tanda tangan digital

TANDA TANGAN DIGITAL UNTUK APLIKASI PERKANTORAN

Ricky Prajoyo

KOMINFO

SERTIFIKAT DIGITAL

- Sertifikat digital adalah *credential* digital yang memberikan informasi tentang identitas dari suatu entitas serta informasi lainnya.
- Sertifikat digital diterbitkan oleh Certificate Authority (CA).
- CA menjamin validitas informasi di dalam sertifikat

JENIS SERTIFIKAT DIGITAL

- Sertifikat user/client
- Sertifikat server

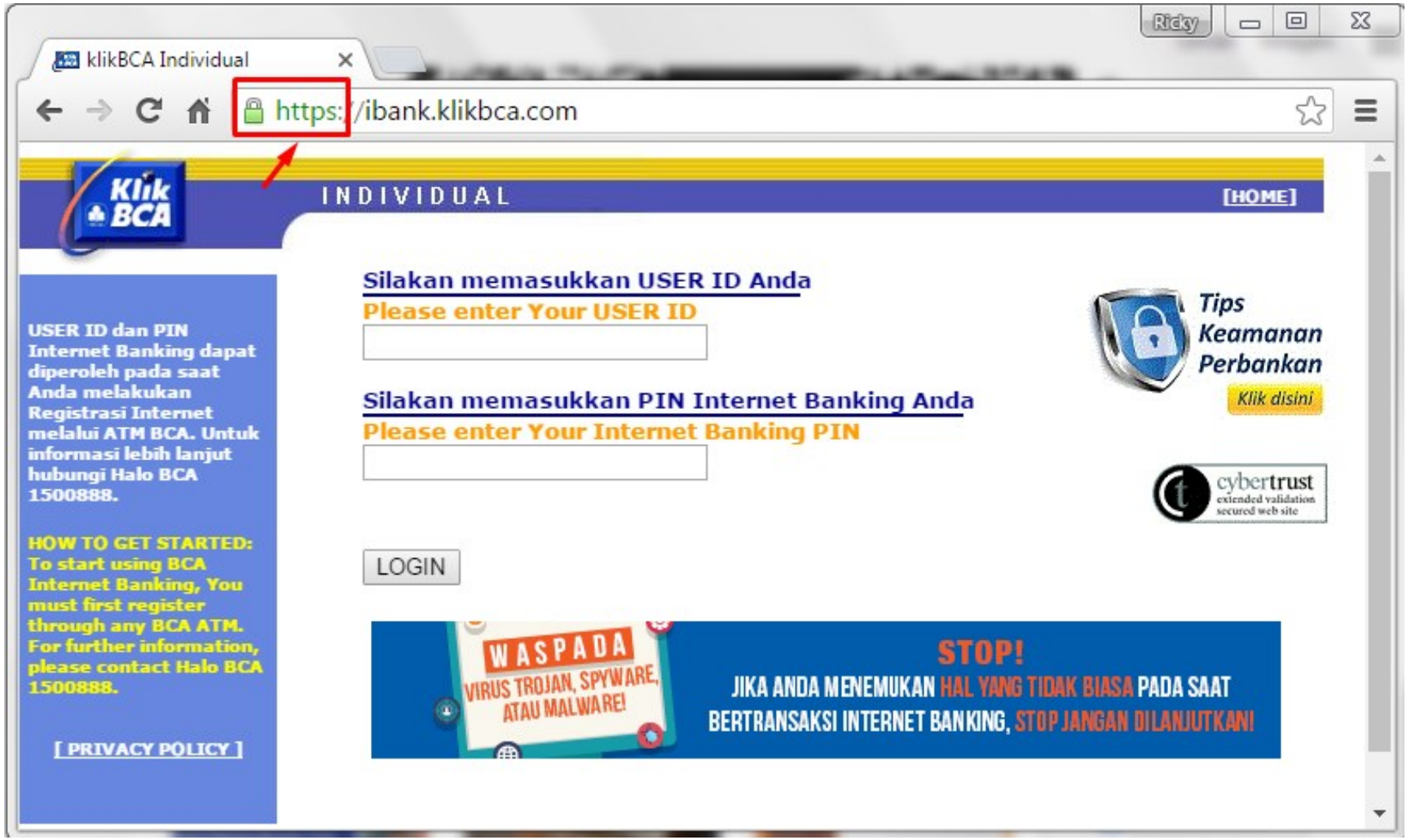
KEGUNAAN SERTIFIKAT DIGITAL

- Enkripsi dan/atau otentikasi email
- Enkripsi dan/atau otentikasi dokumen
- Otentikasi pengguna pada suatu aplikasi
- Mengamankan protokol komunikasi
- Otentikasi software desktop/mobile

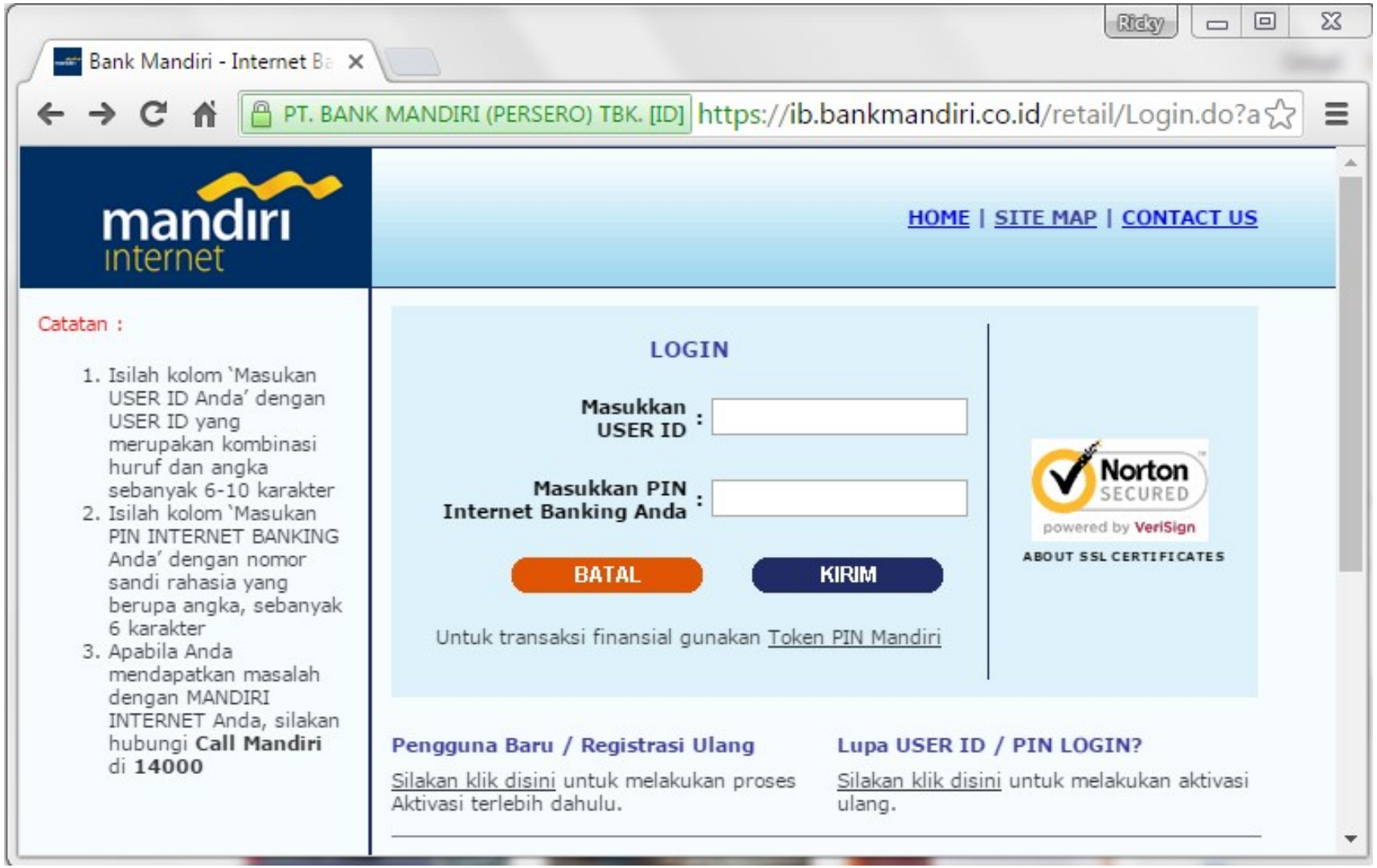
IMPLEMENTASI SERTIFIKAT DIGITAL

- Smartcard
  - Access badge
  - Access control
  - Biometric passport
  - Electronic money
  - Identity document
  - Keycard lock
  - Open Smart Card Development Platform
  - Payment Card Industry Data Security Standard
  - Proximity card
- SSL

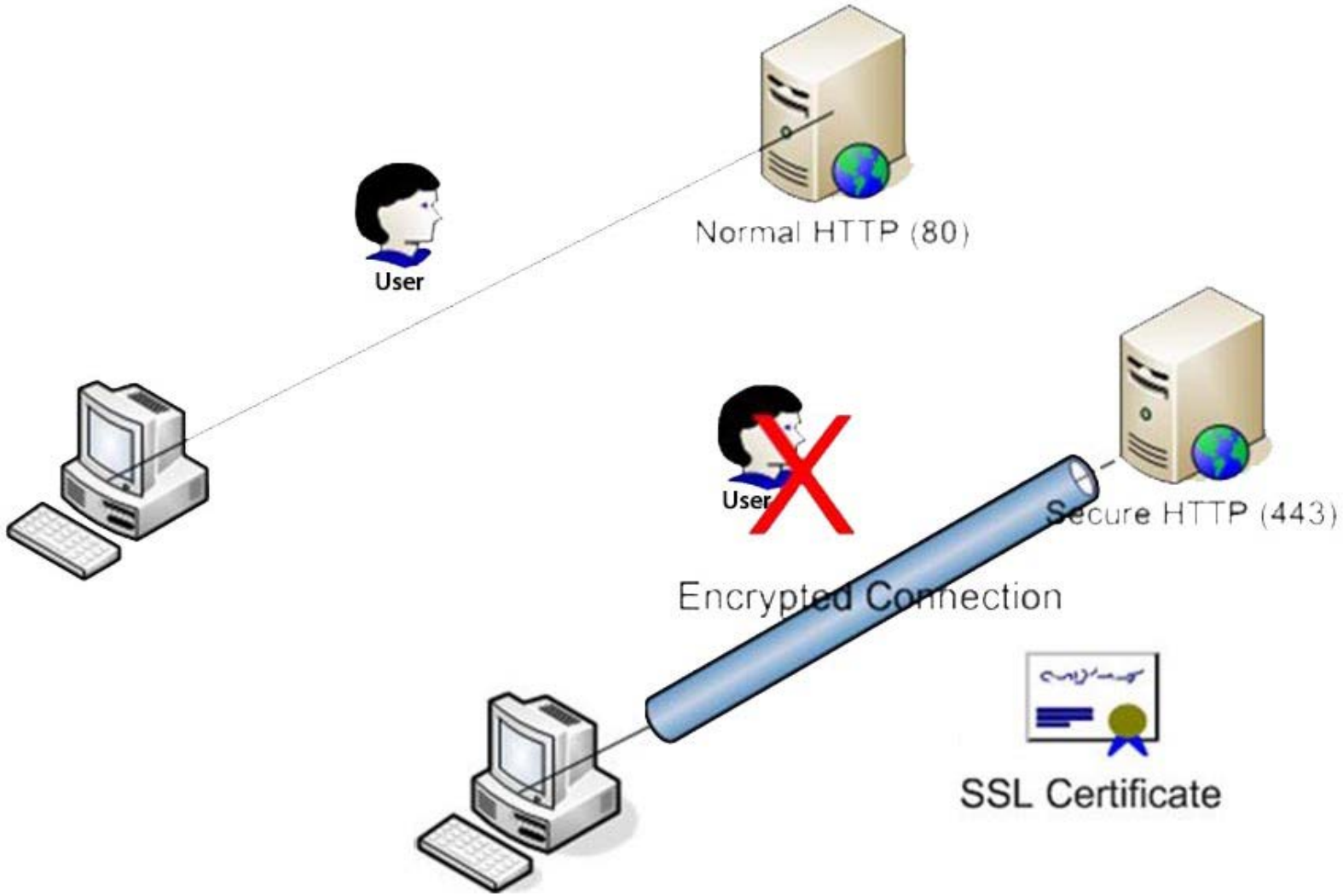
HTTPS/SSL (SECURE SOCKETS LAYER)



SSL –EV (EXTENDED VALIDATION)



HTTP VS HTTPS

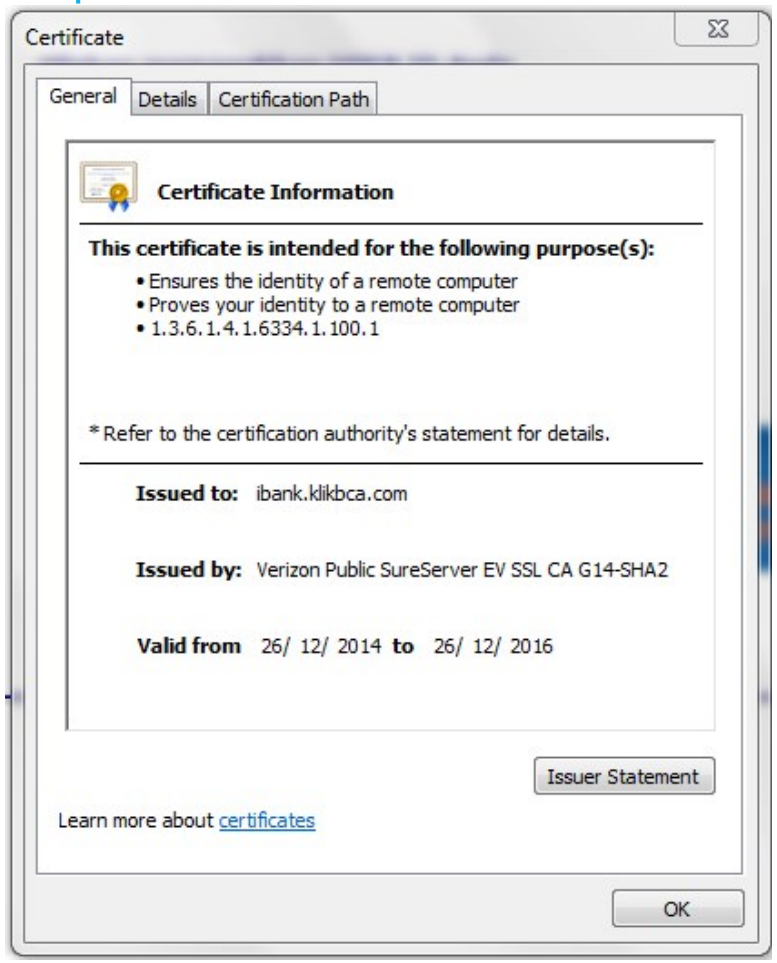


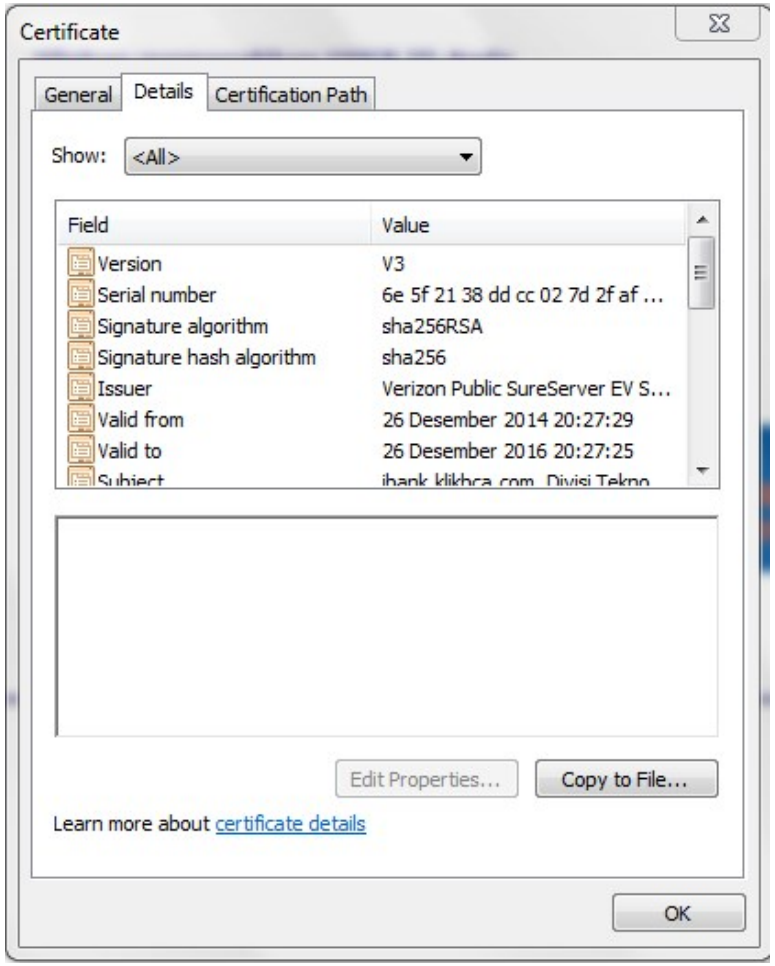
STRUKTUR SERTIFIKAT DIGITAL: X509

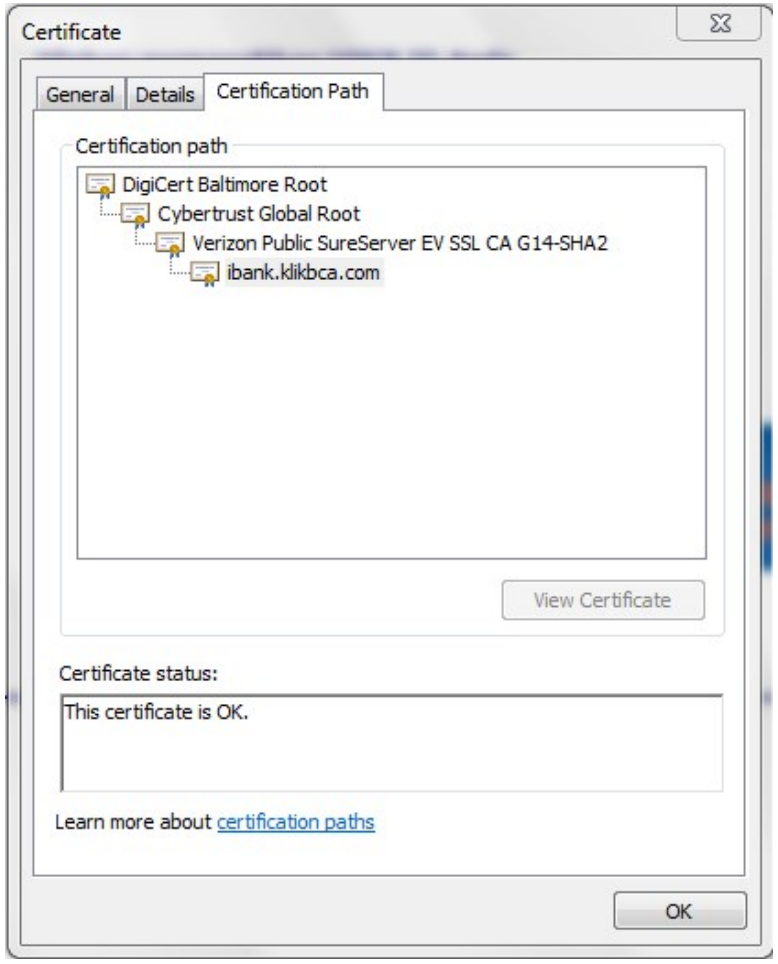
- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
    - ...
- Certificate Signature Algorithm
- Certificate Signature

tanda tangan digital

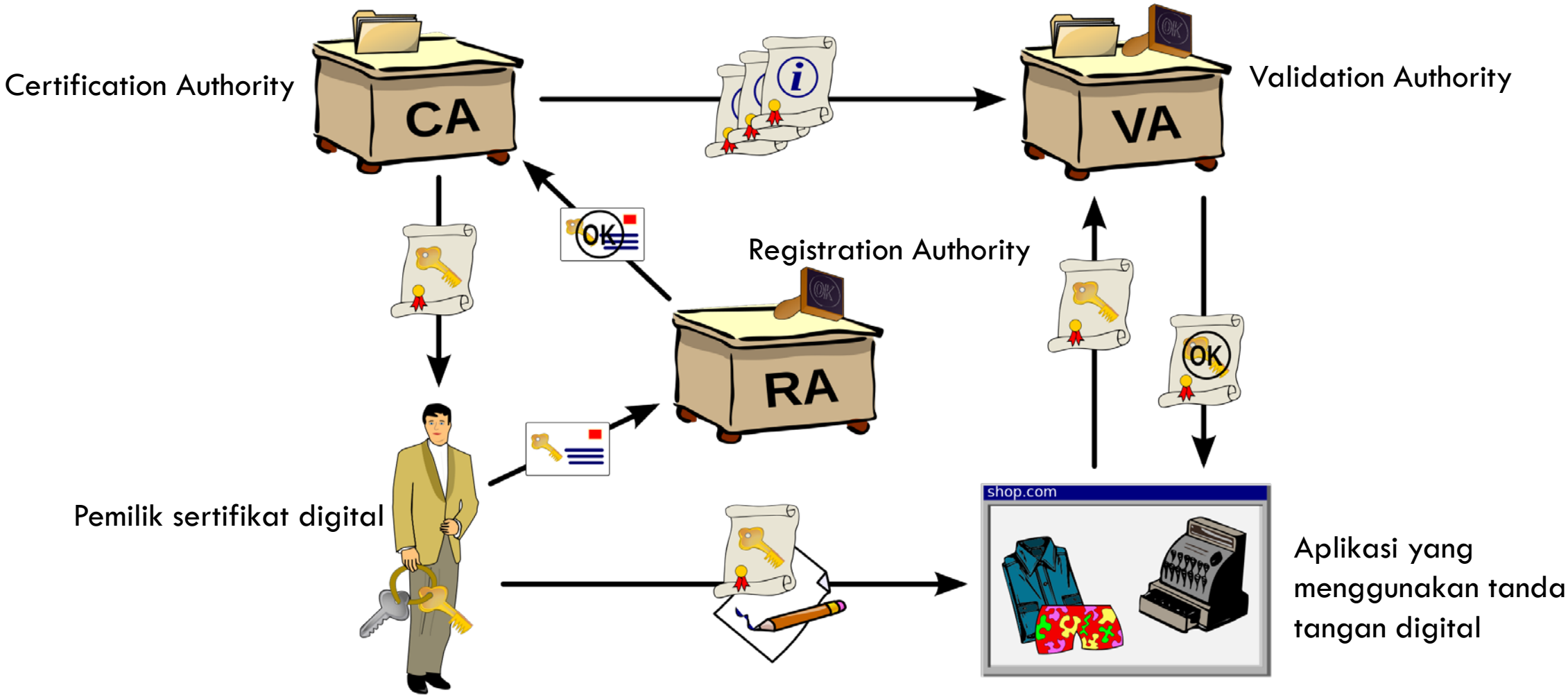
CONTOH SERTIFIKAT DIGITAL



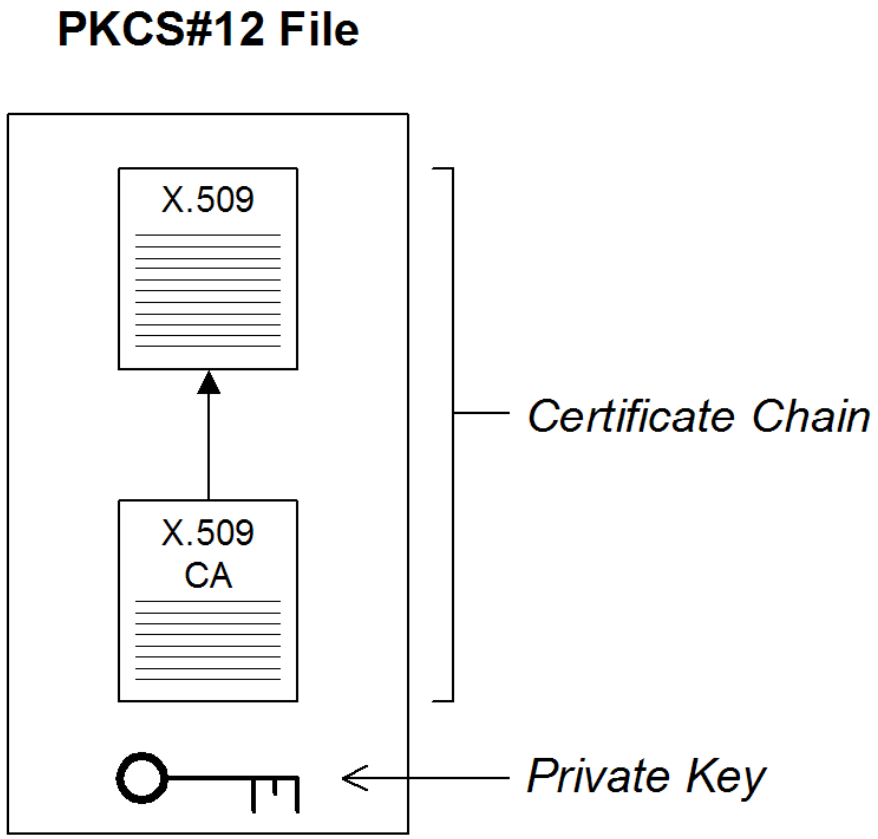


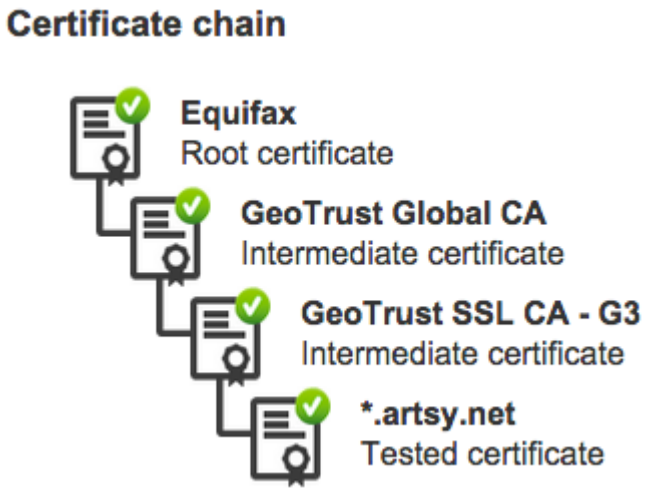


MEMBUAT DAN MEMVERIFIKASI SERTIFIKAT DIGITAL

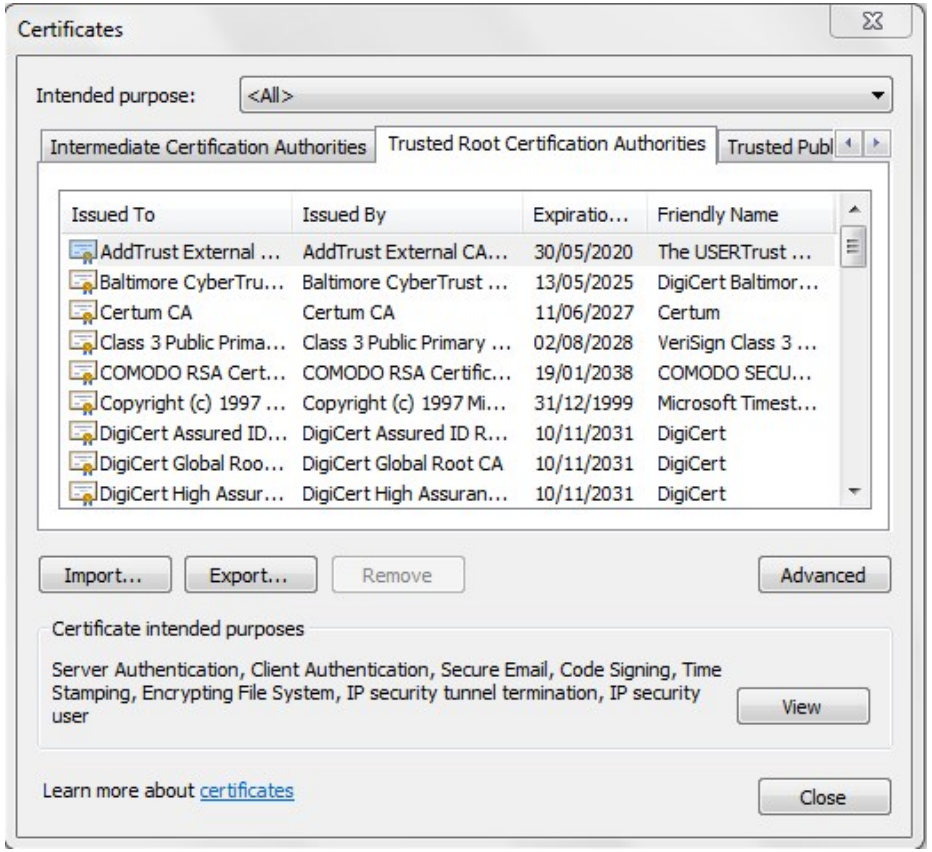


METODE PENYIMPANAN PRIVATE KEY DAN SERTIFIKAT DIGITAL: FORMAT P12

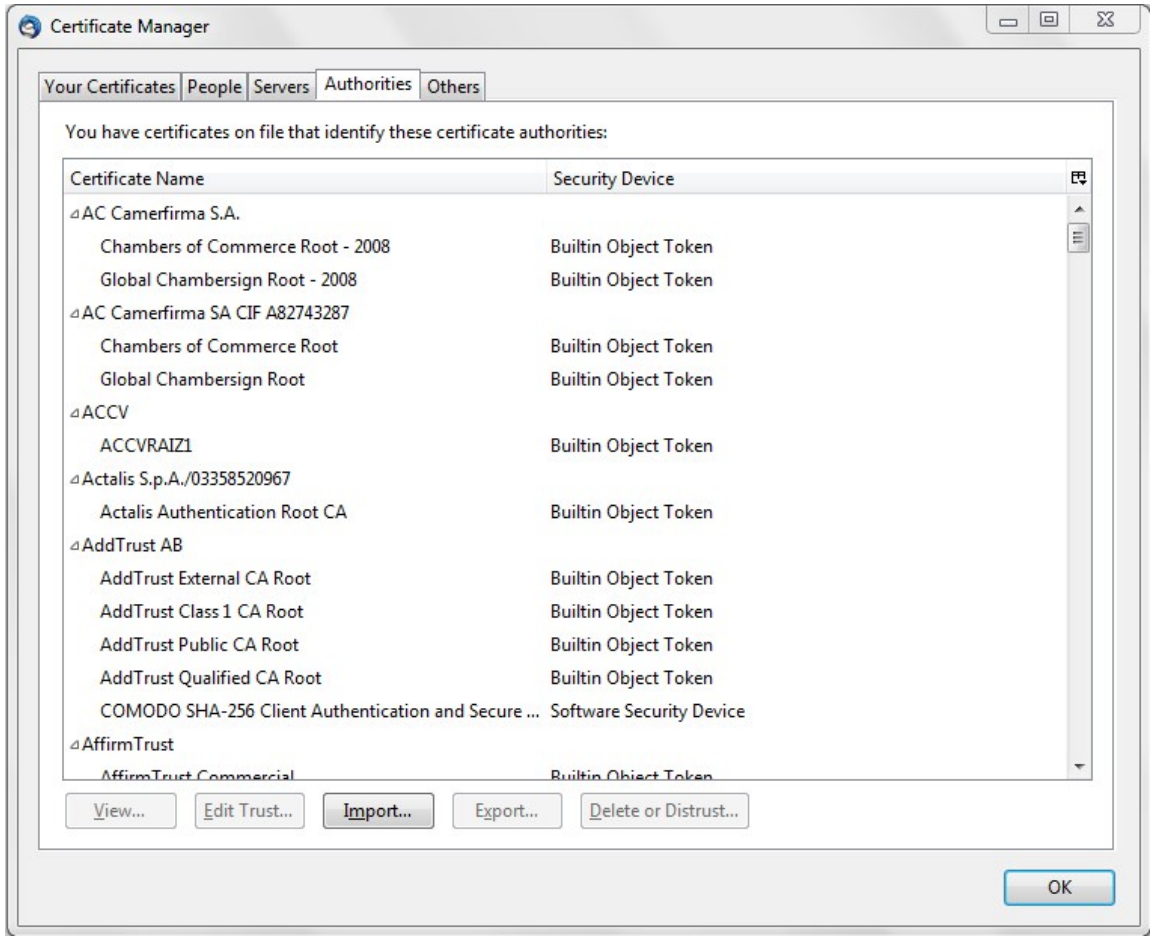




REPOSITORY (TEMPAT PENYIMPANAN) SERTIFIKAT DIGITAL



Microsoft



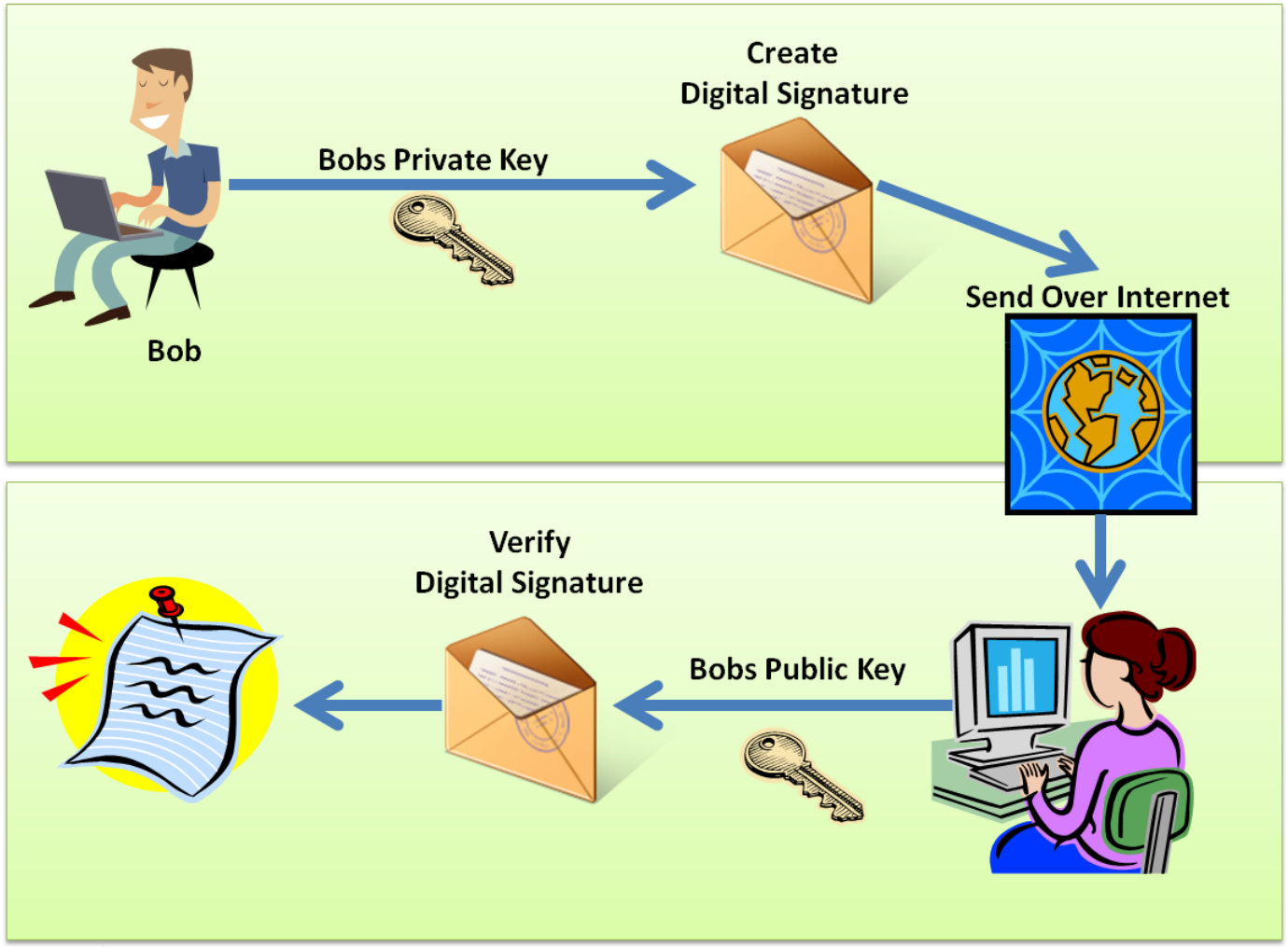
Mozilla

CARA IMPORT SERTIFIKAT DIGITAL

- Double click pada file p12 >> import ke sistem operasi (MS Windows, OSX)
- Import menggunakan Internet Explorer (MS Windows)
- Import menggunakan Google Chrome (MS Windows, OSX, Linux)
- Menggunakan Certificate Manager (CERTMGR) (MS Windows)
- Khusus untuk produk Mozilla, harus diimport terpisah (MS Windows, OSX, Linux)

tanda tangan digital

TANDA TANGAN DIGITAL

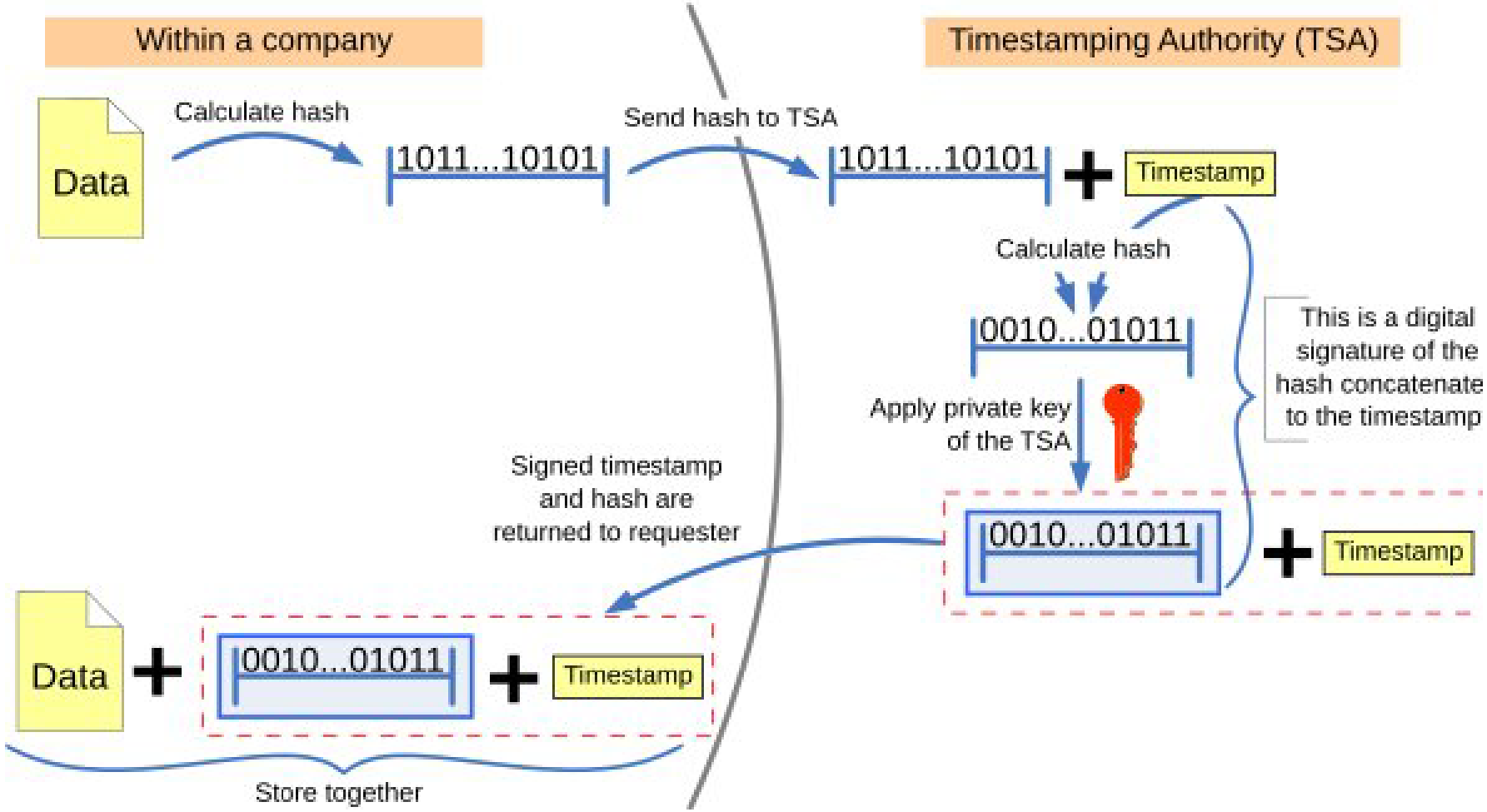


TRUSTED (DIGITAL) TIMESTAMPING

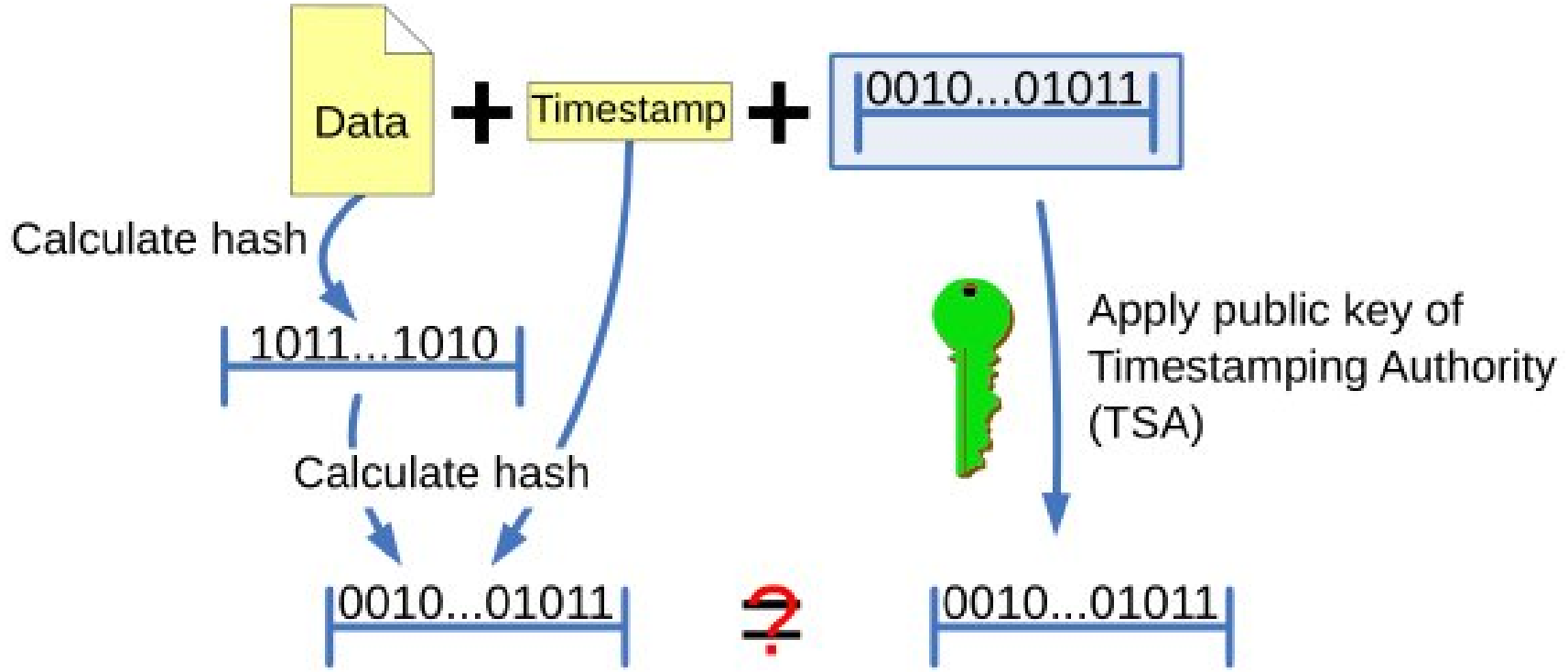
Trusted Timestamping adalah proses untuk menyimpan secara aman segala bentuk perubahan dan modifikasi **waktu** pada dokumen.

Secara aman di atas maksudnya adalah menjaga **integritas waktu** penandatanganan sehingga tidak dapat dimodifikasi (bahkan oleh penandatangan dokumen).

TRUSTED (DIGITAL) TIMESTAMPING



VERIFIKASI TIMESTAMP



If the calculated hashcode equals the result of the decrypted signature, neither the document or timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.

DEMO TANDA TANGAN DIGITAL PADA APLIKASI PERKANTORAN

tanda tangan digital

Tanda Tangan Digital pada Dokumen Microsoft Office, Libre Office

Tanda Tangan Digital pada PDF

Tanda Tangan Digital pada Email (Thunderbird)

CONTOH TIMESTAMP AUTHORITY

https://tsa.rootca.or.id/

TERIMA KASIH

Ricky Prajoyo

ricky.p@kominfo.go.id