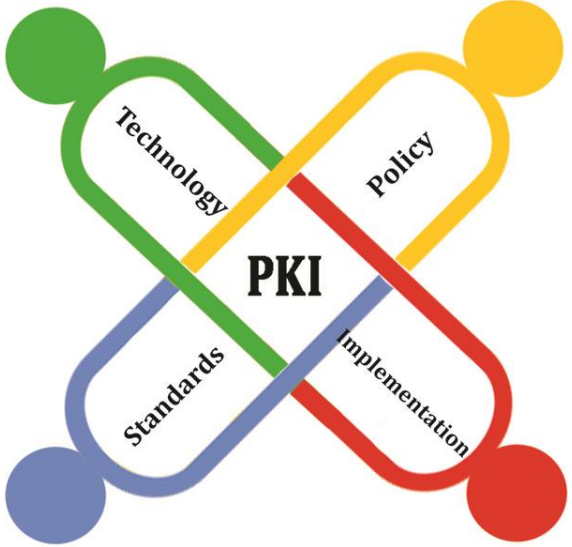


Bahan Kuliah II4031 Kriptografi dan Koding

Public Key Infrastructure (PKI)

Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
STEI-ITB
2024

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*).

- Infrastuktur tersebut dinamakan *Public-Key Infrastructure* (PKI)

- *PKI* adalah teknologi yang terduri dari *hardware*, *software,* aturan, kebijakan, dan prosedur, 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.

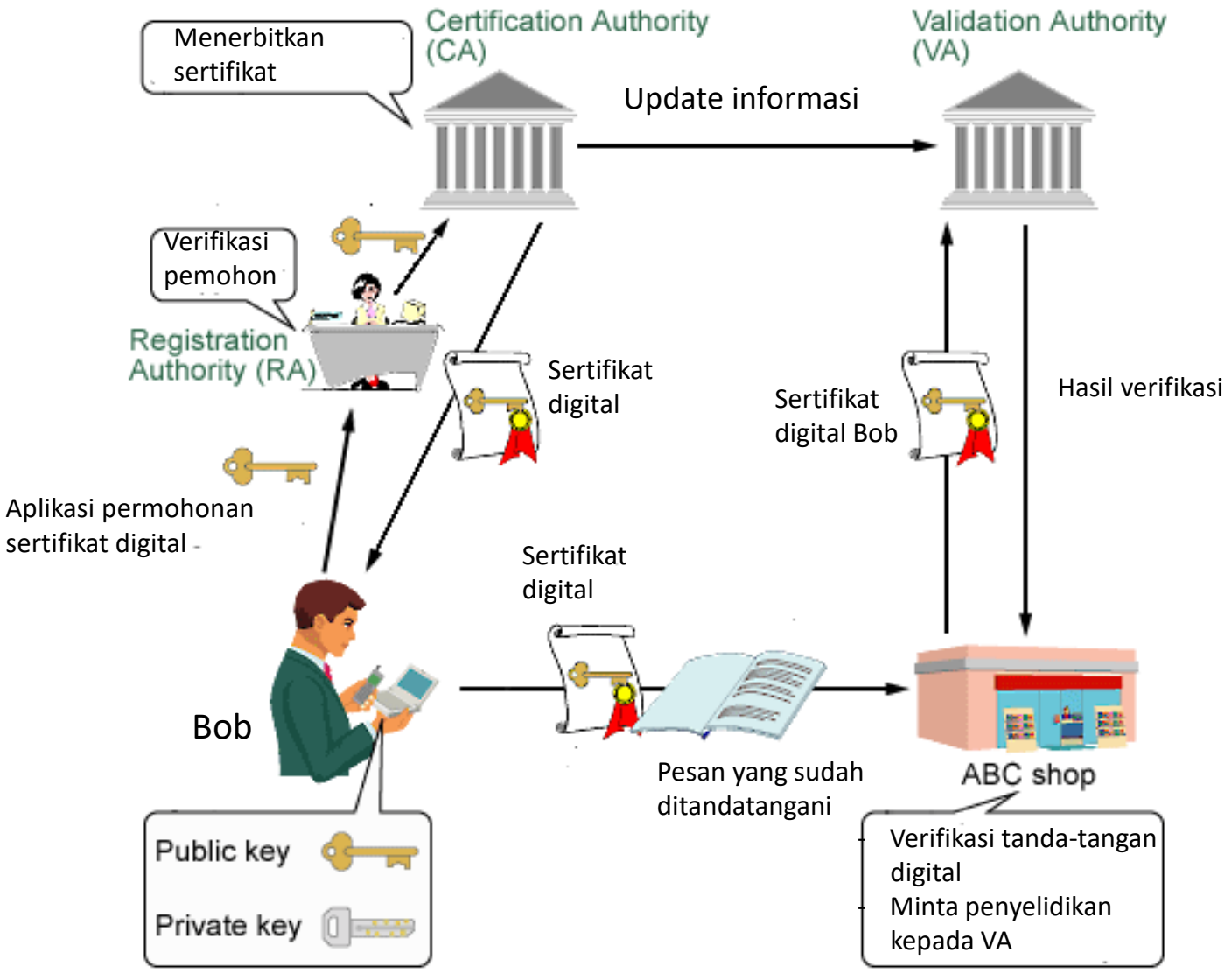
- Tujuan PKI adalah untuk memfasilitasi transaksi elektronik yang aman untuk aktivitas perbankan, *e-commerce,* dan surat-surat elektronik dengan menggunakan sistem kriptografi kunci-publik.

- Sehingga pengguna merasa aman untuk pertukaran data dan informasi melalui saluran yang tidak aman (internet).

Komponen-komponen *PKI:*

1. Sertifikat digital
   - kunci publik, identitas pemilik, tanda-tangan digital, dll
2. CA (*Certification Authority*)
   - otoritas yang menerbitkan sertifikat digital
3. RA (*Registration Authority*)
   - otoritas yang memverifikasi identitas pengguna yang meminta sertifikat
4. Repositori
   - hardware untuk menyimpan sertifikat digital dan *CRL*
5. Aturan/kebijakan (*policy*)
   - berisi sekumpulan prosedur dan aturan yang terkait dengan PKI
6. PKI client
   - :Pihak yang bergantung pada PKI (bank, webserver, dll)

Alur pembuatan dan penggunaan sertifikat digital di dalam PKI



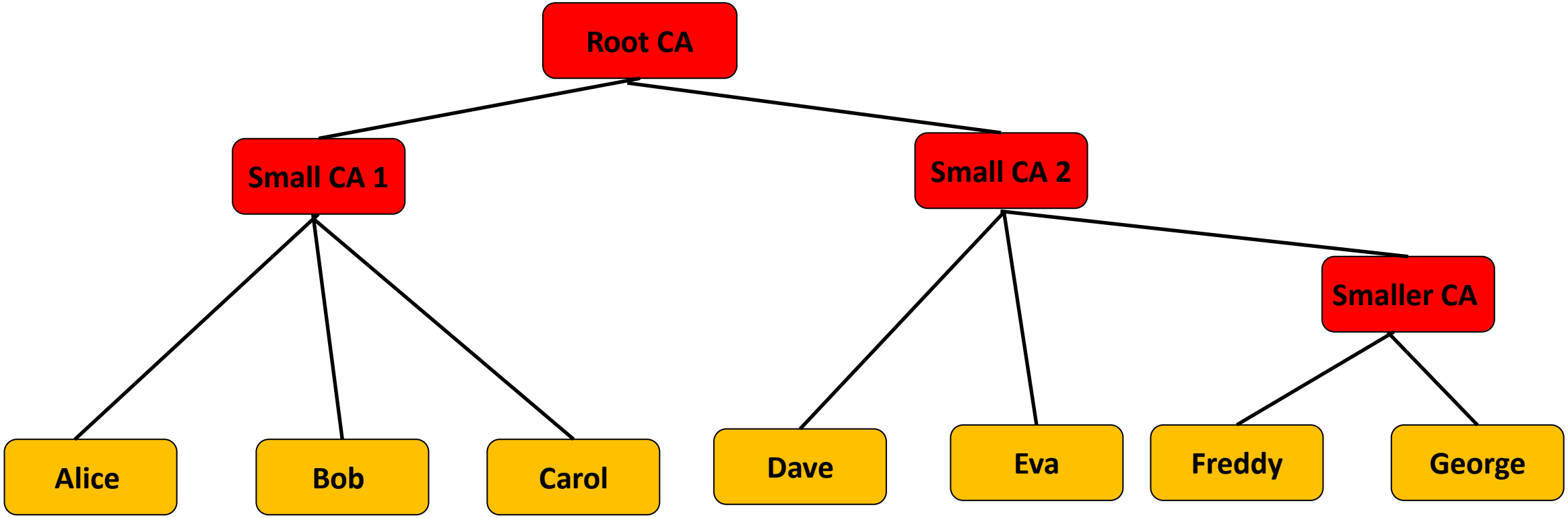
*) VA khusus di Amerika

Beberapa Penyedia PKI

- *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 dan mendefinisikan standard bermacam-macam dokumen dan protokol.

- Bentuk *PKI* yang sederhana adalah hirarkhi *CA* dalam struktur pohon:



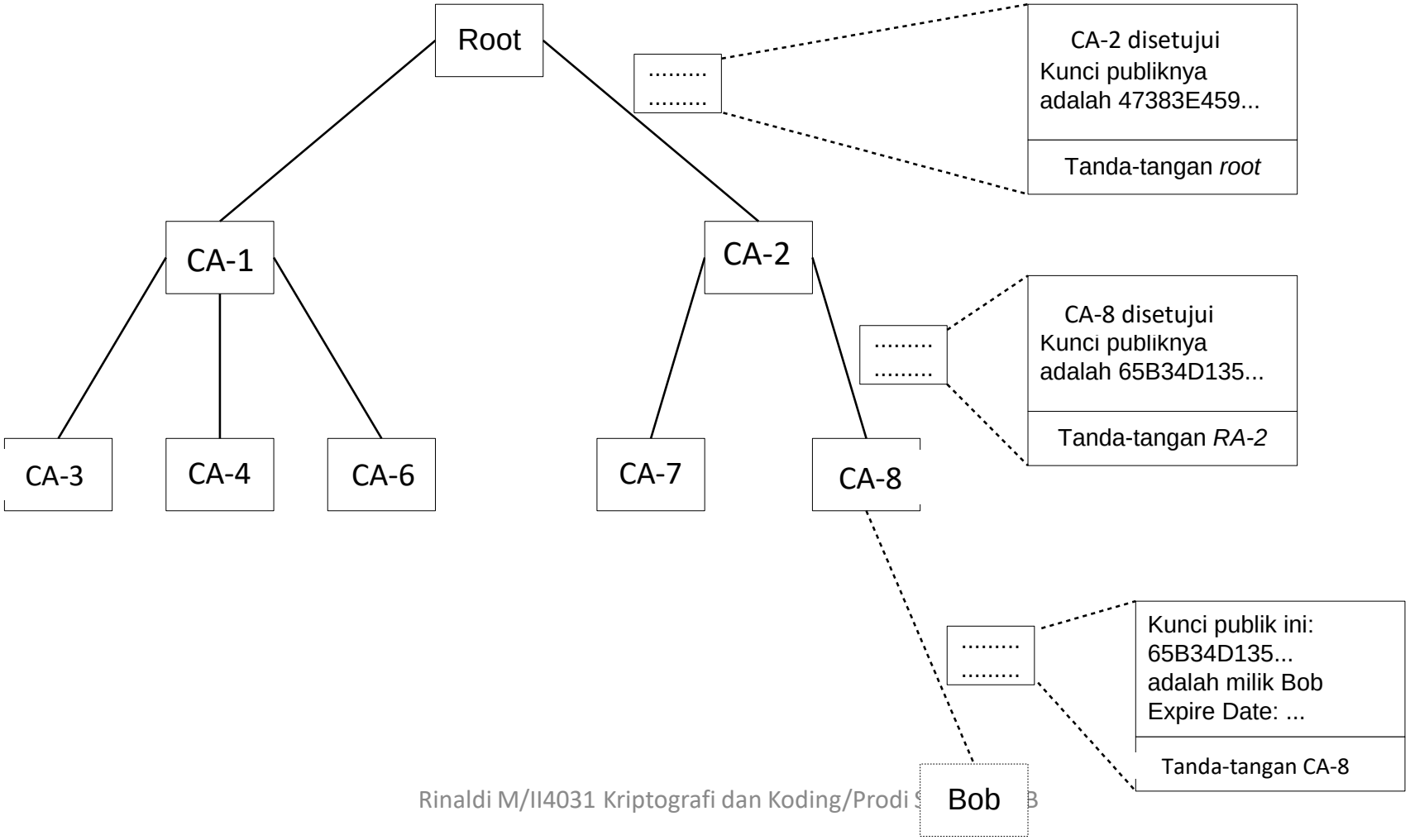
- *Root* CA merupakan *root certificate authority*, yaitu pembuat kebijakan mengenai manajemen sertifikat digital. Semua pengguna mempercayai (trust) root CA

- *Root* mensertifikasi *CA* aras satu dengan menggunakan privat *root* yang disebut *root key*.

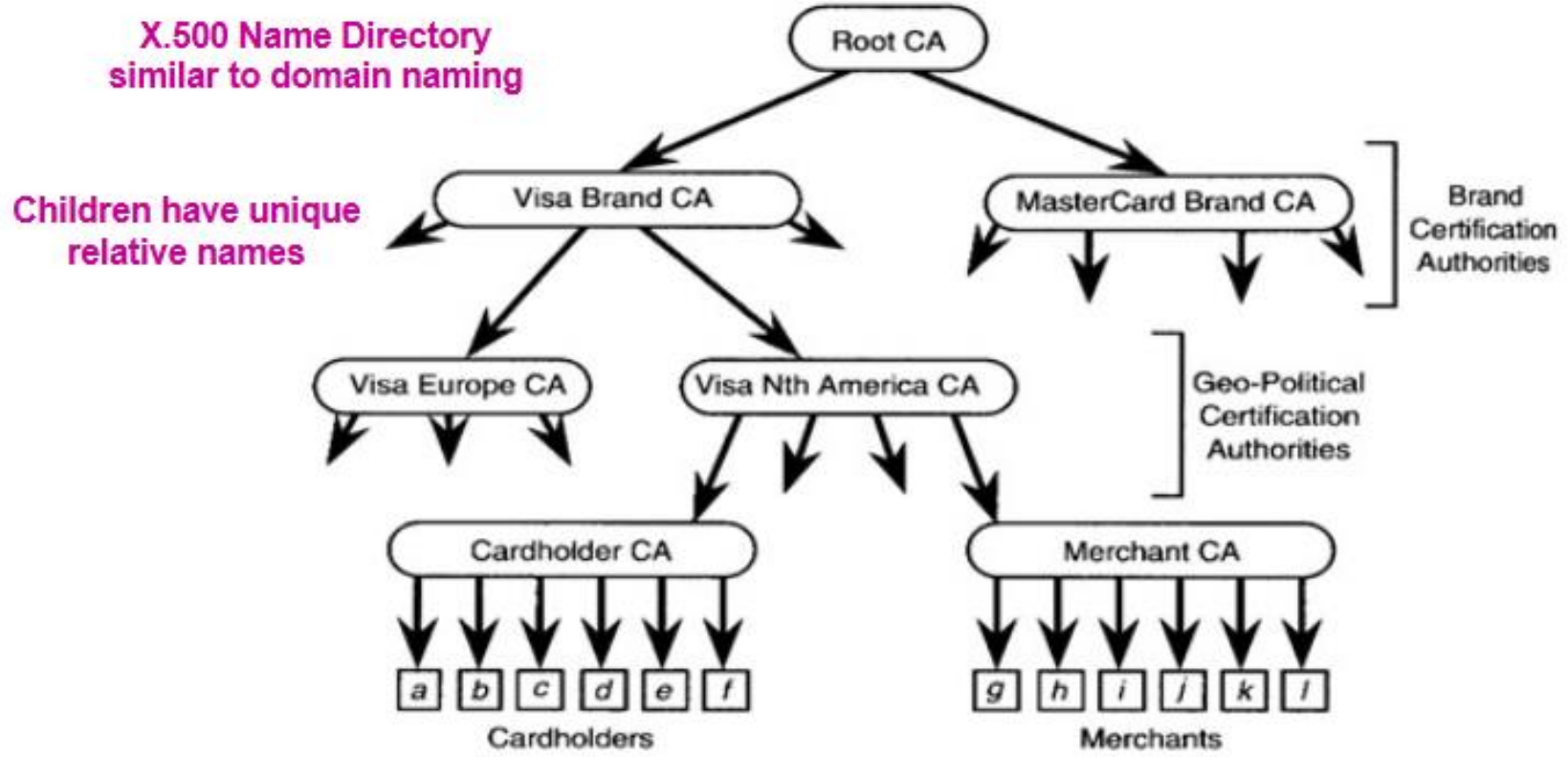
- *CA* aras satu, dua, dst adalah CA yang lebih kecil atau yang lebih spesifik.

- Dengan cara ini PKI dapat berkembang tanpa seluruh beban dibebankan pada Root CA

- 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.*



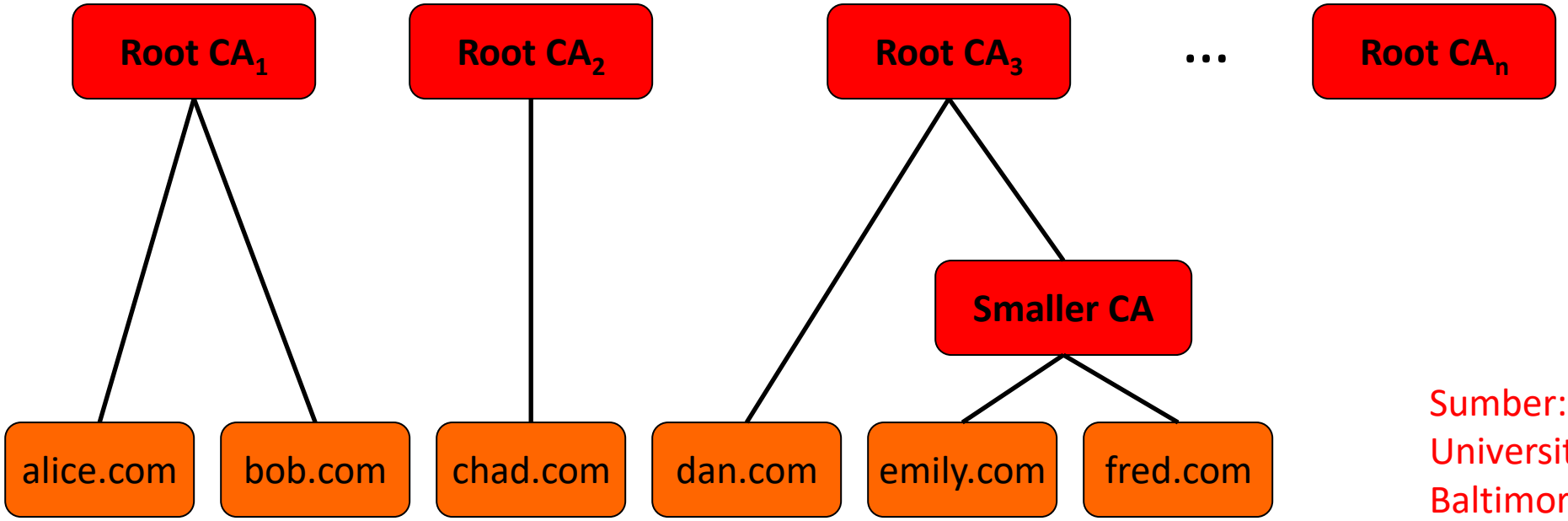
Contoh sebuah rantai sertifikat untuk CA penyedia sertifikat kartu kredit Visa dan Mastercard:



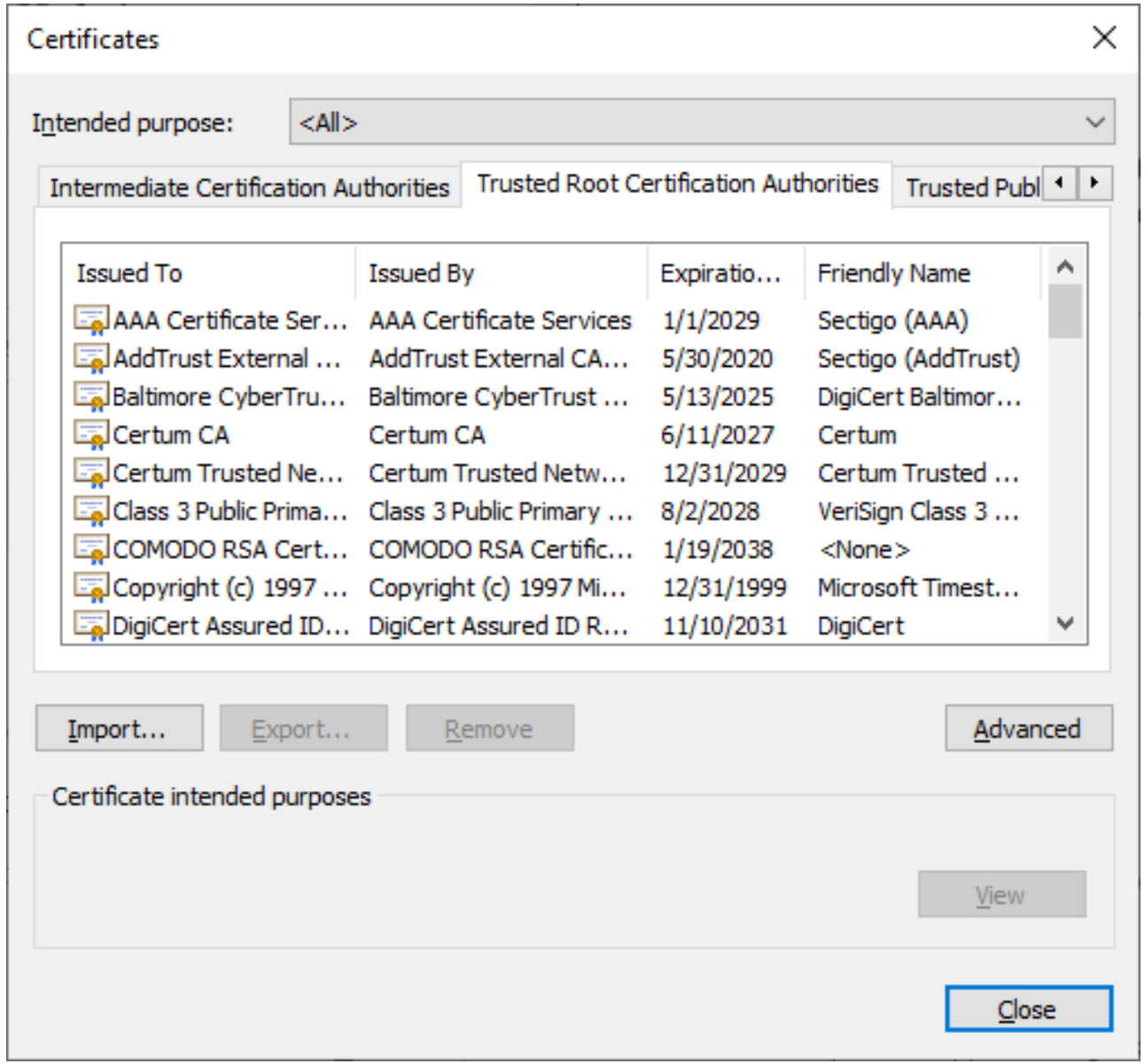
SOURCE: FORD & BAUM, *SECURE ELECTRONIC COMMERCE*

Organisasi CA di dalam Web Browser

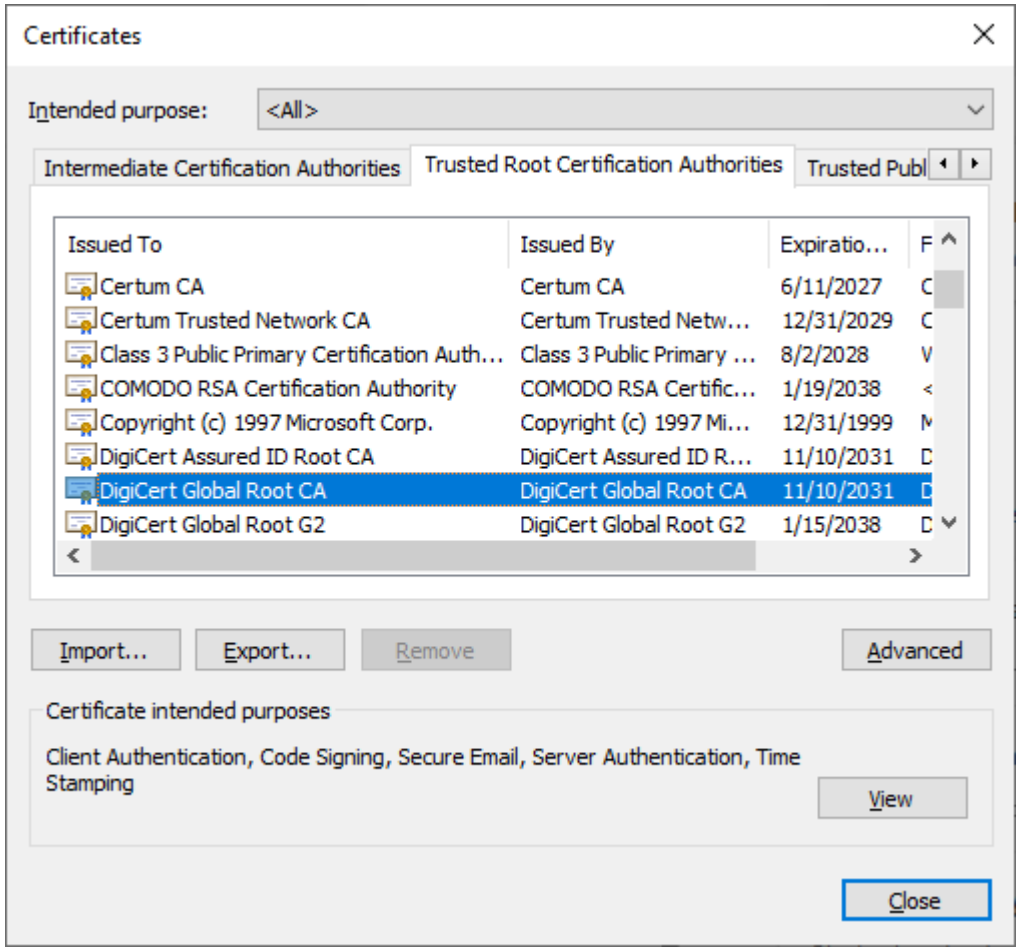
- Web browser menyimpan daftar Root CA yang tepercaya
- Sertifikat apa pun yang ditandatangani oleh salah satu Root CA ini dapat dipercaya
- Pada dasarnya organisasi CA di dalam web browser disusun dalam model hirakhi



Sumber: Jerad Bates
University of Maryland,
Baltimore County, PKI


Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Issued To
Issued By
Expiratio...
Friendly Name
AAA Certificate Ser...
AAA Certificate Services
1/1/2029
Sectigo (AAA)
AddTrust External ...
AddTrust External CA...
5/30/2020
Sectigo (AddTrust)
Baltimore CyberTru...
Baltimore CyberTrust ...
5/13/2025
DigiCert Baltimor...
Certum CA
Certum CA
6/11/2027
Certum
Certum Trusted Ne...
Certum Trusted Netw...
12/31/2029
Certum Trusted ...
Class 3 Public Prima...
Class 3 Public Primary ...
8/2/2028
VeriSign Class 3 ...
COMODO RSA Cert...
COMODO RSA Certific...
1/19/2038
<None>
Copyright (c) 1997 ...
Copyright (c) 1997 Mi...
12/31/1999
Microsoft Timest...
DigiCert Assured ID...
DigiCert Assured ID R...
11/10/2031
DigiCert
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

- Contoh *Root CA* adalah *Digicert Global Root C2*
- Contoh *intermediate CA* (aras 1) adalah *Digicert EV RSA CA G2*



SELAMAT BELAJAR