RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Jerarquías PKI del Estado Peruano

Maria Paula Encinas Zevallos
Analista de Servicios PKI

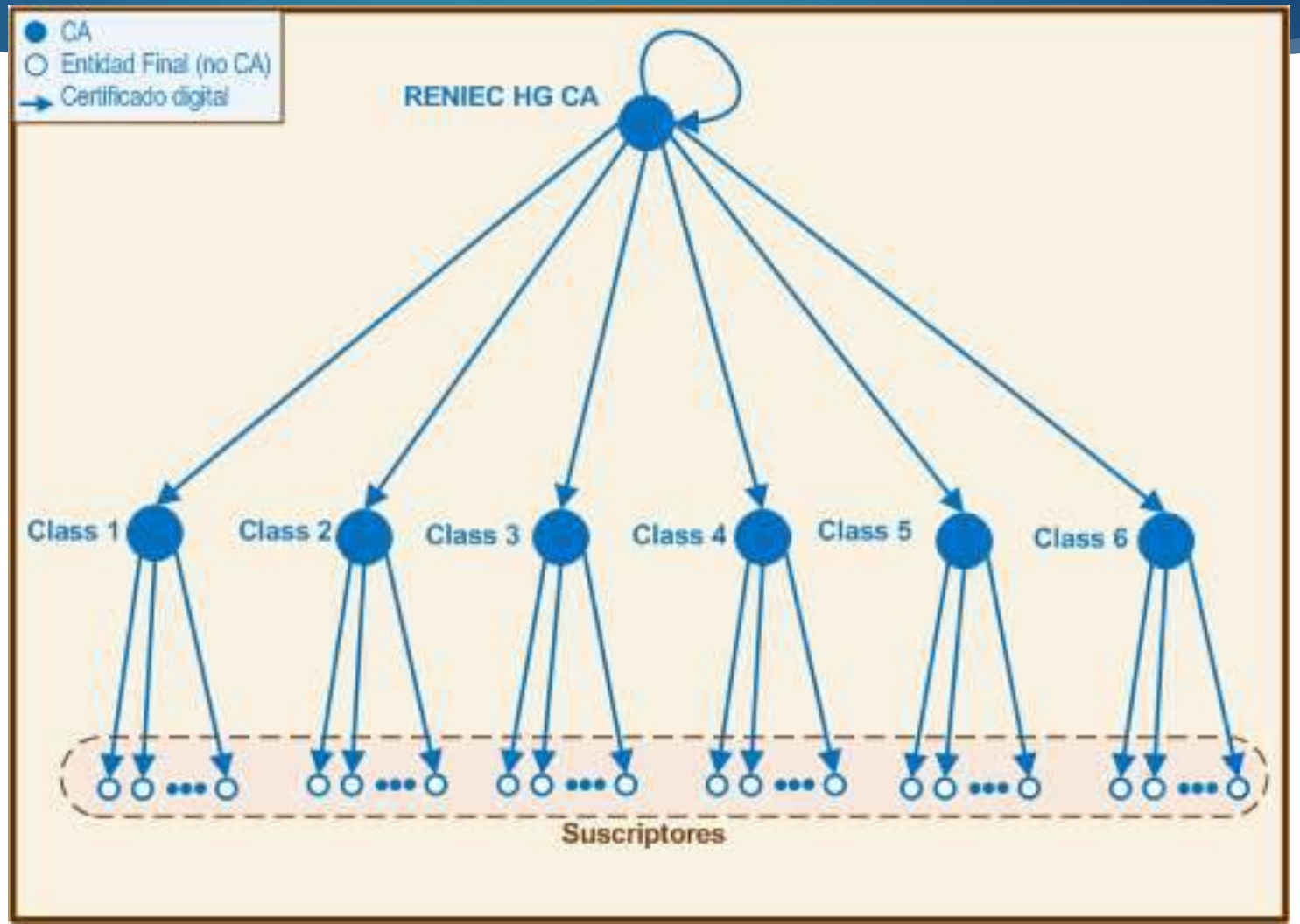
GERENCIA DE CERTIFICACIÓN Y REGISTRO DIGITAL
SUB GERENCIA DE CERTIFICACIÓN E IDENTIDAD DIGITAL

MARZO 2018

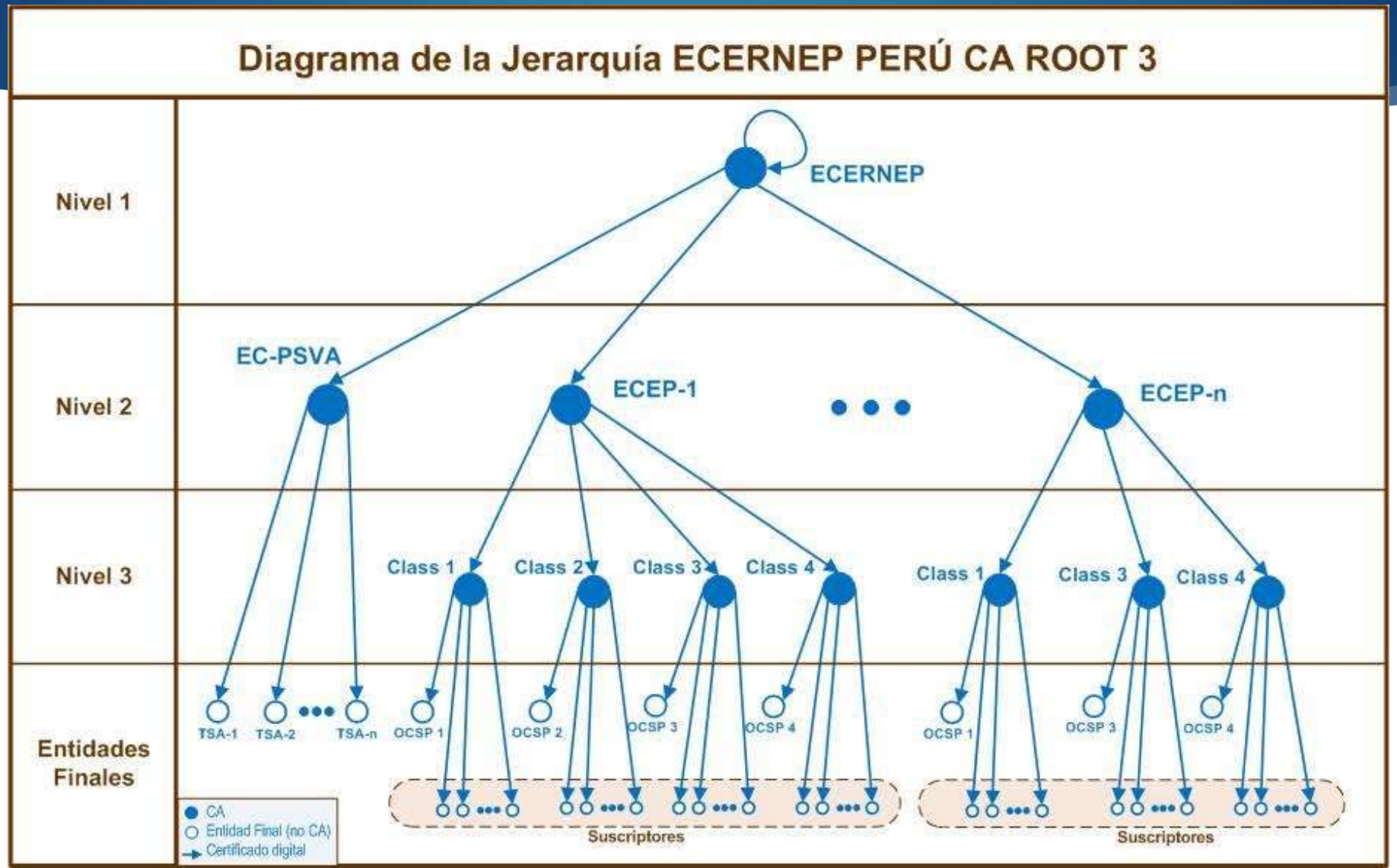
Contenido

1. Jerarquía: RENIEC High Grade Certification Authority (SHA-256)
2. Jerarquía: ECERNEP PERU CA ROOT 3 (SHA-2)
3. Jerarquía: ECERNEP PERU CA ROOT 3 (implementación actual)
4. Diagrama físico y lógico ECERNEP PERU CA ROOT 3
5. Clases de la Jerarquía ECERNEP PERU CA ROOT 3
6. Perfiles por Clase
7. Lectura de los perfiles en la CPS de la ECEP-RENIEC

Jerarquía: RENIEC High Grade Certification Authority (SHA-256)



Jerarquía: ECERNEP PERU CA ROOT 3 (SHA-2)



Jerarquía: ECERNEP PERU CA ROOT 3 (implementación actual)

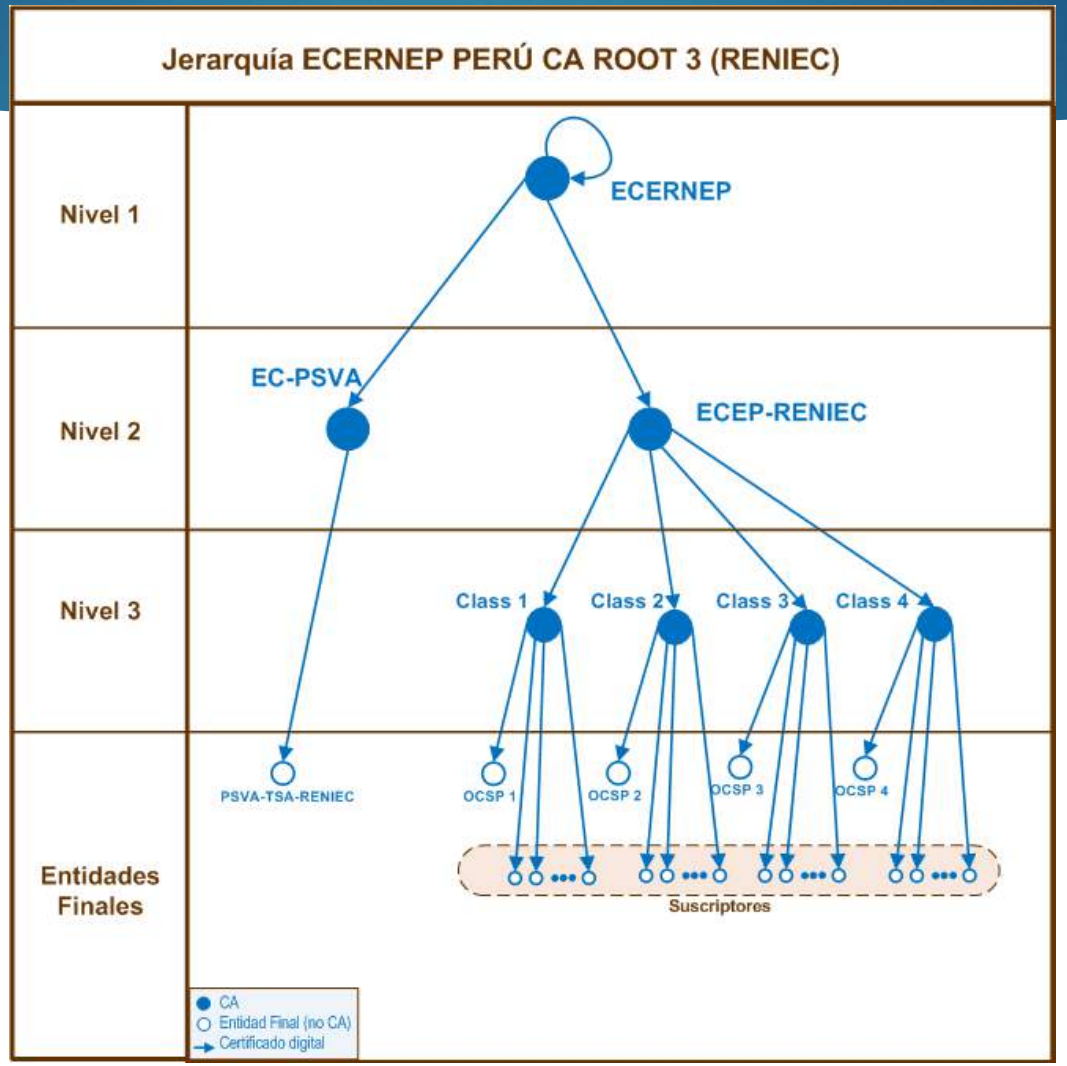
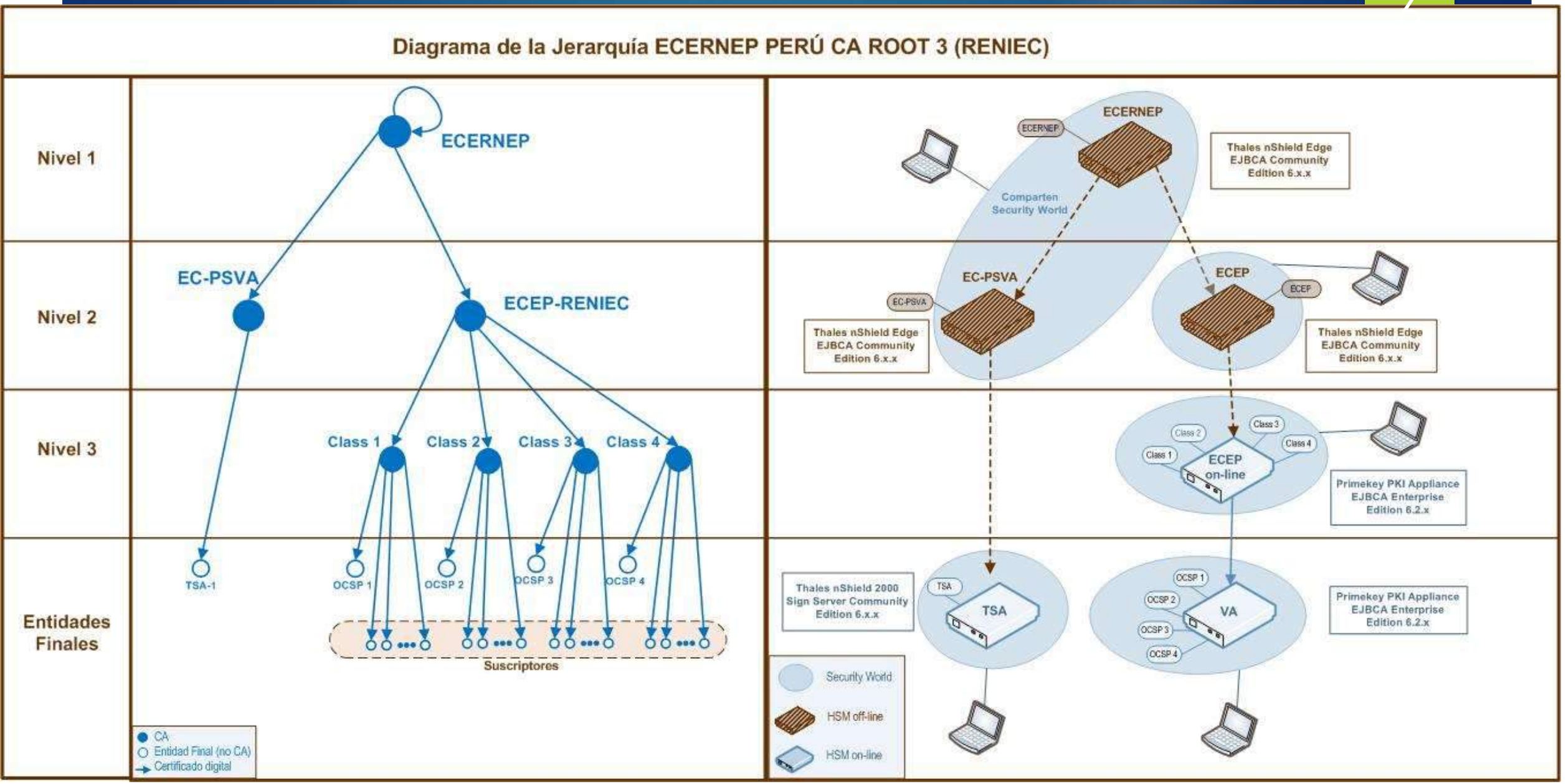


Diagrama de la Jerarquía ECERNEP PERÚ CA ROOT 3 (RENIEC)



ECEP-RENIEC CA Class {1,2,3,4}

Clase	Descripción
Class 1	Certificados digitales para usos específicos
Class 2	Certificados digitales para Ciudadanos (contenidos en el DNI electrónico)
Class 3	Certificados digitales para Trabajadores de la Administración Pública
Class 4	Certificados digitales para Sistemas de Información

Tabla 1: Certificados digitales de nivel 3 de la ECEP-RENIEC

Fuente: CPS de la ECEP-RENIEC, numeral 1.3.2, página 12

ETSI EN 319411-1(emisión en hard y soft)

3.1 Definitions

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

4.2.5 Certificate Policy

As described in IETF RFC 3647 [i.3], clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The present document defines seven CPs:

1) A Normalized Certificate Policy (NCP) which meets general recognized best practice for TSPs issuing certificates used in support of any type of transaction.

2) An extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the NCP for use where a secure cryptographic device (signing or decrypting) is considered necessary. The requirements for this CP include the policy requirements for the issuance and management of NCP certificates.

6.3.5 Key pair and certificate usage

f) [NCP+] only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;

g) [NCP+] [CONDITIONAL] if the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the secure cryptographic device;

Perfiles por cada Clase

Clase	Class 1		Class 2		Class 3		Class 4	Totales
Contenedor	hard	soft	hard	soft	hard	soft		
AUT			X					1
P_AUT			X					1
FIR			X					1
P_FIR			X					1
FAU	X	X			X	X		4
P_FAU	X	X			X	X		4
CIF			X		X	X		3
P_CIF			X		X	X		3
AA							X	1
P_AA							X	1
DC							X	1
P_DC							X	1
SSL							X	1
P_SSL							X	1
SSL_EV								0
P_SSL_EV								0
Sub Total	2	2	6	0	4	4	6	**24**
Total	**4**		**6**		**8**		**6**	
	Class 1		**Class 2**		**Class 3**		**Class 4**	
OCSP	X		X		X		X	4
Total	1		1		1		1	**4**

La ECEP-RENIEC implementa los siguientes perfiles:

Veintiocho (28) perfiles de certificado digital organizados en cuatro (04) clases.

- Veinticuatro (24) son perfiles para suscriptor
- Cuatro (04) perfiles para certificados OCSP Responder.

OCSP Responder Class {1,2,3,4}

PERFIL DE CERTIFICADO

Perfil de Certificado OCSP Responder Class {1, 2, 3, 4}

Nombre	Atributo	Valor	Obligatorio	Crítica
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class {1, 2, 3, 4}	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	15 días	Sí	-
Subject	CN	OCSP Responder Class {1, 2, 3, 4}	Sí	-
	SERIALNUMBER	-	-	
	O	Registro Nacional de Identificación y Estado Civil	Sí	
	C	PE	Sí	
	OI	NTRPE-20295613620	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	No

Key Usage	-	digitalSignature	Sí	No
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el emisor: Class 1 -->1.3.6.1.4.1.35300.2.1.3.3.1.103.1010.2, Class 2 -->1.3.6.1.4.1.35300.2.1.3.3.2.103.1010.2, Class 3 -->1.3.6.1.4.1.35300.2.1.3.3.3.103.1010.2, Class 4-->1.3.6.1.4.1.35300.2.1.3.3.4.103.1010.2}	Sí	No
	cPSuri	-		
	explicitText	OCSP Responder Class {1, 2, 3, 4}		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	
Extended Key Usage	-	OcspSigning (1.3.6.1.5.5.7.3.9)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	-	-	-
Authority Information Access	cAIssuers	{Elegir una de las siguientes URL, según el emisor: Class 1 -->http://www.reniec.gob.pe/crt/sha2/caclass1.crt, Class 2 -->http://www.reniec.gob.pe/crt/sha2/caclass2.crt, Class 3 -->http://www.reniec.gob.pe/crt/sha2/caclass3.crt, Class 4-->http://www.reniec.gob.pe/crt/sha2/caclass4.crt}	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	NULL	Sí	No

Class 3 FAU {hard, soft}

PERFIL DE CERTIFICADO

Perfil de Certificado Class 3 FAU {soft, hard}

Nombre	Atributo	Valor	Obligatorio	Crítica
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 8 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 3	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
Validity	(Not After - Not Before)	máximo 1 año	Sí	-
Subject	CN	*<APELLIDOS Nombres>* FAU *<número de RUC> {soft, hard}*	Sí	-
	SN	*<APELLIDOS>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	No	
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		

Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Declaración de Prácticas de Certificación ECEP-RENIEC		

	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 0.4.0.2042.1.1 Emitido en hard --> 0.4.0.2042.1.2}	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Política de Certificado Normalizado **NCP** de acuerdo con ETSI EN 319411-1, Emitido en hard --> Política de Certificado Normalizado **NCP+** de acuerdo con ETSI EN 319411-1}		
	policyIdentifier (OID)	{Elegir uno de los siguientes OID, según el tipo de certificado: Emitido en soft --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.1 Emitido en hard --> 1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.2 }	Sí	No
	cPSuri	-		
	explicitText	{Elegir uno de los siguientes textos, según el tipo de certificado: Emitido en soft --> Certificado Digital Class 3 de firma y autenticación en software Emitido en hard --> Certificado Digital Class 3 de firma y autenticación en hardware}		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-

Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/crl/sha2/caclass3.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/caclass3.crt	Sí	No
	ocsp (URI)	http://ocsp.reniec.gob.pe	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	No
	QcLimitValue	-	No	
	QcPDS	https://www.reniec.gob.pe/repository/,es	Sí	

¡Gracias!