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

ABRIL 2018

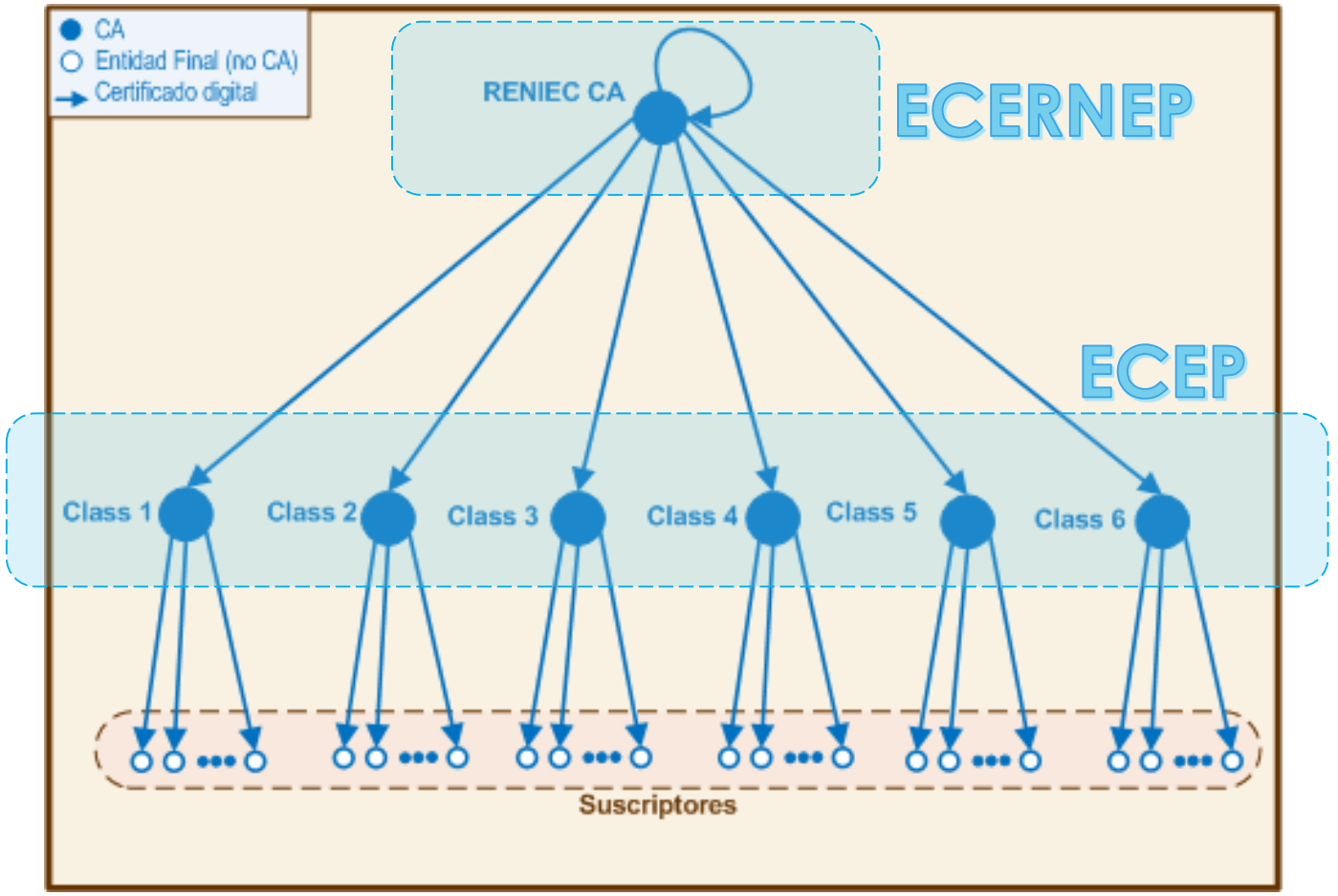
Contenido

1. Jerarquía RENIEC Certification Authority (SHA-1)
2. Jerarquía: RENIEC High Grade Certification Authority (SHA-256)
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. Emisión diferenciada para hardware y software
7. Perfiles por cada Clase
8. Jerarquías de prueba (TRIAL)
   a) RENIEC High Grade Certification Authority TRIAL
   b) ECERNEP PERU CA ROOT 3 TRIAL

Ceremonia de Llaves Año 2010

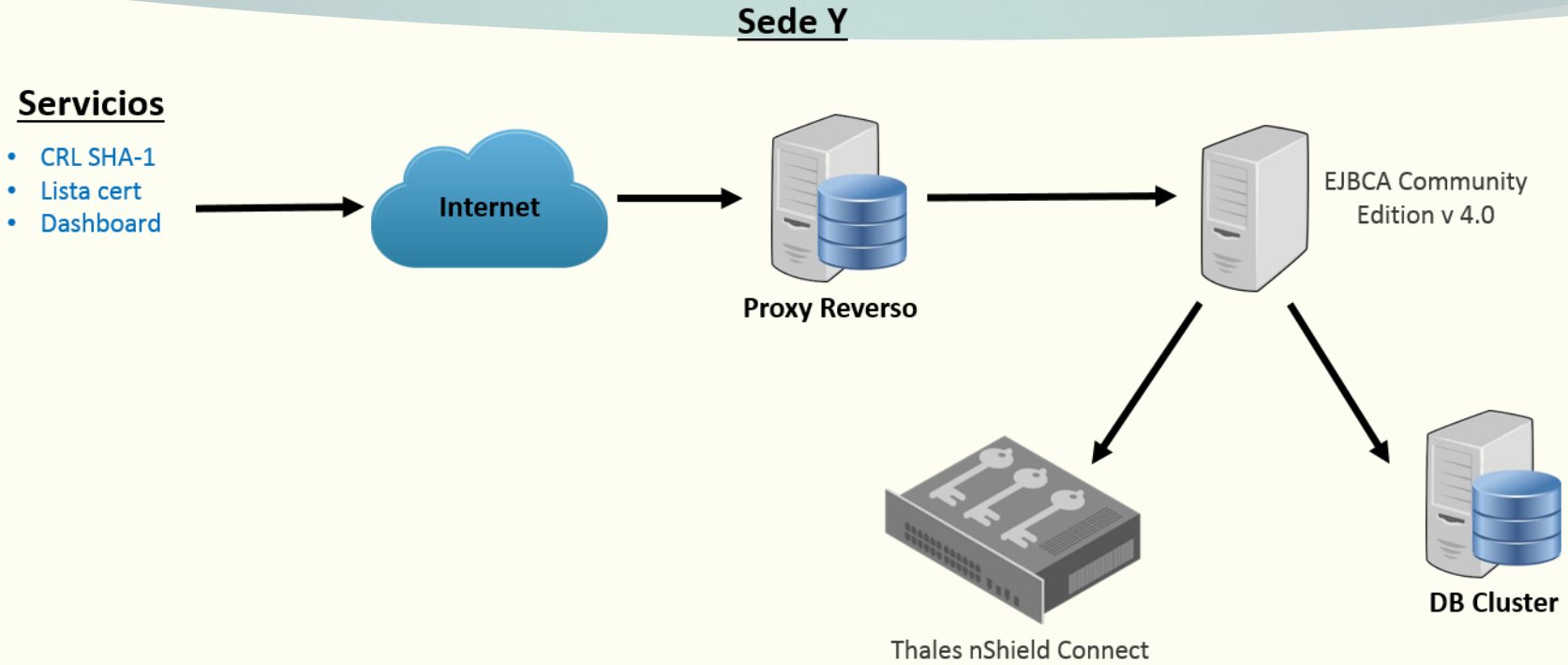
Ceremonia de Llaves Año 2017

Jerarquía: RENIEC Certification Authority (SHA-1)

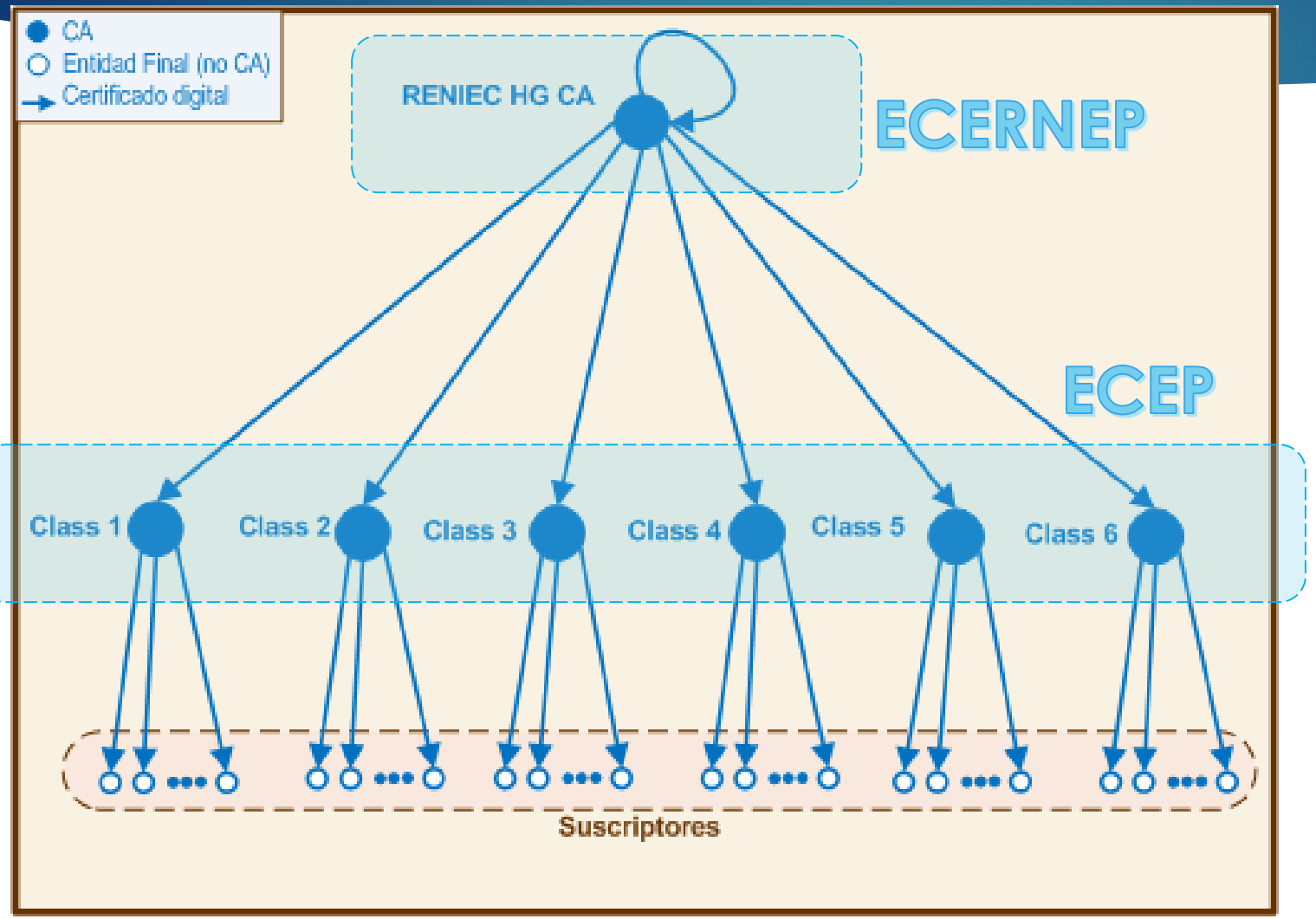


- **Ceremonia de Llaves Año 2010**
- **Dejó de emitir en Junio 2017**

ARQUITECTURA DE LA JERARQUÍA RENIEC CERTIFICATION AUTHORITY (SHA-1)

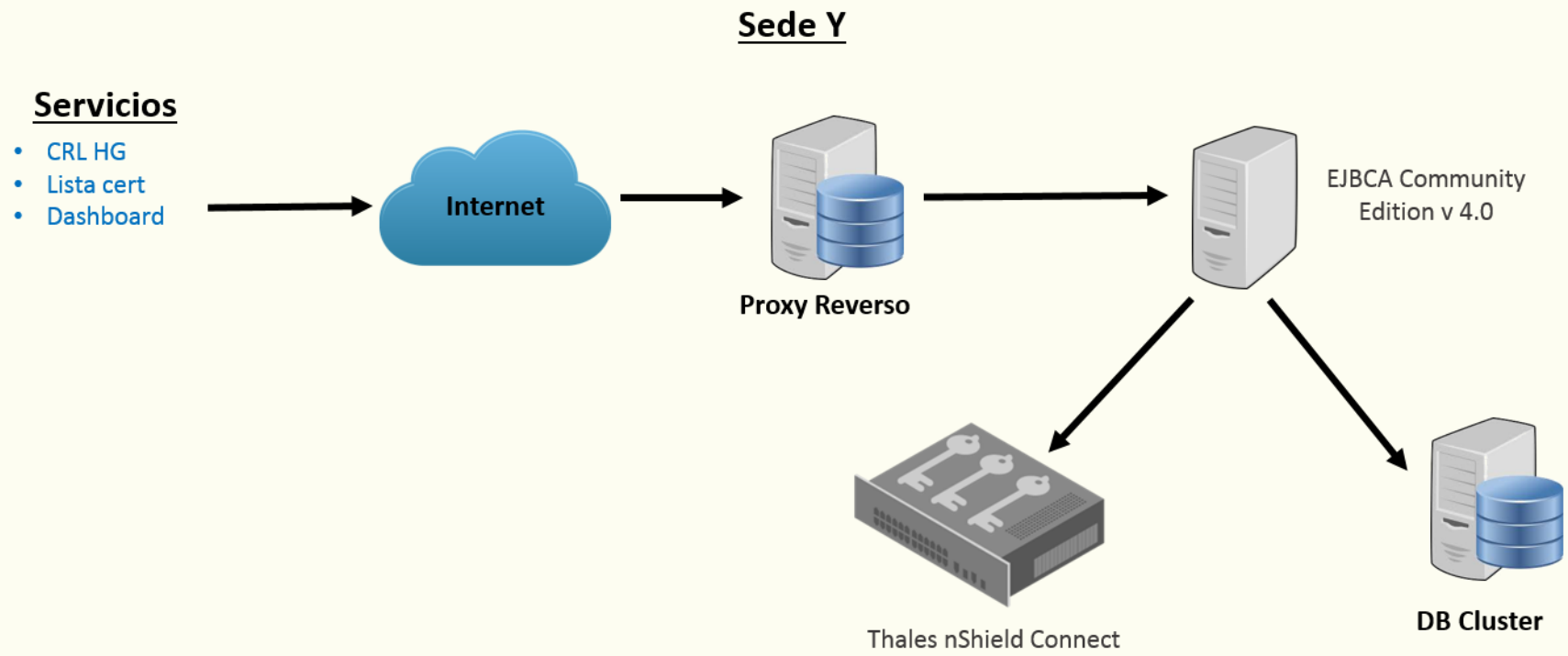


Jerarquía: RENIEC High Grade Certification Authority (SHA-256)

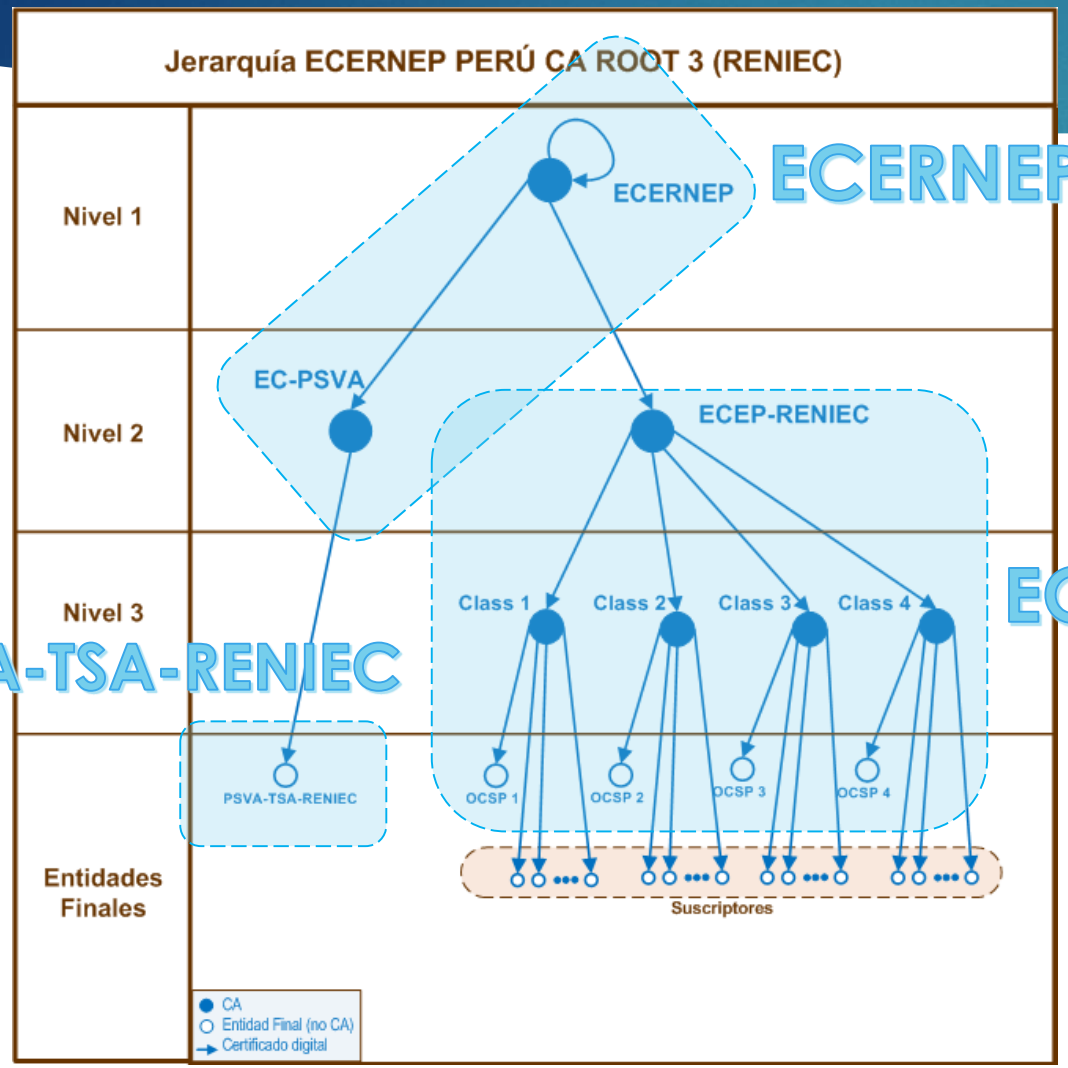


- **Ceremonia de Llaves Año 2010**
- **Dejó de emitir Class 3 en Enero 2018**

ARQUITECTURA DE LA JERARQUÍA RENIEC HIGH GRADE CERTIFICATION AUTHORITY (SHA-256)



Jerarquía: ECERNEP PERU CA ROOT 3 (implementación actual)



- **Ceremonia de Llaves Año 2017**
- **Empezó a emitir Class 3 en Enero 2018**

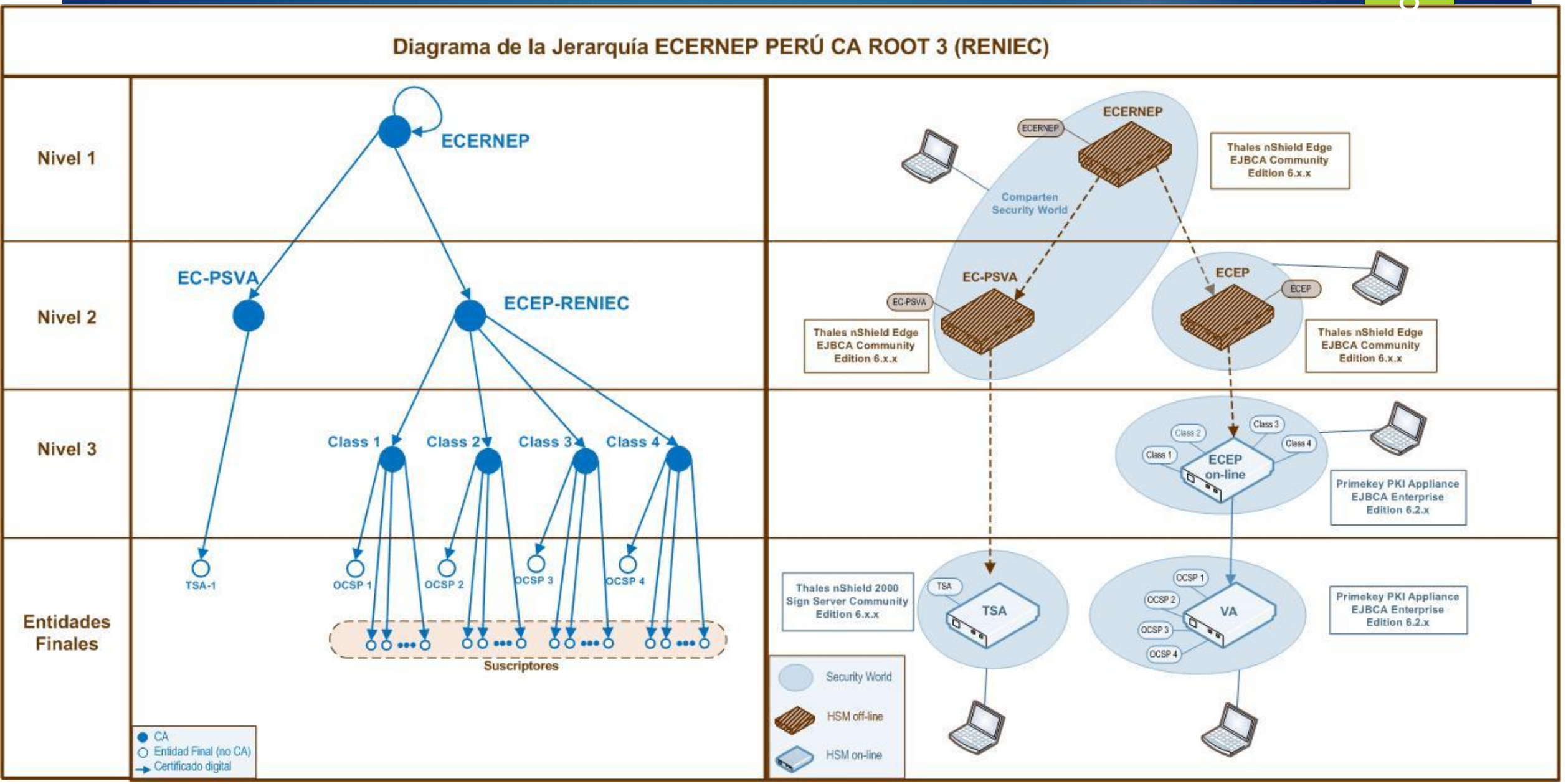
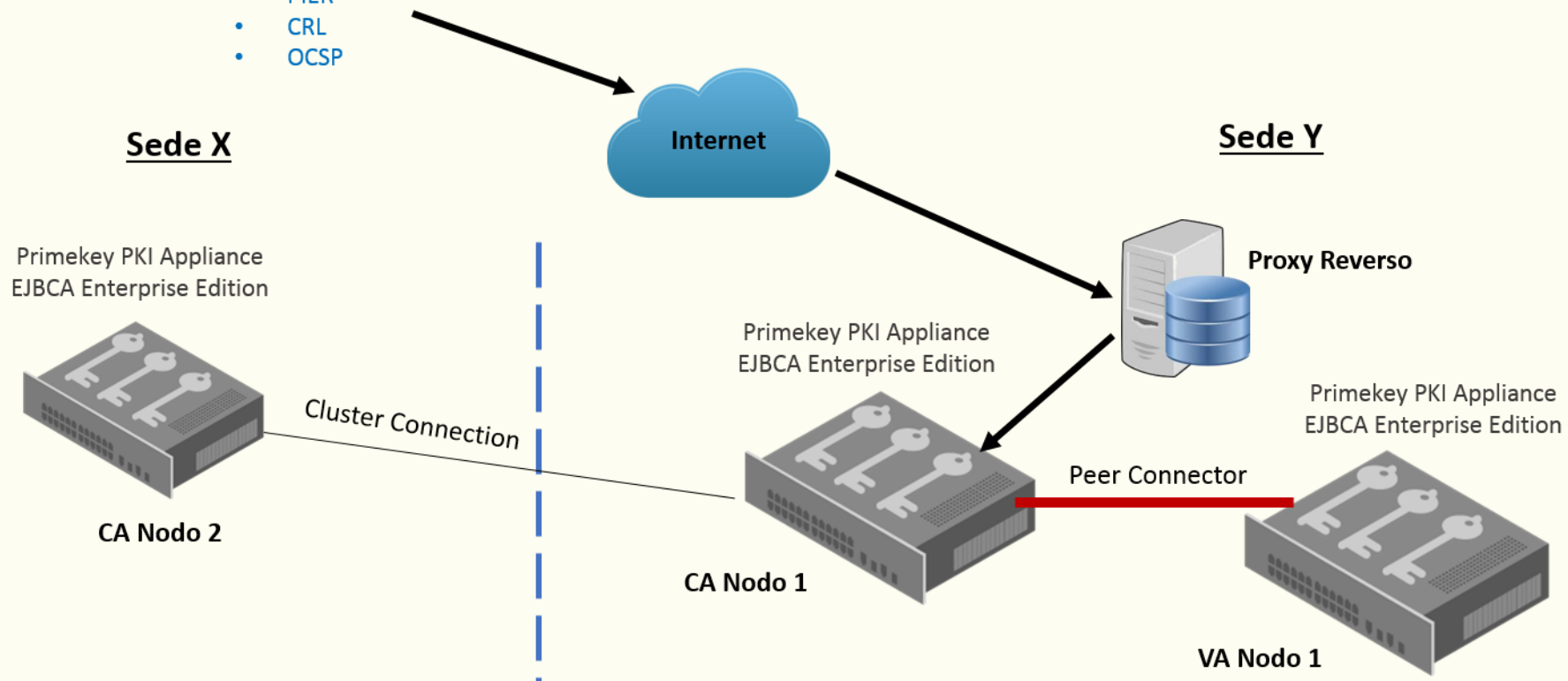


Diagrama de la Jerarquía ECERNEP PERÚ CA ROOT 3 (RENIEC)
Nivel 1
Nivel 2
Nivel 3
Entidades Finales
ECERNEP
EC-PSVA
ECEP-RENIEC
Class 1
Class 2
Class 3
Class 4
TSA-1
OCSP 1
OCSP 2
OCSP 3
OCSP 4
Suscriptores
CA
Entidad Final (no CA)
Certificado digital
ECERNEP
Thales nShield Edge EJBCA Community Edition 6.x.x
Comparten Security World
EC-PSVA
Thales nShield Edge EJBCA Community Edition 6.x.x
ECEP
Thales nShield Edge EJBCA Community Edition 6.x.x
ECEP on-line
Primekey PKI Appliance EJBCA Enterprise Edition 6.2.x
Thales nShield 2000 Sign Server Community Edition 6.x.x
TSA
VA
Primekey PKI Appliance EJBCA Enterprise Edition 6.2.x
Security World
HSM off-line
HSM on-line

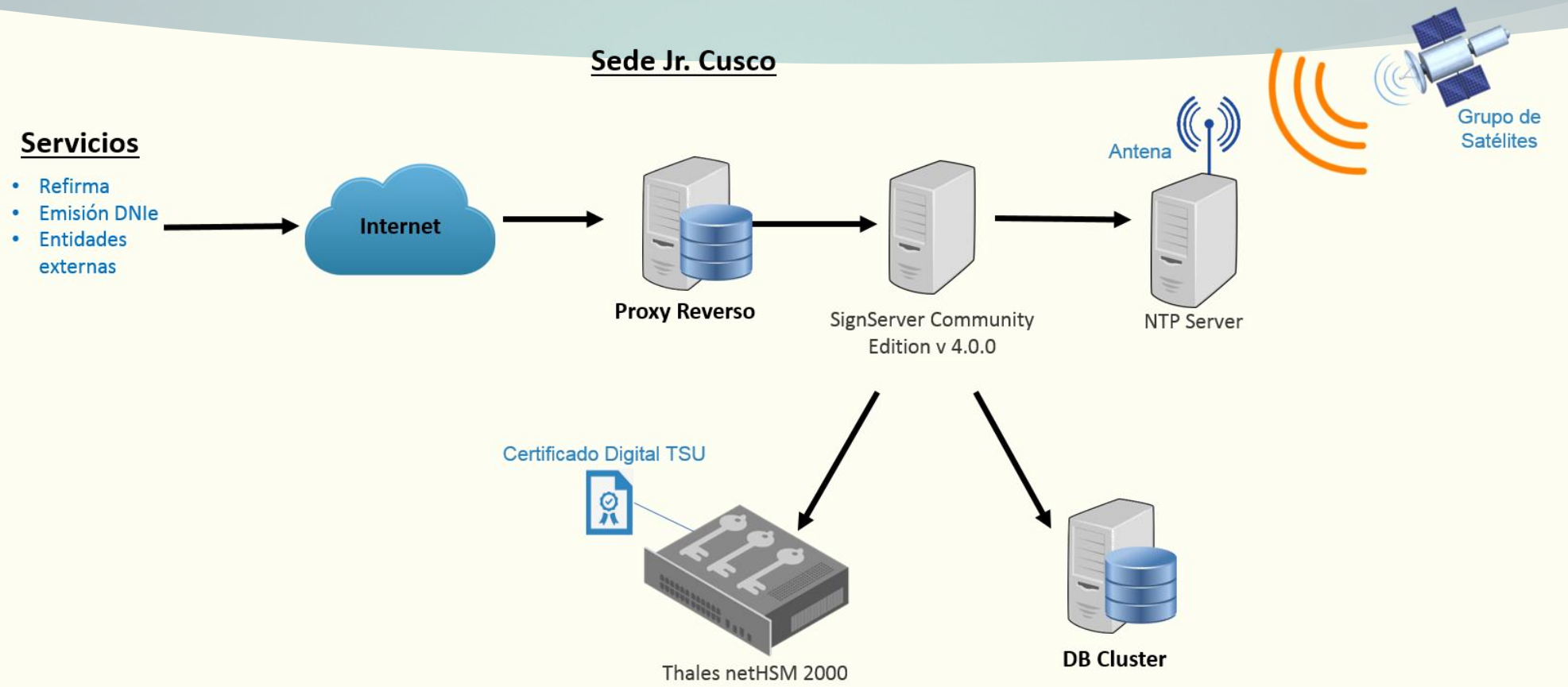
ARQUITECTURA DE LA JERARQUÍA ECERNEP PERÚ CA ROOT 3

Servicios

- SSCPP 3
- DCDelivery 3
- PIER
- CRL
- OCSP



ARQUITECTURA DEL PSVA-TSA-RENIEC DE LA JERARQUÍA ECERNEP PERU CA ROOT 3



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:

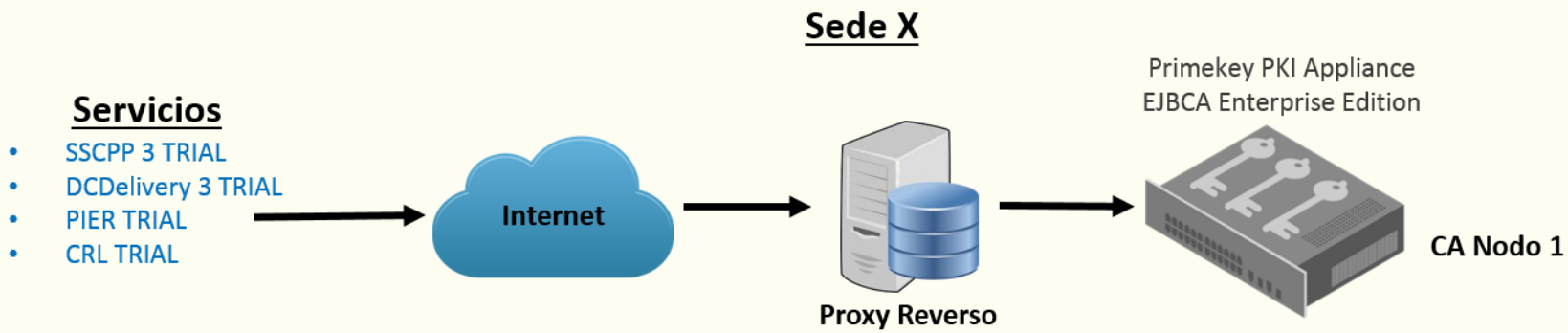
Veintiocho (28) perfiles de certificado digital organizados en cuatro (04) clases.

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

Jerarquías de prueba (TRIAL)

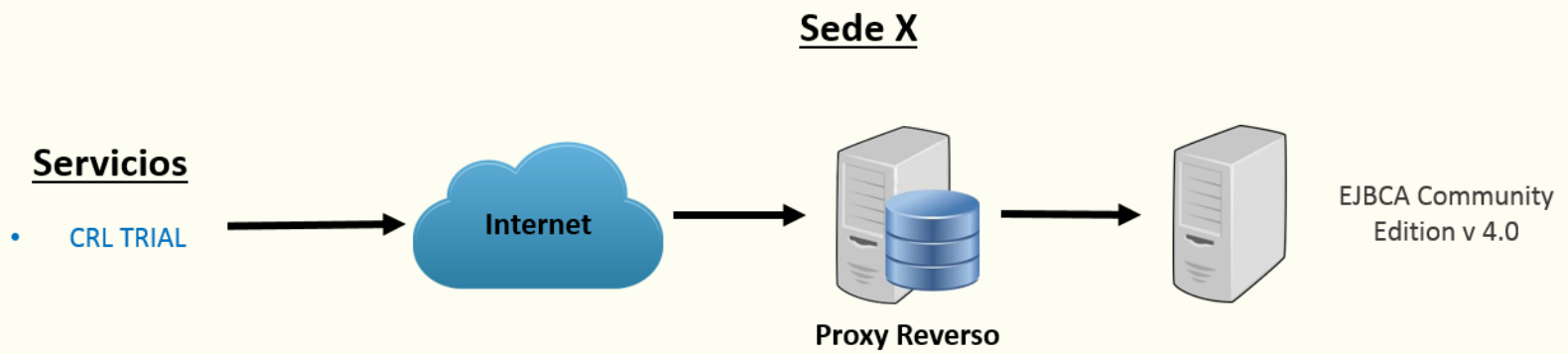
RENIEC High Grade Certification Authority TRIAL

ARQUITECTURA DE LA JERARQUÍA ECERNEP PERÚ CA ROOT 3 TRIAL



ECERNEP PERU CA ROOT 3 TRIAL

ARQUITECTURA DE LA JERARQUÍA RENIEC HIGH GRADE CERTIFICATION AUTHORITY TRIAL



рахмат
danke
謝謝
ngiyabonga
Баярлалаа
teşekkür ederim
mersi
barka
welalin
tack
спасибо
taafetai lava
vinaka
blagodaram
dank je
misaotra
matondo
paldies
mahalo
tapadh leat
kiitos
dankie
спасибі
thank you
gracias
хвала
asante
manana
bedankt
hvala
mauruuru
obrigada
enkosi
dziękuję
mochchakkeram
djiere dieuf
mamnun
chnorakaloutioun
gràcies
sulpay
go raibh maith agat
sobodi
dekuji
sukriya
kop khun krap
taiku
obrigado
mèsi
sagolun
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
najis tuke
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
мерси
kam sah hamnida
감사합니다
xiexie
ευχαριστώ
merci