SERVICIO DE SELLADO DE TIEMPO

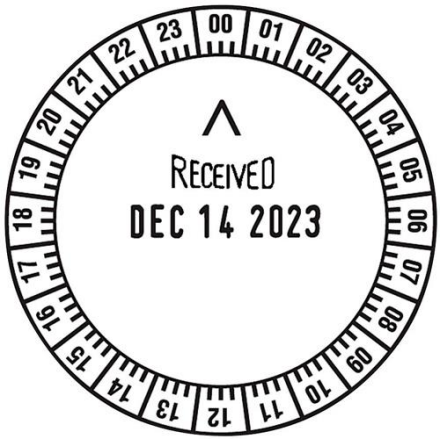
PSVA-TSA-RENIEC

Ing. Maria Paula Encinas Zevallos | Analista de Servicios PKI

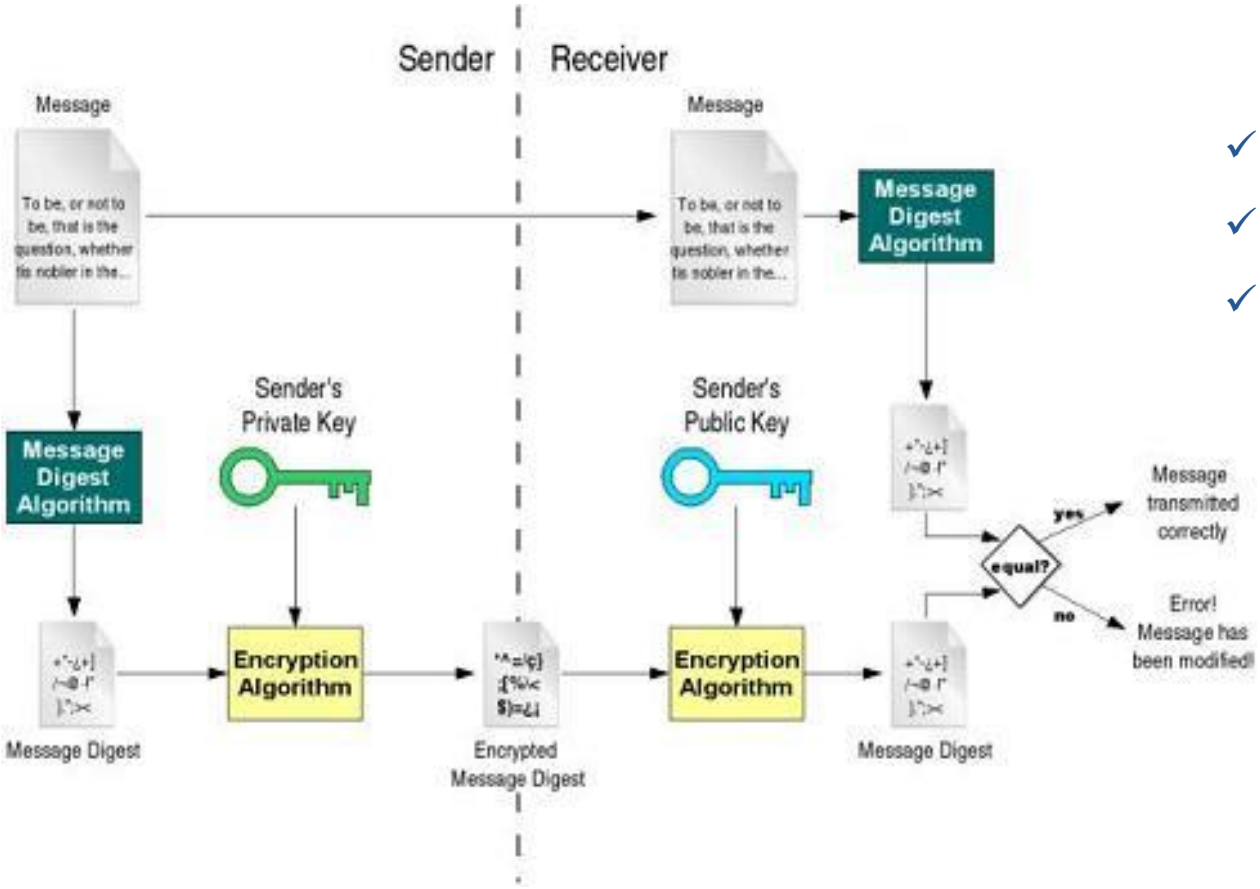
Sub Gerencia de Certificación e Identidad Digital

CONTENIDO

1. Conceptos: Firmas digitales, Sello y sellado de Tiempo
2. Estándares internacionales
3. Normativa Peruana
4. PSVA-TSA-RENIEC
5. Usos del sello de tiempo
6. Preguntas



1. CONCEPTOS BÁSICOS – FIRMA DIGITAL



- ✓ *Identidad del firmante*
- ✓ *Mensaje no alterado*
- ✓ *No repudio*

1. CONCEPTOS BÁSICOS – SELLO DE TIEMPO

- ✓ *Mensaje no alterado*
- ✓ *Existencia del mensaje en el momento que se selló*

1. CONCEPTOS BÁSICOS – SELLO DE TIEMPO

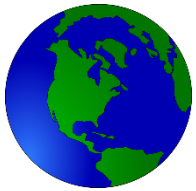
"A time-stamp on a document shows that this document existed at a certain point in time and has not been changed since."

Msc. Martín Augusto Gagliotti Vigil

Tustworthy and Efficient Protection Schemes for Digital Archiving

"Un sello de tiempo en un documento indica que ese documento existió en un determinado instante de tiempo y que no ha cambiado desde entonces"

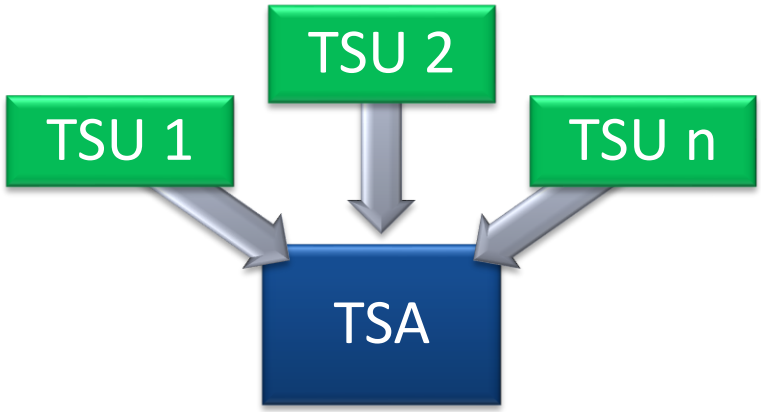
1. CONCEPTOS BÁSICOS – AUTORIDAD DE SELLADO DE TIEMPO



- ✓ *TSA: Time-Stamping Authority*

- ✓ *PSVA-TSA: Prestador de Servicios de Valor Añadido en modalidad de TSA*
- ✓ *PSVA-TSA-RENIEC: PSVA en modalidad TSA del RENIEC.*

1. CONCEPTOS BÁSICOS – TSU



- ✓ ***Hardware***
- ✓ ***Software*** — SignServer PKI by PrimeKey
- ✓ ***Llaves***
- ✓ ***Certificado***

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

ETSI EN 319-422

TSU: El conjunto de hardware y software que es gestionado como una unidad y tiene asociada una llave de emisión de sellos de tiempo a la vez.

2. ESTÁNDARES INTERNACIONALES

- Normativos
- Técnicos

IETF

RFC 3628
Internet X.509 Public Key Infrastructure
Time-Stamp Protocol (TSP)

RFC 3161
Internet X.509 Public Key Infrastructure
Time-Stamp Protocol (TSP)

ETSI

ETSI EN 319 421
Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

ETSI EN 319 422
Time-stamping protocol and time-stamp token profiles

PKI Estándares

3. NORMATIVA PERUANA

1

- Ley de Firmas y Certificados Digitales
  Ley N° 27269

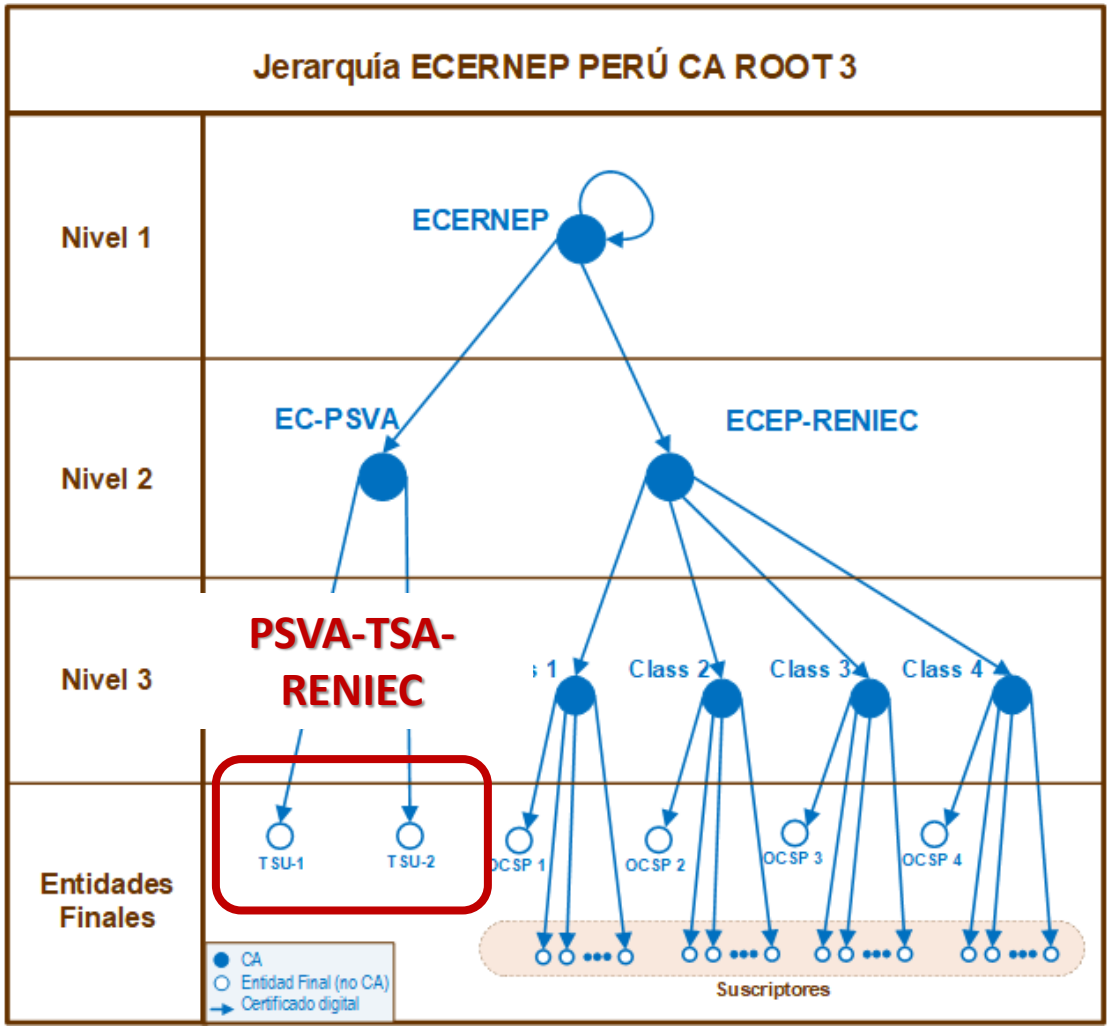
2

- Reglamento de la Ley de Firmas y Certificados Digitales D.S. 052-2008-PCM (19JUL2008)
- Modificatoria D.S. 026-2016-PCM (29ABR2016)

3

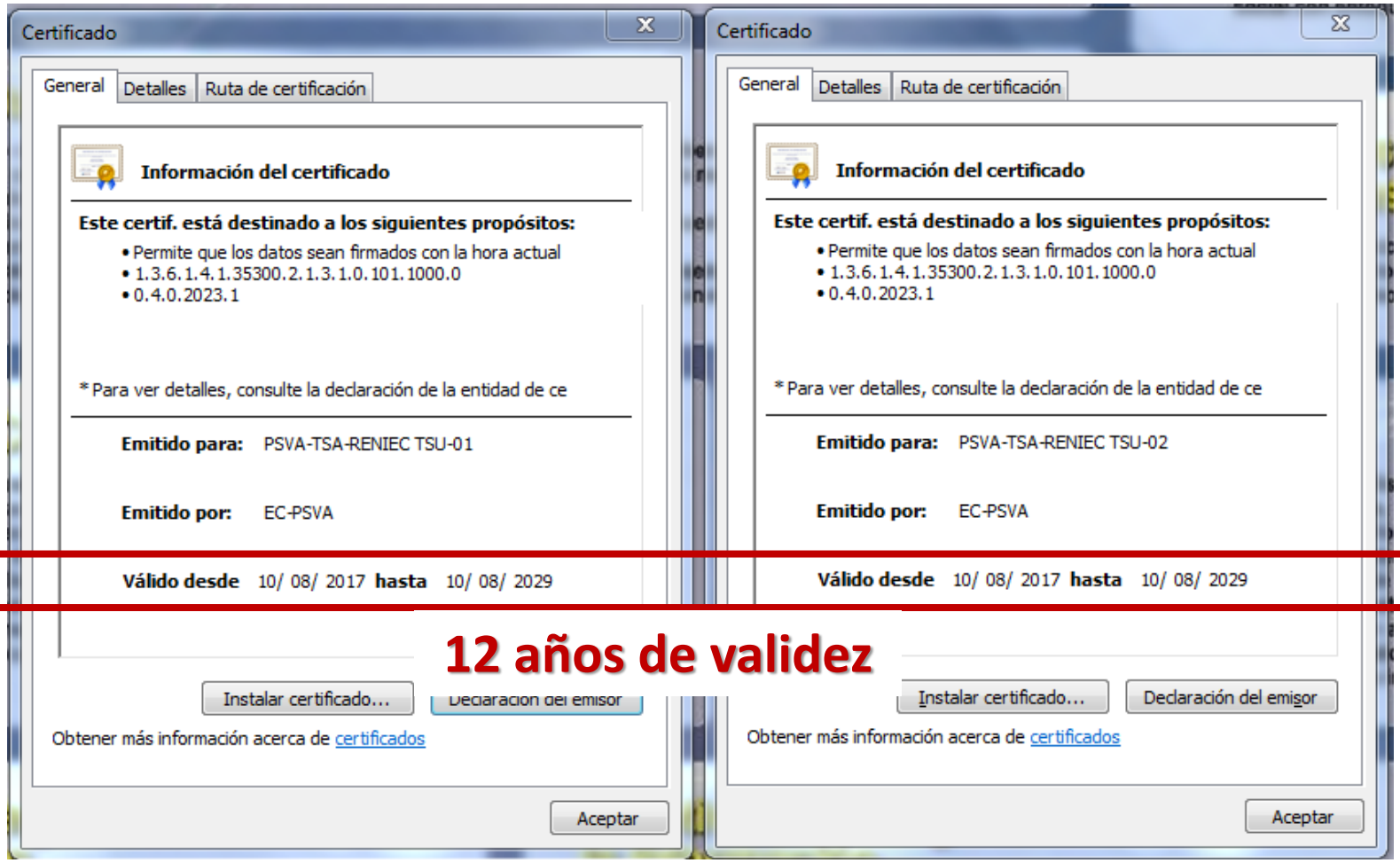
- Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA

4. PSVA-TSA-RENIEC



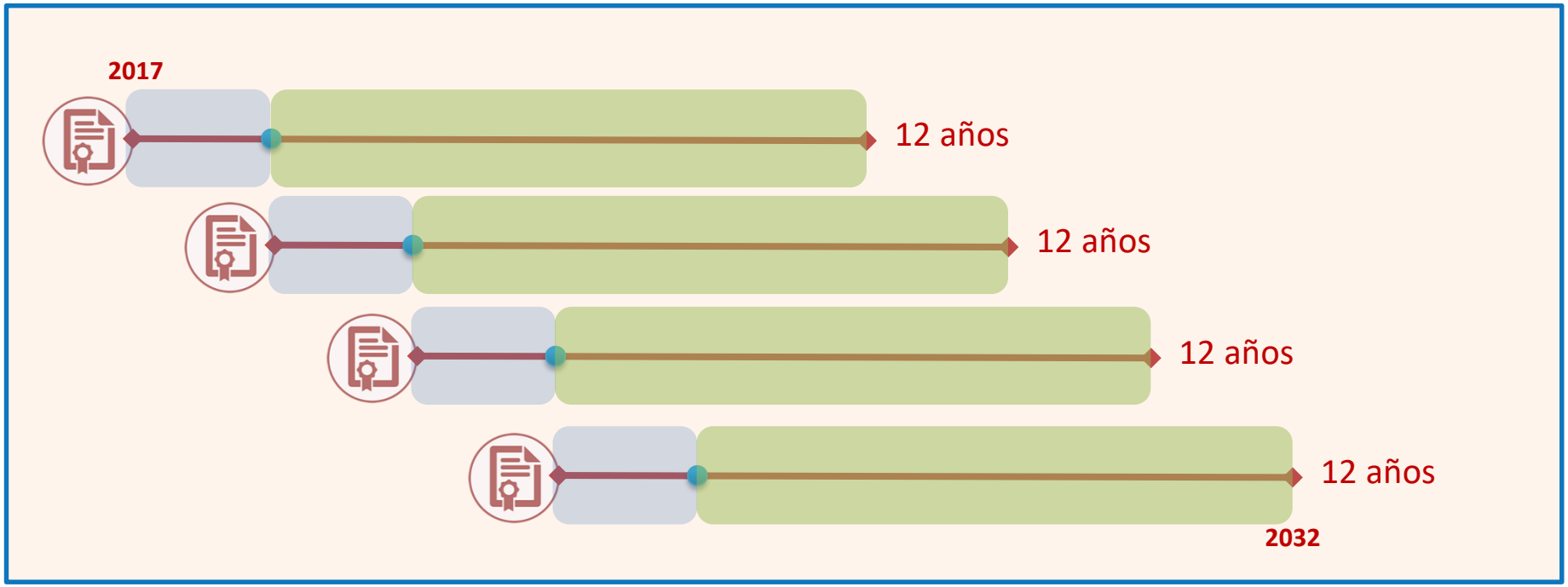
- ✓ *2 certificados TSU*

4. PSVA-TSA-RENIEC



12 años de validez

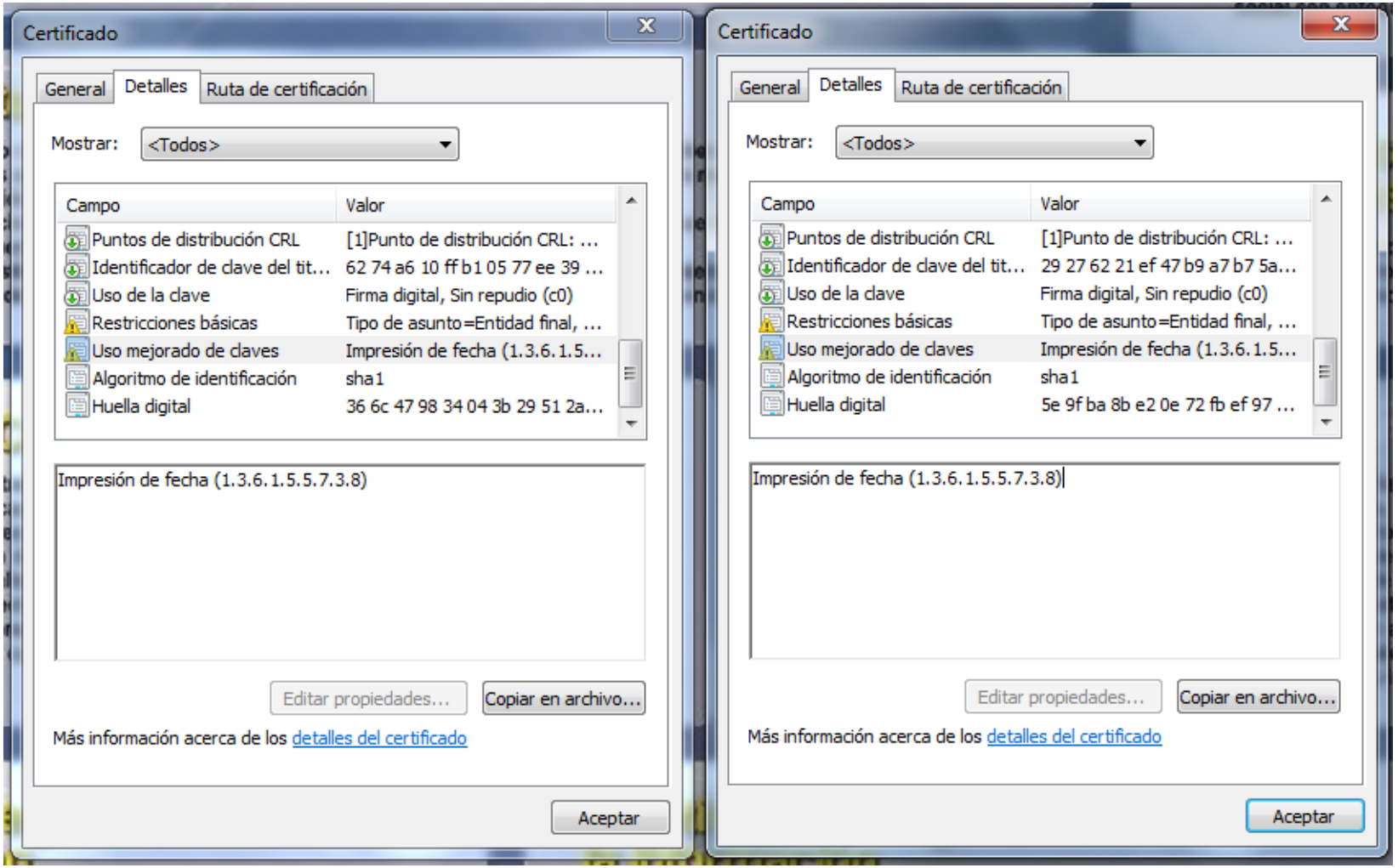
4. PSVA-TSA-RENIEC: CICLO DE VIDA DEL CERTIFICADO TSU



Periodo de uso de la llave privada: 1 año

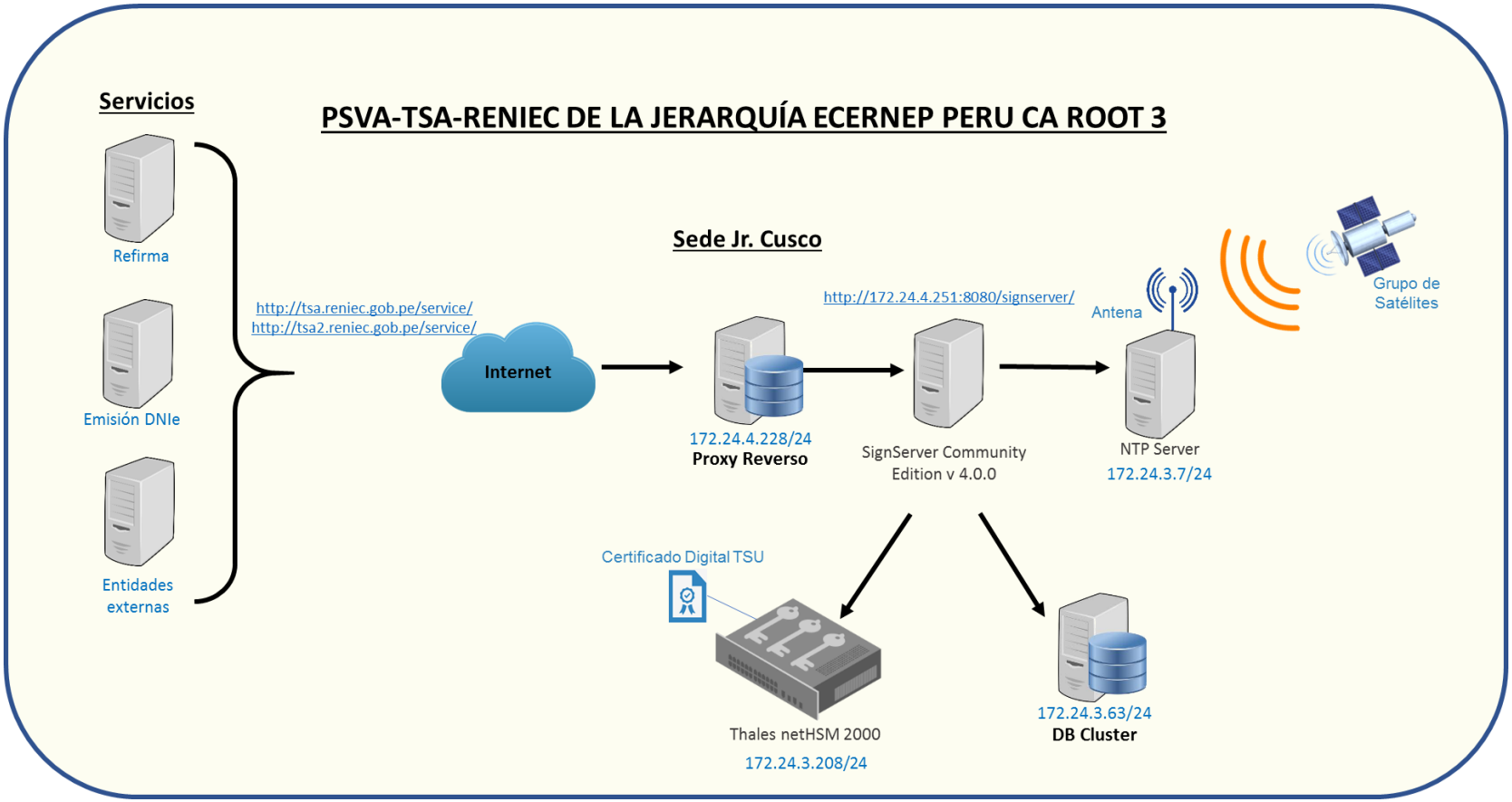
Periodo mínimo de verificación: 11 años

4. CERTIFICADOS TSU



4. PSVA-TSA-RENIEC

http://tsa.reniec.gob.pe/service/
http://tsa2.reniec.gob.pe/service/



5. USOS DEL SELLO DE TIEMPO

1

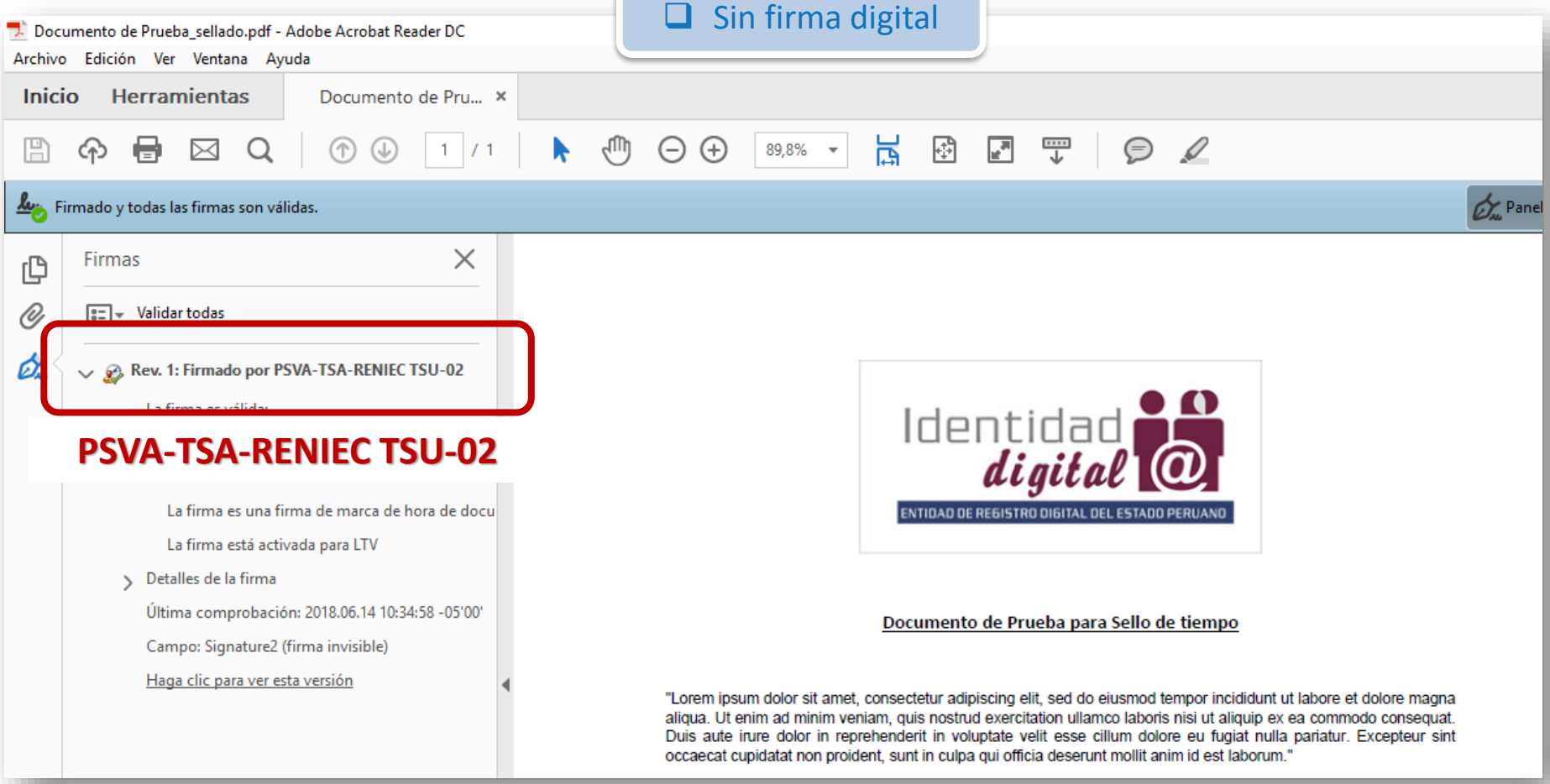
❖ Sin firma digital

2

❖ Con firma digital

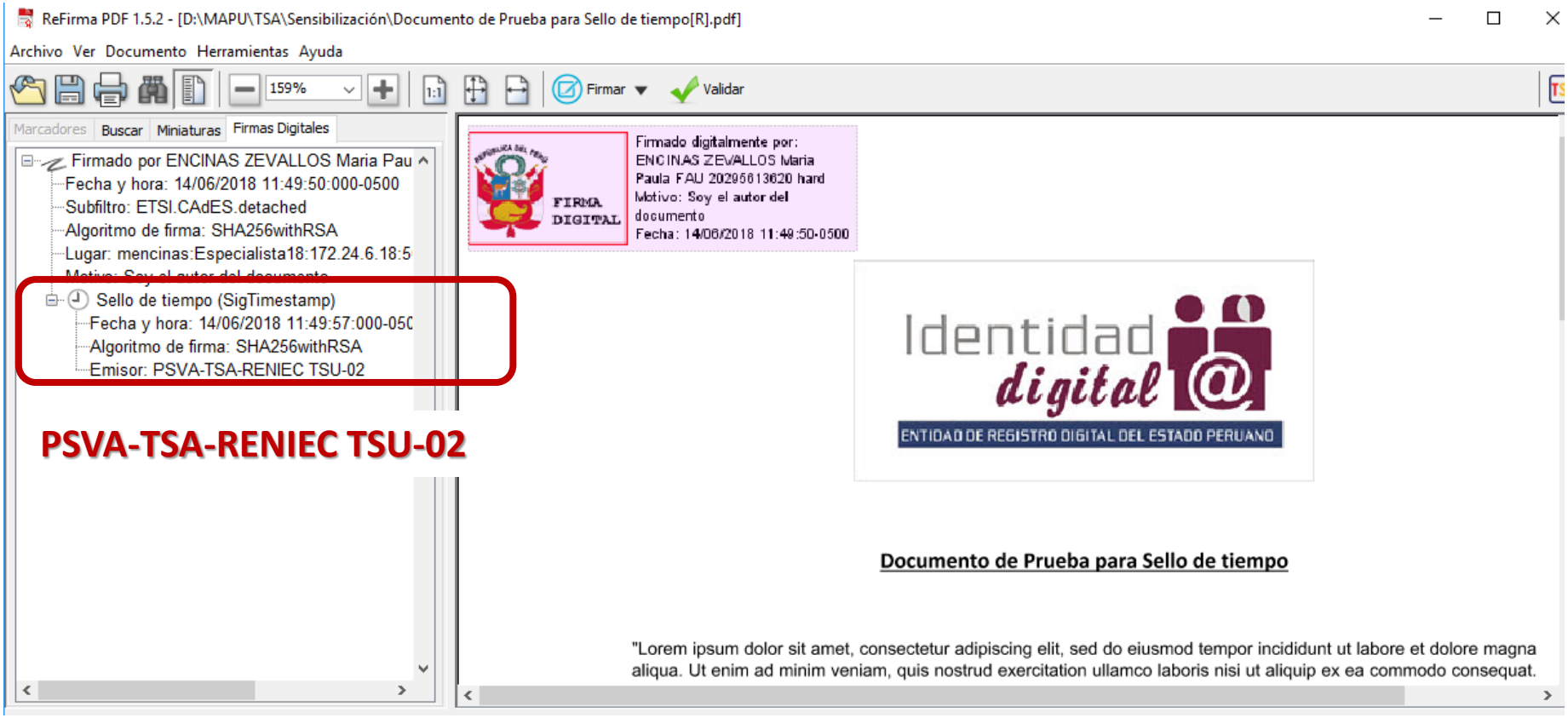
5. USOS DEL SELLO DE TIEMPO

❑ Sin firma digital

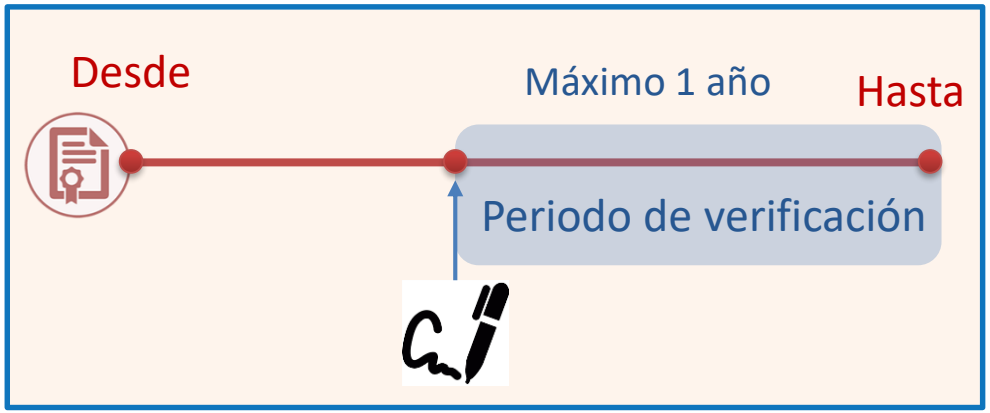


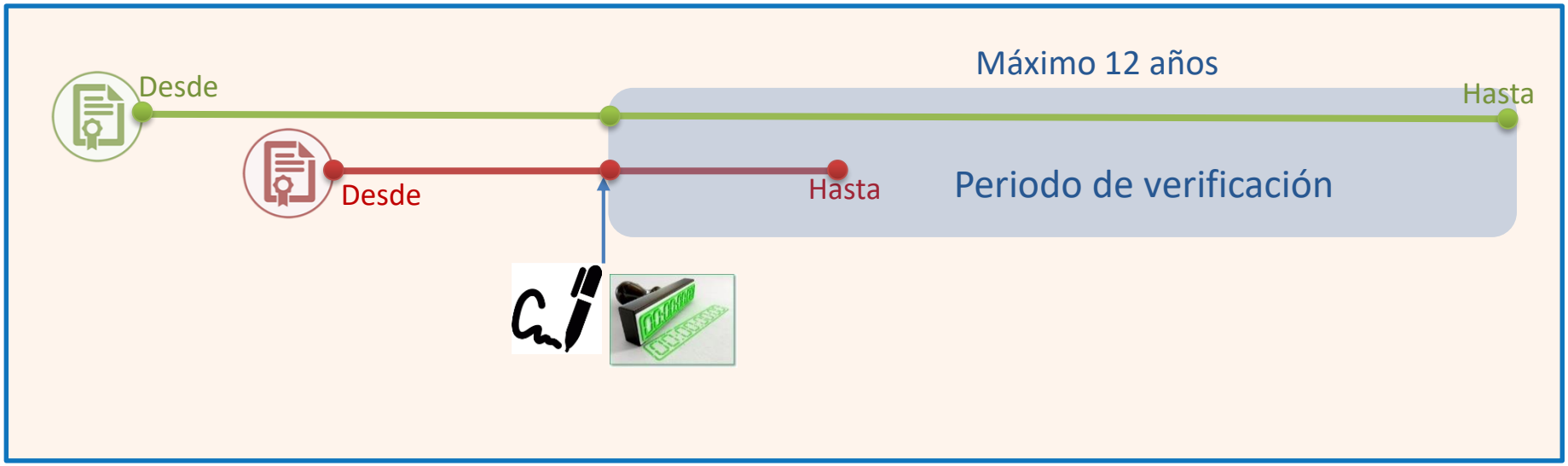
5. USOS DEL SELLO DE TIEMPO

❑ Con firma digital



5. USOS COMUNES





5. USOS DEL SELLO DE TIEMPO

❑ Sin firma digital

- Resellado periódico
- Long-term Validation (LVT)
  → Validez a largo plazo

❑ Con firma digital

- Microformas
- Facturas electrónicas
- Planillas del personal

SERVICIO DE SELLADO DE TIEMPO

PSVA-TSA-RENIEC