#27

Syahrul Imardi, MT

STMIK Amik Riau

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

Digital Signature Standard (DSS)

P27

STMIK
Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

P27: **Digital Signature Standard**

Standar Tanda-tangan Digital (*DSS*)

Pendahuluan

- DSS adalah bakuan (standard) untuk tanda-tangan digital.
- Diresmikan pada bulan Agustus 1991 oleh NIST (*The National Institute of Standard and Technology*)

- *DSS* terdiri dari dua komponen:

  1. Algoritma tanda-tangan digital: *Digital Signature Algorithm* (*DSA*).

  2. Fungsi *hash* standard: *Secure Hash Algorithm* (*SHA-1*).

Digital Signature Algorithm (*DSA*)

- *DSA* termasuk ke dalam algoritma kriptografi kunci-publik.
- *DSA* tidak dapat digunakan untuk enkripsi; *DSA* dispesifikasikan khusus untuk tanda-tangan digital.

- *DSA* mempunyai dua fungsi utama:

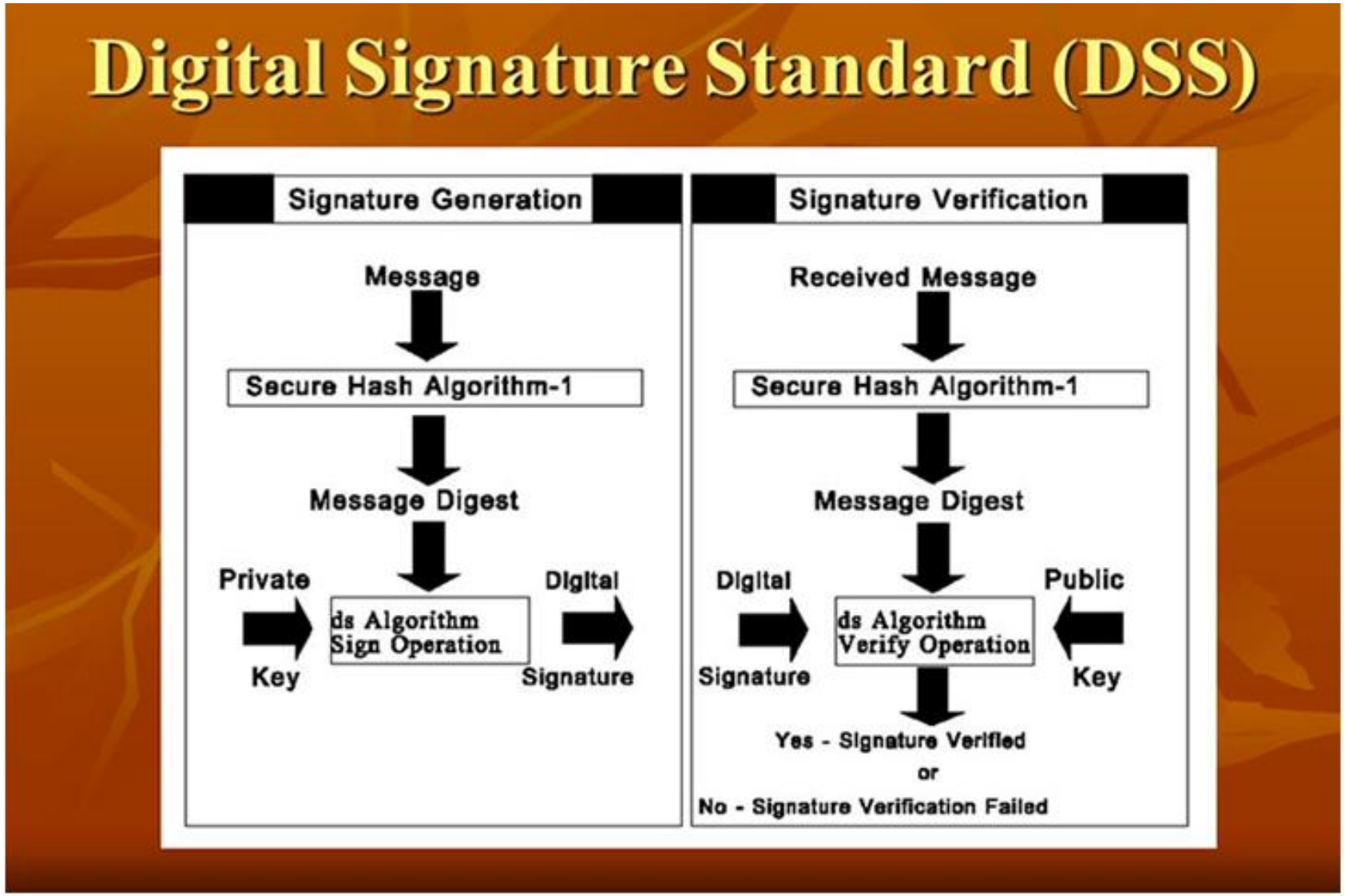
  1. Pembangkitan tanda-tangan (*signature generation*),
  2. Pemeriksaan keabsahan tanda-tangan (*signature verification*).

- *DSA* dikembangkan dari algoritma *ElGamal.*

- *DSA* menggunakan dua buah kunci, yaitu kunci publik dan kunci privat.

- Pembentukan tanda-tangan menggunakan kunci privat, sedangkan verifikasi tanda-tangan menggunakan kunci publik.

- DSA menggunakan fungsi *hash SHA-1* (*Secure Hash Algorithm*) untuk menghasilkan *message digest* yang berukuran 160 bit (SHA-sudah dijelaskan pada materi kuliah sebelumnya).



Sumber: https://signx.wondershare.com/knowledge/digital-signature-algorithm.html

Parameter DSA

1. *p,* bilangan prima, panjangnya *L* bit, $512 \leq L \leq 1024$ dan *L* harus kelipatan 64. Parameter *p* bersifat publik.
2. *q,* bilangan prima 160 bit, merupakan faktor dari $p - 1$. Dengan kata lain, $(p - 1) \bmod q = 0$. Parameter *q* bersifat publik.
3. $g = h^{(p-1)/q} \bmod p$, $h < p - 1$ sedemikian sehingga $h^{(p-1)/q} \bmod p > 1$. Parameter *g* bersifat publik.
4. *x*, kunci privat, adalah bilangan bulat kurang dari *q*.
5. $y = g^x \bmod p$, kunci publik.
6. *m,* pesan yang akan diberi tanda-tangan.

Pembangkitan Sepasang Kunci

1. Pilih bilangan prima p dan q, yang dalam hal ini $(p - 1) \bmod q = 0$.
2. Hitung $g = h^{(p-1)/q} \bmod p$, yang dalam hal ini $1 < h < p - 1$ dan $h^{(p-1)/q} \bmod p > 1$.
3. Tentukan kunci privat x, yang dalam hal ini $x < q$.
4. Hitung kunci publik $y = g^x \bmod p$.

Prosedur di atas menghasilkan:

parameter publik: (p, q, g, y)

parameter privat: x

Pembangkitan Tanda-tangan (*Signing*)

1. Hitung *message digest* pesan *m* dengan fungsi *hash* SHA-1, $H(m)$.

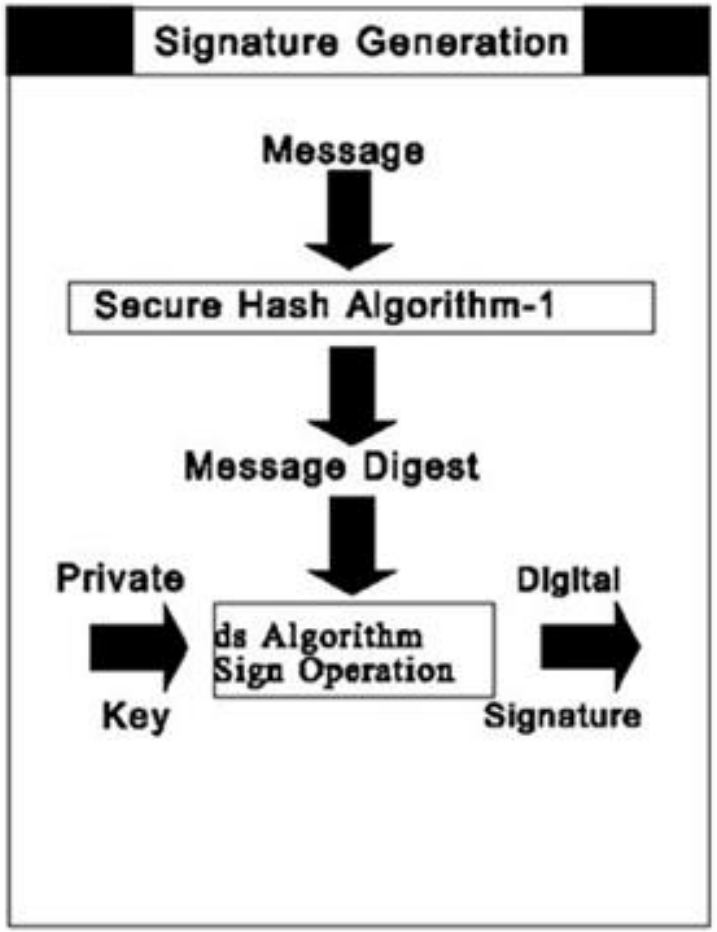
2. Tentukan bilangan acak $k < q$.

3. Tanda-tangan dari pesan *m* adalah bilangan *r* dan *s*. Hitung *r* dan *s* sebagai berikut (kunci privat = *x*):

   $r = (g^k \bmod p) \bmod q$

   $s = (k^{-1}(H(m) + x \cdot r)) \bmod q$

4. Kirim pesan *m* beserta tanda-tangan *r* dan *s*.



Verifikasi Keabsahan Tanda-tangan (*Verifying*)

1. Hitung *message digest* pesan *m* dengan fungsi *hash* SHA-1, $H(m)$.

2. Verifikasi tanda-tangan, *r* dan *s*, sebagai berikut (kunci publik = *y*): :

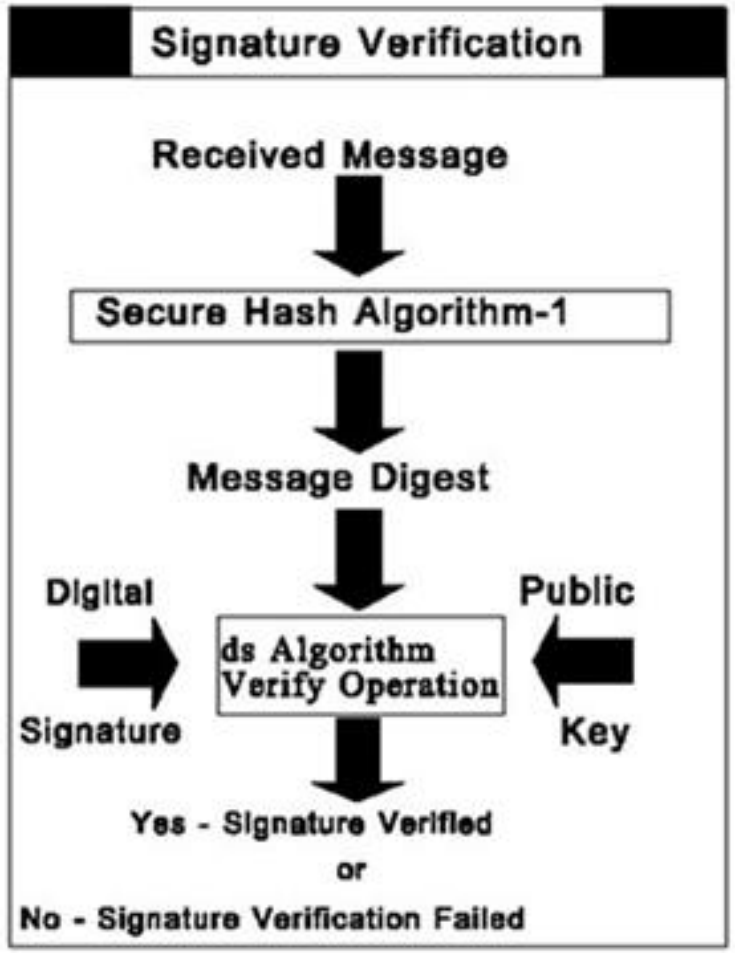
$$w = s^{-1} \bmod q$$

$$u_1 = (H(m) \cdot w) \bmod q$$

$$u_2 = (r \cdot w) \bmod q$$

$$v = ((g^{u1} \cdot y^{u2}) \bmod p) \bmod q)$$

2. Jika $v = r$, maka tanda-tangan digital sah (terverifikasi), sebaliknya tidak sah.



Contoh Perhitungan *DSA*

A. Prosedur Pembangkitan Sepasang Kunci

1. Pilih bilangan prima p dan q, yang dalam hal ini $(p - 1) \bmod q = 0$.

   $p = 59419$

   $q = 3301$ (memenuhi $(59419 - 1) \bmod 3301 = 0$)

2. Hitung $g = h^{(p-1)/q} \bmod p$, yang dalam hal ini $1 < h < p - 1$ dan $h^{(p-1)/q} \bmod p > 1$.

   $g = 100^{(59419-1)/3301} \bmod (59419) = 18870$ (dengan $h = 100$)

3. Tentukan kunci privat x, yang dalam hal ini $x < q$.

   $x = 3223$

4. Hitung kunci publik $y = g^x \bmod p$.

   $y = 18870^{3223} \bmod 59419 = 29245$ (cek dengan Wolframalpha ☺)

B. Prosedur Pembangkitan Tanda-tangan (Signing)

1. Hitung nilai *hash* dari pesan *m*, misalkan $H(m) = 4321$

2. Tentukan bilangan acak $k < q$.

   $k = 997$

   $k^{-1} \equiv 2907 \pmod{3301}$

parameter publik: (p = 59419 , q = 3301, g = 18870)
parameter privat: x = 3223

3. Hitung tanda-tangan digital, *r* dan *s*, sebagai berikut:

   $r = (g^k \bmod p) \bmod q = (18870^{997} \bmod 3301) = 848$

   $s = (k^{-1}(H(m) + x \cdot r)) \bmod q = (2907\ (4321 + 3223 \cdot 848)) \bmod 3301$

   $= 7957694475 \bmod 3301 = 183$

4. Kirim pesan *m* dan tanda-tangan, (*r*, s) = (848, 183)

C. Prosedur Verifikasi Keabsahan Tanda-tangan

1. Hitung nilai *hash* dari pesan *m*, misalkan $H(m) = 4321$
2. Verifikasi tanda-tangan, $(r, s) = (848, 183)$, sebagai berikut:

parameter publik: (p = 59419 , q = 3301, g = 18870, y = 29245)

$$s^{-1} \equiv 469 \pmod{3301}$$

$$w = s^{-1} \bmod q = 469 \bmod 3301 = 469$$

$$u_1 = (H(m) \cdot w) \bmod q = (4321 \cdot 469)\ 2026549 \bmod 3301 = 3036$$

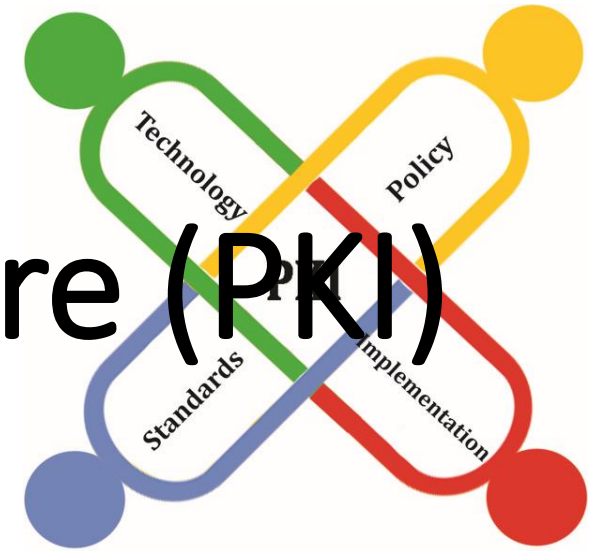
$$u_2 = (r \cdot w) \bmod q = (848 \cdot 469) = 397712 \bmod 3301 = 1592$$

$$v = ((g^{u1} \cdot y^{u2}) \bmod p) \bmod q) = (18870^{3086} \cdot 29245^{1592}) \bmod 3301$$

$$= 3036\ 848 \bmod 3301 = 848$$

3. Karena $v = r$, maka tanda-tangan sah.

Public Key Infrastructure (PKI)



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 sekumpulan aturan, kebijakan, prosedur, *hardware* dan *software* yang dibutuhkan untuk membuat, mendistribusikan, menggunakan, menyimpan, mengelola, dan membuang sertifikat digital.

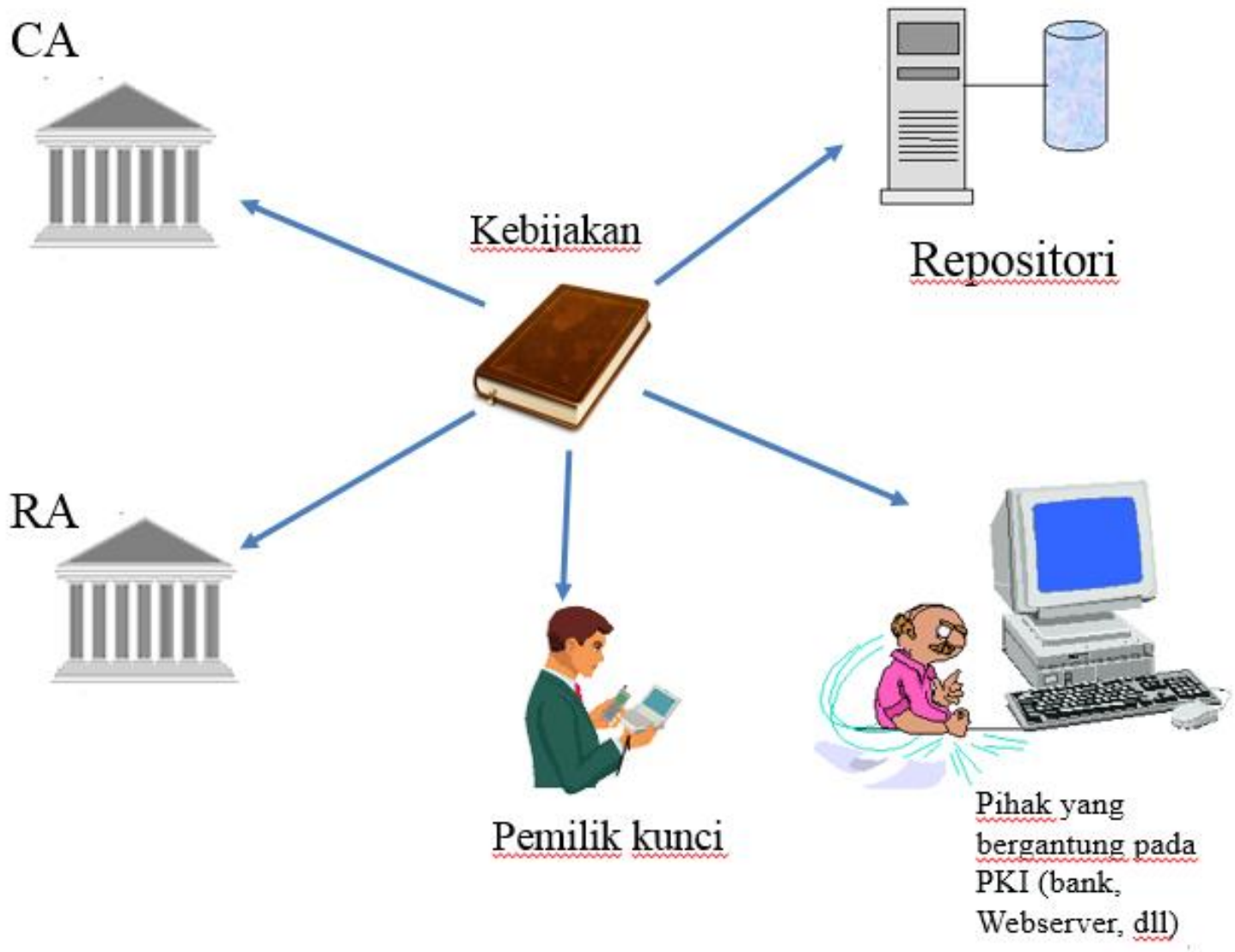
- PKI mengintegrasikan kriptografi kunci-publik dengan sertifikat digital dan *CA* untuk mengotentikasi pihak-pihak dalam suatu transaksi elektronik.

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

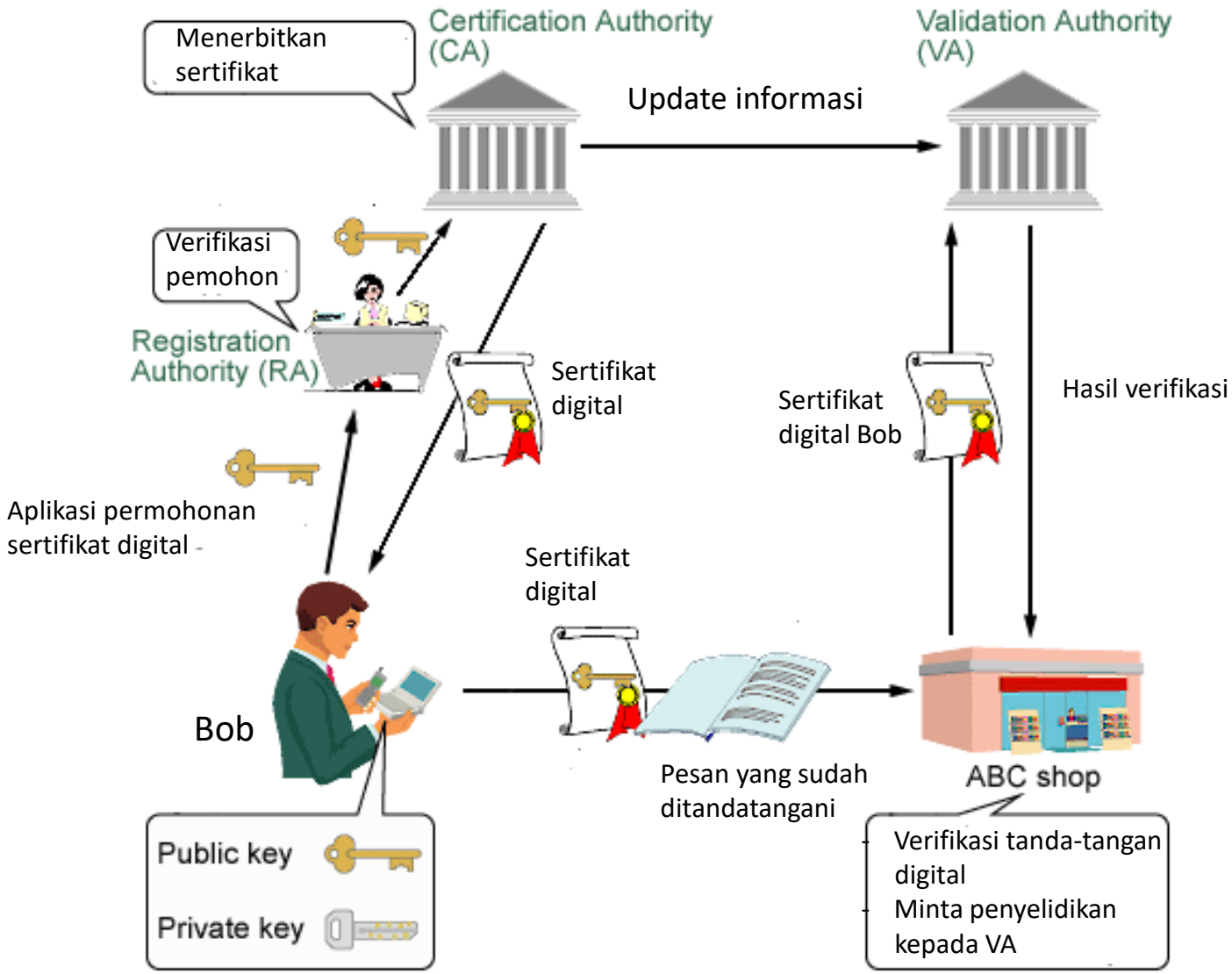
Komponen-komponen *PKI:*

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



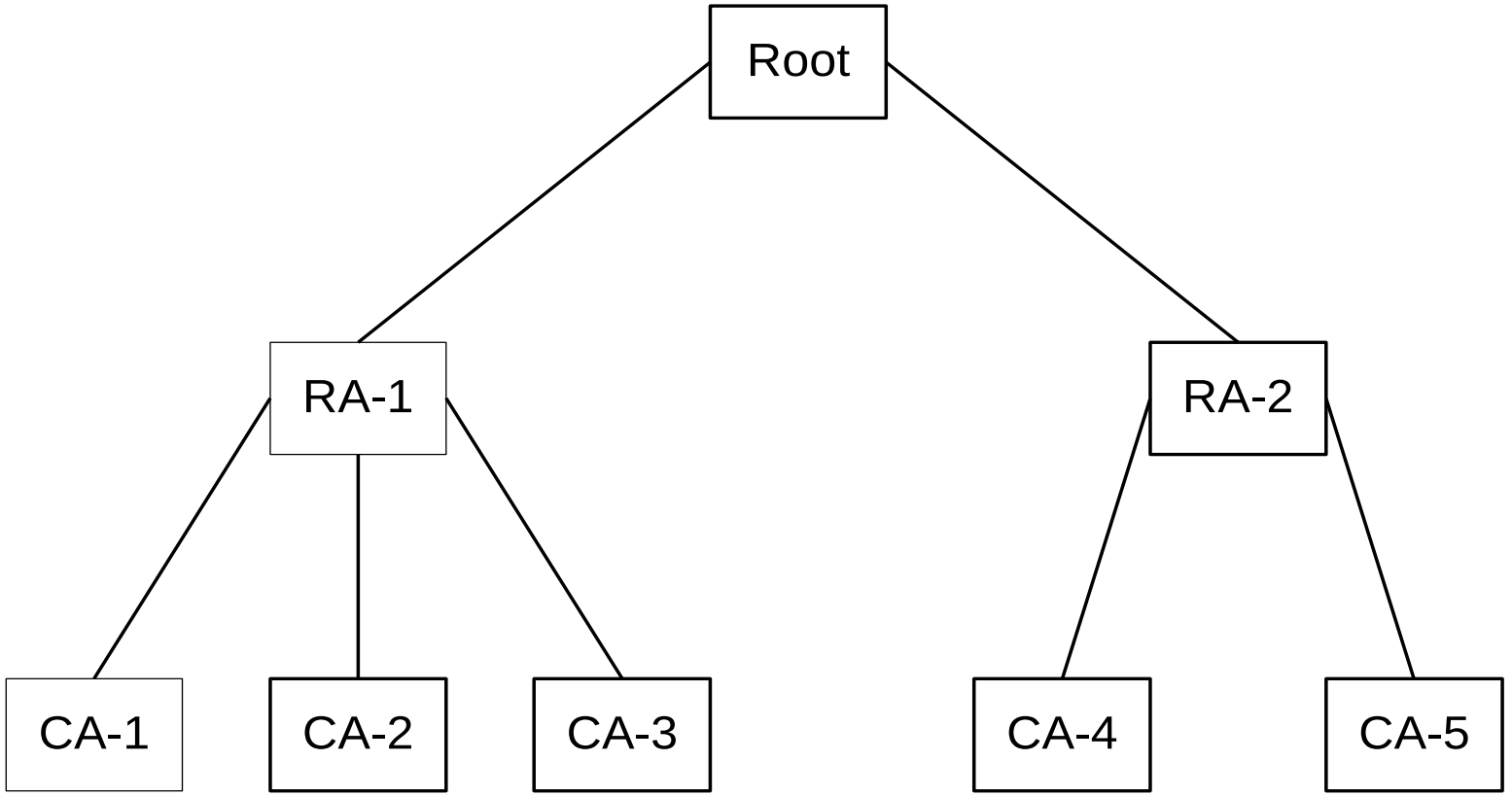
Beberapa Penyedia PKI

Among PKI leaders are:

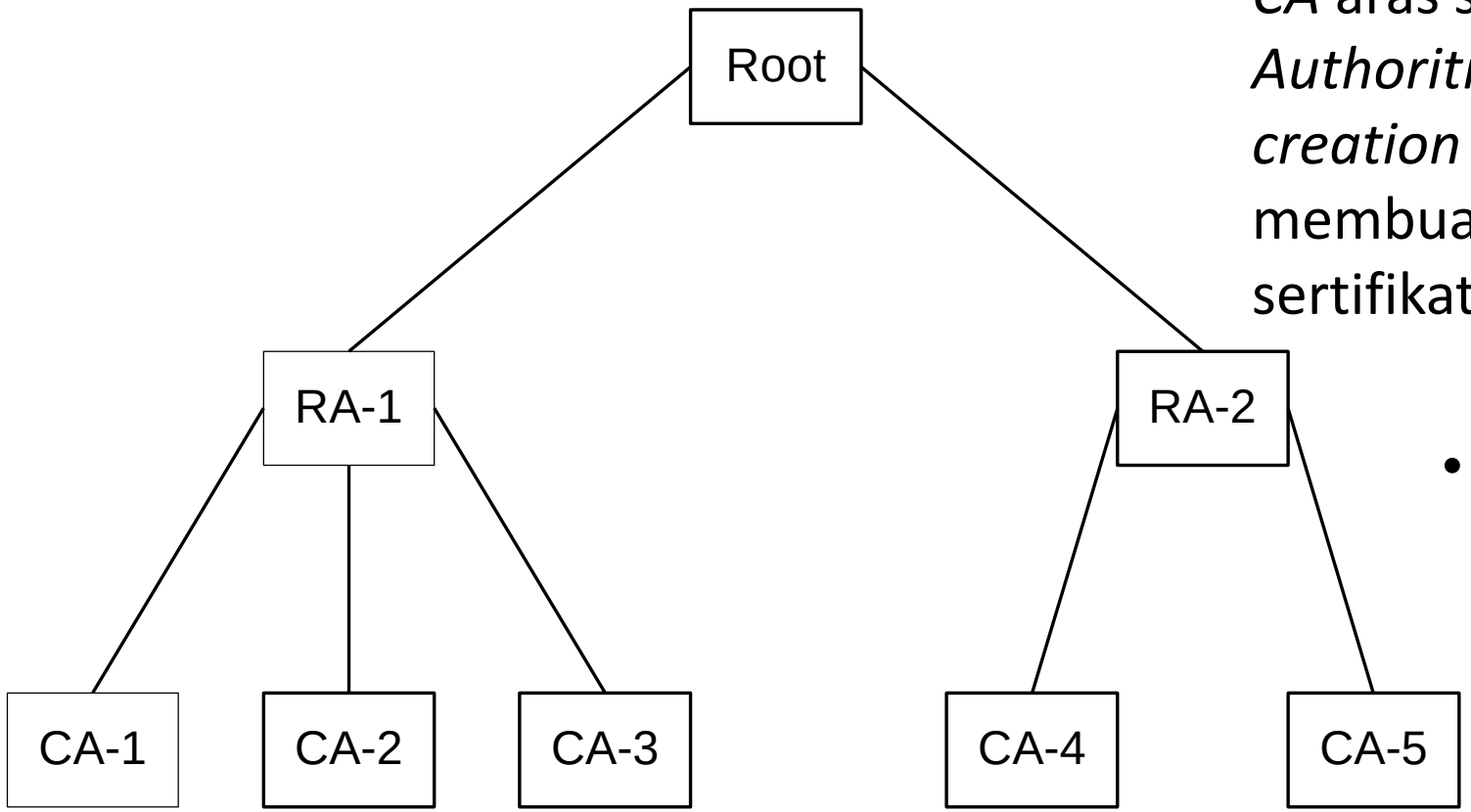
- *RSA*, which has developed the main algorithms used by PKI vendors
- *Verisign*, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities
- *GTE CyberTrust*, which provides a PKI implementation methodology and consultation service that 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:

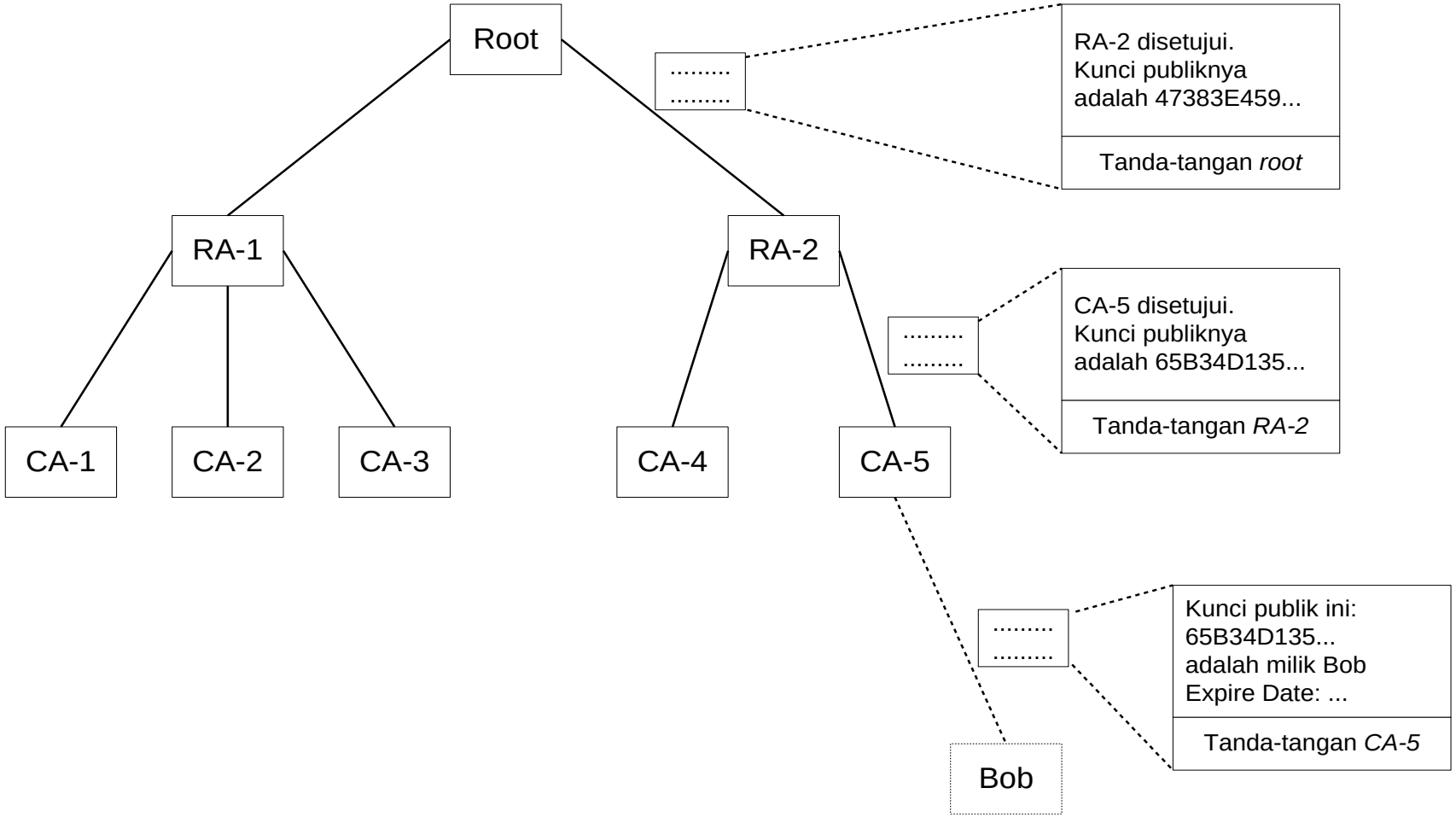


- *Root* merupakan *root certificate authority*, yaitu pembuat kebijakan mengenai manajemen sertifikat digital .
- *Root* mensertifikasi *CA* aras satu dengan menggunakan privat *root* yang disebut *root key*.

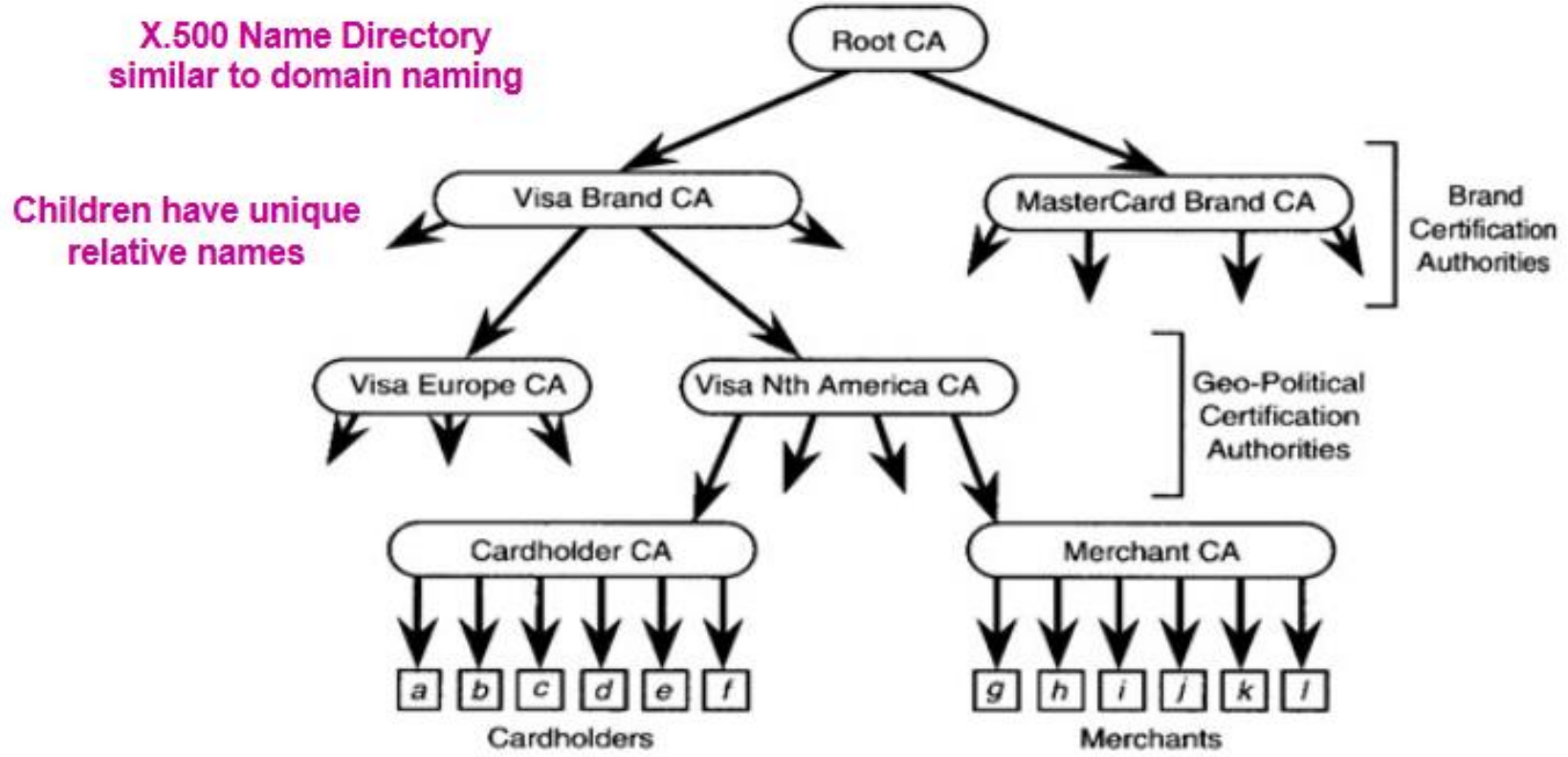


- *CA* aras satu adalah *RA* (*Registration Authorities*), yang bertindak sebagai *policy creation authority*, yaitu oganisasi yang membuat kebijakan untuk memperoleh sertifikat digital.
- Sebuah *RA* mungkin mencakup beberapa area geografis, seperti negara bagian, negara, atau benua.

- 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.*

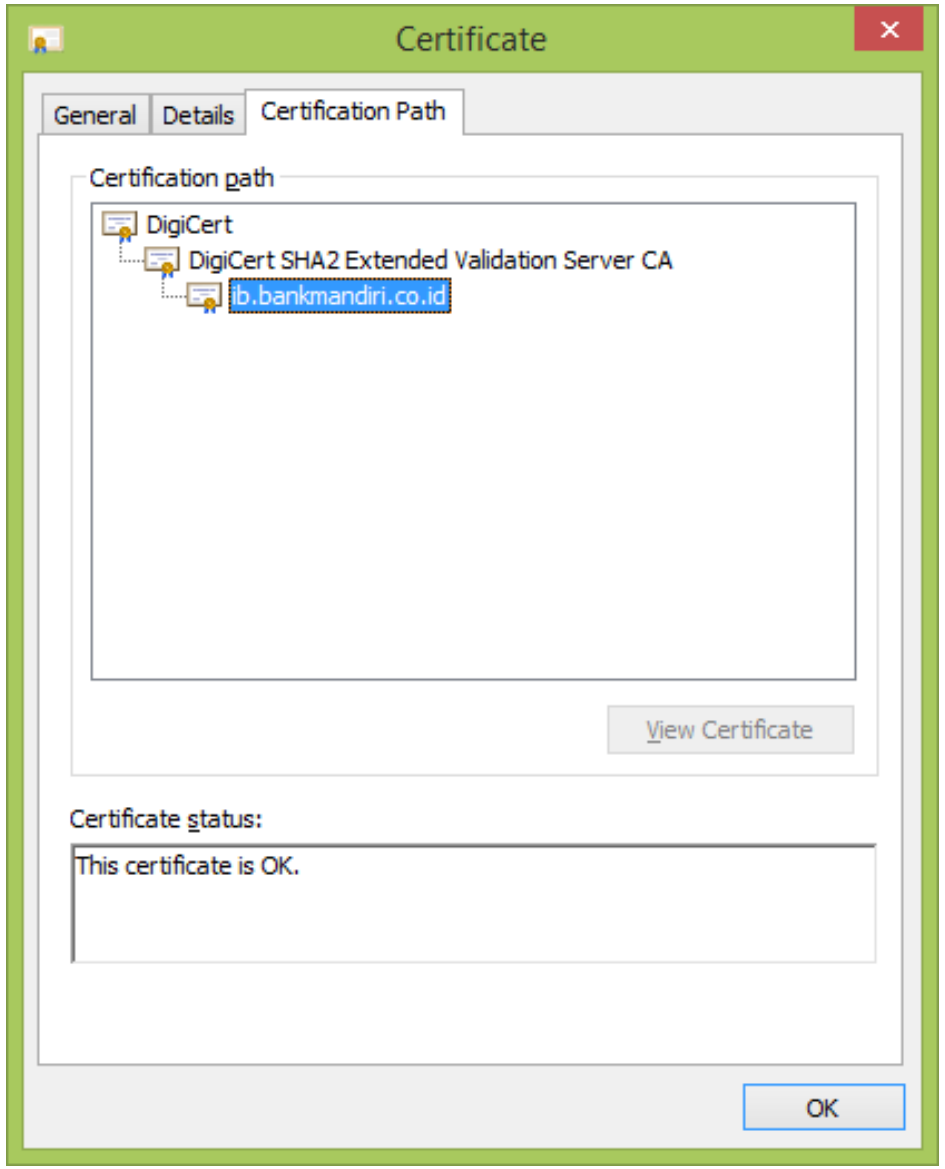


Contoh sebuah rantai sertifikat untuk CA penyedia sertifikat kartu kredit Visa dan Mastercard:



SOURCE: FORD & BAUM, *SECURE ELECTRONIC COMMERCE*

Rantai sertifikat digital untuk server Bank Mandiri :

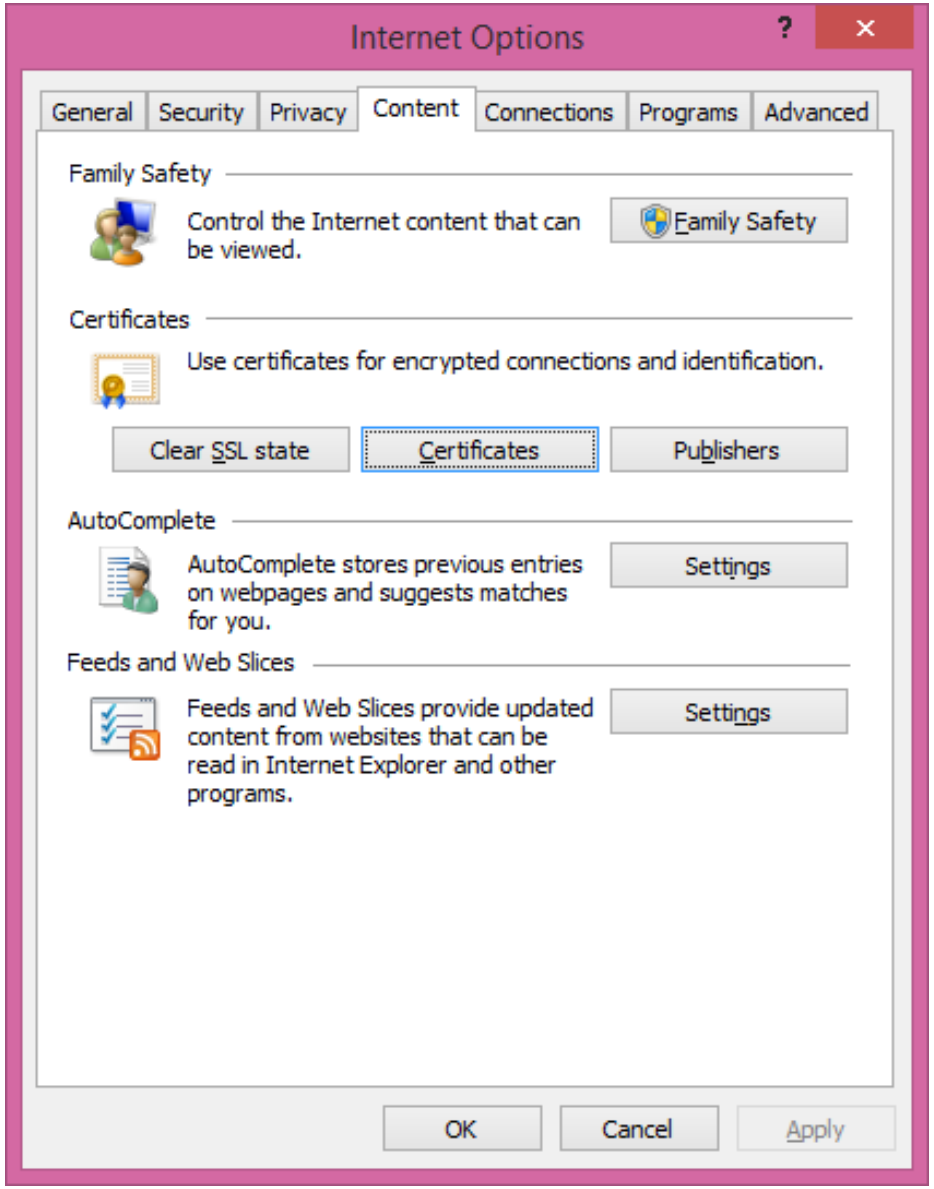


- *Digicert* adalah CA pada aras 0 (*root*),
- *Digicert SHA2* adalah CA pada aras 1,
- daunnya adalah web Bank Mandiri.

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

- Pilih:

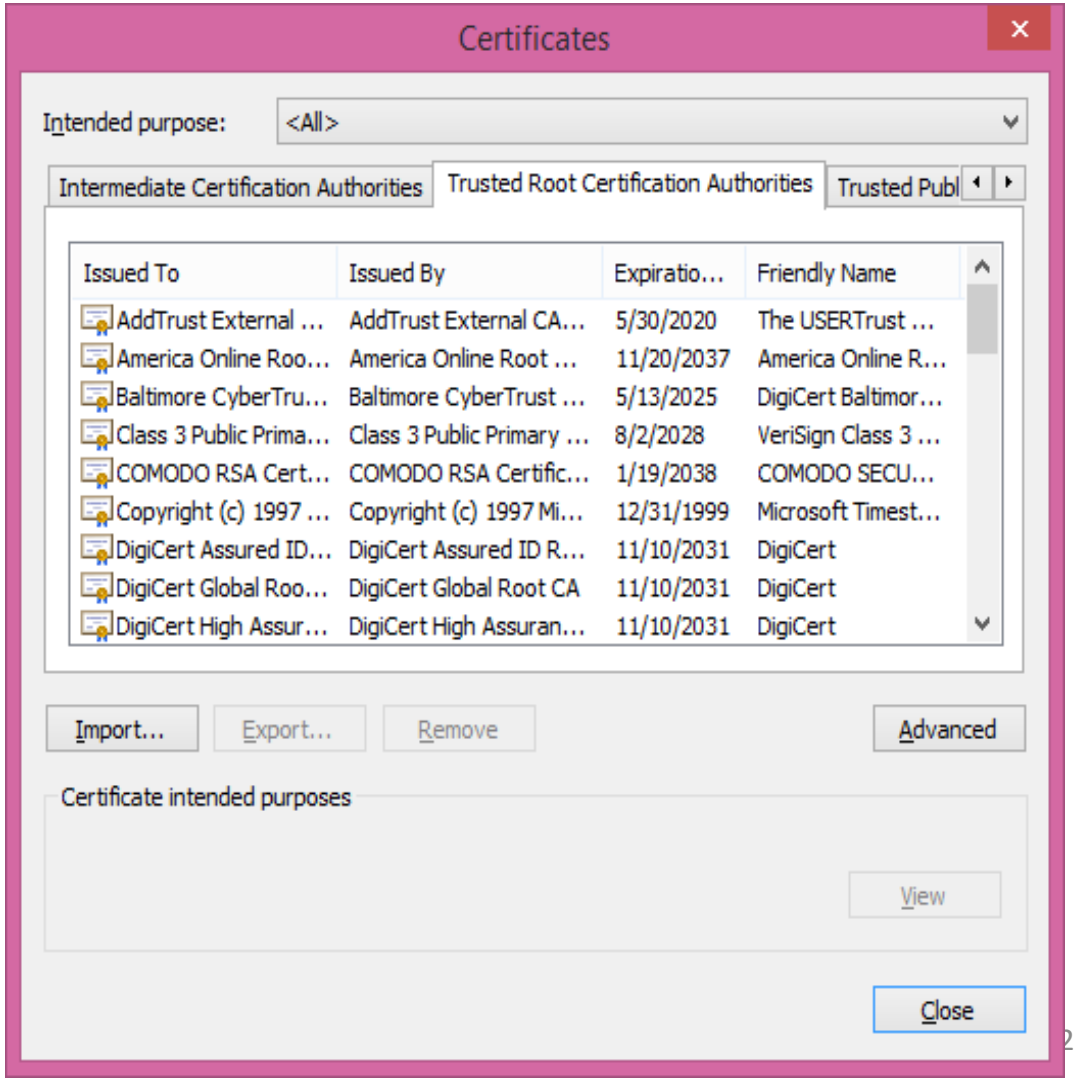
  Internet Options → *Content*



- Kemudian, klik tab:

  Certificates → Trusted Root Certification Authorities

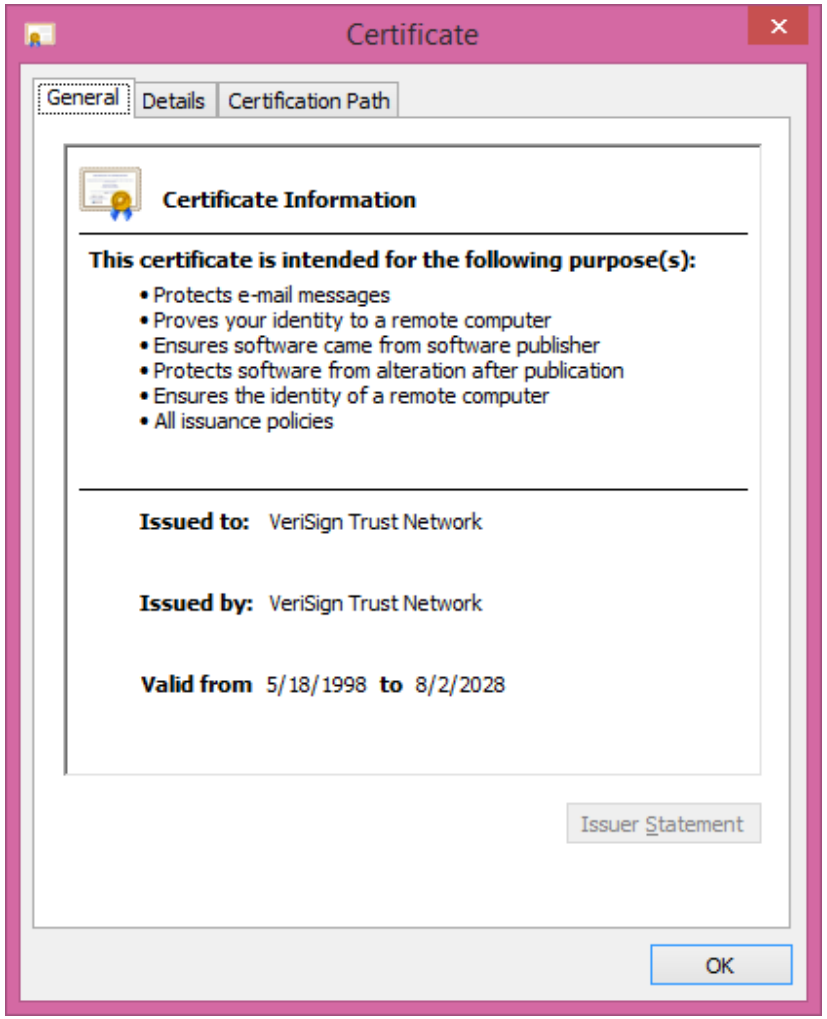
- *Trusted Root CA* adalah *root* di dalam *PKI* dan memiliki cabang berupa *Intermediate CA*.

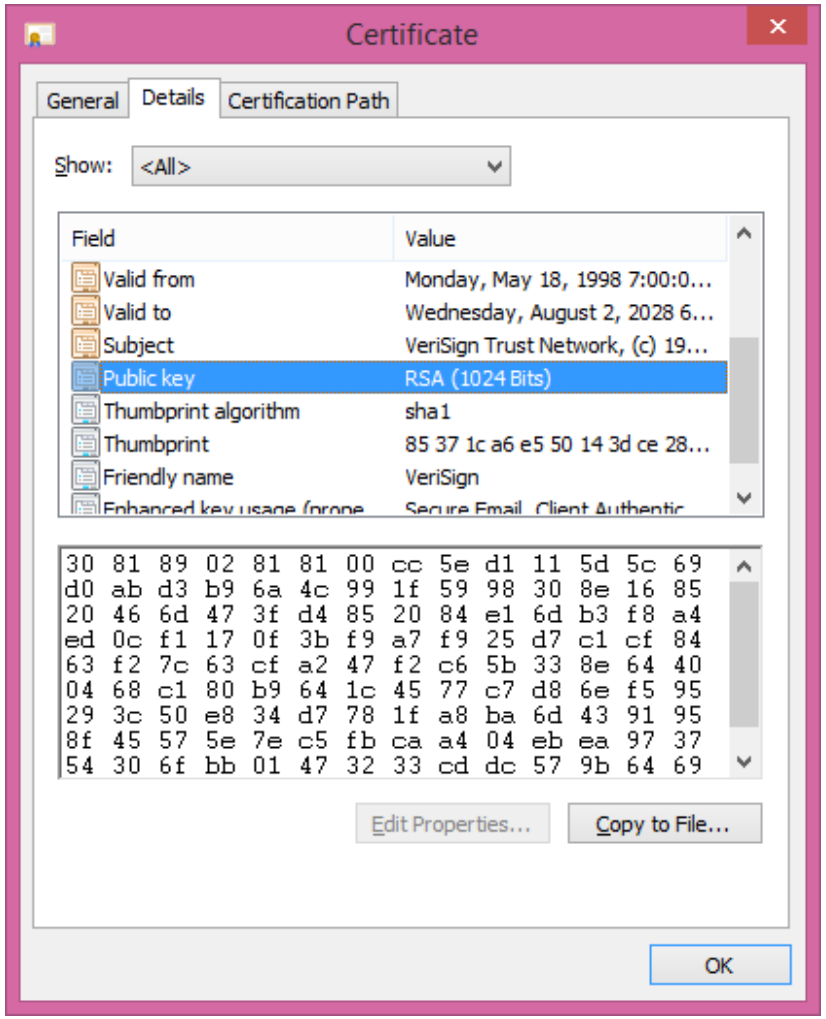


- Bila terdapat *server* di internet yang diberi sertifikat oleh perusahaan yang tidak tercantum di dalam daftar *CA* di atas, maka *IE* akan memperingatkan bahwa *IE* tidak mengenal *CA* tersebut.

- Jika pengguna mempercayai *server* tersebut, maka *CA* tersebut akan ditambahkan ke dalam *IE*.

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





Referensi utama :

>> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.

>> Nancy R. Mead, Carol Woody - Cyber Security Engineering_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)

>> James Helfrich - Security for Software Engineers-CRC Press (2019)

>> Pete Loshin - Simple Steps to Data Encryption_ A Practical Guide to Secure Computing-Syngress (2013)

>> Tevfik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017


Ada pertanyaan?