



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

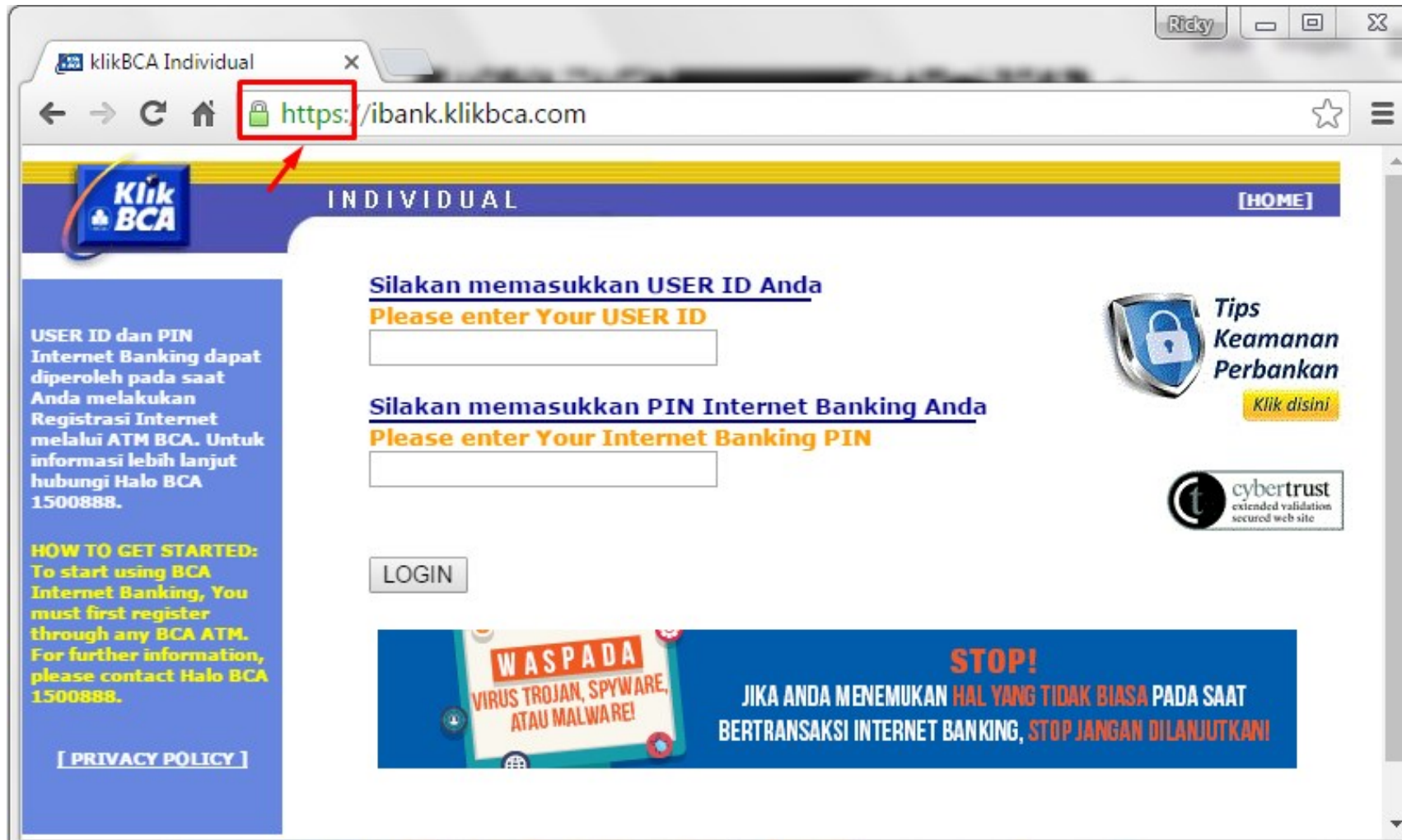
- Enkripsi dan/atau otentikasi email
- Enkripsi dan/atau otentikasi dokumen
- Otentikasi pengguna pada suatu aplikasi
- Mengamankan protokol komunikasi
- Otentikasi software desktop/mobile

# IMPLEMENTASI SERTIFIKAT DIGITAL

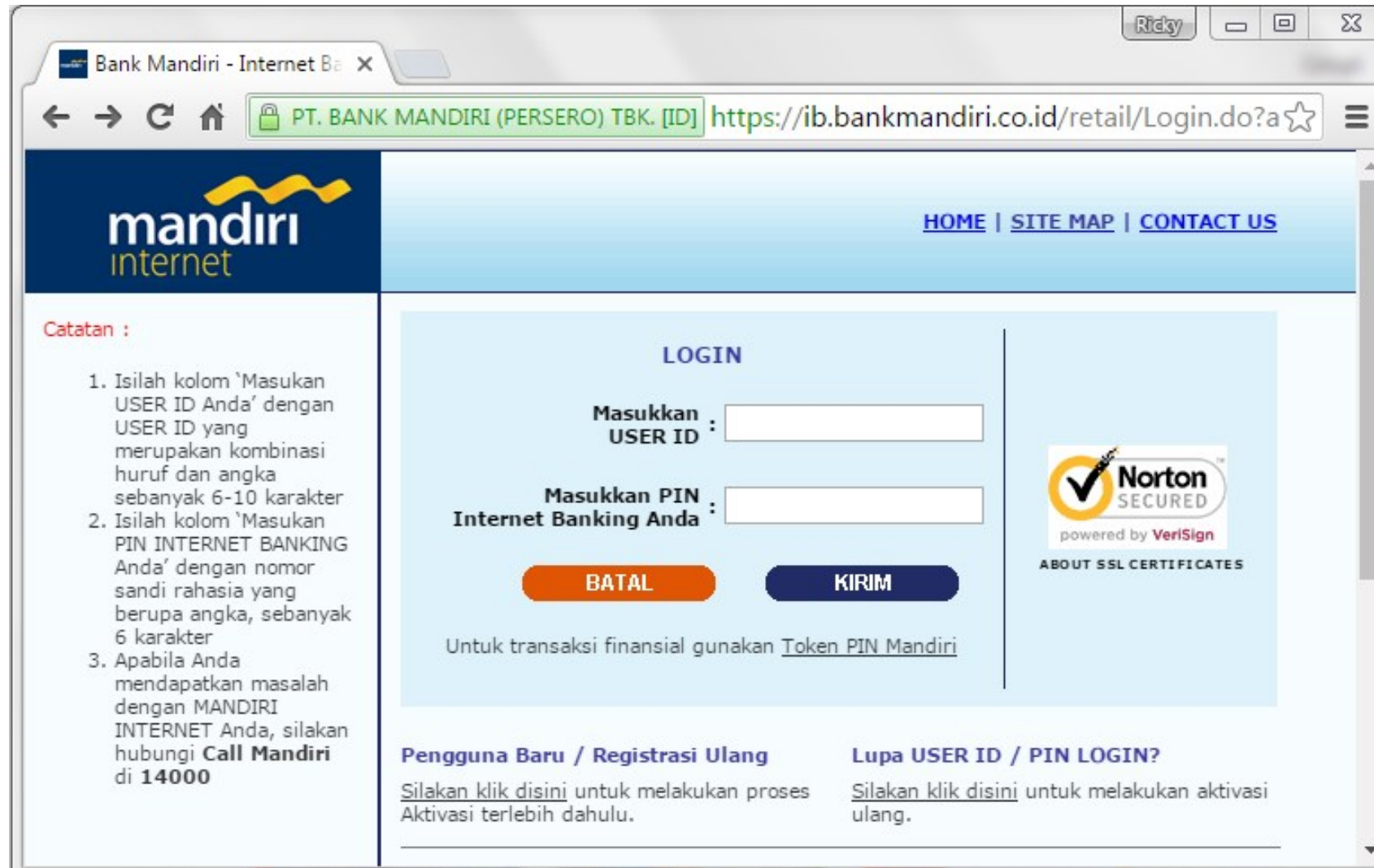
- Smartcard
  - Access badge
  - Access control
  - Biometric passport
  - Electronic money
  - Identity document
  - Keycard lock
  - Open Smart Card Development Platform
  - Payment Card Industry Data Security Standard
  - Proximity card
- SSL



# HTTPS/SSL (SECURE SOCKETS LAYER)



# SSL —EV (EXTENDED VALIDATION)



Bank Mandiri - Internet Banking

PT. BANK MANDIRI (PERSERO) TBK. [ID] [https://ib.bankmandiri.co.id/retail/Login.do?...](https://ib.bankmandiri.co.id/retail/Login.do?)

**mandiri internet**

[HOME](#) | [SITE MAP](#) | [CONTACT US](#)

**Catatan :**

1. Isilah kolom 'Masukan USER ID Anda' dengan USER ID yang merupakan kombinasi huruf dan angka sebanyak 6-10 karakter
2. Isilah kolom 'Masukan PIN INTERNET BANKING Anda' dengan nomor sandi rahasia yang berupa angka, sebanyak 6 karakter
3. Apabila Anda mendapatkan masalah dengan MANDIRI INTERNET Anda, silakan hubungi **Call Mandiri** di **14000**

**LOGIN**

Masukkan USER ID :

Masukkan PIN Internet Banking Anda :

**BATAL** **KIRIM**

Untuk transaksi finansial gunakan [Token PIN Mandiri](#)

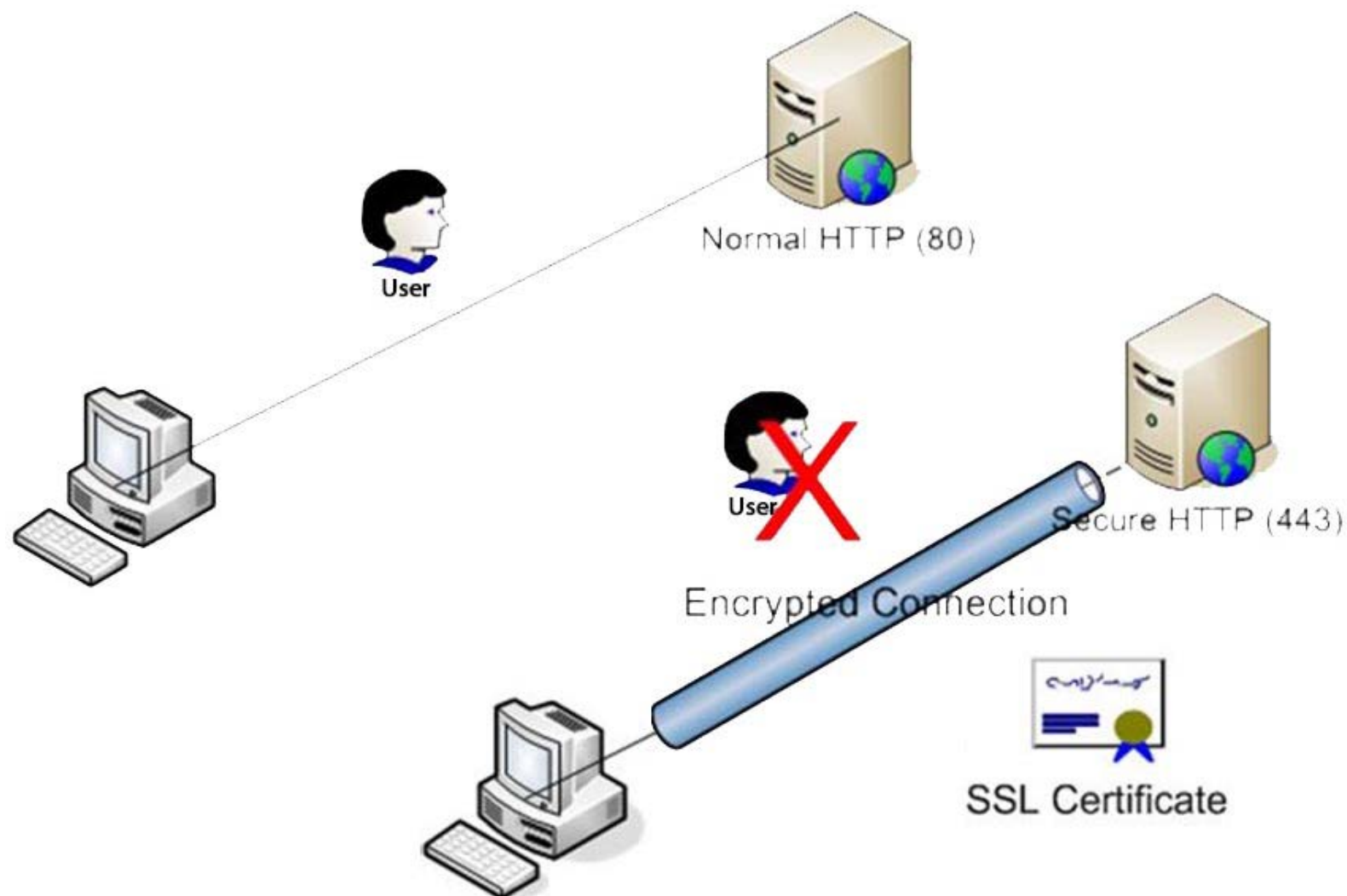
**Pengguna Baru / Registrasi Ulang**  
[Silakan klik disini](#) untuk melakukan proses Aktivasi terlebih dahulu.

**Lupa USER ID / PIN LOGIN?**  
[Silakan klik disini](#) untuk melakukan aktivasi ulang.

**Norton SECURED**  
powered by VeriSign  
ABOUT SSL CERTIFICATES



# HTTP VS HTTPS

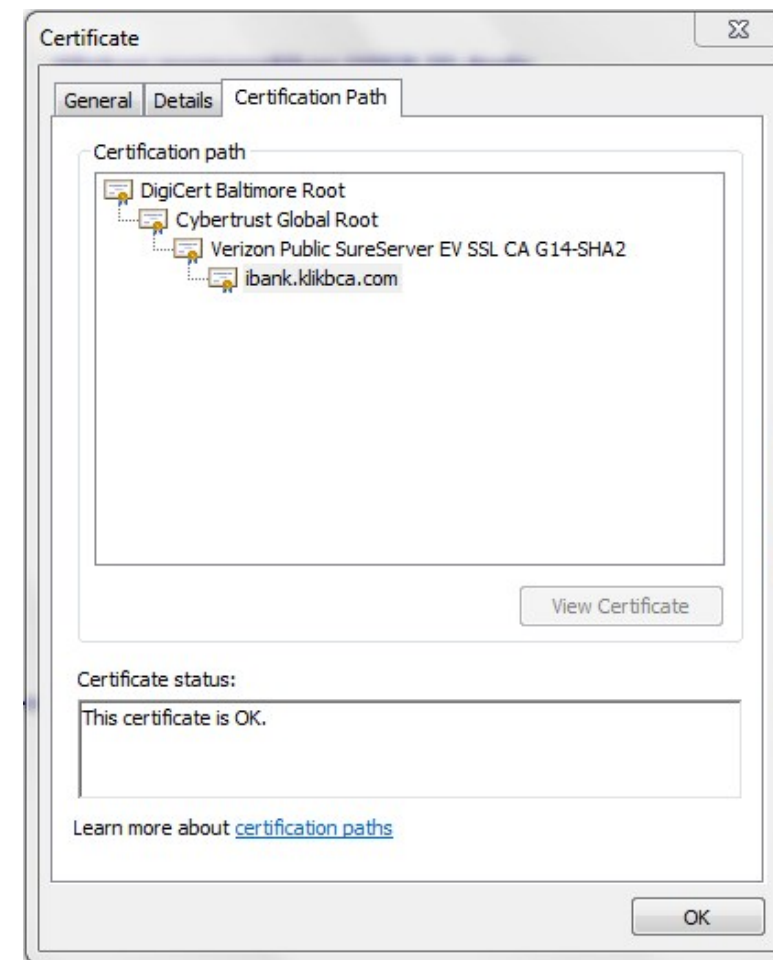
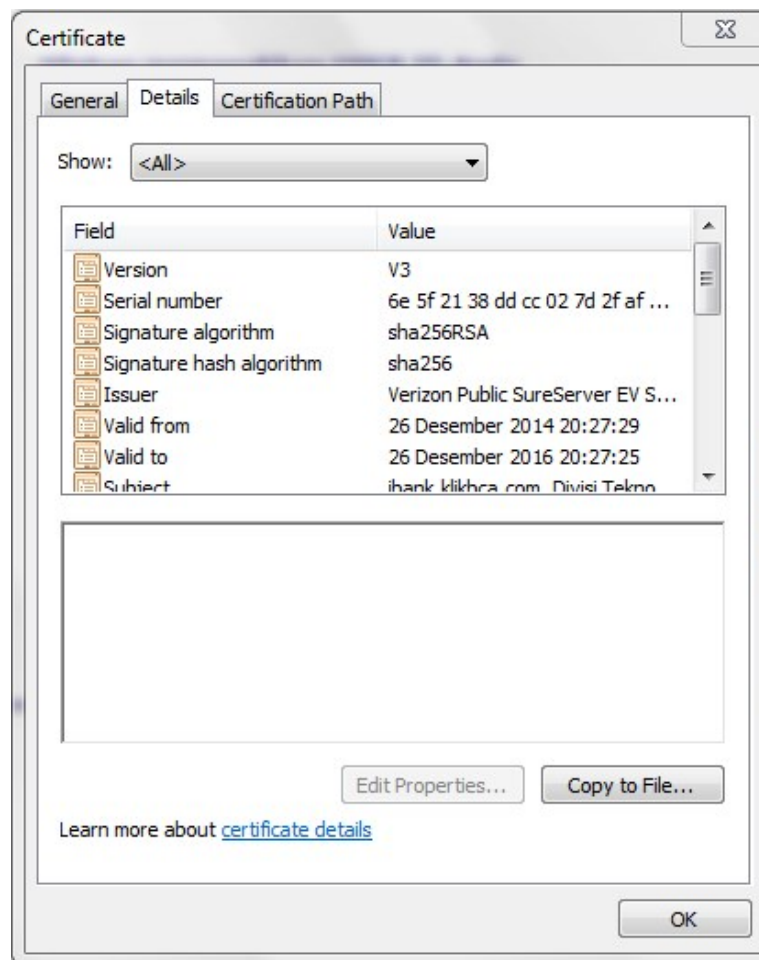
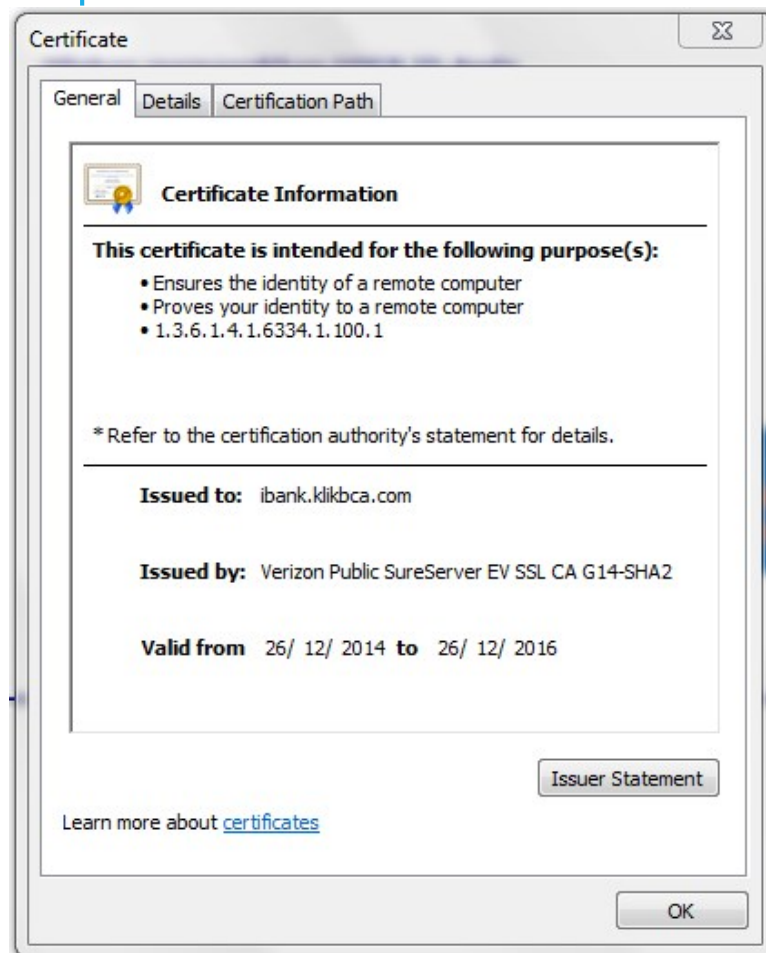




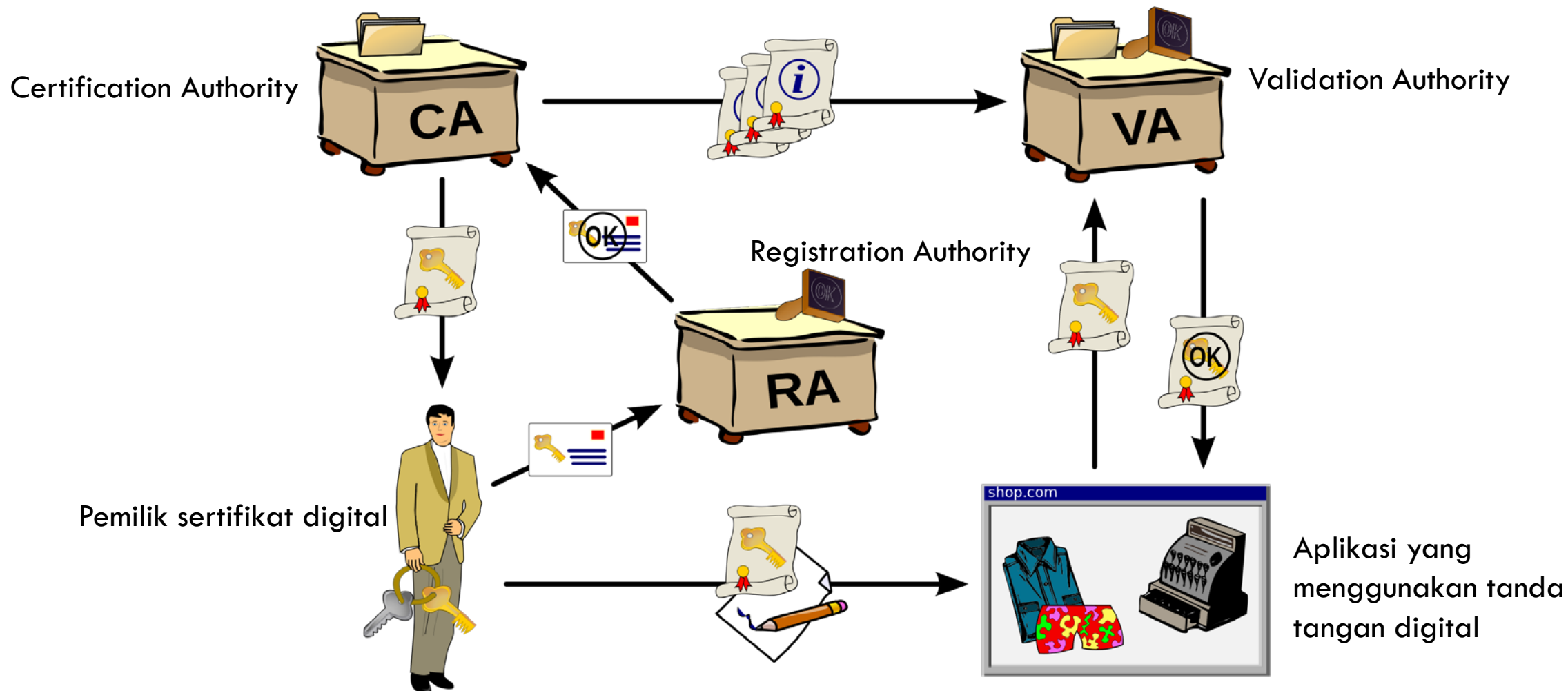
# STRUKTUR SERTIFIKAT DIGITAL: X509

- 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

# CONTOH SERTIFIKAT DIGITAL

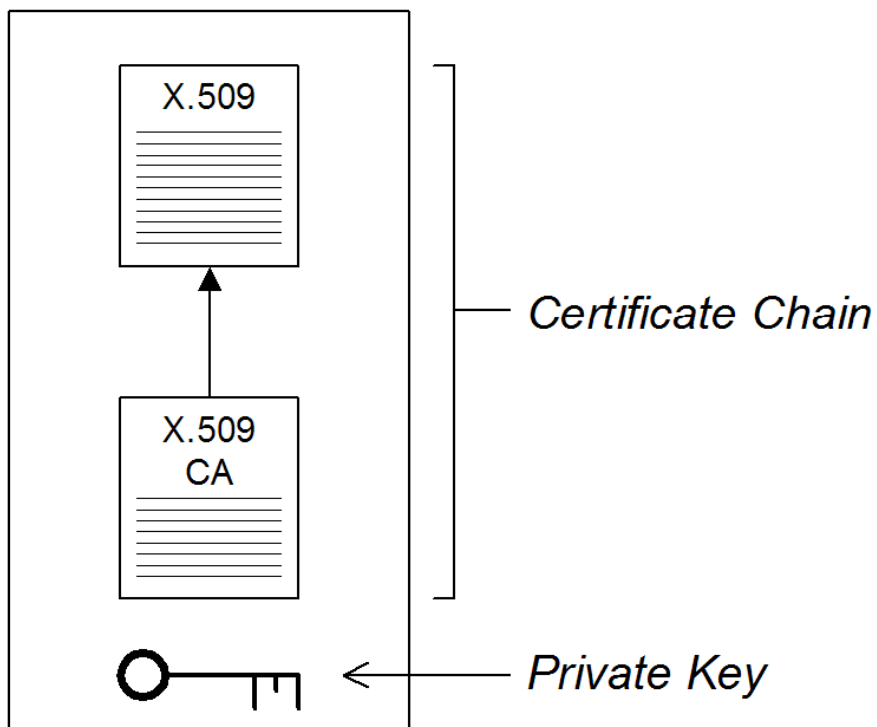


# MEMBUAT DAN MEMVERIFIKASI SERTIFIKAT DIGITAL

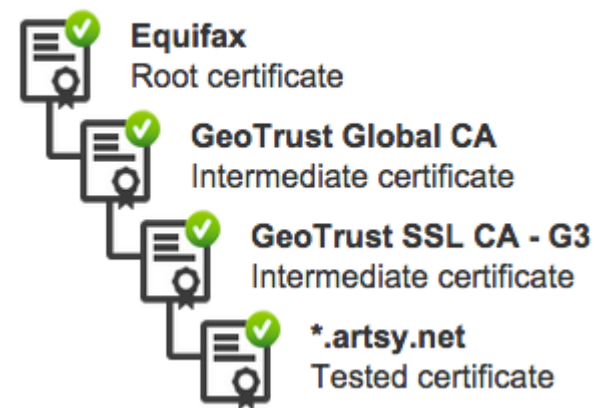


# METODE PENYIMPANAN PRIVATE KEY DAN SERTIFIKAT DIGITAL: FORMAT P12

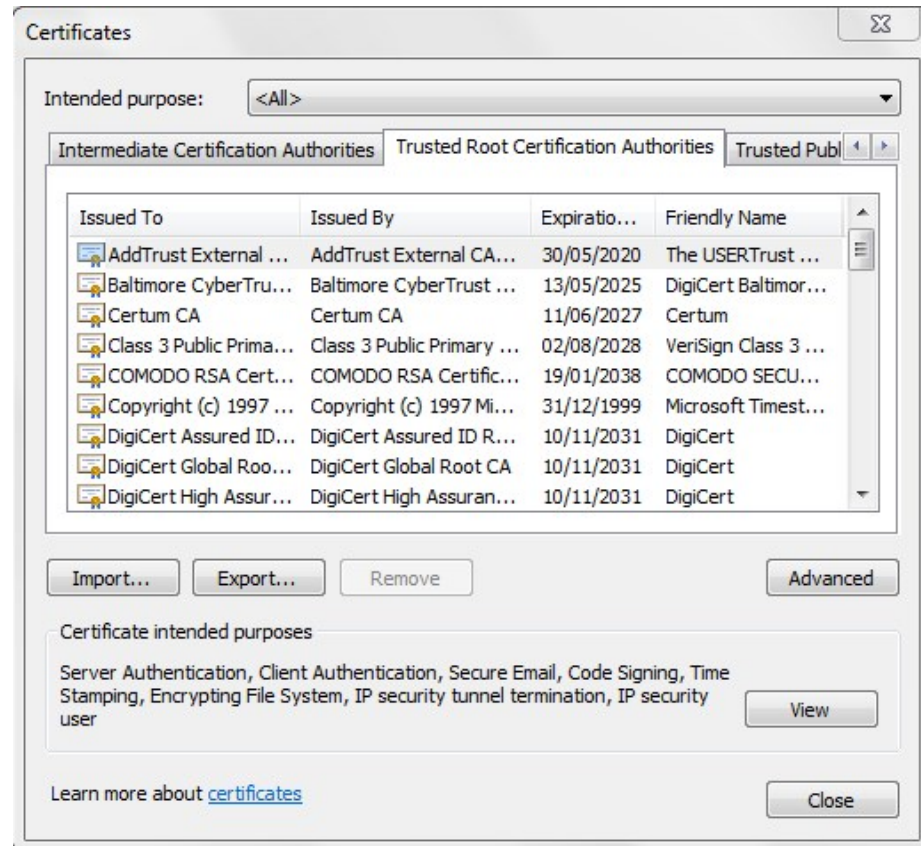
## PKCS#12 File



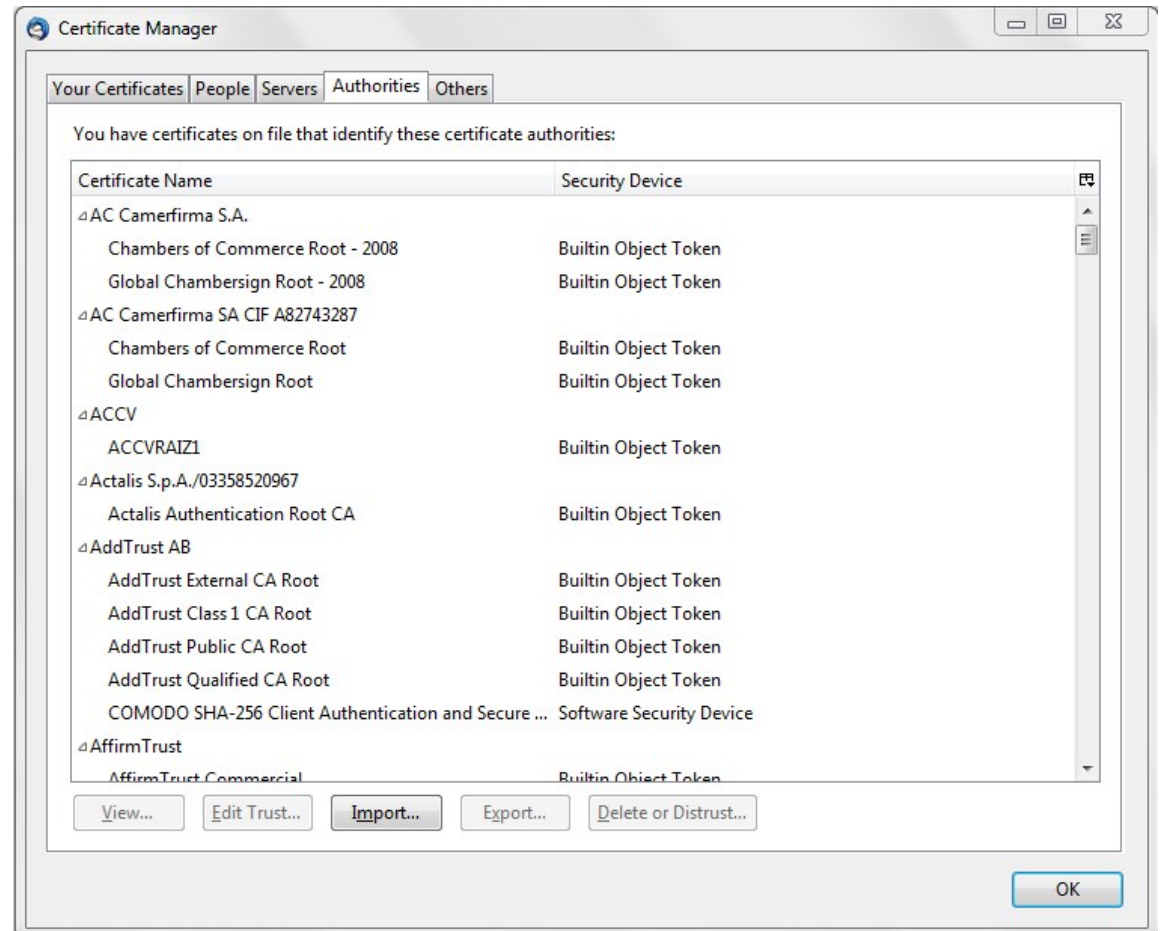
## Certificate chain



# REPOSITORY (TEMPAT PENYIMPANAN) SERTIFIKAT DIGITAL



Microsoft

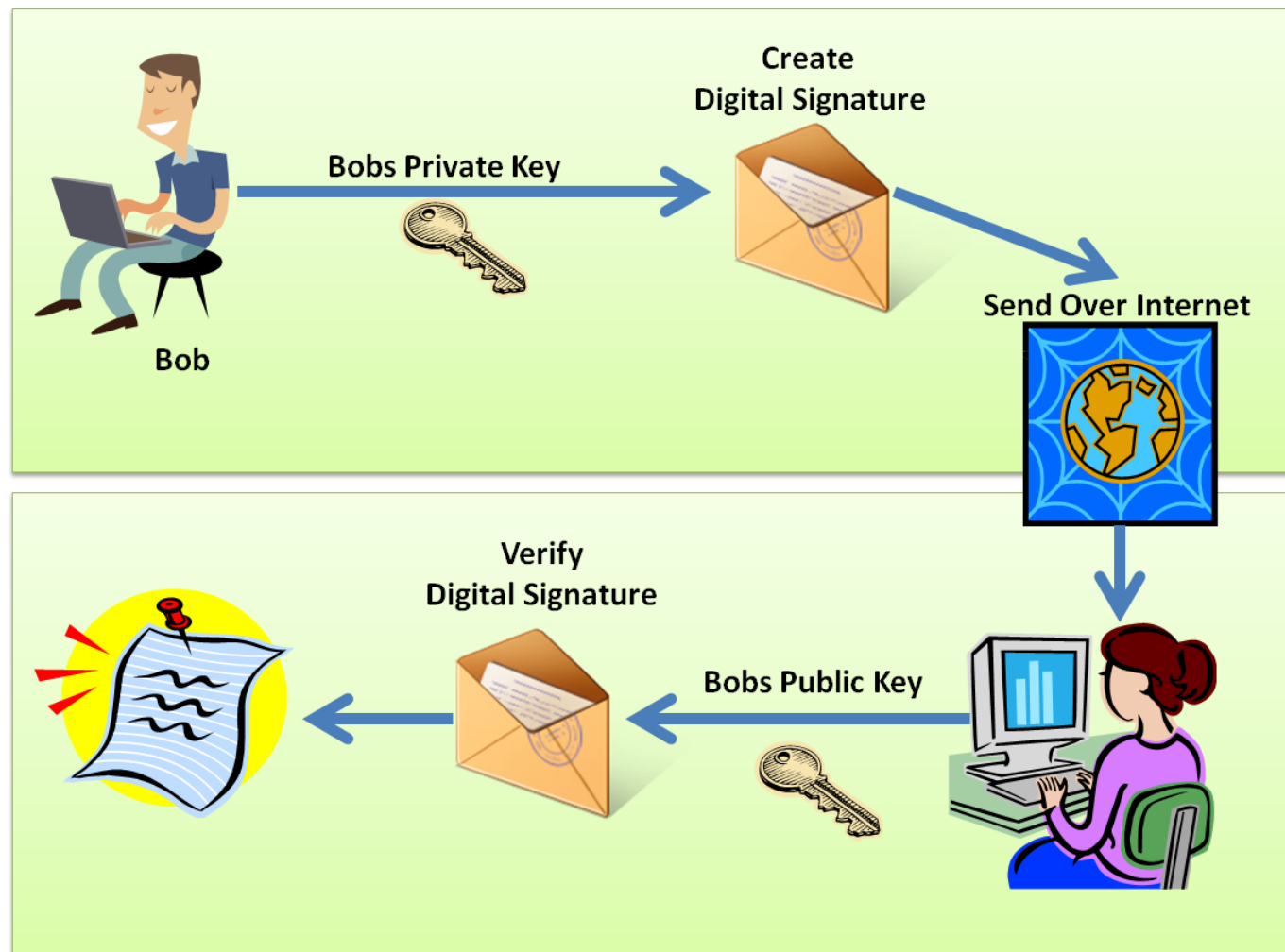


Mozilla

# 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



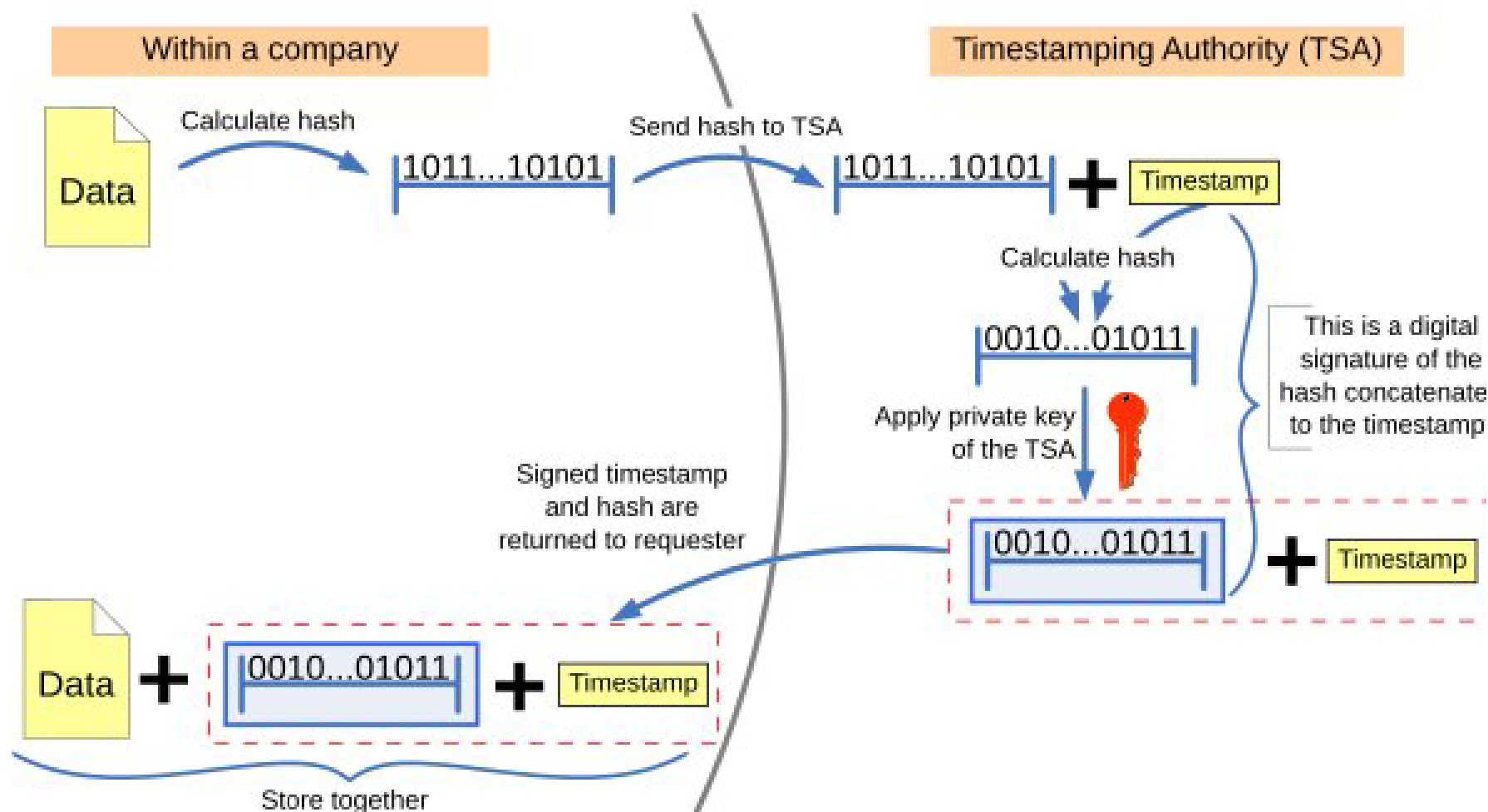


# TRUSTED (DIGITAL) TIMESTAMPING

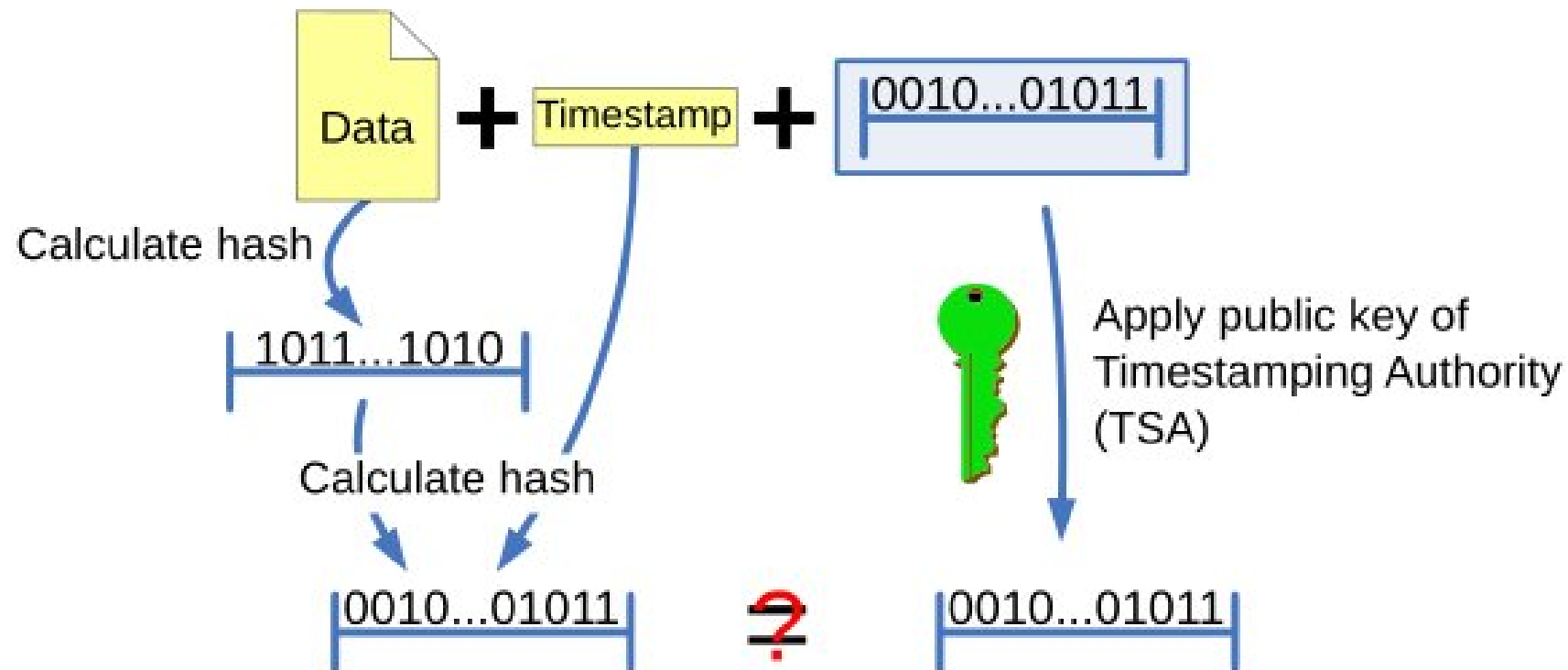
Trusted Timestamping adalah proses untuk menyimpan secara aman segala bentuk perubahan dan modifikasi **waktu** pada dokumen.

Secara aman di atas maksudnya adalah menjaga **integritas waktu** penandatanganan sehingga tidak dapat dimodifikasi (bahkan oleh penandatanganan 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 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](mailto:ricky.p@kominfo.go.id)