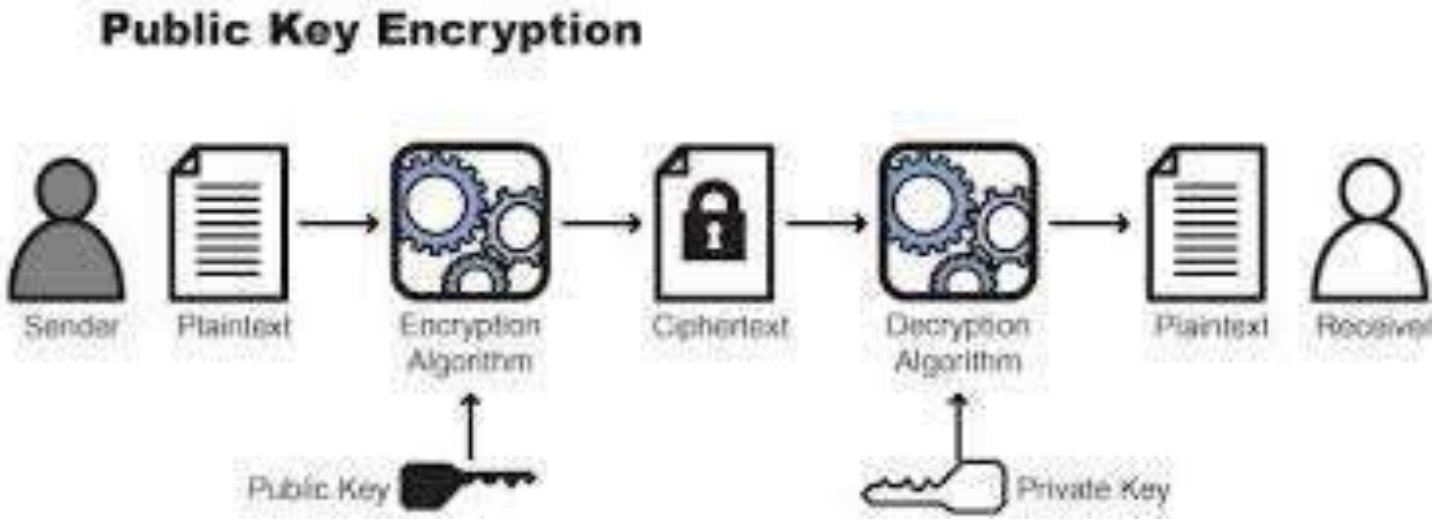


Firma Digital





Cifrado con llave pública



CRL: Certificate Revocation List (RFC 5280)

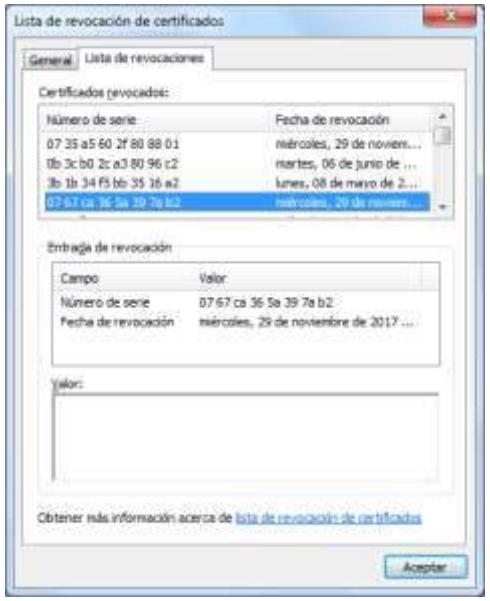
Buscar en la CRL

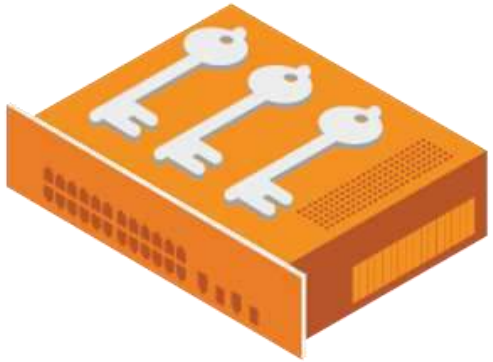
1C721028B75E6F08

Respuesta

- **Presente: Cancelado**
- **Ausente: No cancelado**

CRL



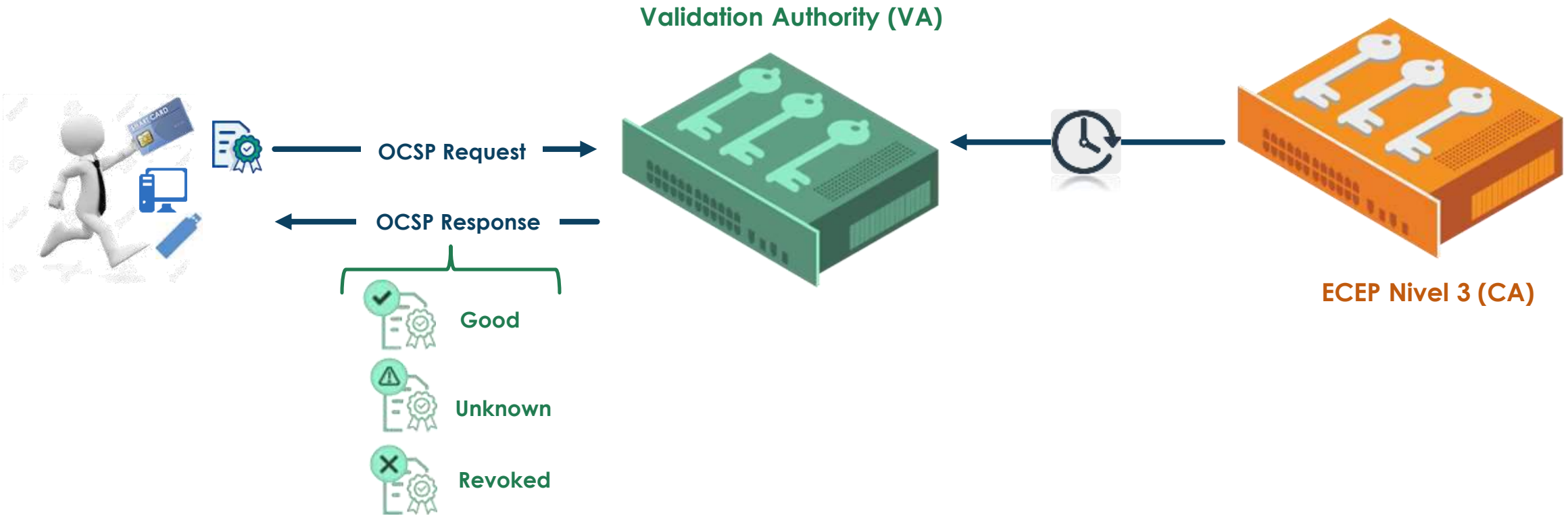


ECEP Nivel 3 (CA)

CRL: Certificate Revocation List (RFC 5280)

Nivel	Emisor	Cancela Certificados	Frecuencia
2	ECEP-RENIEC	ECEP-RENIEC CA Class {1, 2, 3, 4}	6 meses
3	ECEP-RENIEC CA Class {1, 2, 3, 4}	Entidad Final	24 horas

OCSP: On-line Certificate Status Protocol (RFC 6960)



Autoridades PKI

- CA: Certification Authority → EC: Entidad de Certificación
- RA: Registration Authority → ER: Entidad de Registro
- VA: Validation Authority → Servicio CRL o servicio OCSP
- TSA: Time Stamping Authority → PSVA- TSA: Prestador de Servicios de Valor Añadido en Modalidad de Sellado de Tiempo

Object Identifier (OID)

Private Enterprise Number (PEN) Modification Request

This is a request to modify the information associated with an existing registered Private Enterprise Number (PEN
will be asked to confirm any changes.

THIS IS NOT A REQUEST FOR A NEW PRIVATE ENTERPRISE NUMBER ASSIGNMENT.

Upon receipt, a confirmation request will be sent to the contact email provided below and the listed email address
provided below). Once these changes are verified, an activation URL will be sent to the email address provided b
indicated with an asterisk (*).

Registered PEN: 35300

Organization

Organization Name: * REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO

Organization Address: *
Avenida Bolivia Nº 144.
Torre Centro Cívico.
Lima 01.
PERÚ.

Organization Phone: (00511) 315 – 2700.

Contact

Contact Name: * Ricardo Saavedra Mavila

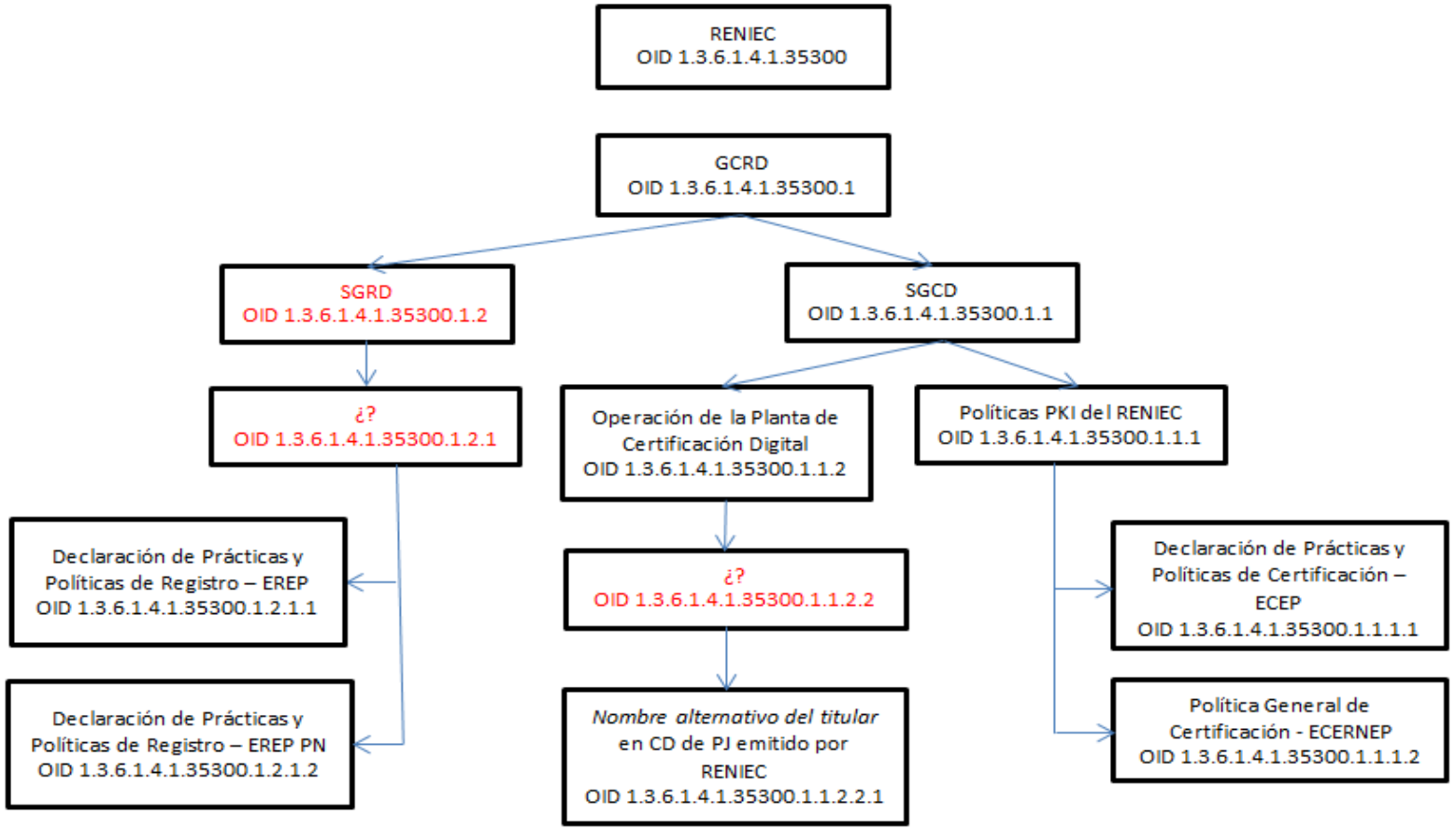
Contact Address:
Avenida Bolivia Nº 144.
Torre Centro Cívico.
Lima 01.
PERÚ.

Contact Phone: (00511) 315 – 2700, extension 1192.

Contact Fax: (00511) 332 – 0172.

Contact Email: * iana@pkiep.reniec.gob.pe

OID Jerarquías SHA1 y SHA2



OID Jerarquía ROOT 3

X =1, OIDs PKI
Y = 3, Jerarquía ECERNEP PERÚ CA Root 3
La forma de OIDs propuesta para la nueva jerarquía PKI es: **1.3.6.1.4.1.35300.2.1.3.A.B.C.D.E**, tomando los valores que se indican, a

OID Jerarquía ROOT 3

A: Infraestructura
○ A = 1, certificados digitales producción
○ A = 2, TSA
○ A = 3, OCSP
○ A = 4, certificados digitales para pruebas

B: SubCAs online dentro de la infraestructura (Clases)
○ B = 0, no hay SubCA *online* que emita al certificado identificado
○ B = 1, CA Class 1
○ B = 2, CA Class 2
○ B = 3, CA Class 3
○ B = 4, CA Class 4

C: Tipo de documento normativo
○ C = 101, CP de la ECERNEP
○ C = 102, CPS de la ECERNEP
○ C = 103, CPS de la ECEP-RENIEC
○ C = 104, Política de la EC-PSVA
○ C = 105, Declaración de Prácticas de la PSVA-TSA-RENIEC

D: Tipo de Certificado
○ D = 1000, Documento (NO certificado digital)
○ D = 1001, Firma (FIR)
○ D = 1002, Autenticación (AUT)
○ D = 1003, Firma y Autenticación (FAU)
○ D = 1004, Cifrado (CIF)
○ D = 1005, Agente Automatizado (AA)
○ D = 1006, Domain Controller (DC)
○ D = 1007, SSL/TLS
○ D = 1008, SSL/TLS con EV
○ D = 1009, sellador PSVA-TSA
○ D = 1010, OCSP responder

E: Tipo de Contenedor criptográfico
○ E= 0, Sin Contenedor (Documento)
○ E= 1, Contenedor Software
○ E= 2, Contenedor Hardware
○ E= 3, Contenedor no declarado (solamente Clase 4)

OID Jerarquía ROOT 3

N°		Contenedor	OID	Descripción
Documentos				
1		doc	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	CP de la ECERNEP
2		doc	1.3.6.1.4.1.35300.2.1.3.1.0.102.1000.0	CPS de la ECERNEP
3		doc	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	CPS de la ECEP-RENIEC
4		doc	1.3.6.1.4.1.35300.2.1.3.2.0.105.1000.0	Declaración de Prácticas de la PSVA-TSA-RENIEC
Certificados				
1	FAU	soft	1.3.6.1.4.1.35300.2.1.3.1.1.103.1003.1	Class 1 – Certificado digital de firma y autenticación (FAU)
2	FAU	hard	1.3.6.1.4.1.35300.2.1.3.1.1.103.1003.2	Class 1 – Certificado digital de firma y autenticación (FAU)
3	P_FAU	soft	1.3.6.1.4.1.35300.2.1.3.4.1.103.1003.1	Class 1 – Certificado digital para pruebas de firma y autenticación (P_FAU)
4	P_FAU	hard	1.3.6.1.4.1.35300.2.1.3.4.1.103.1003.2	Class 1 – Certificado digital para pruebas de firma y autenticación (P_FAU)
5	FIR	hard	1.3.6.1.4.1.35300.2.1.3.1.2.103.1001.2	Class 2 – Certificado Digital de firma (FIR)
6	AUT	hard	1.3.6.1.4.1.35300.2.1.3.1.2.103.1002.2	Class 2 – Certificado digital de autenticación (AUT)
7	CIF	hard	1.3.6.1.4.1.35300.2.1.3.1.2.103.1004.2	Class 2 – Certificado digital de cifrado (CIF)
8	P_FIR	hard	1.3.6.1.4.1.35300.2.1.3.4.2.103.1001.2	Class 2 – Certificado digital para pruebas de firma (P_FIR)
9	P_AUT	hard	1.3.6.1.4.1.35300.2.1.3.4.2.103.1002.2	Class 2 – Certificado digital para pruebas de autenticación (P_AUT)
10	P_CIF	hard	1.3.6.1.4.1.35300.2.1.3.4.2.103.1004.2	Class 2 – Certificado digital para pruebas de cifrado (P_CIF)

OID Jerarquía ROOT 3 (parte 2)

11	FAU	soft	1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.1	Class 3 – Certificado digital de firma y autenticación (FAU)
12	FAU	hard	1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.2	Class 3 – Certificado digital de firma y autenticación (FAU)
13	CIF	soft	1.3.6.1.4.1.35300.2.1.3.1.3.103.1004.1	Class 3 – Certificado digital de cifrado (CIF)
14	CIF	hard	1.3.6.1.4.1.35300.2.1.3.1.3.103.1004.2	Class 3 – Certificado digital de cifrado (CIF)
15	P_FAU	soft	1.3.6.1.4.1.35300.2.1.3.4.3.103.1003.1	Class 3 – Certificado digital para pruebas de firma y autenticación (P_FAU)
16	P_FAU	hard	1.3.6.1.4.1.35300.2.1.3.4.3.103.1003.2	Class 3 – Certificado digital para pruebas de firma y autenticación (P_FAU)
17	P_CIF	soft	1.3.6.1.4.1.35300.2.1.3.4.3.103.1004.1	Class 3 – Certificado digital para pruebas de cifrado (P_CIF)
18	P_CIF	hard	1.3.6.1.4.1.35300.2.1.3.4.3.103.1004.2	Class 3 – Certificado digital para pruebas de cifrado (P_CIF)
19	AA	-	1.3.6.1.4.1.35300.2.1.3.1.4.103.1005.3	Class 4 – Certificado Digital de agente automatizado (AA)
20	DC	-	1.3.6.1.4.1.35300.2.1.3.1.4.103.1006.3	Class 4 – Certificado digital de controlador de dominio (DC)
21	SSL	-	1.3.6.1.4.1.35300.2.1.3.1.4.103.1007.3	Class 4 – Certificado digital SSL (SSL)
22	P_AA	-	1.3.6.1.4.1.35300.2.1.3.4.4.103.1005.3	Class 4 – Certificado digital para pruebas de agente automatizado (P_AGA)
23	P_DC	-	1.3.6.1.4.1.35300.2.1.3.4.4.103.1006.3	Class 4 – Certificado digital para pruebas de controlador de dominio (P_DC)
24	P_SSL	-	1.3.6.1.4.1.35300.2.1.3.4.4.103.1007.3	Class 4 – Certificado digital para pruebas de SSL (P_SSL)
25	TSA	hard	1.3.6.1.4.1.35300.2.1.3.2.0.105.1009.2	Certificado digital de TSA sellador
26	OCSP	hard	1.3.6.1.4.1.35300.2.1.3.3.1.103.1010.2	Class 1 - Certificado digital de OCSP responder (OCSP)
27	OCSP	hard	1.3.6.1.4.1.35300.2.1.3.3.2.103.1010.2	Class 2 - Certificado digital de OCSP responder (OCSP)
28	OCSP	hard	1.3.6.1.4.1.35300.2.1.3.3.3.103.1010.2	Class 3 - Certificado digital de OCSP responder (OCSP)
29	OCSP	hard	1.3.6.1.4.1.35300.2.1.3.3.4.103.1010.2	Class 4 - Certificado digital de OCSP responder (OCSP)

¡Gracias!