ECERNEP PERU CA ROOT 3
Nueva jerarquía PKI del Estado Peruano,
Diseño e implementación

REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

Lima, agosto 2018
PERÚ

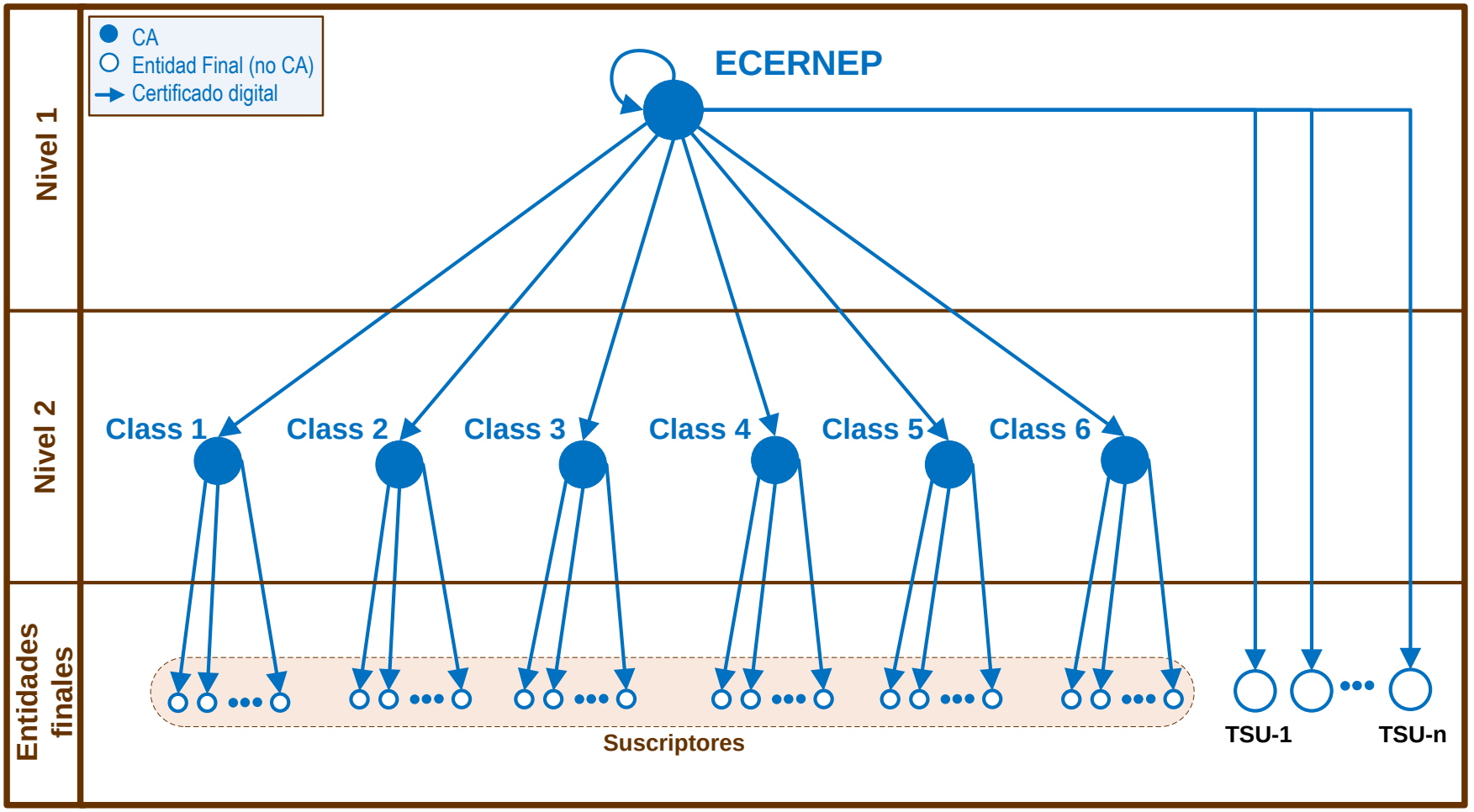
NECESIDAD DE UNA NUEVA JERARQUÍA PKI

Jerarquías *RENIEC Certification Authority* y *RENIEC High Grade Certification Authority* (2010)

Las jerarquías originales operaron sin problemas cubriendo las necesidades locales, sin embargo se identificaron posibilidades de mejora buscando la interoperabilidad con otras EC y su reconocimiento en sistemas de amplio uso a nivel internacional (Windows, Acrobat Reader, etc.)

- *Cambios en el diseño de su arquitectura*
- *Cambios en extensiones y campos de los perfiles de los certificados digitales*
- *Próximo vencimiento de certificados de las EC subordinadas*
- *Carencia del servicio de consulta del estado de certificados en línea (OCSP)*
- *Generación de llaves y firma digital para los usuarios (entidades finales) en dispositivos de hardware y no de software (PKCS#12)*

Jerarquías *RENIEC Certification Authority* y *RENIEC High Grade Certification Authority* (2010)



NUEVA JERARQUÍA PKI ECERNEP PERU CA ROOT 3

Antecedentes

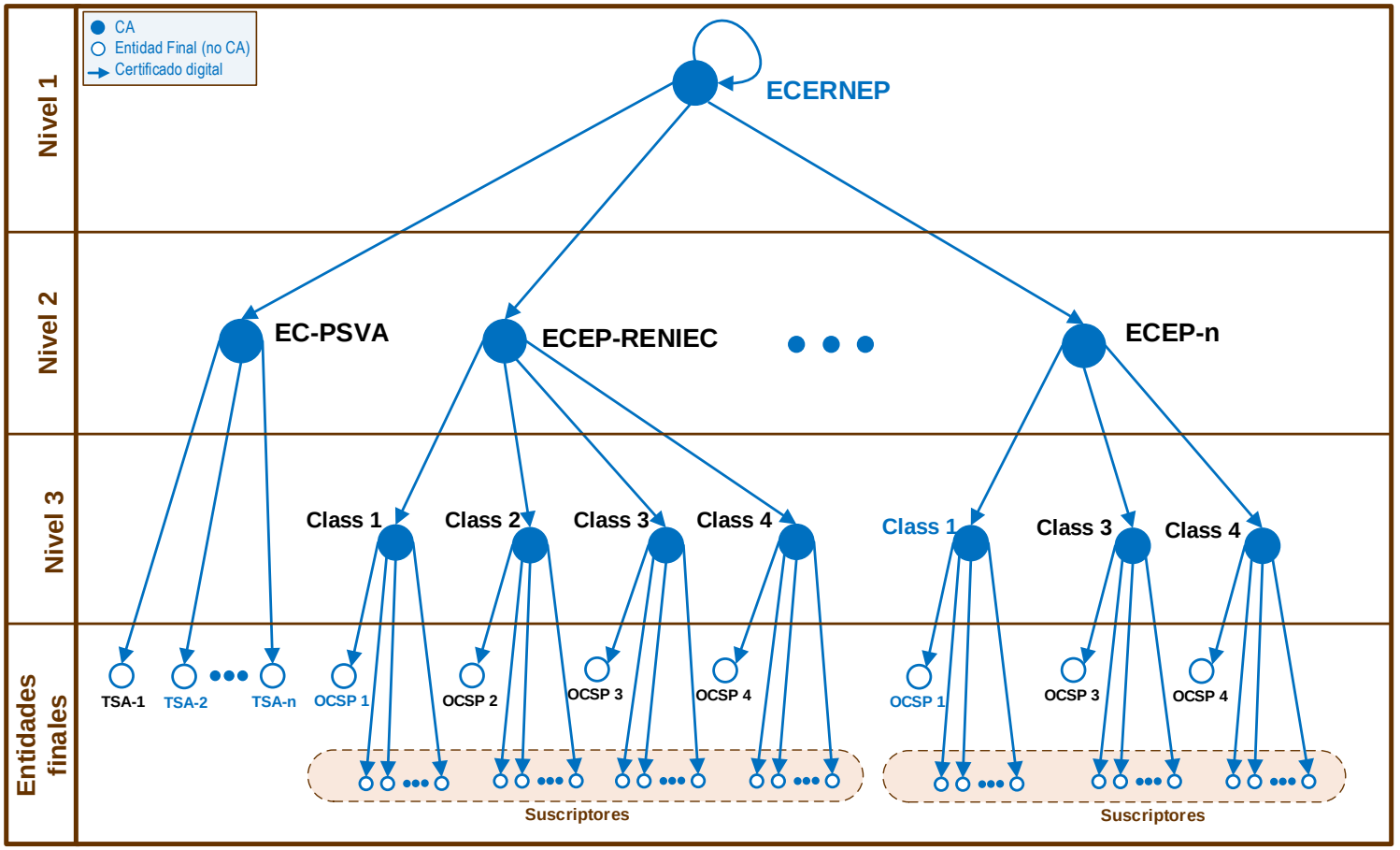
- *Los especialistas de la GRCD investigaron sobre las nuevas tecnologías, buenas prácticas y estándares internacionales con muchos meses de anticipación*
- *La ceremonia de llaves, hito que marca el nacimiento de la nueva jerarquía, fue desarrollada en agosto del 2017 como parte de una consultoría de 120 días que contó con especialistas del exterior*
- *El conocimiento alcanzado por nuestros profesionales posibilitó el lograr un alto nivel de calidad en los entregables y en la posterior puesta en producción de la nueva jerarquía PKI del Estado Peruano*
- *De las jerarquías originales se dio de baja la basada en SHA-1 en junio del 2017 y la basada en SHA-256 durante el presente año, si bien se siguen emitiendo las CRL correspondientes*

Antecedentes

- *La nueva jerarquía asumió primero la emisión de certificados de persona jurídica para los trabajadores de las entidades públicas y en el mes de julio la emisión de certificados de persona natural en el DNIe con 4 años de vigencia*
- *Alrededor de la nueva jerarquía se dispone de una serie de herramientas que posibilitan una gestión más eficiente de la jerarquía y un acceso a los servicios más seguro y fácil para los usuarios*
  - *Plataforma PIER*
  - *DC Delivery*
  - *Homologación de dispositivos criptográficos*
  - *Dashboard en tiempo real*
- *Se posibilitará la prestación de nuevos servicios a usuarios externos como el Sellado de Tiempo (PSVA-TSA-RENIEC)*

A. Etapa de diseño

A.1 Diseño lógico o estructural de la jerarquía (3 niveles)

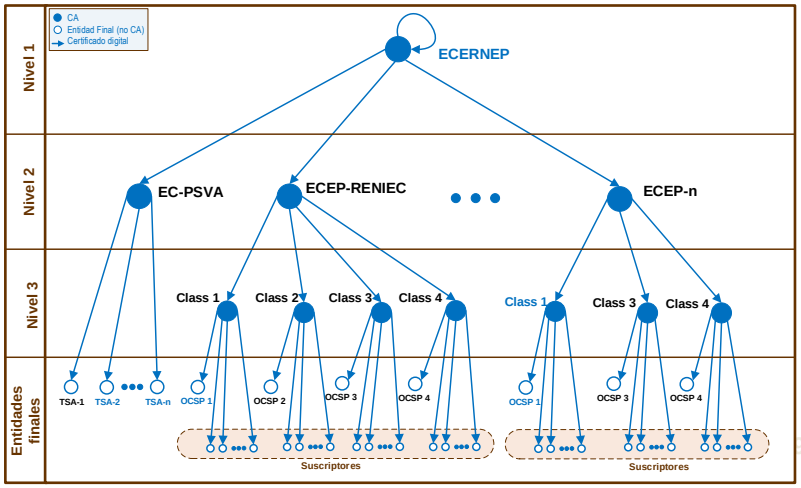


A. Etapa de diseño

A.2 Determinación de clases de certificados de Entidad Final

Se determinó reducir el número de clases de certificados de seis (06) a cuatro (04), distribuyéndolos según el tipo de suscriptor:

- *Clase 1 (para usos específicos)*
- *Clase 2 (para Ciudadanos)*
- *Clase 3 (para Trabajadores de la Administración Pública)*
- *Clase 4 (para Sistemas de Información).*



A. Etapa de diseño

A.3 Definición del período de validez de los certificados digitales

- *Exigencia de Microsoft: máximo 25 años para el certificado de la EC raíz*
- *Certificados para el DNIe con 4 años de vigencia (anteriormente 2)*

Nivel	Entidad	Vigencia	Frecuencia CRL	OCSP
1	ECERNEP	25 años	01 año	No
2	ECEP-X-offline	16 años	06 meses	No
	EC-PSVA	16 años	06 meses	No
3	ECEP-X-online	08 años	24 horas	Si
Entidad final	Clase 2	04 años		
	Clase 1, 3, 4	01 año		
	Para pruebas	40 días		

A. Etapa de diseño

A.4 Definición de periodicidad de emisión de las listas de certificados cancelados (CRL):

- *Para las EC off-line que emiten o cancelan certificados esporádicamente: seis meses y un año*
- *Para las EC on-line que emiten certificados masivamente: 24 horas*

Nivel	Entidad	Vigencia	Frecuencia CRL	OCSP
1	ECERNEP	25 años	01 año	No
2	ECEP-X-offline	16 años	06 meses	No
	EC-PSVA	16 años	06 meses	No
3	ECEP-X-online	08 años	24 horas	Si
Entidad final	Clase 2	04 años		
	Clase 1, 3, 4	01 año		
	Para pruebas	40 días		

A. Etapa de diseño

A.5 Elaboración de un nuevo árbol de OIDs

- *Identificación no solo de los documentos de gestión, sino también de los certificados digitales*
- *Número registrado ante la Internet Assigned Numbers Authority:*

IANA - 1.3.6.1.4.1.35300.2.X.Y.A.B.C.D.E - RENIEC

Ejemplos:

- *OID de la Declaración de Prácticas de Certificación (CPS) de la ECEP-RENIEC:*

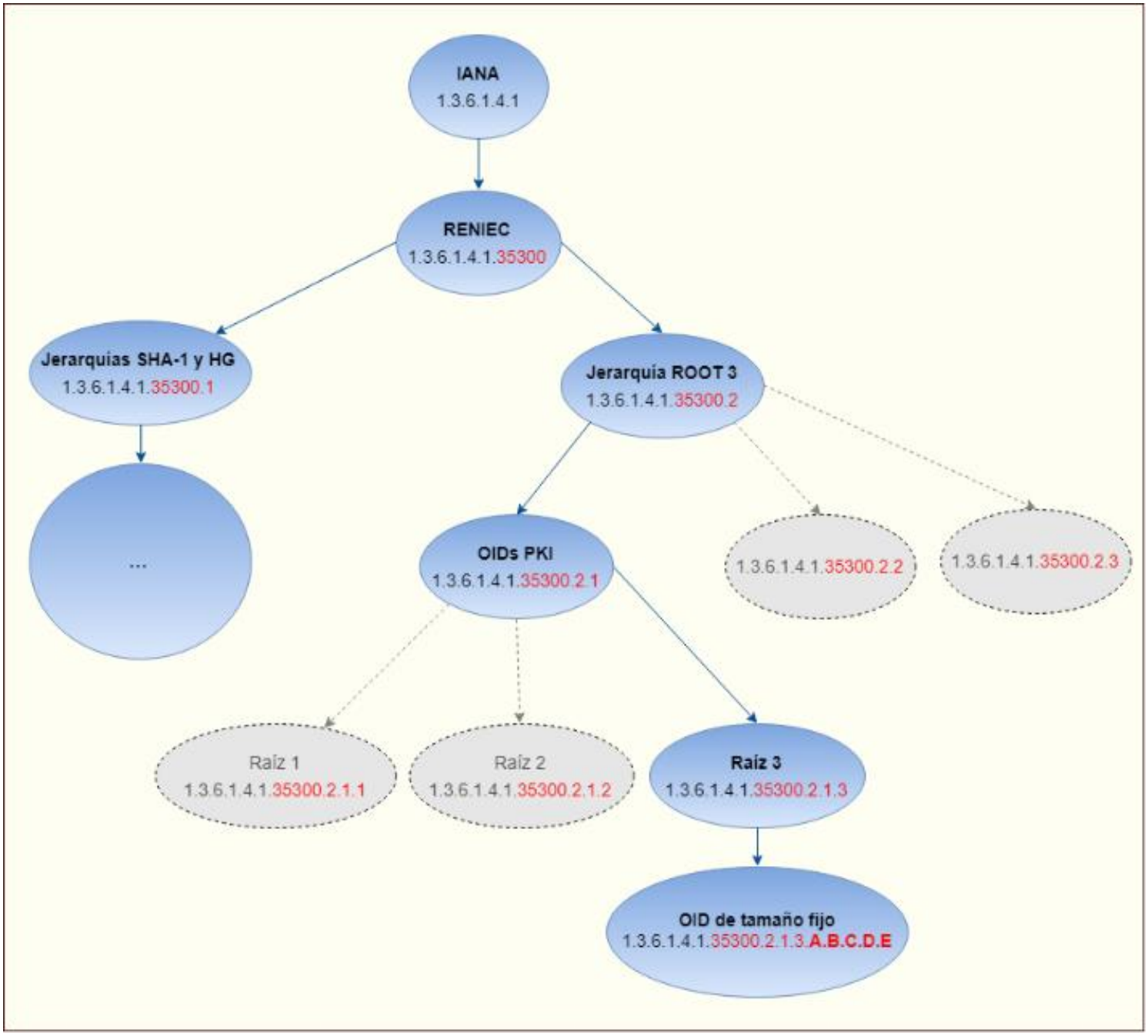
  1.3.6.1.4.1.35300.2.1.3.1.0.103.1000.0

  donde A=1,B=0, C=103, D=1000, E=0

- *OID de un certificado Clase 3 de firma y autenticación:*

  1.3.6.1.4.1.35300.2.1.3.1.3.103.1003.2

  Donde A=1,B=3, C=103, D=1003, E=2


IANA
1.3.6.1.4.1
RENIEC
1.3.6.1.4.1.35300
Jerarquías SHA-1 y HG
1.3.6.1.4.1.35300.1
...
Jerarquía ROOT 3
1.3.6.1.4.1.35300.2
OIDs PKI
1.3.6.1.4.1.35300.2.1
1.3.6.1.4.1.35300.2.2
1.3.6.1.4.1.35300.2.3
Raíz 1
1.3.6.1.4.1.35300.2.1.1
Raíz 2
1.3.6.1.4.1.35300.2.1.2
Raíz 3
1.3.6.1.4.1.35300.2.1.3
OID de tamaño fijo
1.3.6.1.4.1.35300.2.1.3.A.B.C.D.E

A. Etapa de diseño

A.6 Definición de perfiles de certificados digitales

- *Para EC raíz, para ECs subordinadas de nivel 2, para ECs subordinadas de nivel 3 y para entidades finales (personas o TSAs)*
- *Se hicieron mejoras con inclusiones y actualización de extensiones y campos de los perfiles basándonos en los certificados de mayor reconocimiento a nivel mundial y en los más recientes estándares y exigencias de la industria*

Ejemplos:

- *El valor MSsmartcardLogon (1.3.6.1.4.1.311.20.2.2) en la extensión ExtendedKeyUsage recomendado para el acceso con tarjetas inteligentes al SO Windows.*
- *Valor de longitud de la ruta en la variable PathLenConstraints del campo BasicConstaraints*

Perfil de Certificado ECERNEP

Nombre
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject Public Key Inf
Authority Key Identifie
Subject Key Identifie
Key Usage
Certificate Policies
Subject Alternative Name
Basic Constraints
Extended Key Usage
CRL Distribution Point
Authority Information Access
Subject Information Access
OCSP no check

Perfil de Certificado ECEP-RENIEC

Nombre
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject Public Key Info
Authority Key Identifier
Subject Key Identifier
Key Usage
Certificate Policies
Subject Alternative Name
Basic Constraints
Extended Key Usage
CRL Distribution Points
Authority Information Acce
Subject Information Acces
OCSP no check

Perfil de Certificado ECEP-RENIEC CA 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*	Sí	
Signature	algorithm	Sha512		
Issuer	CN			
	O	Registro Nacional		
	C			
Validity	(Not After - Not Before)			
Subject	CN	ECEP-REN		
	O	Registro Nacional		
	C			
Subject Public Key Info	algorithm			
	KeyLength			
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (1 campo Subject*		
Subject Key Identifier	-	*<Resumen SHA-1 (1 campo Su*		
Key Usage	-	keyC		
Certificate Policies	policyIdentifier (OID)			
	cPSuri			
	explicitText			
Subject Alternative Name	-			
Basic Constraints	cA			
	Path Length Constraint			
Extended Key Usage	-	ClientAu		
	-	EmailProte		
	-	SmartcardLog		
	-	OcspSign		
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecep.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecep.crt	Sí	No
	ocsp (URI)	-	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Tipo	Class 1	Class 2	Class 3	Class 4	Totales
AUT		X			1
FIR		X			1
CIF		X	X		2
FAU	X		X		2
AA				X	1
DC				X	1
SSL				X	1
P_AUT		X			1
P_FIR		X			1
P_CIF		X	X		2
P_FAU	X		X		2
P_AA				X	1
P_DC				X	1
P_SSL				X	1
TOTAL	2	6	4	6	18

Tipo	Class 1	Class 2	Class 3	Class 4	Totales
OCSP	X	X	X	X	4
TOTAL	1	1	1	1	4

A. Etapa de diseño

A.7 Definición de algoritmos de resumen (SHA), de firma (RSA o ECC) y longitudes de llaves criptográficas

Nivel	Entidad	Algoritmo de hash	Algoritmo de firma	Longitud de llaves (bits)
1	ECERNEP	SHA-512	RSAwithSHA512	4096
2	ECEP-X-offline	SHA-512	RSAwithSHA512	4096
	EC-PSVA	SHA-512	RSAwithSHA512	4096
3	ECEP-X-online	SHA-512	RSAwithSHA512	4096
Entidad final	Clase 1, 2, 3, 4	SHA-256	RSAwithSHA256	2048
	PSVA-TSA-TSU	SHA-256	RSAwithSHA256	2048
	Para pruebas	SHA-256	RSAwithSHA256	2048

B. Etapa de validación

B.1 Implementación del diseño en un software de gestión de CA validando los perfiles *y los valores de los campos de los certificados*

B.2 Emisión de certificados de prueba *en diferentes medios portadores de software (Windows) y hardware (dispositivos homologados por la ECEP-RENIEC)*

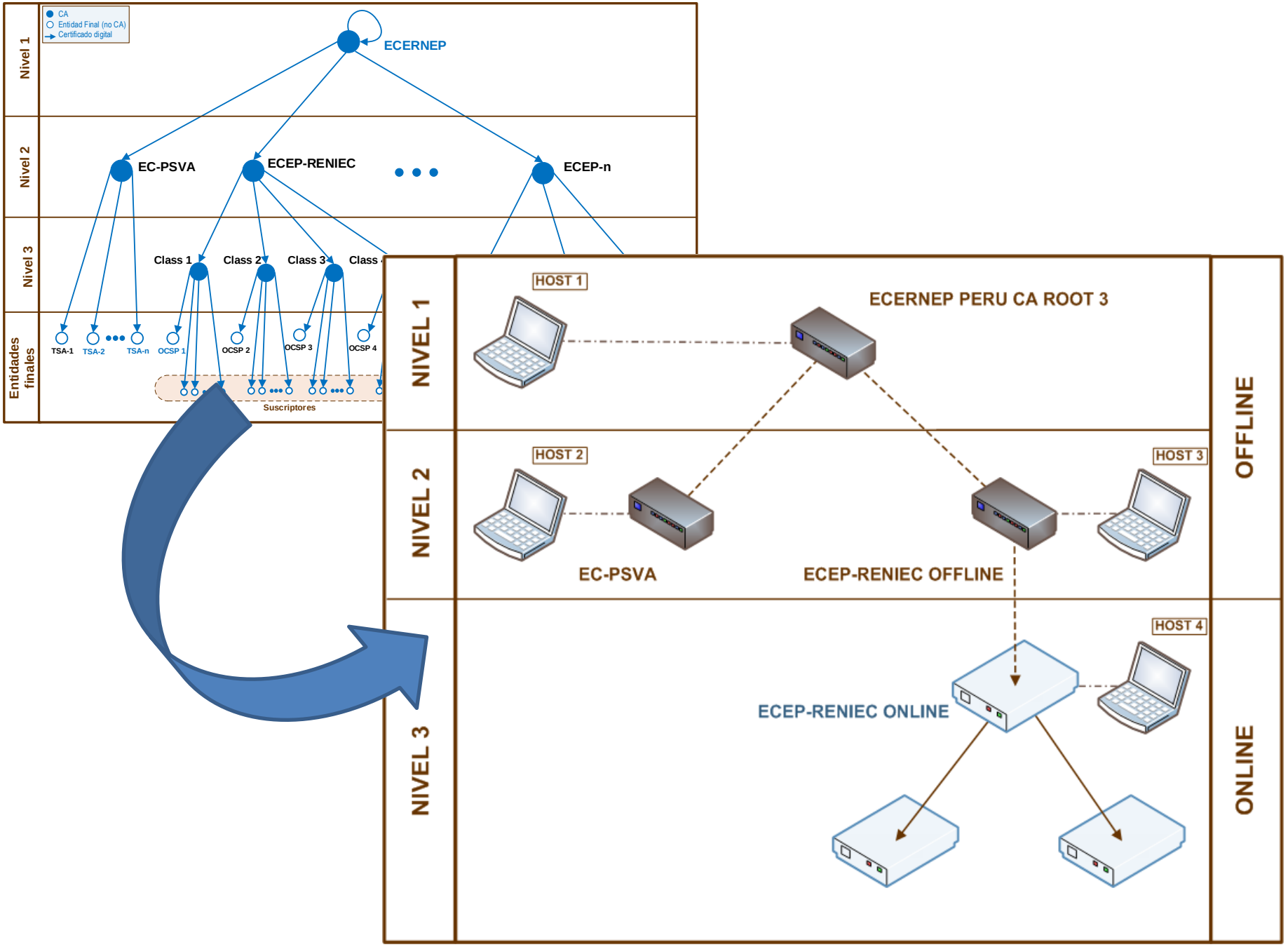
B.3 Ejecución de pruebas de firma *con los certificados de prueba. usando Acrobat Reader*

B.4 Optimización del diseño de la jerarquía

C. Implementación

C.1 Diseño físico de la nueva jerarquía

- *Organización de los equipos implementando el diseño lógico*
- *Para mejorar la seguridad los HSM de los niveles 1 y 2 (off-line) son de pequeño tamaño y de tipo USB, no requieren fuente de poder y se posibilita su resguardo en cajas de seguridad*
- *Los HSM de nivel 3 (on-line) son dispositivos o appliances rackeables que integran un servidor, el HSM y el software*


CA
Entidad Final (no CA)
Certificado digital
Nivel 1
Nivel 2
Nivel 3
Entidades finales
ECERNEP
EC-PSVA
ECEP-RENIEC
ECEP-n
Class 1
Class 2
Class 3
TSA-1
TSA-2
TSA-n
OCSP 1
OCSP 2
OCSP 3
OCSP 4
Suscriptores
NIVEL 1
NIVEL 2
NIVEL 3
HOST 1
ECERNEP PERU CA ROOT 3
HOST 2
HOST 3
EC-PSVA
ECEP-RENIEC OFFLINE
HOST 4
ECEP-RENIEC ONLINE
OFFLINE
ONLINE

C. Implementación

C.2 Ceremonia de llaves

- *Se dividió en dos partes: 1. preparación de equipos y 2. generación de llaves y emisión de certificados digitales*
- *Se elaboró guiones o procedimientos que fueron revisados y ensayados*
- *Cada parte se ejecutó en un día*
- *Fue dirigida por un experto internacional que vino como parte de una consultoría*
- *Fue filmada y contó con la presencia de notario público y testigos*

C. Implementación

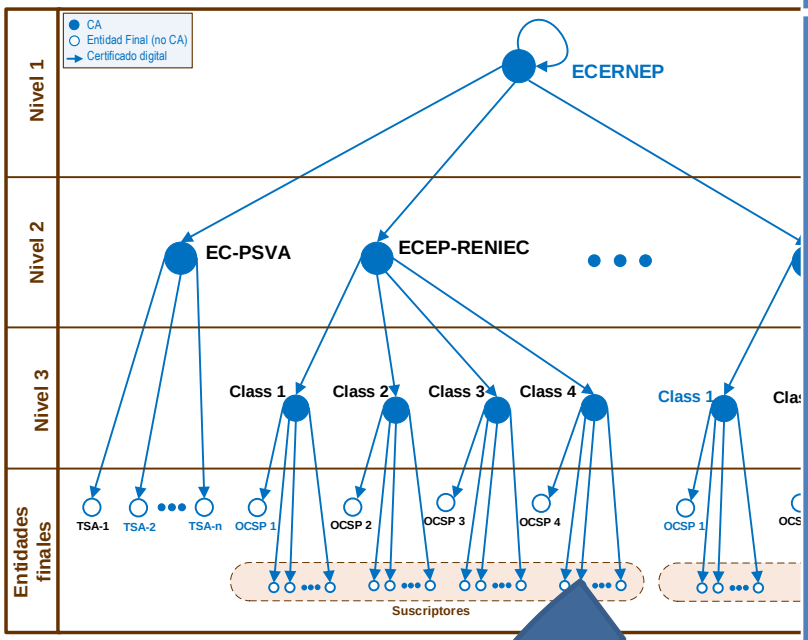
C.2.1 Ceremonia de llaves: Preparación de equipos

- *Contempló instalación del software necesario, así como la configuración de los dispositivos criptográficos (HSM) y de los equipos host*
- *Se verificó el inventario, la operatividad y la integridad de los mismos; de igual manera en lo referido a tokens criptográficos (Smart cards), memorias USB, etc.*
- *Concluyó con el precintado de equipos y su internamiento hasta el día siguiente en un ambiente controlado y físicamente inaccesible*

C. Implementación

C.2.2 Ceremonia de llaves: Generación de llaves y certificación

- *El material de activación de los HSM para el proceso de generación de llaves y la emisión de certificados va por seguridad distribuido en tarjetas Smart card que son entregadas a custodios*
- *Se generó los pares de llaves (llaves públicas y privadas) y se emitió los certificados digitales de las entidades de certificación conteniendo las llaves públicas correspondientes*
  - *Se comenzó con la generación del par de llaves de la AC raíz seguida de su autocertificación.*
  - *Se procedió con la generación de los pares de llaves para las entidades de nivel 2 y con la certificación de sus llaves públicas por la EC raíz*
  - *Finalmente, las llaves de nivel 3 fueron generadas y sus llaves públicas fueron certificadas por la EC de nivel 2*



Security World	Autoridad de Certificación	Card Set	Custodio designado	ID de Tarjeta
SW1	ECERNEP y EC-PSVA	ACS	CT1.1	TN01
			CT1.2	TN02
			CT1.3	TN03
			CT1.4	TN04
			CT1.5	TN05
	ECERNEP	OCS	CT2.1	TN06
			CT2.2	TN07
			CT2.3	TN08
			CT2.4	TN09
			CT2.5	TN10
	EC-PSVA		CT3.1	TN11
			CT3.2	TN12
			CT3.3	TN13
SW2	ECEP-RENIEC-offline	ACS	CT4.1	TN14
			CT4.2	TN15
			CT4.3	TN16
		OCS	CT5.1	TN17
			CT5.2	TN18
			CT5,3	TN19
No aplica	ECEP-RENIEC-online	BKS	CT6.1	TN20
			CT6.2	TN21
			CT6.3	TN22
			CT6.4	TN23
			CT6.5	TN24

C. Implementación

C.3 Alta disponibilidad

- *Para garantizar la alta disponibilidad de los servicios de la ECEP-RENIEC (nivel 3), se desplegó un cluster de equipos basado en el protocolo GRE*
- *El Generic Routing Encapsulation (GRE) es un protocolo para el establecimiento de túneles a través de Internet definido en la RFC 1701 y en la RFC 1702*
- *El nivel de disponibilidad implementado es el denominado Hot stand-by with manual fail-over*

D. Resultados

D.1 Documentos de gestión

- *Política General de Certificación de la ECERNEP aplicable bajo la nueva jerarquía a la misma ECERNEP, a las ECEP y a las EREP*
- *Declaración de Prácticas de Certificación de la ECERNEP*
- *Declaración de Prácticas de Certificación de la ECEP-RENIEC*
- *Política de Servicios de Valor Añadido dictada por la ECERNEP para prestadores del Servicio de Sellado de tiempo*
- *Declaración de Prácticas de Servicios de Valor Añadido para el prestador del Servicio de Sellado de Tiempo del RENIEC, PSVA-TSA-RENIEC*

D. Resultados

D.2 Certificados digitales de las EC de la jerarquía, CRLs (https://pki.reniec.gob.pe/repositorio/) y servicio Online Certificate Status Protocol (OCSP)

Certificados digitales de las Autoridades de Certificación para la nueva jerarquía	
Autoridad de Certificación	CRT
ECERNEP	http://www.reniec.gob.pe/crt/sha2/ecernep.crt
EC-PSVA	http://www.reniec.gob.pe/crt/sha2/ecpsva.crt
ECEP-RENIEC	http://www.reniec.gob.pe/crt/sha2/ecep.crt
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

Lista de Certificados Revocados para la nueva jerarquía	
Autoridad de Certificación	CRL
ECERNEP	http://crl.reniec.gob.pe/arl/sha2/ecernep.crl
	http://crl2.reniec.gob.pe/arl/sha2/ecernep.crl
EC-PSVA	http://crl.reniec.gob.pe/arl/sha2/ecpsva.crl
	http://crl2.reniec.gob.pe/arl/sha2/ecpsva.crl
ECEP-RENIEC	http://crl.reniec.gob.pe/arl/sha2/ecep.crl
	http://crl2.reniec.gob.pe/arl/sha2/ecep.crl
Class 1	http://crl.reniec.gob.pe/crl/sha2/caclass1.crl
	http://crl2.reniec.gob.pe/crl/sha2/caclass1.crl
Class 2	http://crl.reniec.gob.pe/crl/sha2/caclass2.crl
	http://crl2.reniec.gob.pe/crl/sha2/caclass2.crl
Class 3	http://crl.reniec.gob.pe/crl/sha2/caclass3.crl
	http://crl2.reniec.gob.pe/crl/sha2/caclass3.crl
Class 4	http://crl.reniec.gob.pe/crl/sha2/caclass4.crl
	http://crl2.reniec.gob.pe/crl/sha2/caclass4.crl

Protocolo del Estado del Certificado en línea	
Autoridades de Certificación	OCSP
ECEP-RENIEC online Class {1, 2, 3, 4}	http://ocsp.reniec.gob.pe

GRACIAS

ECERNEP PERU CA ROOT 3
Nueva jerarquía PKI del Estado Peruano, Diseño e implementación

REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

Lima, agosto 2018.
PERÚ