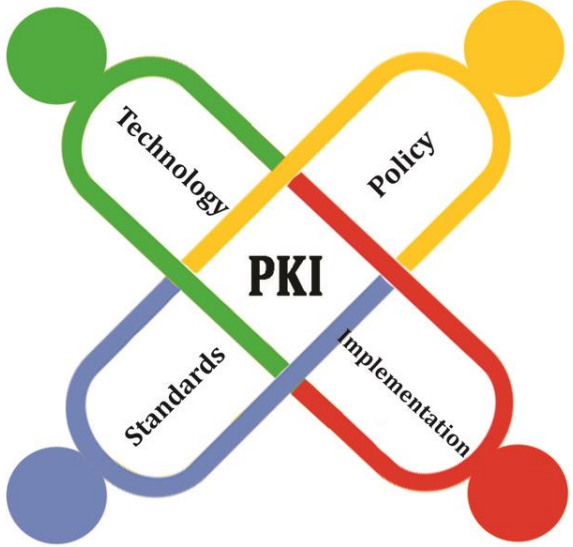



Bahan Kuliah IF4020 Kriptografi

# Public Key Infrastructure (PKI)

**Oleh: Rinaldi M**

Program Studi Sistem dan Teknologi Informasi
STEI-ITB
2026

# *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 terdiri 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.

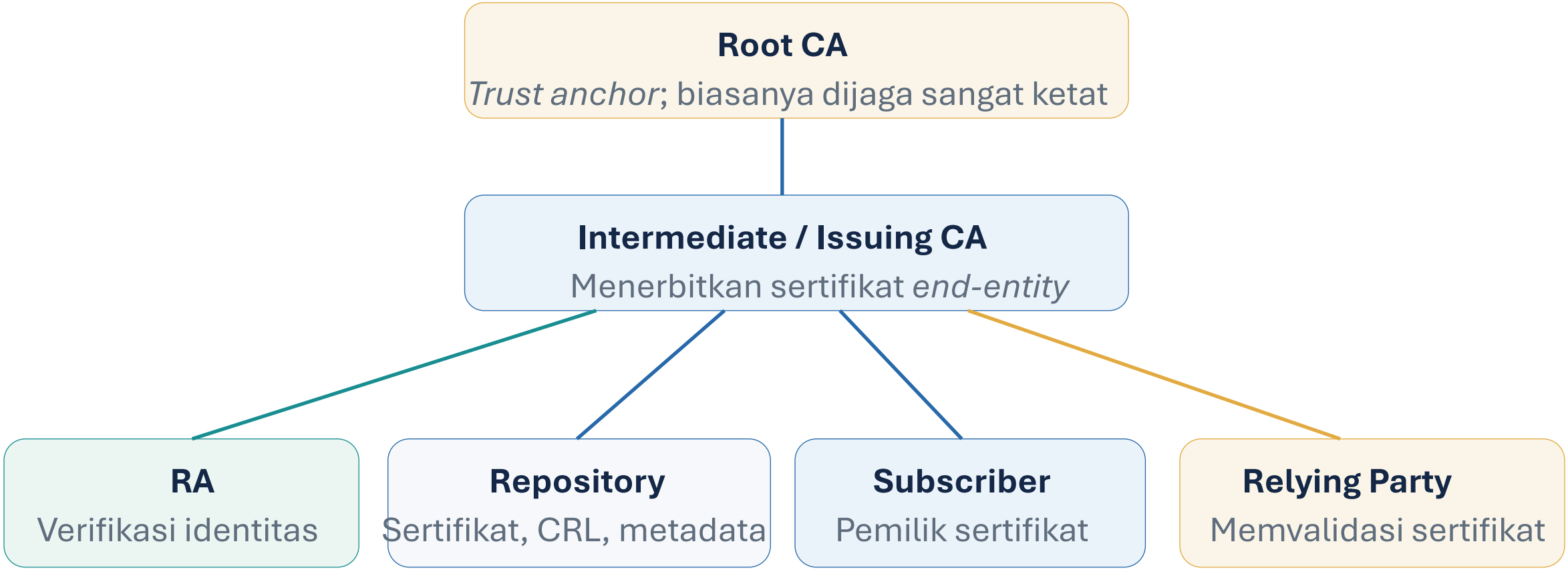
- Sehingga pengguna merasa aman untuk pertukaran data dan informasi melalui saluran yang tidak aman (internet).

Komponen utama *PKI:*

1. Pemilik sertifikat digital (*subscriber)*
   - 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/relying party*
   - Pihak yang mempercayai sertifikat (bank, took online, dll)

# Komponen utama PKI






Komponen dapat tersebar pada organisasi dan sistem yang berbeda; kebijakan dan prosedur mengikat semuanya.

CA, RA, repositori, *subscriber*, dan *relying party* menjalankan fungsi berbeda yang harus diatur melalui kebijakan (*policy*).

# Peran dan tanggung jawab

| Komponen / pihak | Tanggung jawab utama |
| --- | --- |
| *Certification Authority* (CA) | Menerbitkan, menandatangani, memperbarui, dan mencabut sertifikat sesuai kebijakan. |
| *Registration Authority* (RA) | Memeriksa identitas dan kelayakan pemohon; dapat mendelegasikan proses registrasi. |
| *Subscriber* | Entitas yang menjadi subjek sertifikat dan bertanggung jawab menjaga kunci privat. |
| *Relying Party* | Pihak yang memutuskan apakah sertifikat dapat dipercaya untuk transaksi tertentu. |
| Repository / direktori | Menyediakan sertifikat, CRL, dan informasi terkait agar dapat diakses. |
| *Policy Authority* | Menetapkan kebijakan, standar, profil, dan persyaratan operasional PKI. |

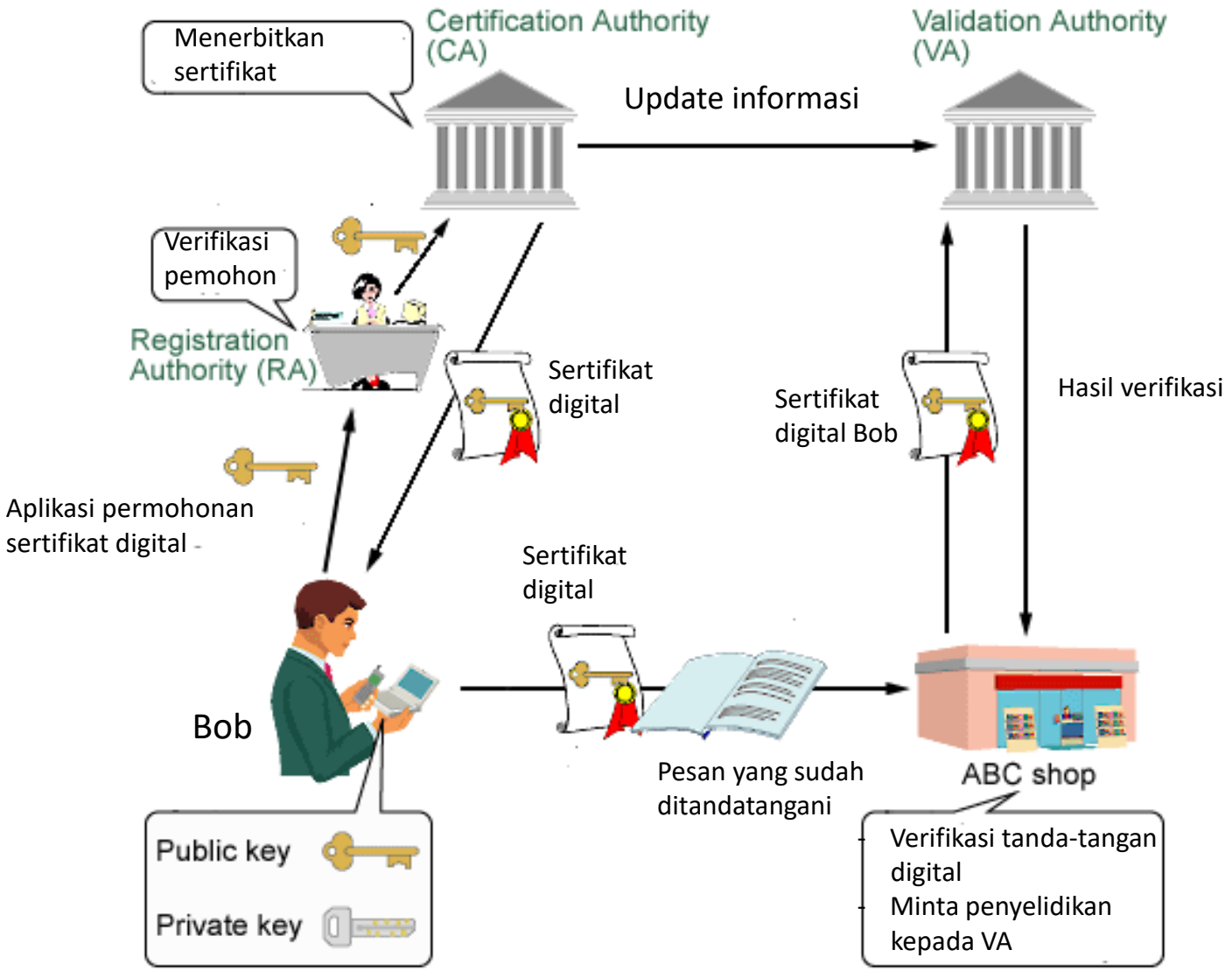
- Dengan demikian, PKI merupakan kerangka (*framework*) terintegrasi yang mengelola sertifikat digital dan pasangan kunci publik–privat sepanjang siklus hidupnya.

- PKI memungkinkan pihak yang belum saling mengenal membangun kepercayaan berbasis sertifikat dan rantai kepercayaan.

- PKI bukan satu produk atau satu *server*; PKI mencakup teknologi, kebijakan, personel, proses, dan pengawasan.

- Standar dan profil sertifikat, seperti X.509, membantu interoperabilitas antar sistem.

# Alur pembuatan dan penggunaan sertifikat digital di dalam PKI




*) VA khusus di Amerika

# Masalah yang diselesaikan PKI



### Autentikasi

Membantu memastikan identitas *server*, pengguna, organisasi, atau perangkat.

### Integritas

Tanda tangan digital memungkinkan deteksi perubahan pada data yang ditandatangani.

### Kerahasiaan

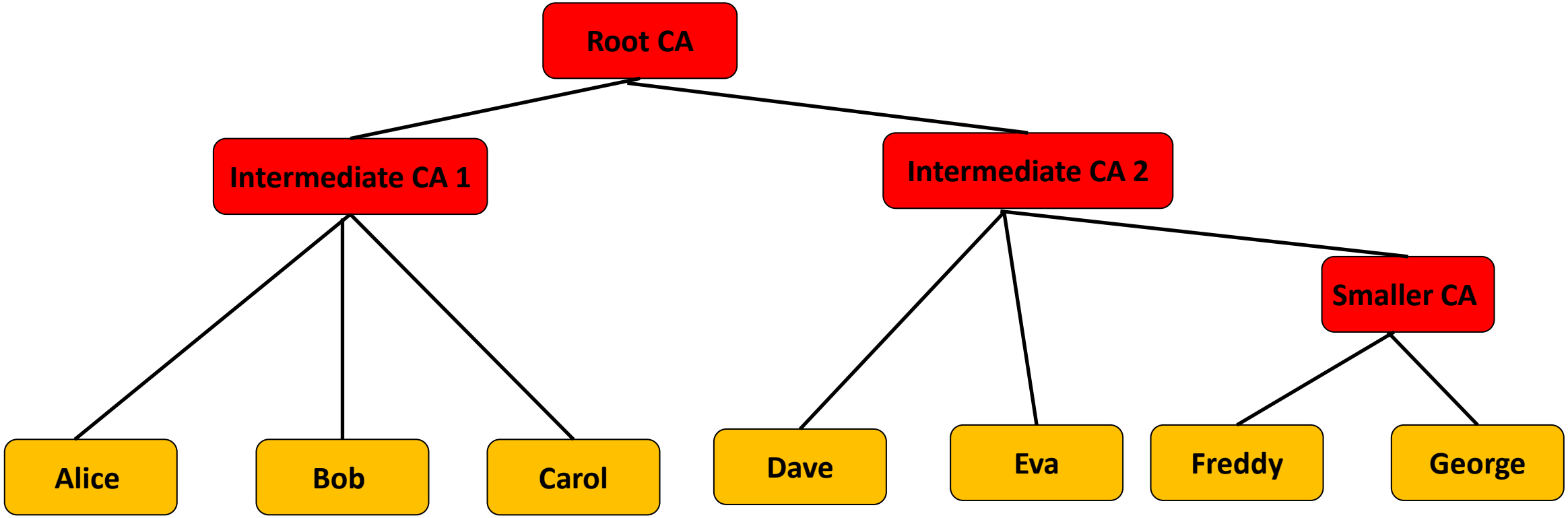
Kunci publik atau mekanisme pertukaran kunci dapat mendukung pembentukan kanal komunikasi data yang terenkripsi.

### Akuntabilitas

Sertifikat, kebijakan, dan log mendukung audit serta penelusuran penggunaan identitas digital.

# Hirarkhi CA di dalam PKI

- *PKI* menyediakan cara penstrukturan komponen-komponennya dan mendefinisikan standard bermacam-macam dokumen dan protokol.
- Hirarkhi CA yang sederhanan adalah dalam struktur pohon:



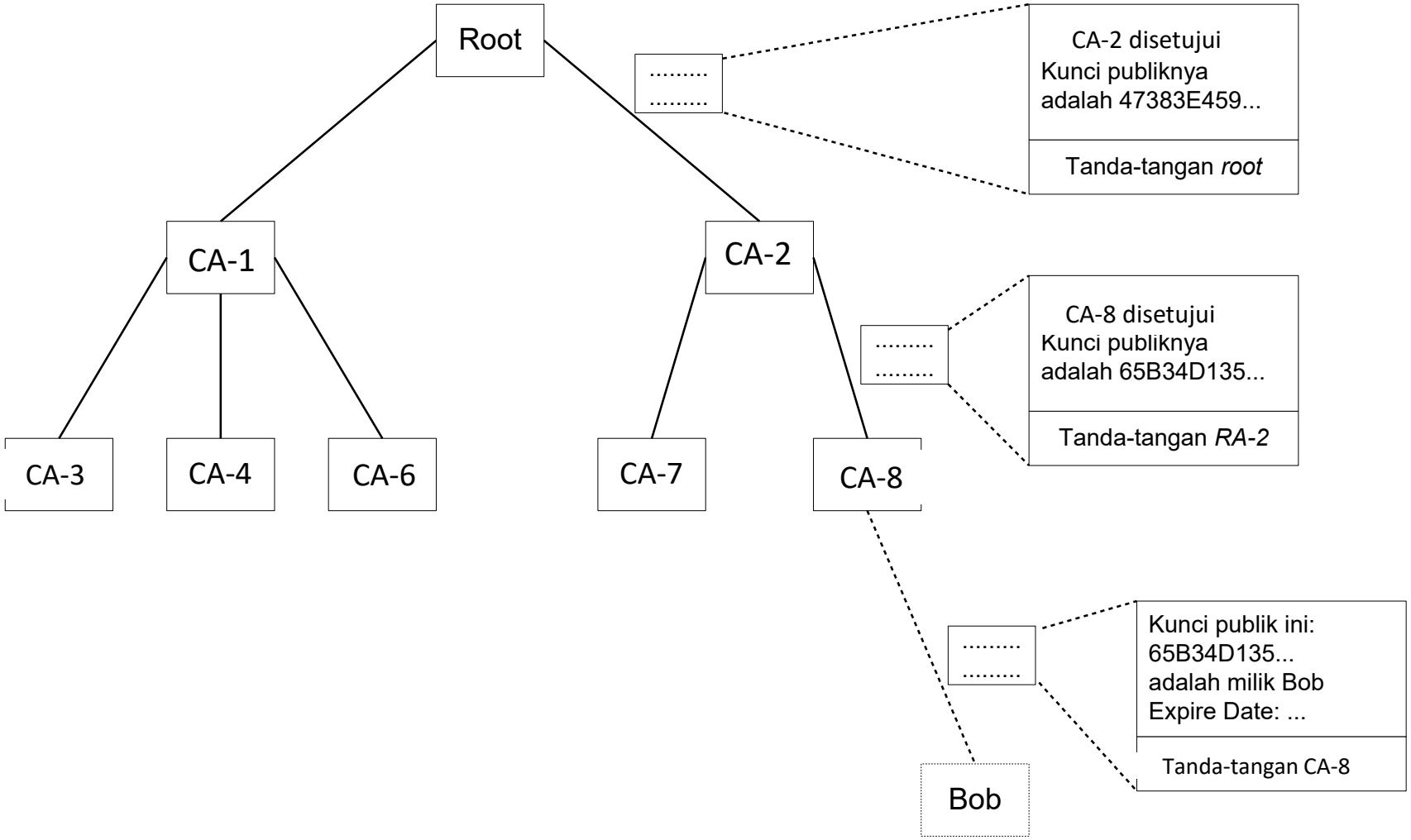
- *Root* CA merupakan *root certificate authority*, yaitu pembuat kebijakan mengenai manajemen sertifikat digital. Semua pengguna mempercayai (*trust*) *root* CA

- *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 (*intermediate* CA).

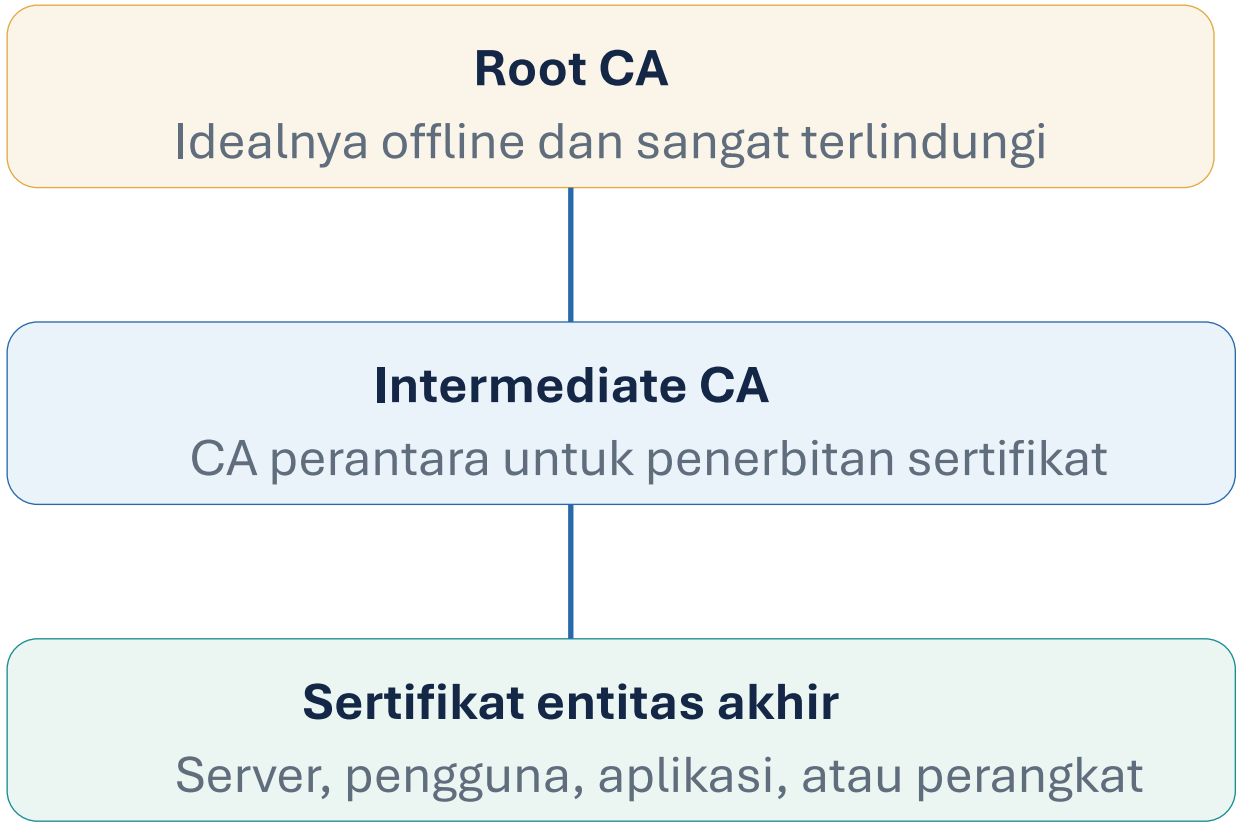
- Dengan cara ini PKI dapat berkembang tanpa seluruh beban dibebankan pada *Root CA*

- 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.*



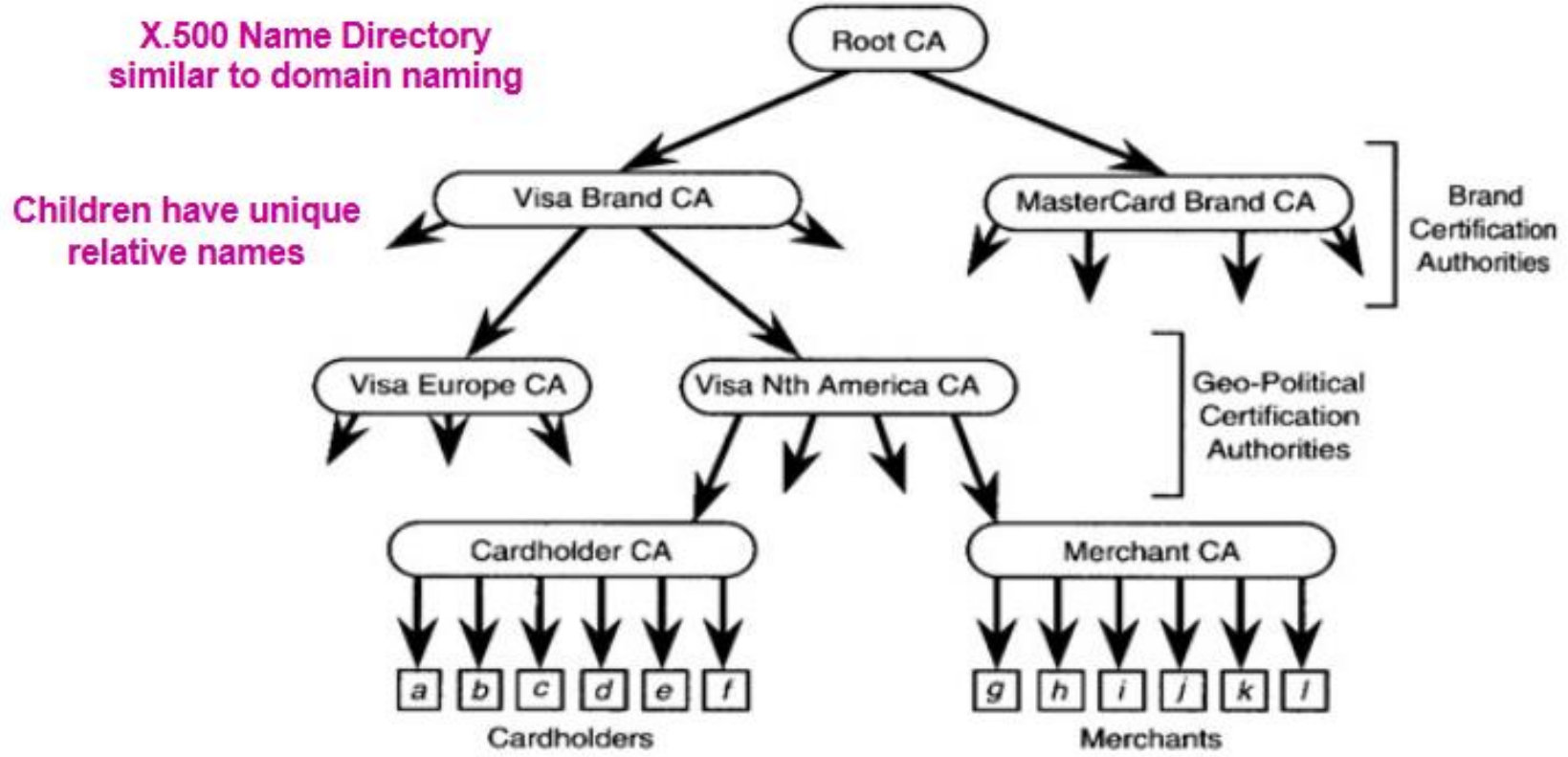
# Hierarki CA dan rantai kepercayaan






Relying party membangun jalur sertifikat dari sertifikat entitas akhir menuju trust anchor yang telah dipercaya.

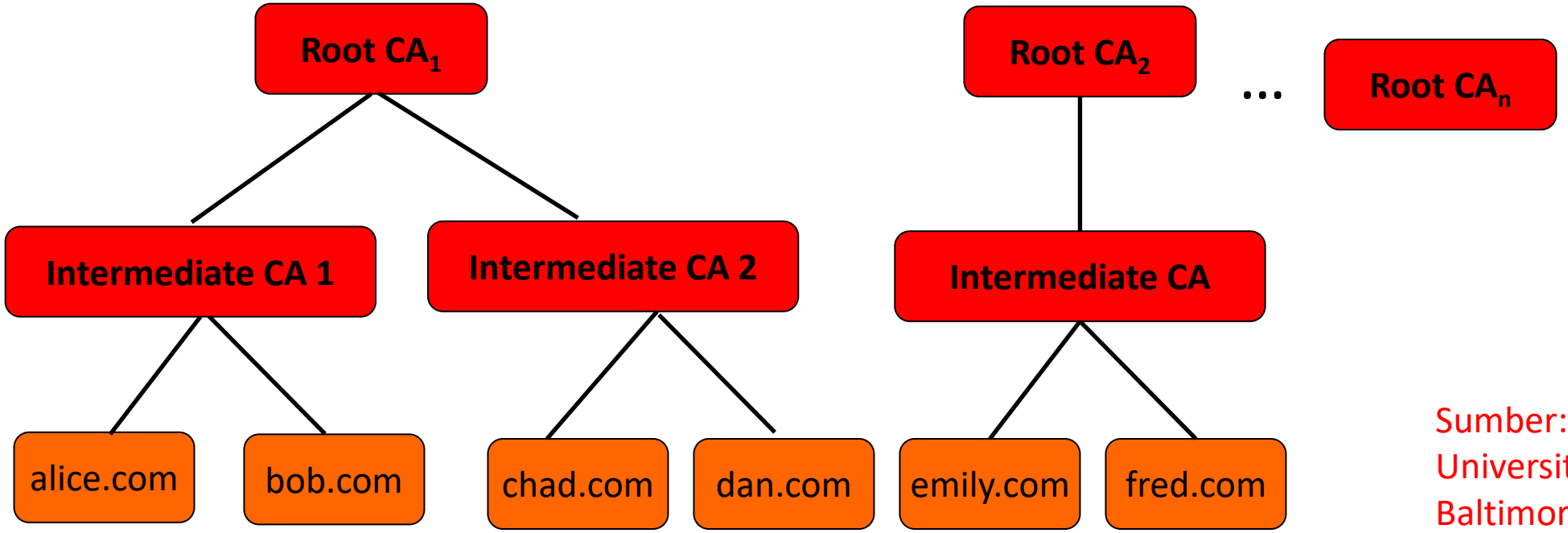
Contoh hirarkhi CA dalam PKI yang menyediakan sertifikat digital kartu kredit Visa dan Mastercard:



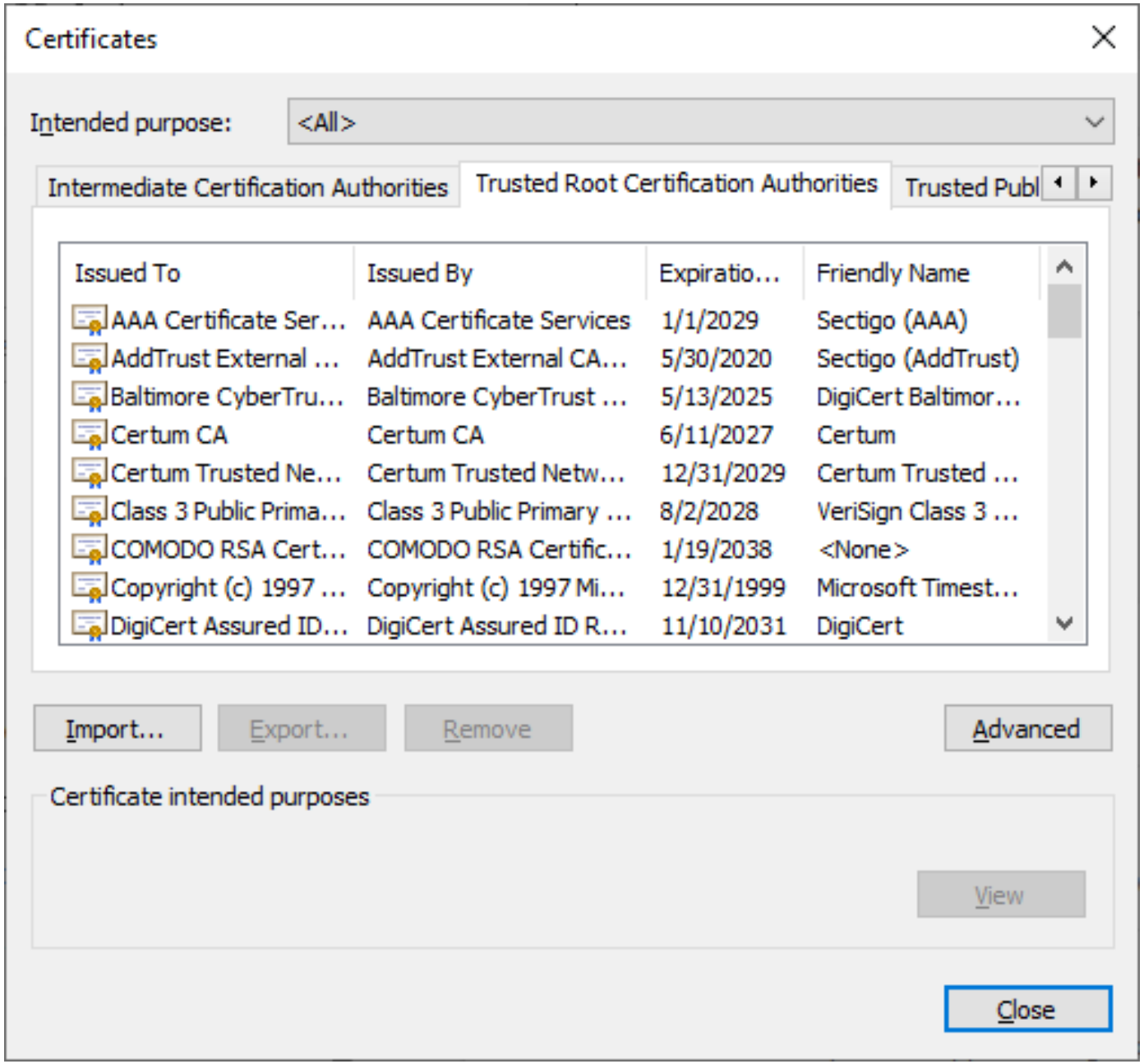

SOURCE: FORD & BAUM, *SECURE ELECTRONIC COMMERCE*

# 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

# Penerapan PKI dalam praktik

### TLS / HTTPS

Autentikasi server dan pembentukan koneksi terenkripsi pada web.

### VPN dan jaringan

Autentikasi perangkat atau pengguna berbasis sertifikat.

### Email dan dokumen

Tanda tangan digital dan, pada skema tertentu, enkripsi pesan/dokumen.

### IoT dan enterprise

Identitas perangkat, autentikasi layanan, serta komunikasi antarmesin.

# Tantangan dan ancaman PKI

## Tantangan tata kelola

- Kesalahan konfigurasi CA, profil sertifikat, atau *trust store*.
- Validasi sertifikat yang tidak lengkap atau dinonaktifkan.
- Pengelolaan masa berlaku, inventaris, dan pencabutan yang buruk.
- Ketergantungan pada ketersediaan layanan dan interoperabilitas.

## Ancaman keamanan

- Kunci privat *subscriber* atau CA berhasil diketahui.
- Penerbitan sertifikat yang keliru atau tanpa verifikasi memadai.
- Serangan terhadap proses registrasi, administrator, atau sistem CA.
- Algoritma dan ukuran kunci yang usang; perlu kebijakan kriptografi yang adaptif.

# Praktik baik membangun PKI

- Tetapkan *Certificate Policy* (CP) dan *Certification Practice Statement* (CPS) yang jelas.
- Pisahkan *Root CA* dari CA penerbit; batasi akses administratif dan gunakan prinsip least privilege.
- Gunakan algoritma, parameter, dan masa berlaku sesuai standar serta kebijakan organisasi.
- Inventarisasi sertifikat dan otomatisasi penerbitan, pemantauan, serta pembaruan.
- Uji prosedur pencabutan, pemulihan, rotasi kunci, audit, dan respons insiden secara berkala.

# PKI dan transisi menuju Kriptografi Pasca-Kuantum (PQC)

- PKI bergantung pada algoritma tanda tangan dan mekanisme kunci yang digunakan oleh CA, sertifikat, dan protokol.
- Komputer kuantum berskala relevan berpotensi mengancam algoritma kunci publik tertentu, terutama RSA dan ECC.
- Transisi PQC perlu mencakup inventaris algoritma, pembaruan profil sertifikat, perangkat CA/HSM, protokol,  , dan interoperabilitas.
- Algoritma PQC standar seperti ML-DSA dapat menjadi bagian dari pembaruan tanda tangan digital; dukungan ekosistem dan profil sertifikat perlu diperhatikan.
- PKI harus dirancang agar mampu mengelola perubahan algoritma dan siklus migrasi secara terukur.

# Beberapa Penyedia PKI

- *DigiCert* — sertifikat TLS dan layanan PKI untuk perusahaan.
- *GlobalSign* — sertifikat digital dan layanan identitas.
- *Sectigo* — sertifikat TLS dan pengelolaan sertifikat.
- *Entrust* — solusi PKI, identitas digital, dan keamanan.
- *Let's Encrypt* — penerbit sertifikat TLS otomatis untuk HTTPS.
- *IdenTrust* — layanan sertifikat digital dan identitas tepercaya.

# Penyedia PKI di Indonesia

- Di Indonesia, penyedia layanan yang berkaitan dengan PKI umumnya dikenal sebagai **Penyelenggara Sertifikasi Elektronik** (PSrE).

- Mereka menerbitkan dan mengelola sertifikat elektronik untuk mendukung tanda tangan digital, autentikasi, dan layanan kepercayaan digital lainnya.

- Perlu diingat bahwa PSrE bukan PKI itu sendiri. PSrE merupakan penyelenggara yang dapat mengoperasikan komponen PKI, terutama CA dan layanan sertifikat elektronik, dalam kerangka regulasi Indonesia.

- Dalam konteks regulasi Indonesia, sertifikat digital dinamakan sertifikat elektronik

# Daftar PrSE di Indonesia:

| No. | Nama penyedia | Situs web |
|---|---|---|
| 1 | BSrE – BSSN (Balai Sertifikasi Elektronik) | bsre.bssn.go.id |
| 2 | Peruri | ca.peruri.co.id |
| 3 | Privy | privy.id |
| 4 | VIDA (PT Indonesia Digital Identity) | vida.id |
| 5 | DigiSign (PT Solusi Net Internusa) | digisign.id |
| 6 | Tilaka | tilaka.id |
| 7 | Xignature | xignature.co.id |

- Daftar ini disusun berdasarkan informasi yang tersedia dari Komdigi, BSSN, dan Direktorat Jenderal Pajak.
- Untuk keperluan akademik, daftar resmi dapat diperiksa melalui Direktori PSrE Komdigi (https://tte.komdigi.go.id/listpsrenew )
- Untuk penggunaan sertifikat elektronik pada Coretax, DJP secara khusus mencantumkan empat PSrE noninstansi yang ditunjuk Menteri Keuangan: Privy, VIDA, Vipas Inovasi Teknologi, dan Digital Tandatangan Asli.

tte.komdigi.go.id/listpsrenew

KOMDIGI

TandaTangan DIGITAL
Legalitas Pasti di Ujung Jari

Informasi | Berita dan Kegiatan | Verifikasi PDF

# Bersatu dan Bersama Wujudkan Layanan Digital Terpercaya melalui PSrE Indonesia



Cari Nama PSrE Disini ...

**Kategori PSrE**

- [x] Semua
- [ ] PSrE Instansi
- [ ] PSrE Non-Instansi

**PT Solusi Identitas Global Net**
https://ezsign.id PSrE Non-Instansi

Info Detail

TTE | Segel Elektronik

- Ada perbedaan defenisi antara sertifikat elektronik menurut PrSE dan sertifikat digital menurut kriptografi.

- Sertifikat Elektronik adalah dokumen yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

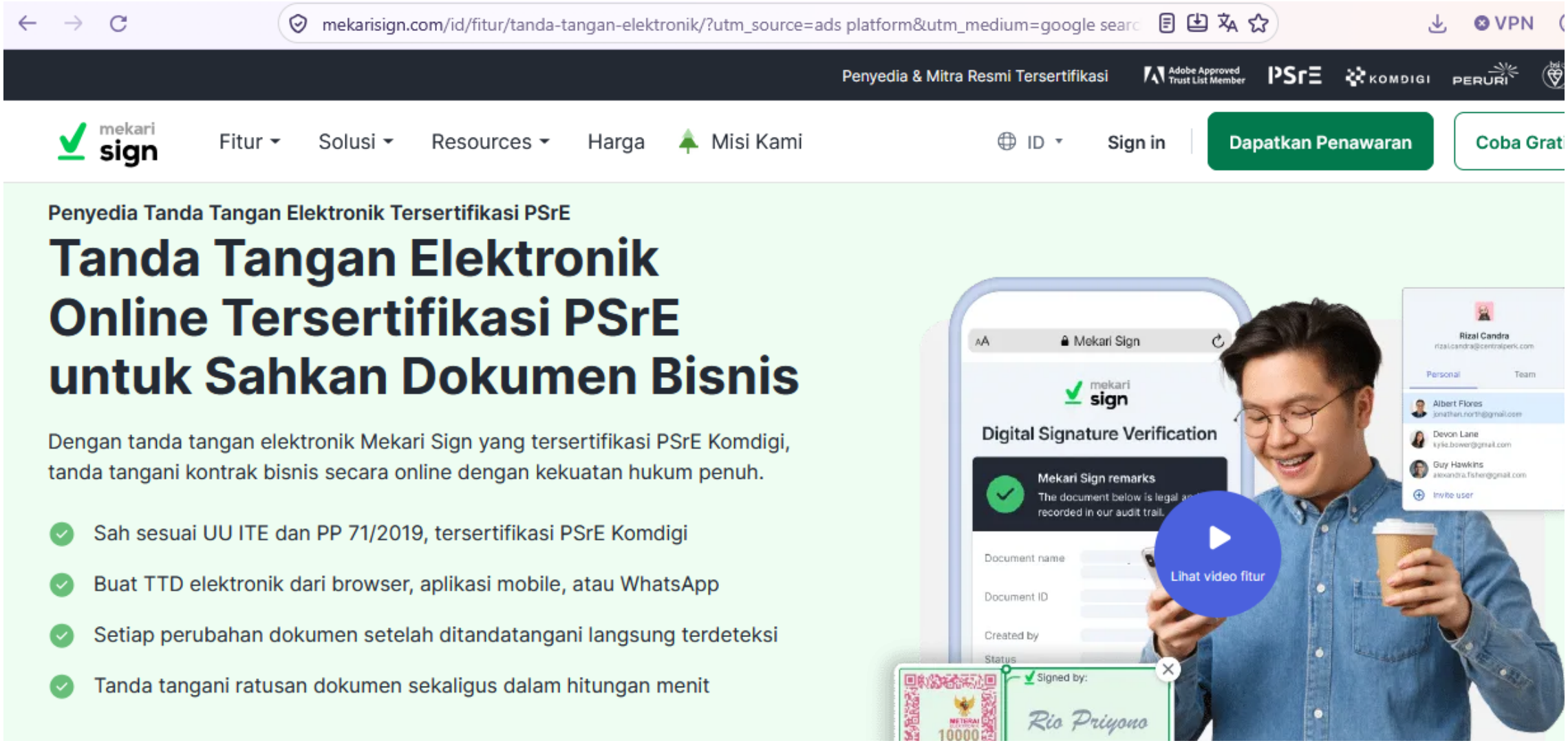
- Tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

https://tte.komdigi.go.id/apaitu

## Fungsi Tanda Tangan Elektronik antara lain:

1. TTE menggantikan fungsi tanda tangan basah pada dokumen elektronik karena tanda tangan basah tidak dapat memberikan kekuatan hukum pada dokumen elektronik.
2. TTE merupakan pemungkin terselenggaranya sistem perkantoran pemerintah dan swasta tanpa kertas.
3. TTE dibuat menggunakan Sertifikat Elektronik yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia.
4. Implementasi TTE telah dilindungi oleh UU ITE Pasal 11 sejak tahun 2008.
5. Dipercaya oleh Swasta, Pemerintah, dan Sistem Peradilan Nasional.

# Contoh website sebuah PrSE:



# SELAMAT BELAJAR