ECERNEP PERU CA ROOT 3
DCDelivery: Entrega de certificados digitales Class 3

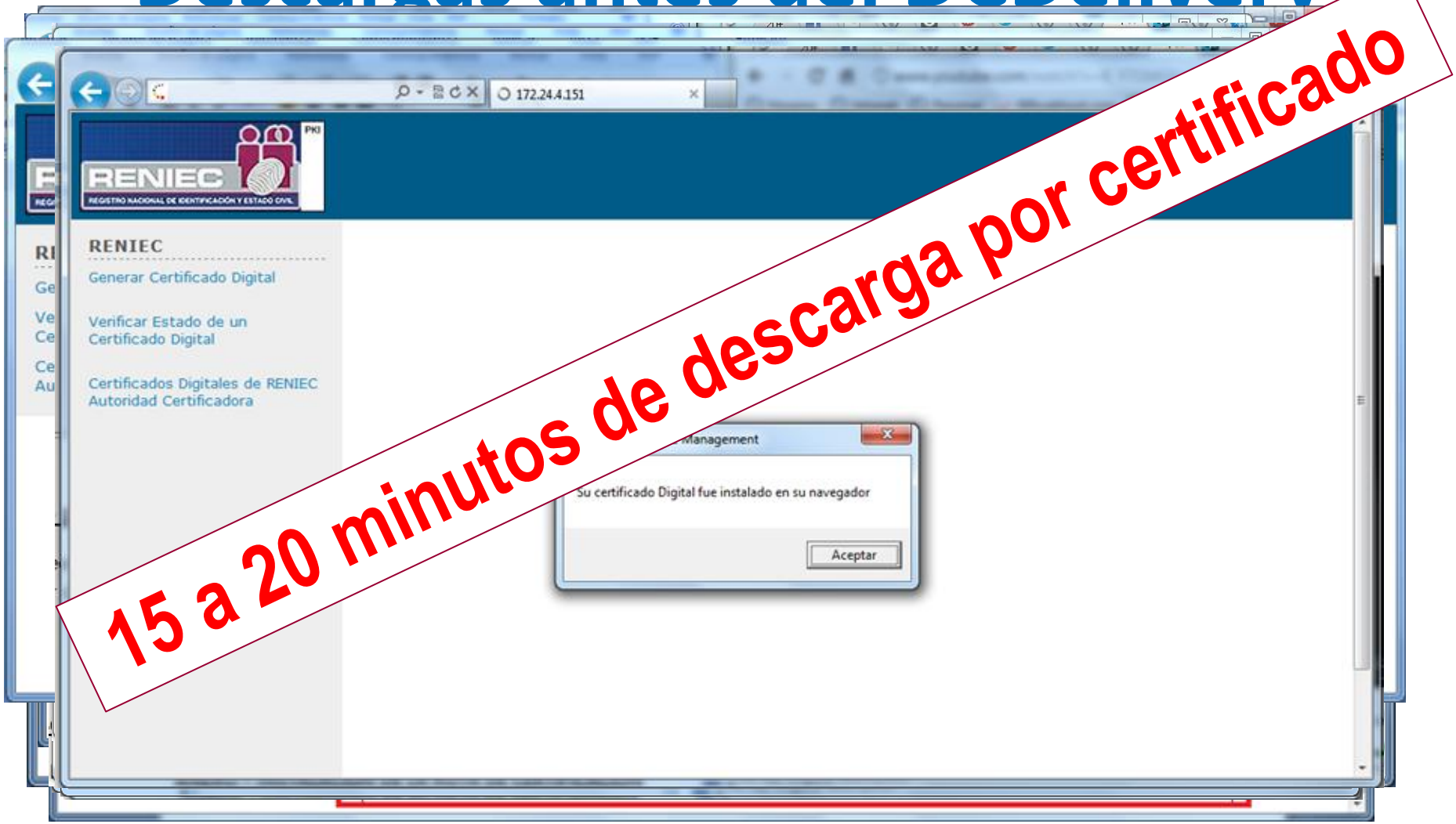
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

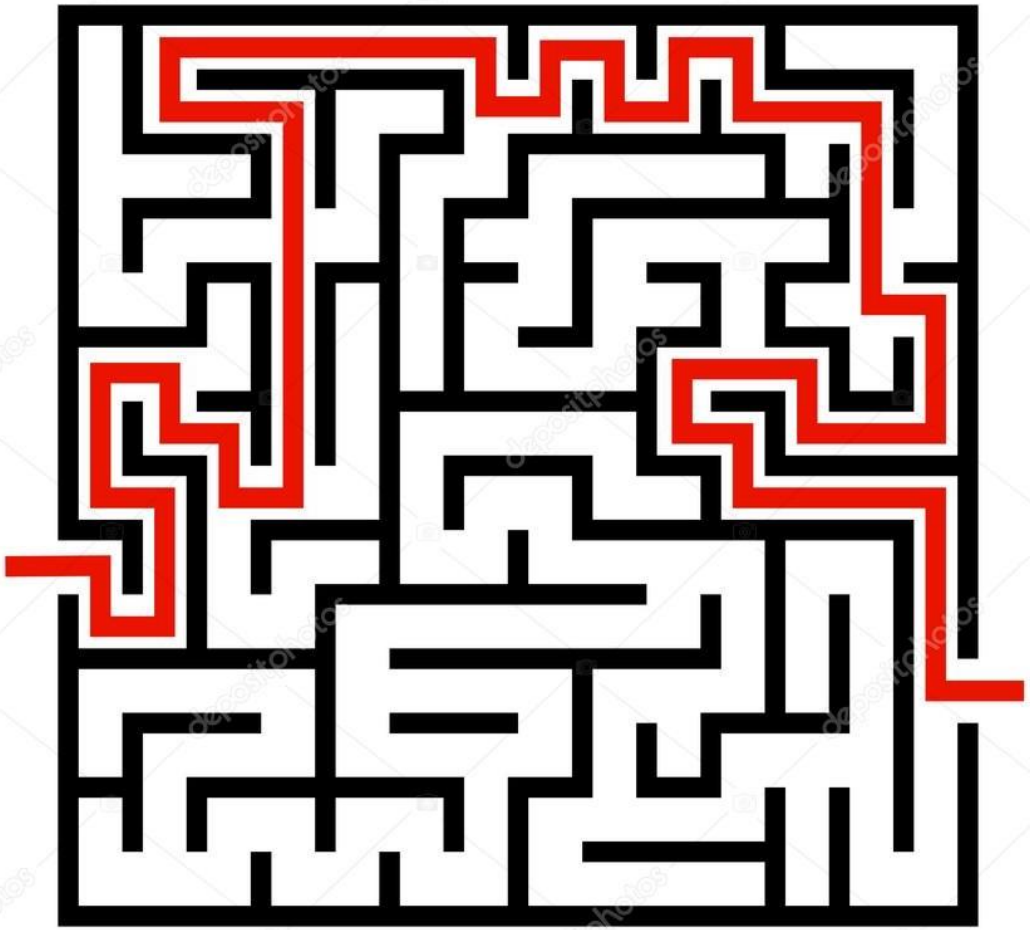
Lima, agosto 2018
PERÚ

Agenda

1. Descargas antes del DCDelivery
2. Problemas de descarga
3. DCDelivery primera versión
4. Jerarquía ECERNEP PERU CA ROOT 3
5. DCDelivery actual
6. Estándar PKCS#11
7. Homologación de dispositivos
8. Marcas homologadas
9. Demostración del uso de la Plataforma DCDelivery

Descargas antes del DCDelivery

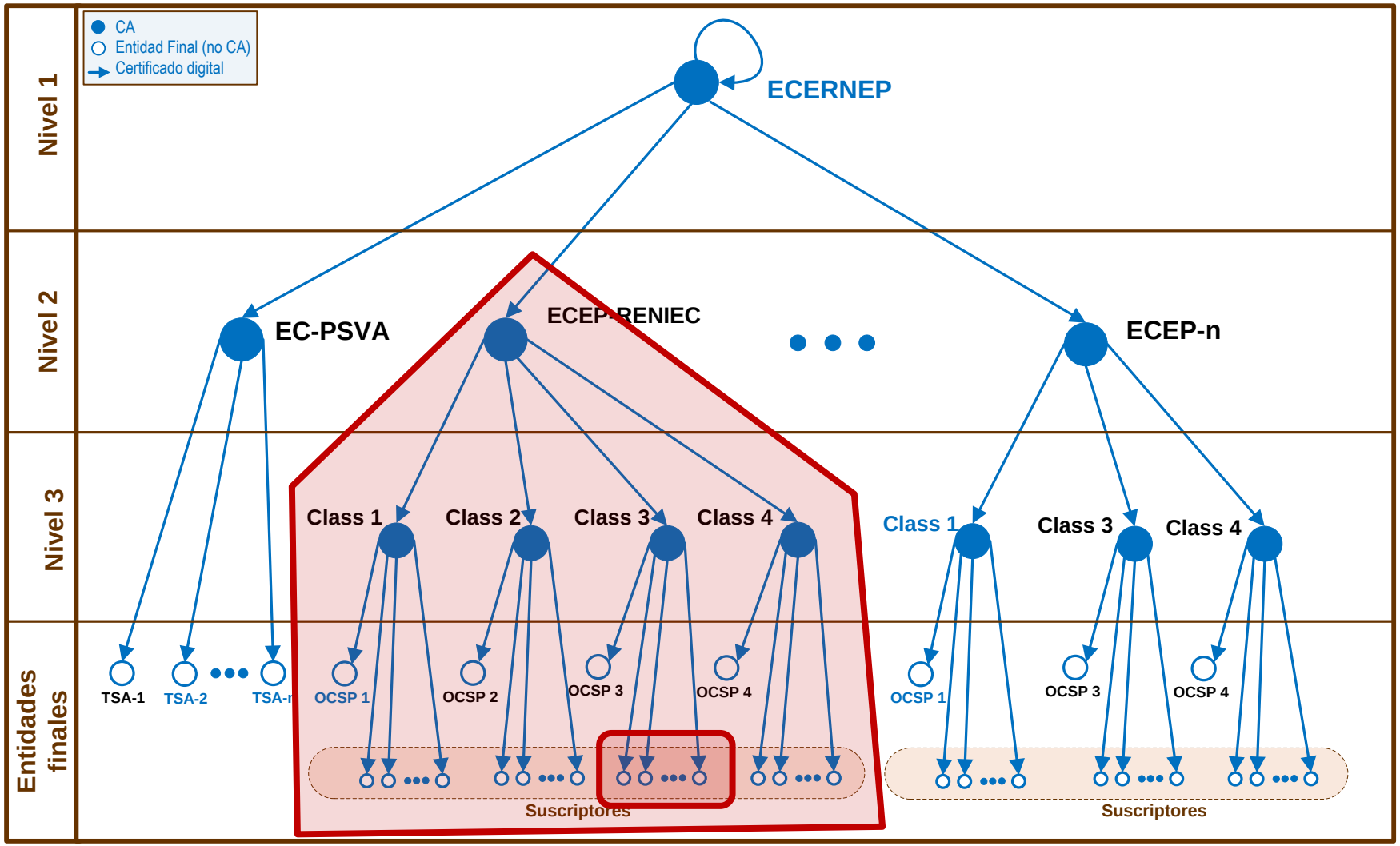




Problemas de descarga

- Demora en las descargas por certificado
- Procedimiento engorroso
- Casos diarios en Soporte al Cliente
- Un procedimiento diferente por cada dispositivo

Jerarquía ECERNEP PERU CA ROOT 3



RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Guía de usuario | Preguntas Frecuentes | Dispositivos Homologados

DCDelivery

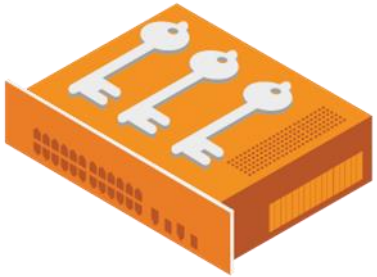
Generación y Descarga de Certificados Digitales de Clase III

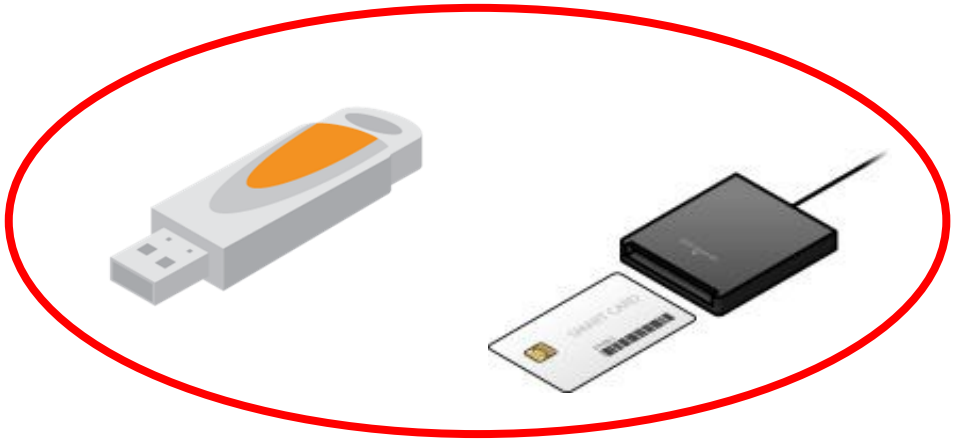
Para PC Windows

Para Token o Smartcard

Estándar PKCS #11

- Define interfaz programable, llamada **Cryptoki** (CRYPTOGRAPHIC TOKEN INTERFACE STANDARD) para la interacción con dispositivos criptográficos
- Presenta un enfoque simple **basado en objetos**
- Es independiente del **tipo de dispositivo** criptográfico





Fabricante: ACS
Modelo: CryptoMate Nano

Fabricante: Bit4ID
Modelo: DigitalDNA

Fabricante: Bit4ID
Modelo: Crypto Java Card

Fabricante: SafeNet
Modelo: SafeNet eToken 5110

Fabricante: Cryptovision
Modelo: JCOP 2.4.2 R3
Certificación: Common Criteria

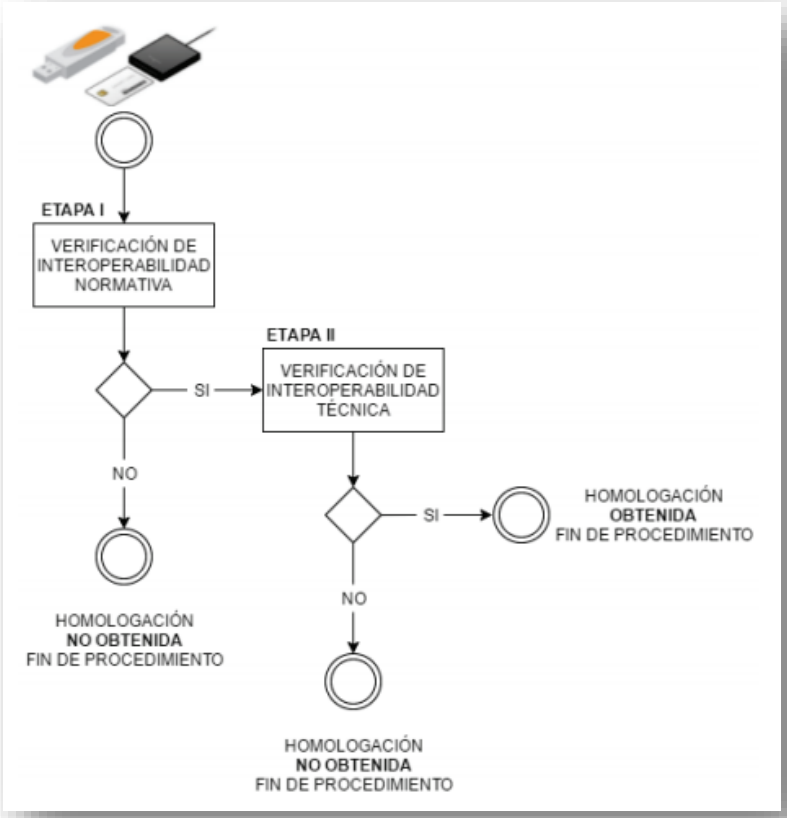
acospkcs11.dll

bit4ipki.dll

eTPKCS11.dll

cvP11.dll

Procedimiento de Homologación



Etapa 1 - Normativa

- FIPS 140-2 Nivel 1
- Common Criteria EAL 4+

Etapa 2 - Técnica

Funciones criptográficas (en el chip)	10	Generación de llaves RSA de 2048 bits
	11	Generación de Firma Digital
	12	Verificación de Firma Digital
	13	Operación de resumen (Hashing)
	14	Importación de cadenas de certificados digitales
	15	Uso de PIN como la credencial de autorización a las operaciones criptográficas en el dispositivo
	16	Almacenamiento seguro de llaves privadas protegidas con PINes
Middleware para PC	17	Librerías PKCS#11 v2.20 o superior para Windows
	18	Microsoft Minidriver

Dispositivos Homologados

Fabricante: Bit4ID
Modelo: IAm
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: Bit4ID
Modelo: CryptoKey
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: Bit4ID
Modelo: Touch&Sign 2048
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: SafeNet
Modelo iKey 4000
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: SafeNet
Modelo: eToken 5100
Certificación: FIPS 140-2
Diploma: Múltiple
Security Policy
Reporte de Homologación

Fabricante: SafeNet
Modelo: eToken PRO (Java)
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: Feitian
Modelo: ePass 2003
Certificación: FIPS 140-2
Diploma: Múltiple
Security Policy
Reporte de Homologación

Fabricante: Athena Smartcard
Modelo: IDProtect Key with LASER PKI
Certificación: FIPS 140-2
Diploma: Múltiple
Security Policy
Reporte de Homologación

Fabricante: Bit4ID
Modelo: tokenME
Certificación: FIPS 140-2
Diploma: Múltiple
Security Policy
Reporte de Homologación

24
dispositivos

Dispositivos Homologados

FEITIAN
WE BUILD SECURITY

bit4id

athena
Smartcard

LONGMAI
Shaping Your Information Security

acs

SAFRAN
Morpho

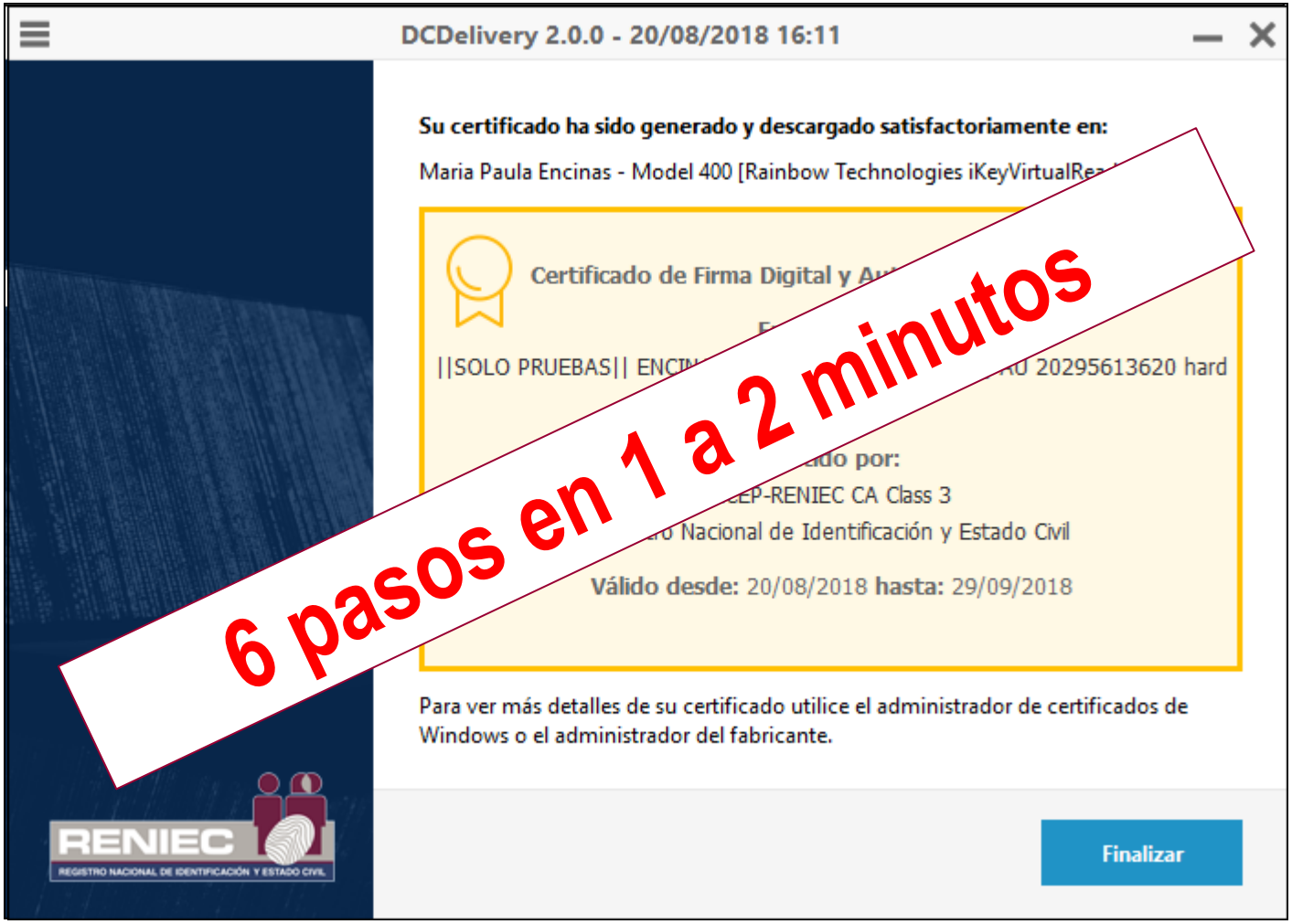
Sagem Orga
SAFRAN Group

cryptoVision

gemalto
SafeNet

RENIEC

Identidad digital



6 pasos en 1 a 2 minutos

Resultados

- ✓ Descarga rápida
- ✓ Procedimiento intuitivo
- ✓ Reducción de casos de soporte técnico (1 a 2 casos semanales)
- ✓ Único procedimiento para todos los dispositivos

RENIEC

Identidad digital

ECERNEP PERU CA ROOT 3
DCDelivery: Entrega de certificados digitales Class 3

REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC

Lima, agosto 2018.
PERÚ