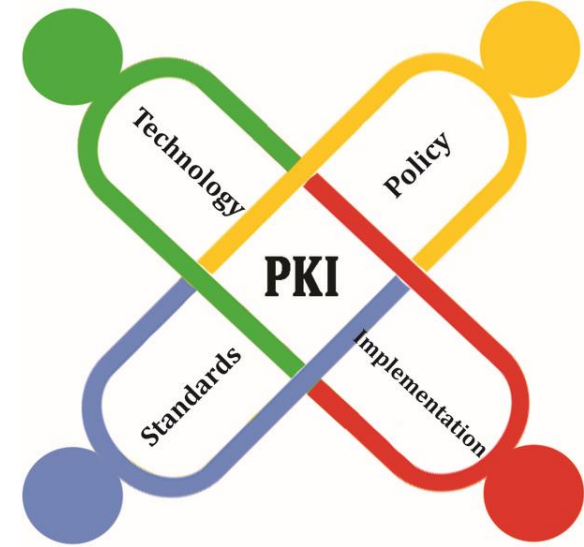


Bahan Kuliah IF4020 Kriptografi



Public Key Infrastructure (PKI)

Oleh: Rinaldi Munir

Program Studi Teknik Informatika

STEI-ITB

2023

Public Key Infrastructure (PKI)

- Luasnya penggunaan sistem kriptografi kunci-publik di Internet membutuhkan sebuah infrastruktur yang menyediakan layanan terintegrasi untuk:
 - membuat,
 - menyimpan,
 - memverifikasi,
 - dan membuang sertifikat digital.
- Infrastruktur tersebut juga mengatur CA dan membuat kebijakan (*policy*).
- Infrastruktur tersebut dinamakan *Public-Key Infrastructure (PKI)*

- *PKI* adalah sekumpulan aturan, kebijakan, prosedur, *hardware* dan *software* yang dibutuhkan untuk membuat, mendistribusikan, menggunakan, menyimpan, mengelola, dan membuang sertifikat digital.
- PKI mengintegrasikan kriptografi kunci-publik dengan sertifikat digital dan *CA* untuk mengotentikasi pihak-pihak dalam suatu transaksi elektronik.
- Tujuan PKI adalah untuk memfasilitasi transaksi elektronik yang aman untuk aktivitas perbankan, *e-commerce*, dan surat-surat elektronik dengan menggunakan sistem kriptografi kunci-publik.

Komponen-komponen *PKI*:

1. Sertifikat digital

- kunci publik, identitas pemilik, tanda-tangan digital, dll

2. Pemilik kunci publik

- personal, bank, perusahaan, dll

3. CA (*Certification Authority*)

- otoritas yang menerbitkan sertifikat digital

4. RA (*Registration Authority*)

- otoritas yang memverifikasi identitas pengguna yang meminta sertifikat

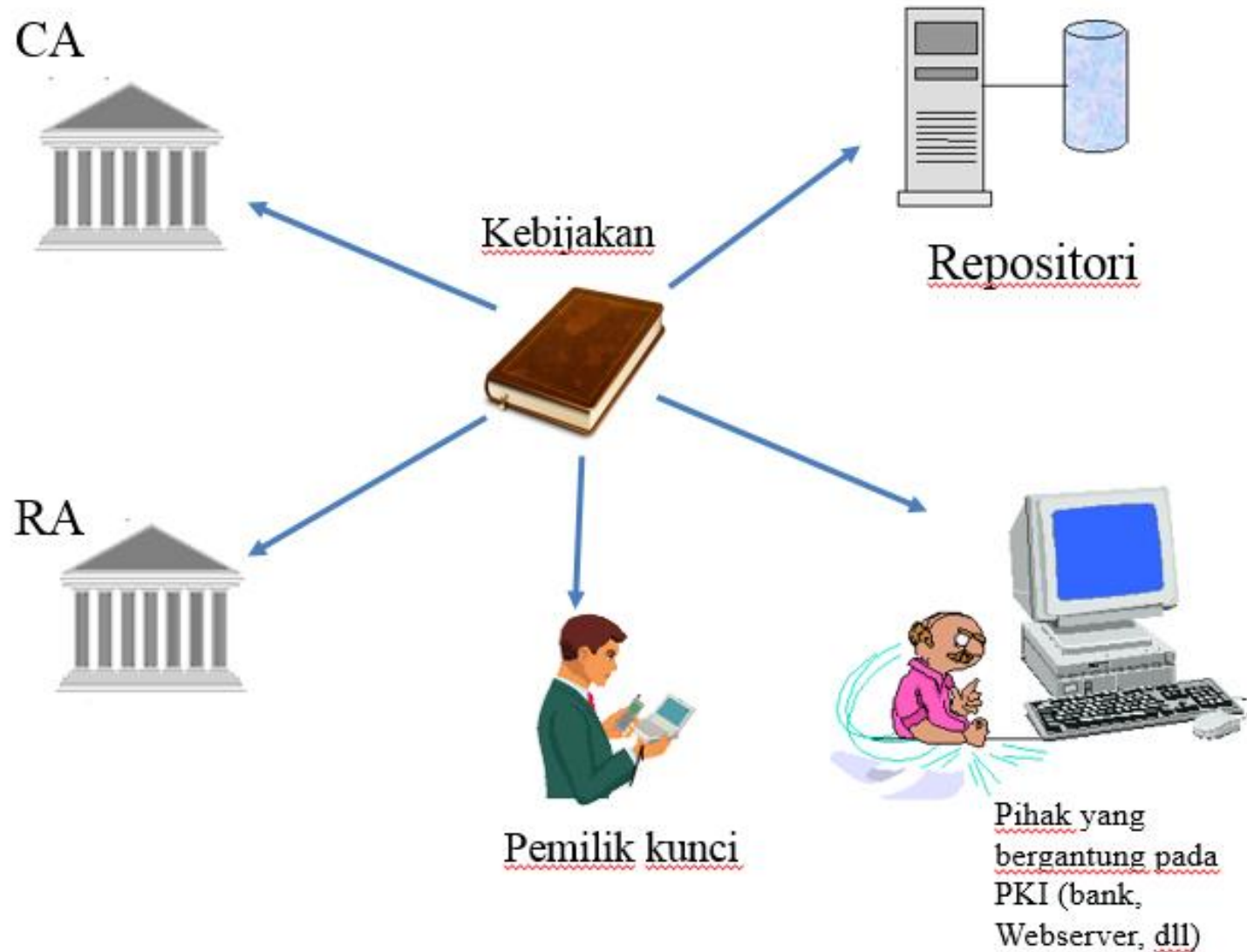
5. Repositori

- menyimpan sertifikat digital dan *CRL*

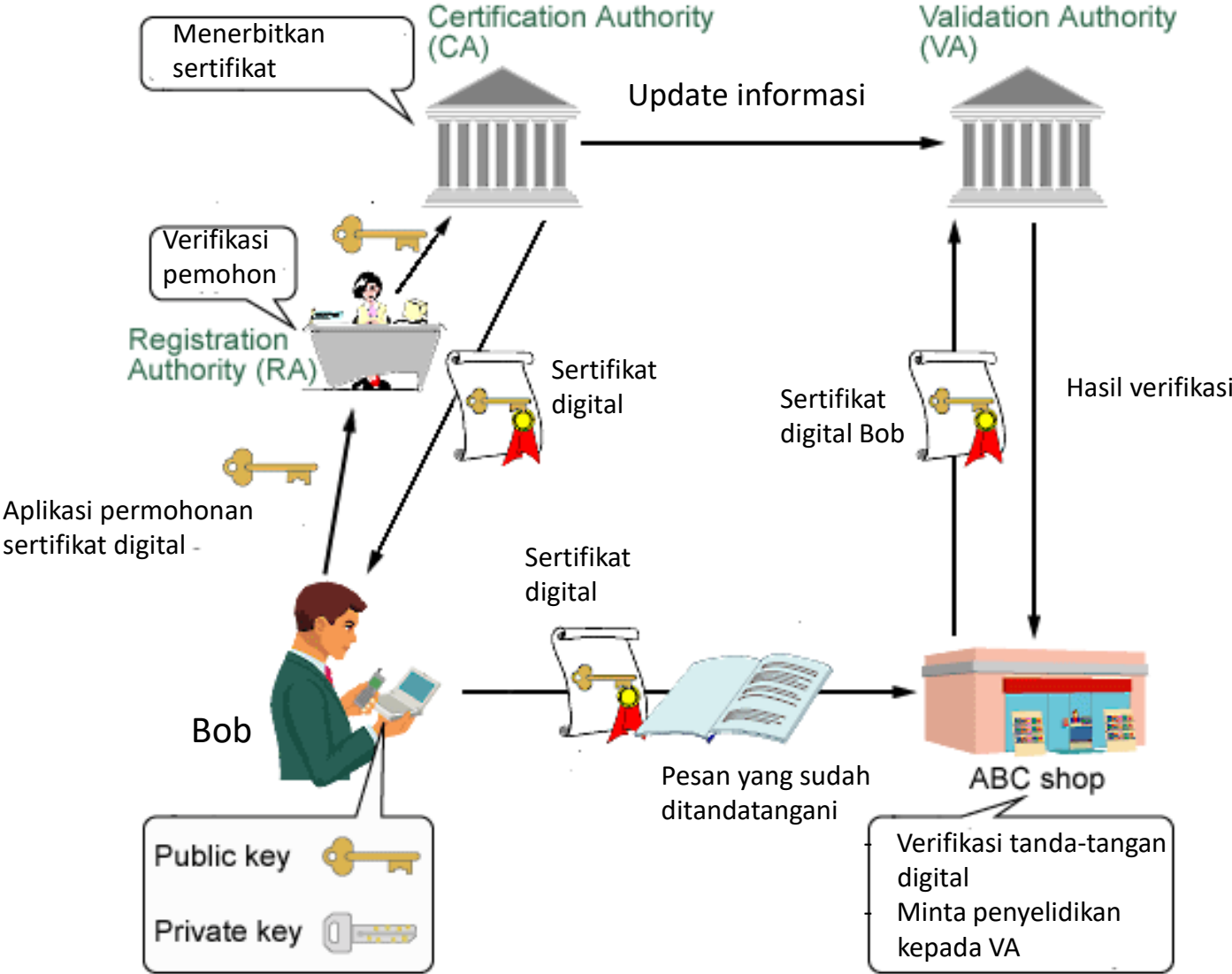
6. Aturan/kebijakan (*policy*)

- berisi sekumpulan prosedur dan aturan yang terkait dengan PKI

Komponen-komponen PKI



Alur pembuatan dan penggunaan sertifikat digital di dalam PKI

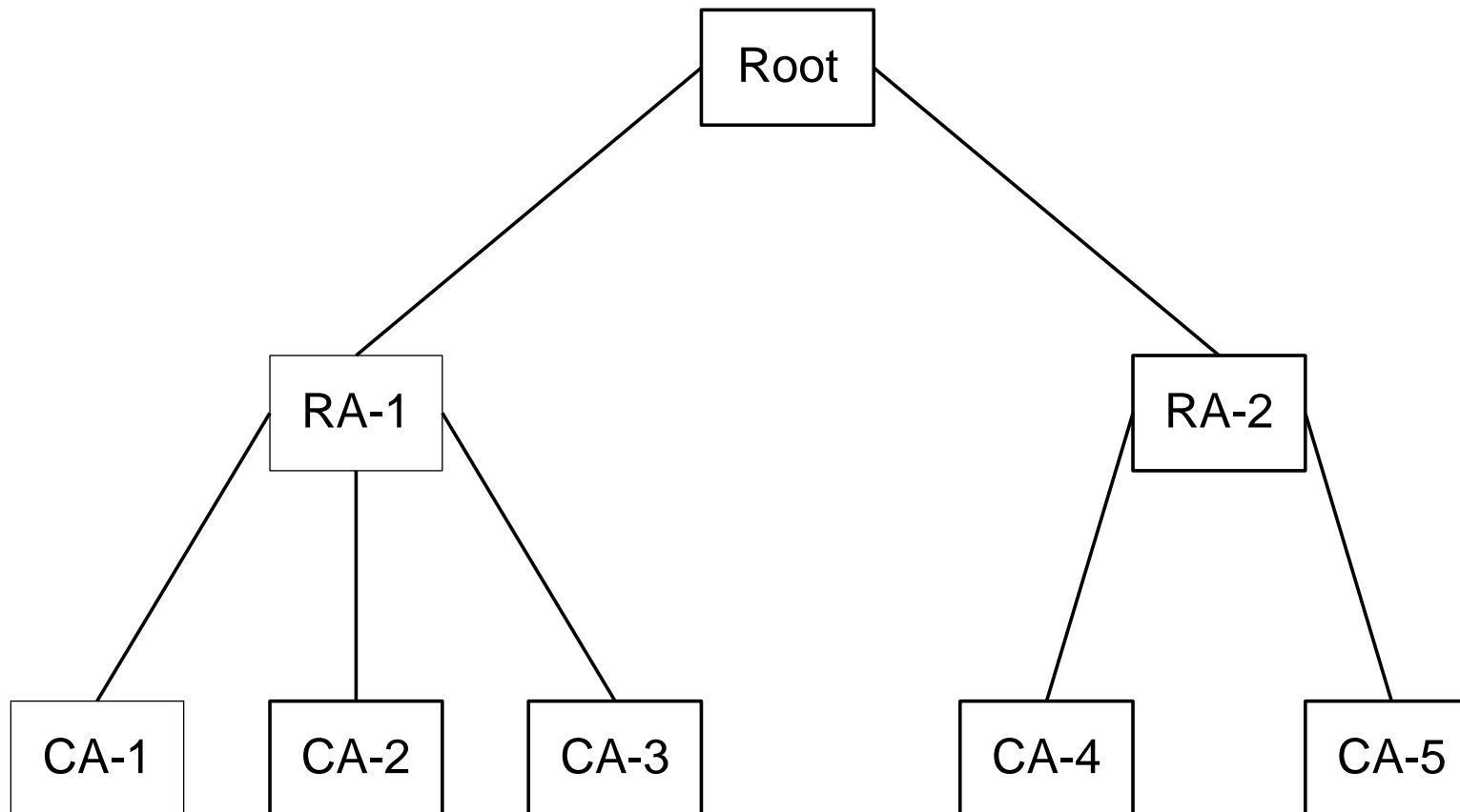


Beberapa Penyedia PKI

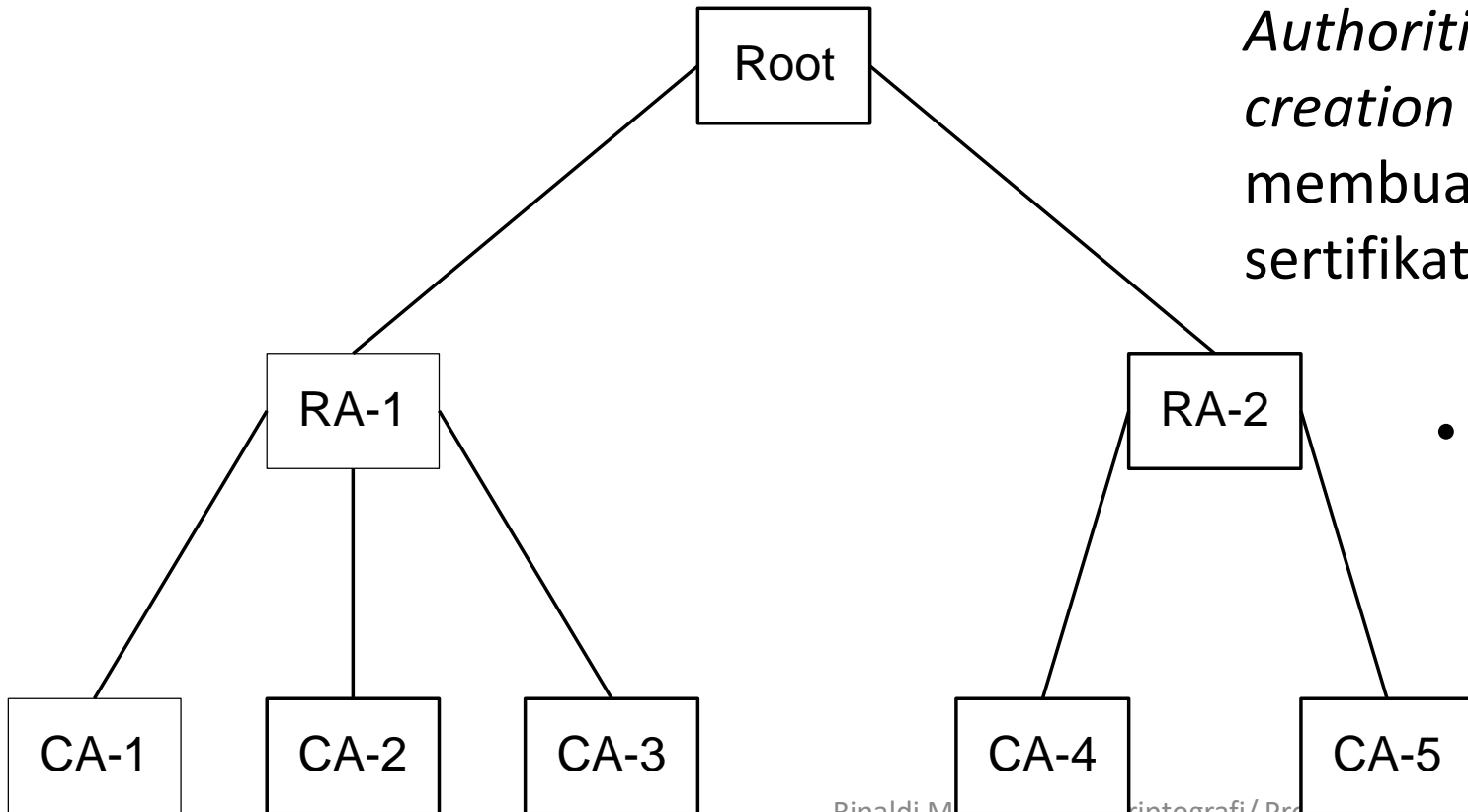
Among PKI leaders are:

- *RSA*, which has developed the main algorithms used by PKI vendors
- *Verisign*, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities
- *GTE CyberTrust*, which provides a PKI implementation methodology and consultation service that it plans to vend to other companies for a fixed price.
- *Xcert*, whose Web Sentry product that checks the revocation status of certificates on a server, using the Online Certificate Status Protocol (OCSP)
- *Netscape*, whose Secure E-Commerce, which allows a company or [extranet](#) manager to manage digital certificates;

- *PKI* menyediakan cara penstrukturan komponen-komponennya (CA, RA) dan mendefinisikan standard bermacam-macam dokumen dan protokol.
- Bentuk *PKI* yang sederhana adalah hirarkhi CA dalam struktur pohon:



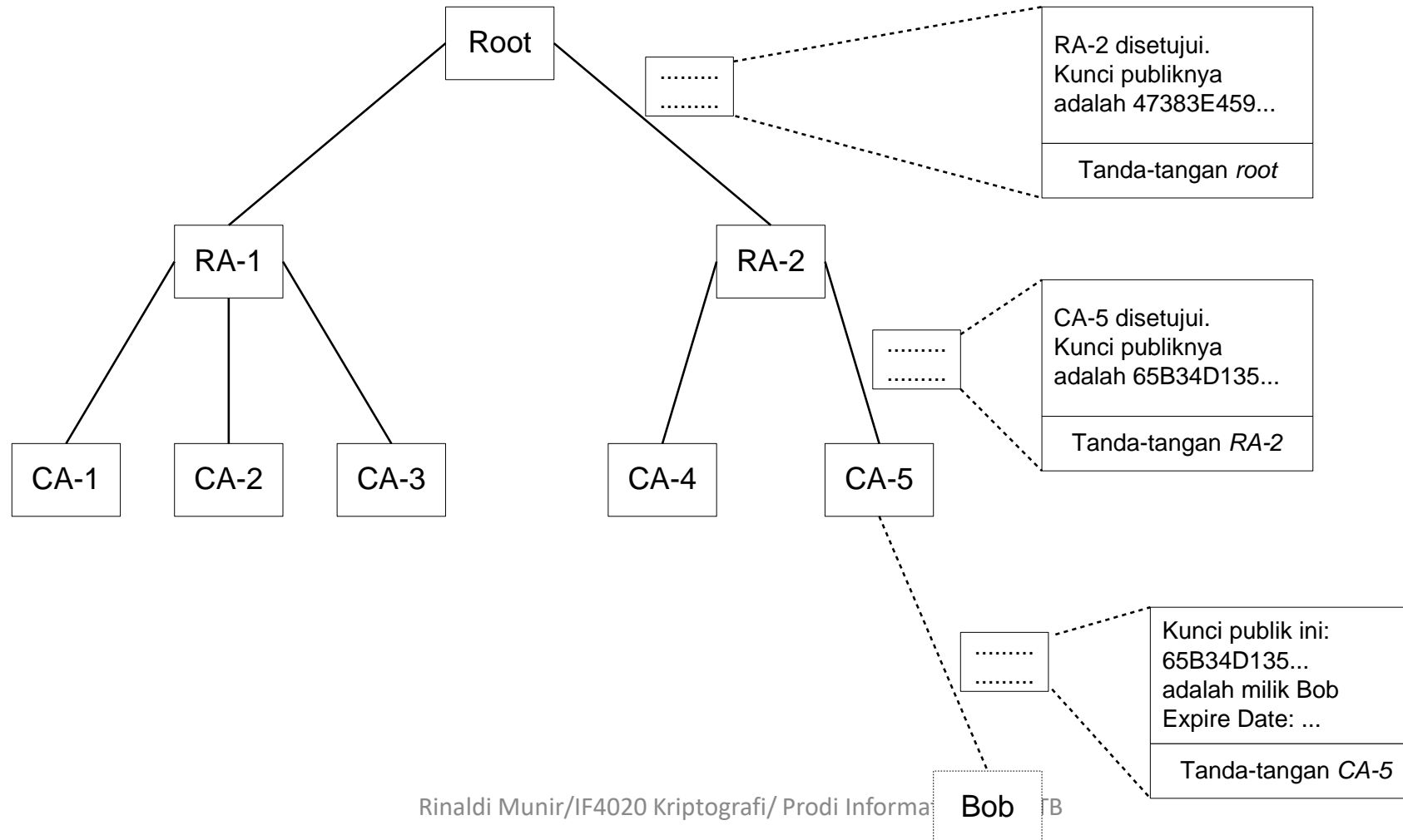
- *Root* merupakan *root certificate authority*, yaitu pembuat kebijakan mengenai manajemen sertifikat digital .
- *Root* mensertifikasi *CA* aras satu dengan menggunakan privat *root* yang disebut *root key*.



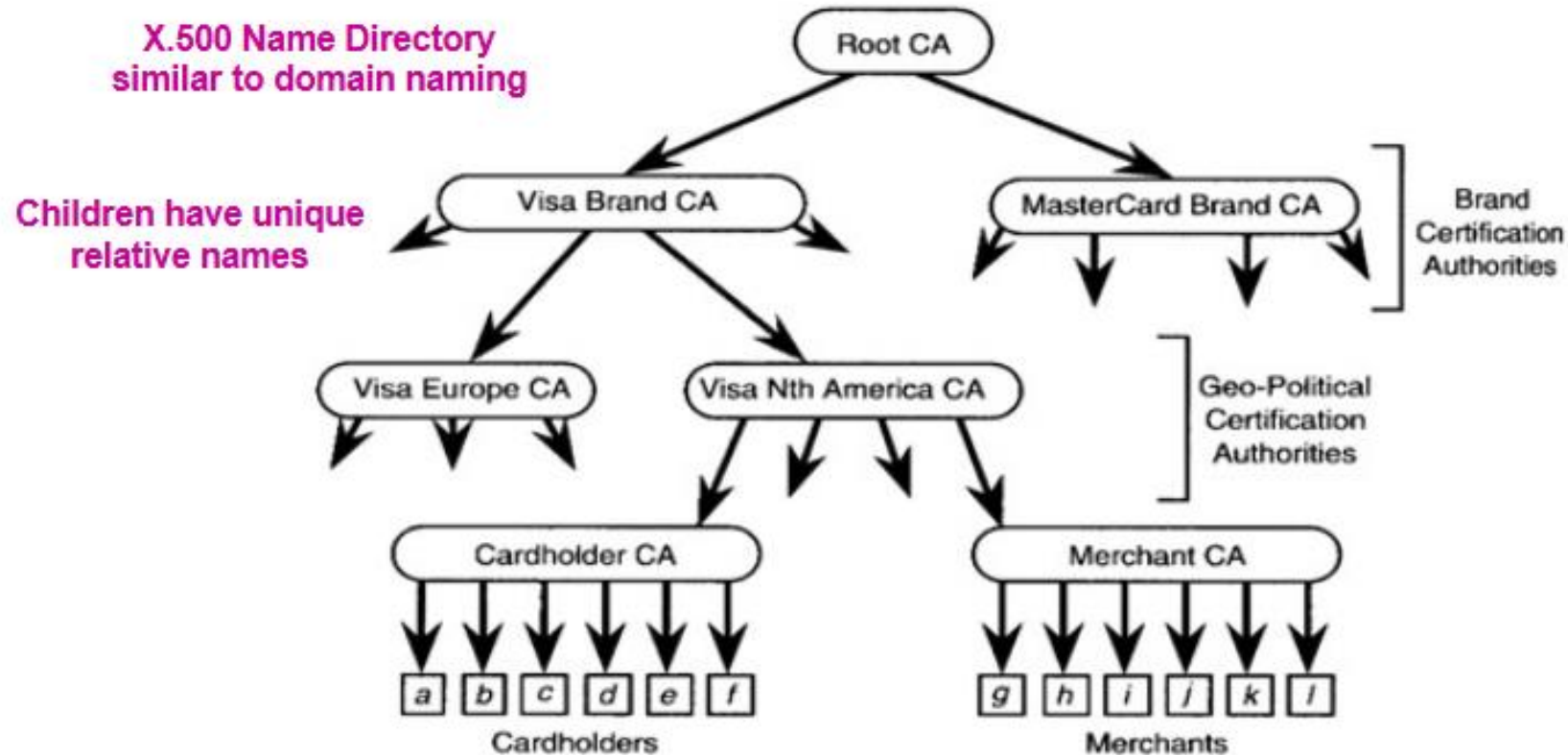
- *CA* aras satu adalah *RA (Registration Authorities)*, yang bertindak sebagai *policy creation authority*, yaitu organisasi yang membuat kebijakan untuk memperoleh sertifikat digital.

- Sebuah *RA* mungkin mencakup beberapa area geografis, seperti negara bagian, negara, atau benua.

- Penstrukturan *PKI* seperti pohon menghasilkan lintasan yang dinamakan *certificate path* atau *certificate chain*.
- *Certificate path* memberikan alur untuk memverifikasi tanda-tangan di dalam sertifikat mulai dari aras daun hingga mencapai *root*.

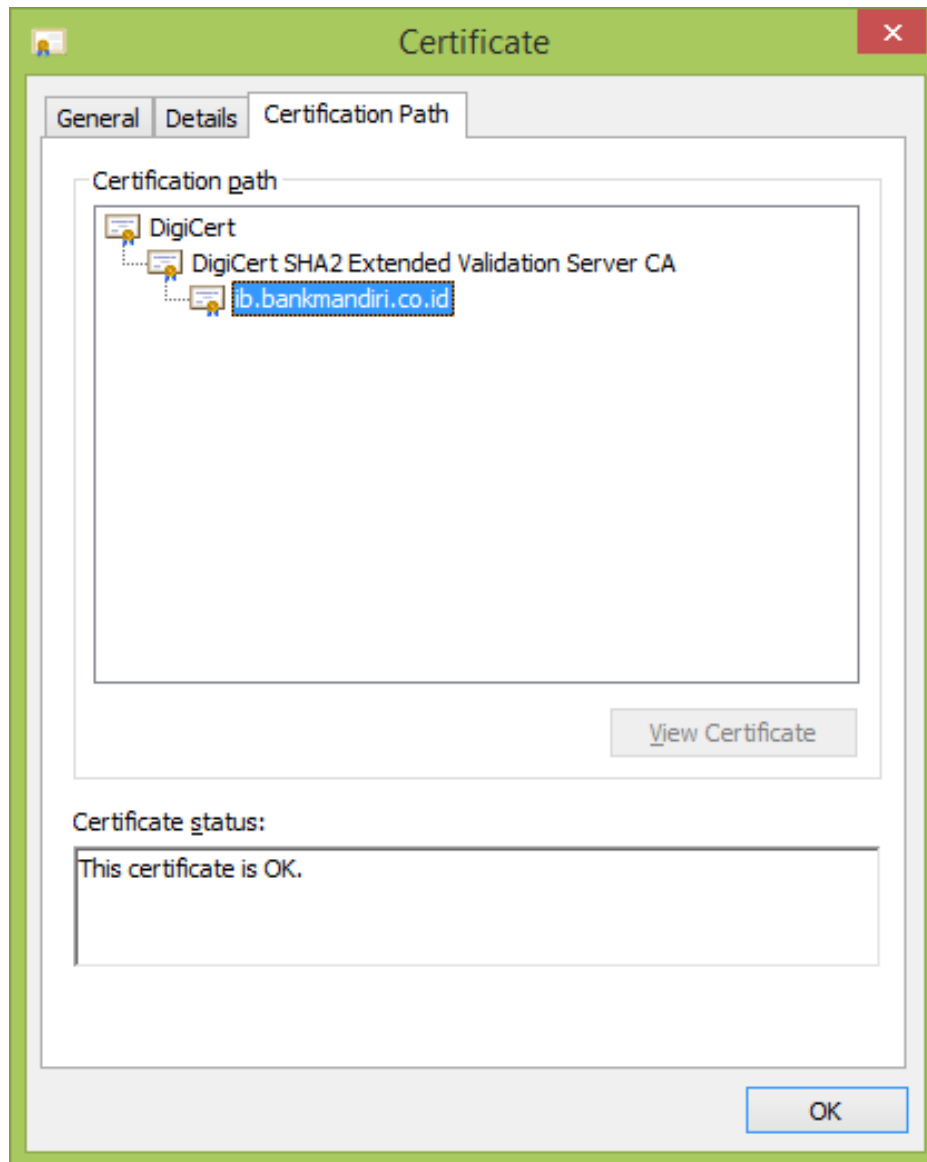


Contoh sebuah rantai sertifikat untuk CA penyedia sertifikat kartu kredit Visa dan Mastercard:



SOURCE: FORD & BAUM,
*SECURE ELECTRONIC
COMMERCE*

Rantai sertifikat digital untuk server Bank Mandiri :

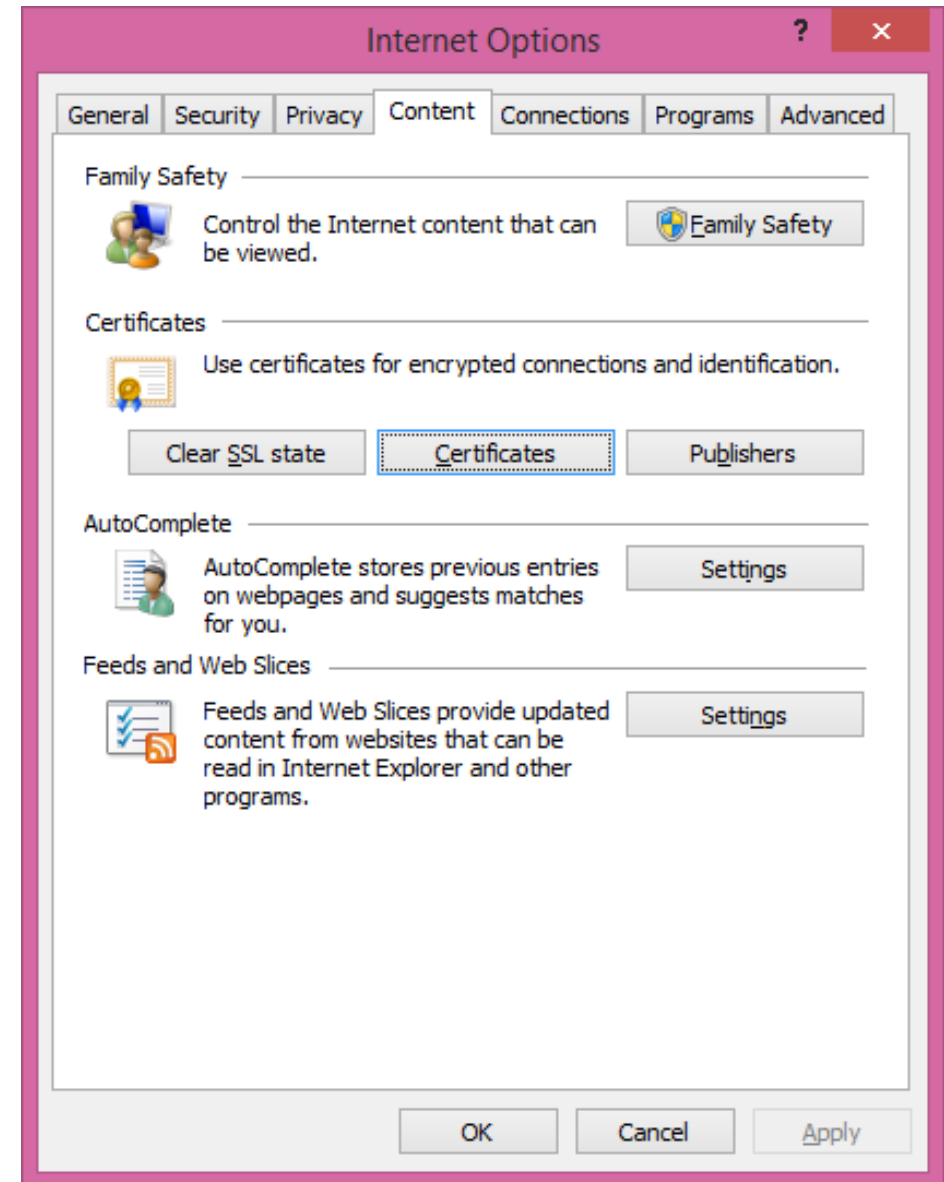


- *Digicert* adalah CA pada aras 0 (*root*),
- *Digicert SHA2* adalah CA pada aras 1,
- daunnya adalah web Bank Mandiri.

- Untuk melihat CA dan sertifikat digitalnya yang yang telah dipasang di dalam *Internet Explorer (IE)*, lakukan sebagai berikut.

- Pilih:

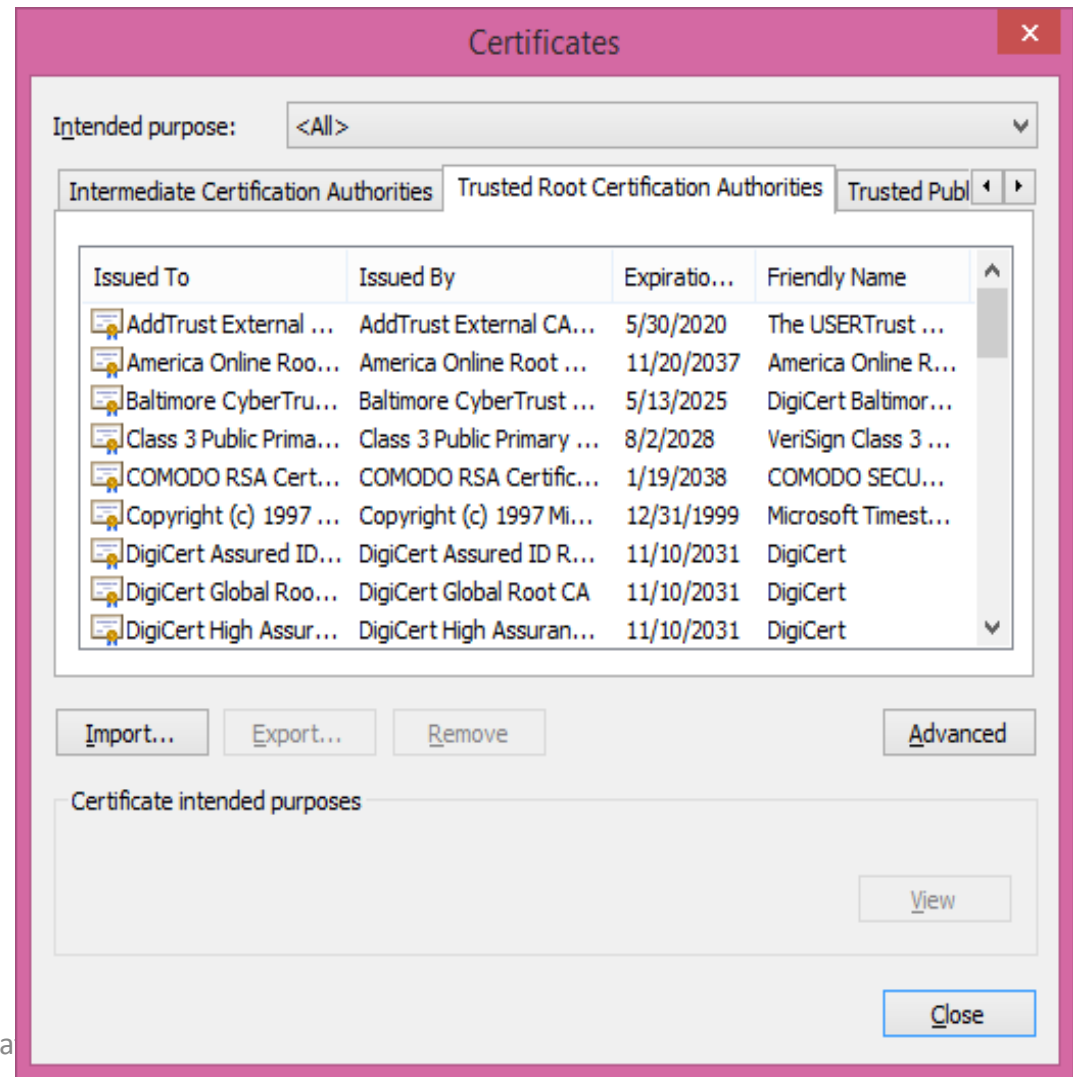
Internet Options → *Content*



- Kemudian, klik tab:

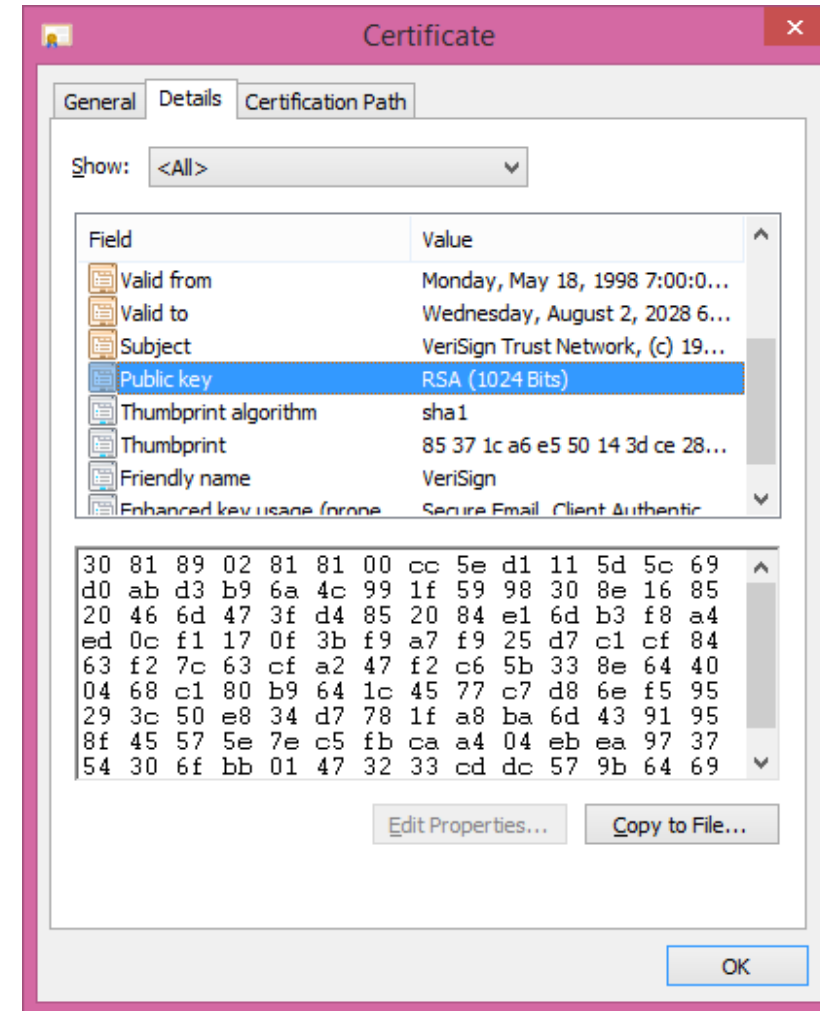
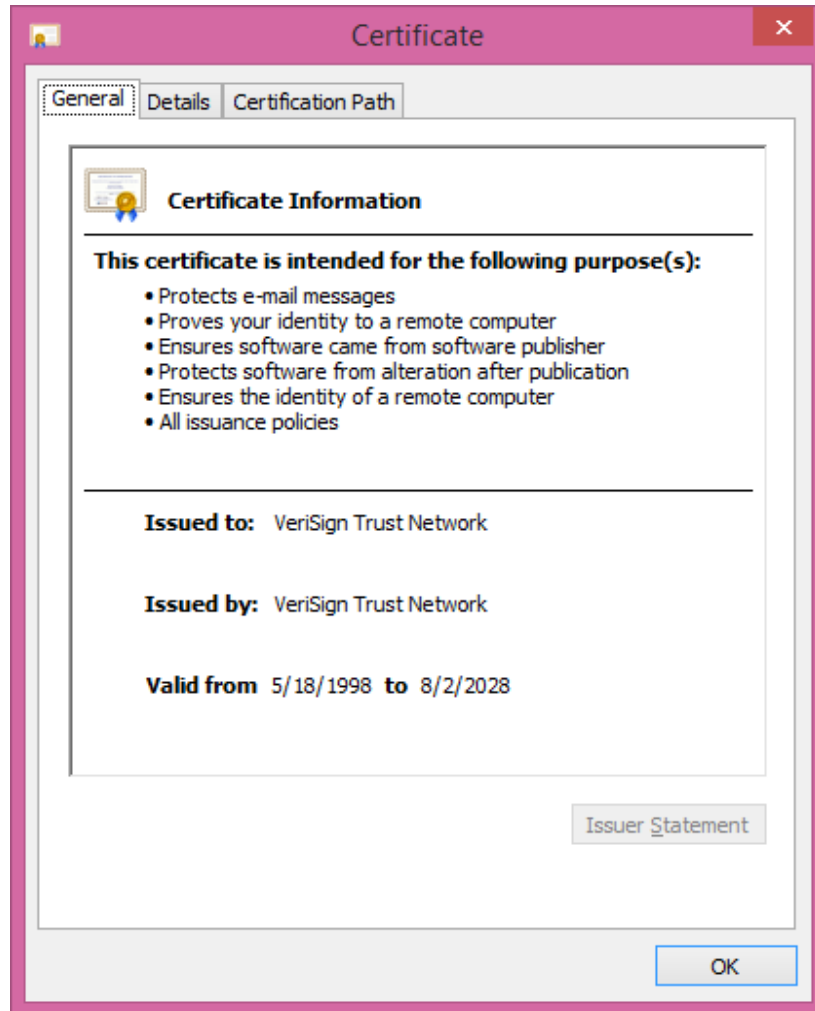
Certificates → *Trusted Root Certification Authorities*

- *Trusted Root CA* adalah *root* di dalam *PKI* dan memiliki cabang berupa *Intermediate CA*.



- Bila terdapat *server* di internet yang diberi sertifikat oleh perusahaan yang tidak tercantum di dalam daftar *CA* di atas, maka *IE* akan memperingatkan bahwa *IE* tidak mengenal *CA* tersebut.
- Jika pengguna mempercayai *server* tersebut, maka *CA* tersebut akan ditambahkan ke dalam *IE*.

- Untuk melihat isi sertifikat digital sebuah CA, klik salah satu sertifikat.



SELAMAT BELAJAR