Sertifikat Digital dan *Public Key Infrastructure* (*PKI*)

Bahan Kuliah IF4020 Kriptografi

Oleh:
Rinaldi Munir
Program Studi Informatika ITB

Pengantar

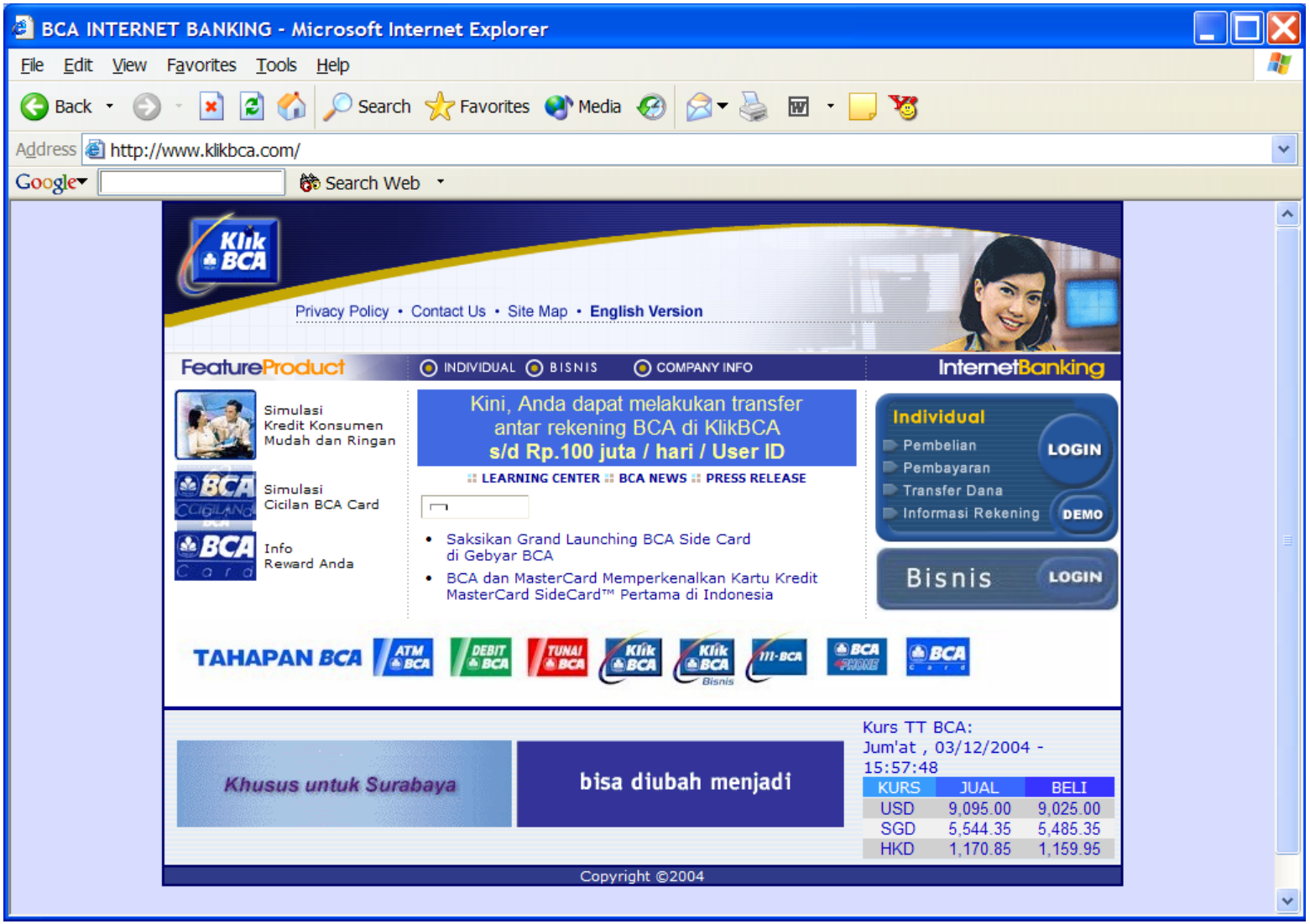
- Sistem kriptografi kunci-publik merupakan metode yang umum digunakan di Internet untuk enkripsi pesan dan otentikasi pengirim.
- Saat ini penggunaan sistem kriptografi kunci-publik telah memiliki aplikasi yang sangat luas, khususnya dalam bidang *e-commerce* .
- Seperti kita ketahui, sistem kriptografi kunci-publik mensyaratkan pengguna memiliki sepasang kunci: kunci privat dan kunci publik.
- Kunci privat dan kunci publik dapat dimiliki oleh individu, komputer *server*, atau perusahaan (*enterprise*).
- Contoh penggunaan: *client* perlu mengotentikasi server (via tanda-tangan digital) dengan menggunakan kunci publik *server.*

- Kunci privat hanya diketahui oleh pemilik, tidak dibagi kepada pihak lain, tetapi kunci publik tersedia untuk umum.

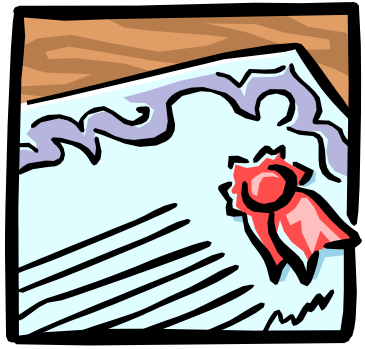
- Masalah: Kunci publik tidak mempunyai suatu kode yang mengidentifikasi pemiliknya.

- Pihak lain dapat menyalahgunakan kunci publik yang bukan miliknya untuk *impersonation attack* .

- Kasus *impersonation attack* yang pernah terjadi di Indonesia: peniruan *website* BCA.

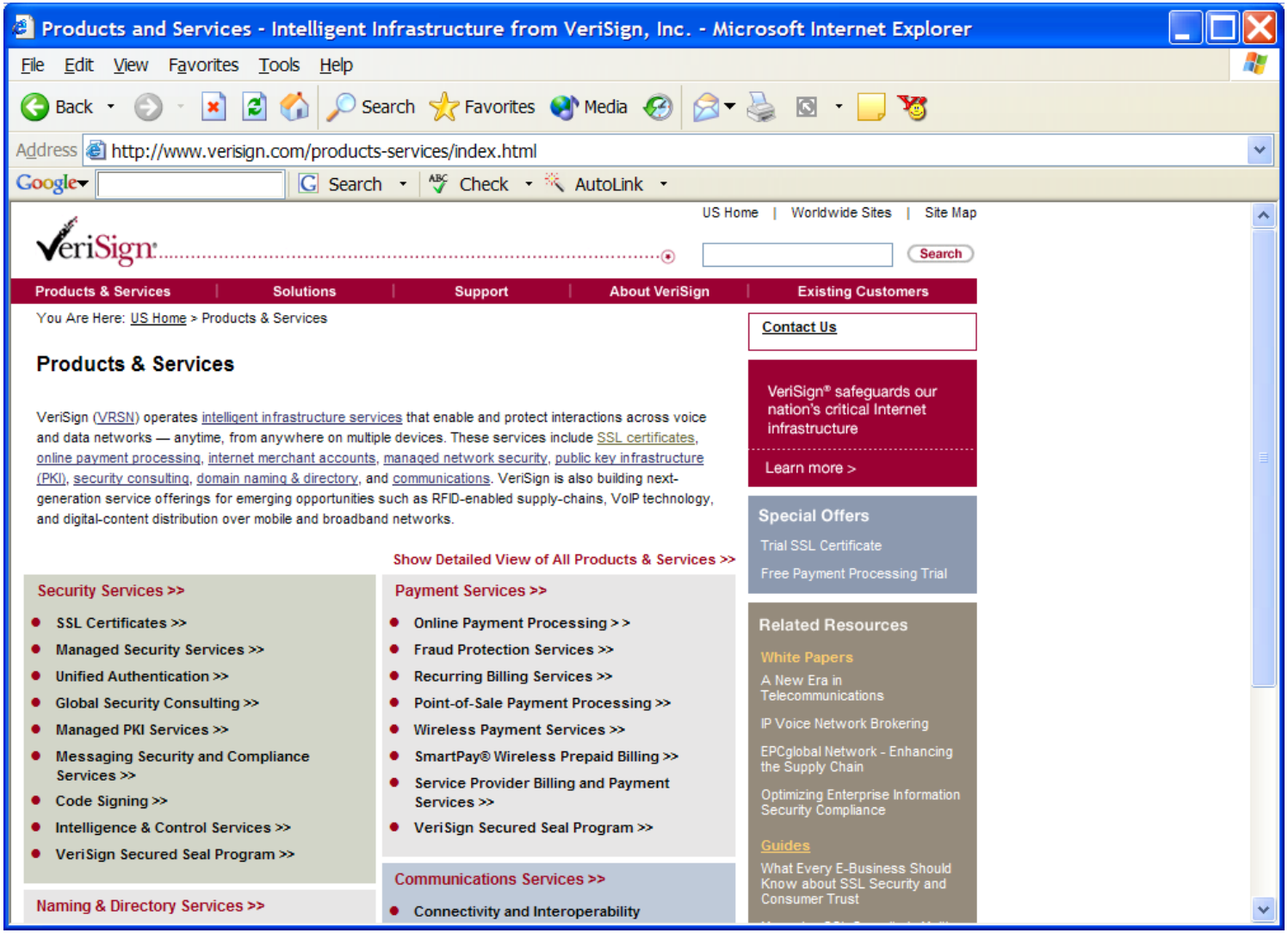

BCA INTERNET BANKING - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.klikbca.com/
Google Search Web
Privacy Policy • Contact Us • Site Map • English Version
FeatureProduct
INDIVIDUAL BISNIS COMPANY INFO
InternetBanking
Simulasi Kredit Konsumen Mudah dan Ringan
Simulasi Cicilan BCA Card
Info Reward Anda
Kini, Anda dapat melakukan transfer antar rekening BCA di KlikBCA s/d Rp.100 juta / hari / User ID
LEARNING CENTER BCA NEWS PRESS RELEASE
Saksikan Grand Launching BCA Side Card di Gebyar BCA
BCA dan MasterCard Memperkenalkan Kartu Kredit MasterCard SideCard™ Pertama di Indonesia
Individual
Pembelian
Pembayaran
Transfer Dana
Informasi Rekening
LOGIN
DEMO
Bisnis
LOGIN
TAHAPAN BCA
Khusus untuk Surabaya
bisa diubah menjadi
Kurs TT BCA:
Jum'at , 03/12/2004 - 15:57:48
KURS JUAL BELI
USD 9,095.00 9,025.00
SGD 5,544.35 5,485.35
HKD 1,170.85 1,159.95
Copyright ©2004

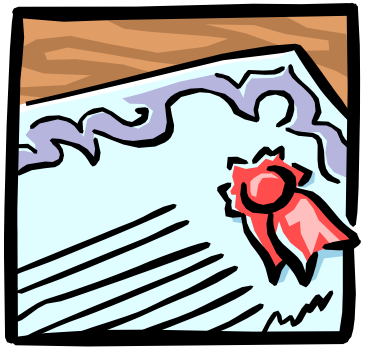
Sertifikat Digital



- Karena kunci publik tersedia secara publik, maka kunci publik perlu disertifikasi dengan memberikan **sertifikat digital**.
- Sertifikat digital adalah dokumen digital yang mengikat kunci publik dengan informasi pemiliknya.
- Sertifikat digital dikeluarkan (*issued*) oleh pemegang otoritas sertifikasi yang disebut *Certification Authority* atau *CA*.
- Di dalam sertifikat digital terdapat tanda tangan CA.
- Sertifikat digital mempunyai fungsi yang sama seperti SIM atau paspor.

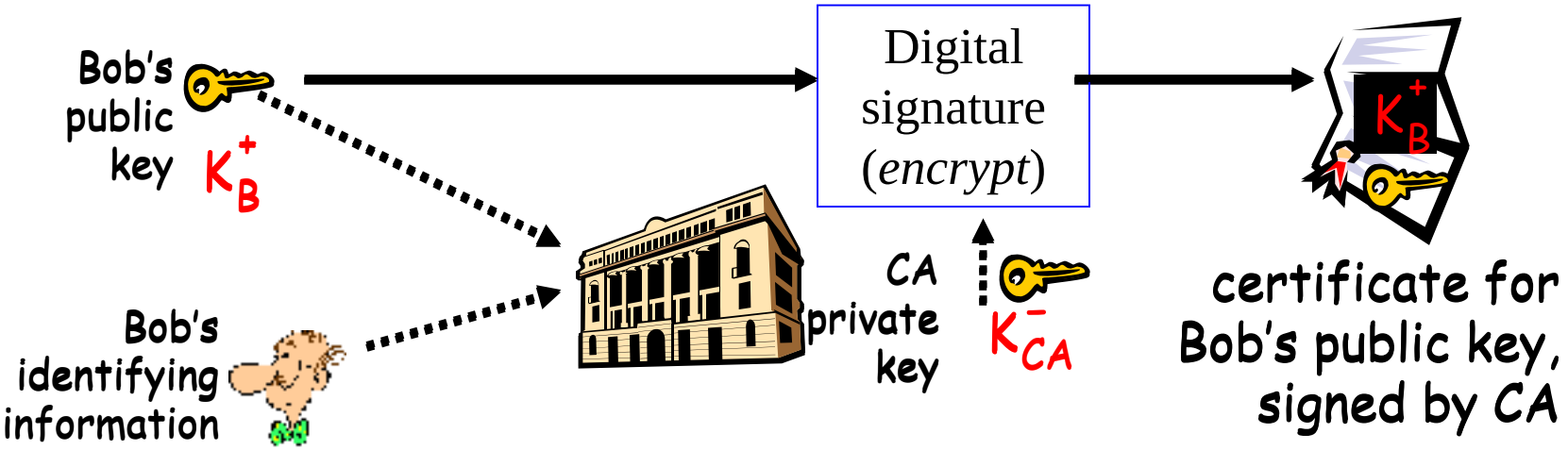
- *CA* biasanya adalah bank atau institusi institusi yang terpercaya.
- Contoh CA terkenal: *Verisign* (www.verisign.com)


Products and Services - Intelligent Infrastructure from VeriSign, Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.verisign.com/products-services/index.html
Google Search Check AutoLink
US Home | Worldwide Sites | Site Map
VeriSign
Search
Products & Services | Solutions | Support | About VeriSign | Existing Customers
You Are Here: US Home > Products & Services
Products & Services
VeriSign (VRSN) operates intelligent infrastructure services that enable and protect interactions across voice and data networks — anytime, from anywhere on multiple devices. These services include SSL certificates, online payment processing, internet merchant accounts, managed network security, public key infrastructure (PKI), security consulting, domain naming & directory, and communications. VeriSign is also building next-generation service offerings for emerging opportunities such as RFID-enabled supply-chains, VoIP technology, and digital-content distribution over mobile and broadband networks.
Show Detailed View of All Products & Services >>
Security Services >>
SSL Certificates >>
Managed Security Services >>
Unified Authentication >>
Global Security Consulting >>
Managed PKI Services >>
Messaging Security and Compliance Services >>
Code Signing >>
Intelligence & Control Services >>
VeriSign Secured Seal Program >>
Payment Services >>
Online Payment Processing > >
Fraud Protection Services >>
Recurring Billing Services >>
Point-of-Sale Payment Processing >>
Wireless Payment Services >>
SmartPay® Wireless Prepaid Billing >>
Service Provider Billing and Payment Services >>
VeriSign Secured Seal Program >>
Communications Services >>
Connectivity and Interoperability
Naming & Directory Services >>
Contact Us
VeriSign® safeguards our nation's critical Internet infrastructure
Learn more >
Special Offers
Trial SSL Certificate
Free Payment Processing Trial
Related Resources
White Papers
A New Era in Telecommunications
IP Voice Network Brokering
EPCglobal Network - Enhancing the Supply Chain
Optimizing Enterprise Information Security Compliance
Guides
What Every E-Business Should Know about SSL Security and Consumer Trust



- Di dalam sertifikat digital terdapat informasi sebagai berikut:
  - Nama pemegang sertifikat (*holder*)
  - Kunci publik pemegang sertifikat
  - Tanda tangan CA
  - Waktu kadaluarsa sertifikat (*expired time*)
  - informasi relevan lain seperti nomor seri sertifikat, e-mail pemegang sertifikat, dll

Proses Mendapatkan Sertifikat Digital



Sumber gambar: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

- Contoh: Bob meminta sertifikat digital kepada *CA* untuk kunci publiknya :

  `198336A8B03030CF83737E3837837FC387092827FFA15C76B01`

- CA membuat sertifikat digital untuk Bob lalu menandatanganinya dengan kunci privat *CA*.

- Caranya:
  1. *CA* membangkitkan nilai *hash* dari kunci publik dan semua informasi pemohon sertifikat. Fungsi *hash* yang digunakan contohnya: *MD5* atau *SHA.*

  2. Kemudian, *CA* mengenkripsi nilai *hash* tersebut dengan menggunakan kunci privat *CA*. Hasilnya adalah tanda tangan CA.

I hereby certifiy that the public key
198336A8B03030CF83737E3837837FC387092827FFA15C76B01
belongs to
Bob Anderson
12345 University Avenue
Barkeley, CA94702
E-mail: bob@barkeley.com
Expiration Date: 13-Jul-2018

Tanda tangan digital: Nilai *hash* (SHA) dari sertifikat digital yang dienkripsi dengan menggunakan kunci privat CA

Contoh ilustrasi sebuah sertifikat digital

- Jadi, sertifikat digital mengikat kunci publik dengan identitas pemilik kunci publik.

- Sertifikat ini dapat dianggap sebagai ‘surat pengantar’ dari *CA*.

- Supaya sertifikat digital itu dapat diverifikasi (dicek kebenarannya), maka kunci publik *CA* harus diketahui secara luas.

- Pihak yang mengetahui kunci publik *CA* dapat memverifikasi tanda tangan digital di dalam sertifikat.

- Sertifikat digital tidak rahasia, tersedia secara publik, dan disimpan oleh *CA* di dalam *certificate repositories*.

Proses Penggunaan Sertifikat Digital

- Misalkan pemilik kunci publik menandatangani pesan dengan kunci privatnya dan mengirim pesan + tanda tangan digital kepada pihak kedua.

- Penerima pesan memverifikasi tanda tangan digital dengan kunci publik pengirim pesan, dan meminta verifikasi sertifikat digital pengirim pesan melalui repositori CA yang tersedia secara publik.

- Repositori CA melaporkan status sertifikat si pengirim pesan.

Proses Verifikasi Sertifikat Digital

- Do I trust the CA? (Is it in my list of trust root certification authorities?)
- Is the certificate genuine?
  - Look up the CA's public key; use it to decrypt the signature
  - Compute the certificate's hash; compare with decrypted signature
- Is the holder genuine? This requires a challenge
- If the holder is genuine, he must know the private key corresponding to the pubic key in the certificate
- Having the certificate is not enough. (They are exchanged over the Internet all the time)
- Send him a *nonce* (random 128-bit number)

Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

Challenge by Nonce

- For example: If you're really Shamos, you must know his private key
- So please encrypt this nonce:
  "A87B1003 9F60EA46 71A837BC 1E07B371"

- When the answer comes back, decrypt it using the public key in the certificate
- If the result matches, the remote user knew the correct private key
- Never use the same nonce twice

Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

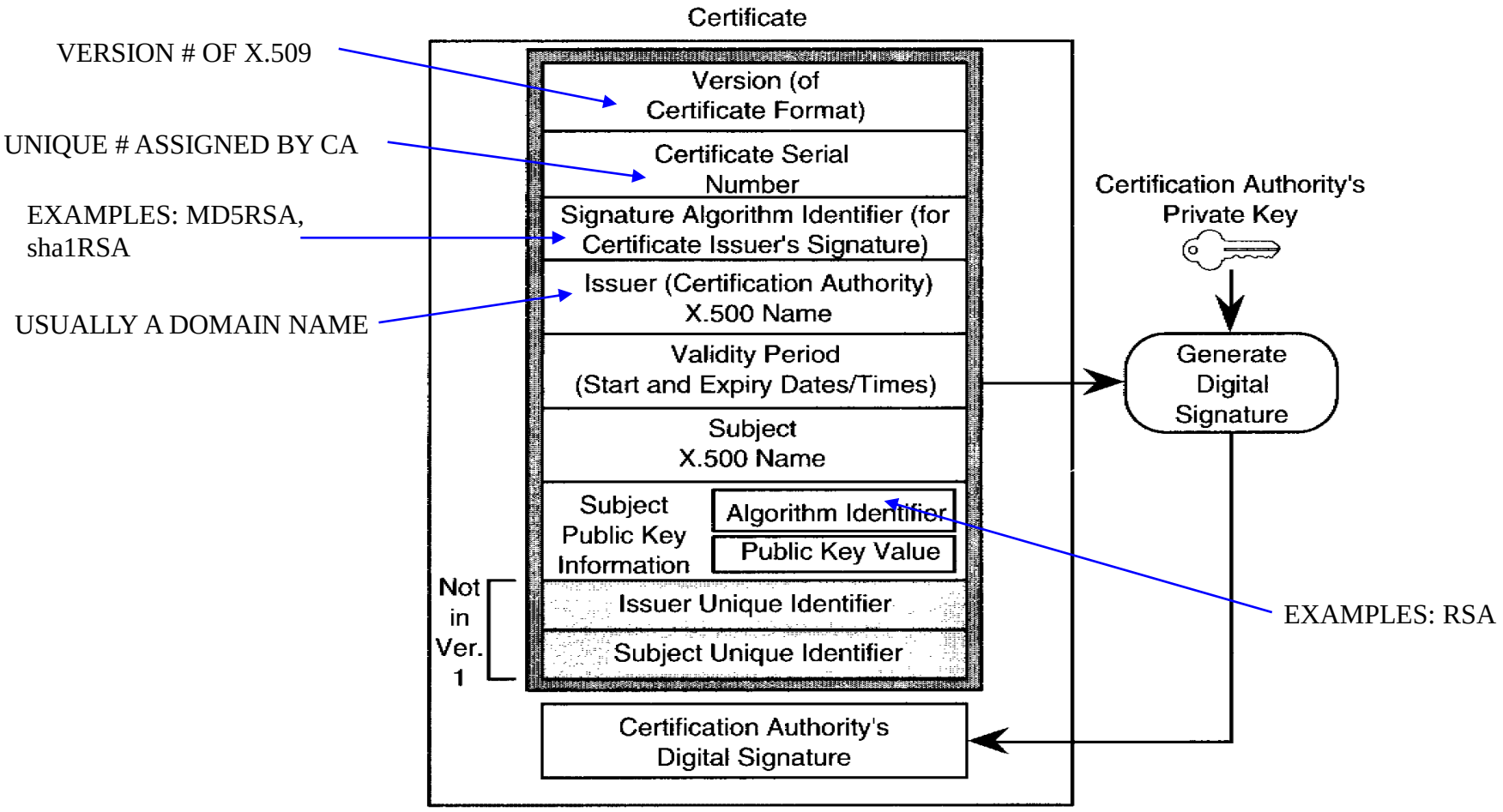
X.509

- Ada banyak format sertifikat digital yang bisa dibuat.
- Agar semua sertifikat digitak seragam, maka ITU mengeluarkan standard untuk sertifikat digital.
- Standard tersebut dinamakan X.509 dan digunakan secara luas di internet.
- Ada tiga versi standard X.509, yaitu V1, V2, dan V3.

Field-field utama di dalam sertifikat standard X.509:

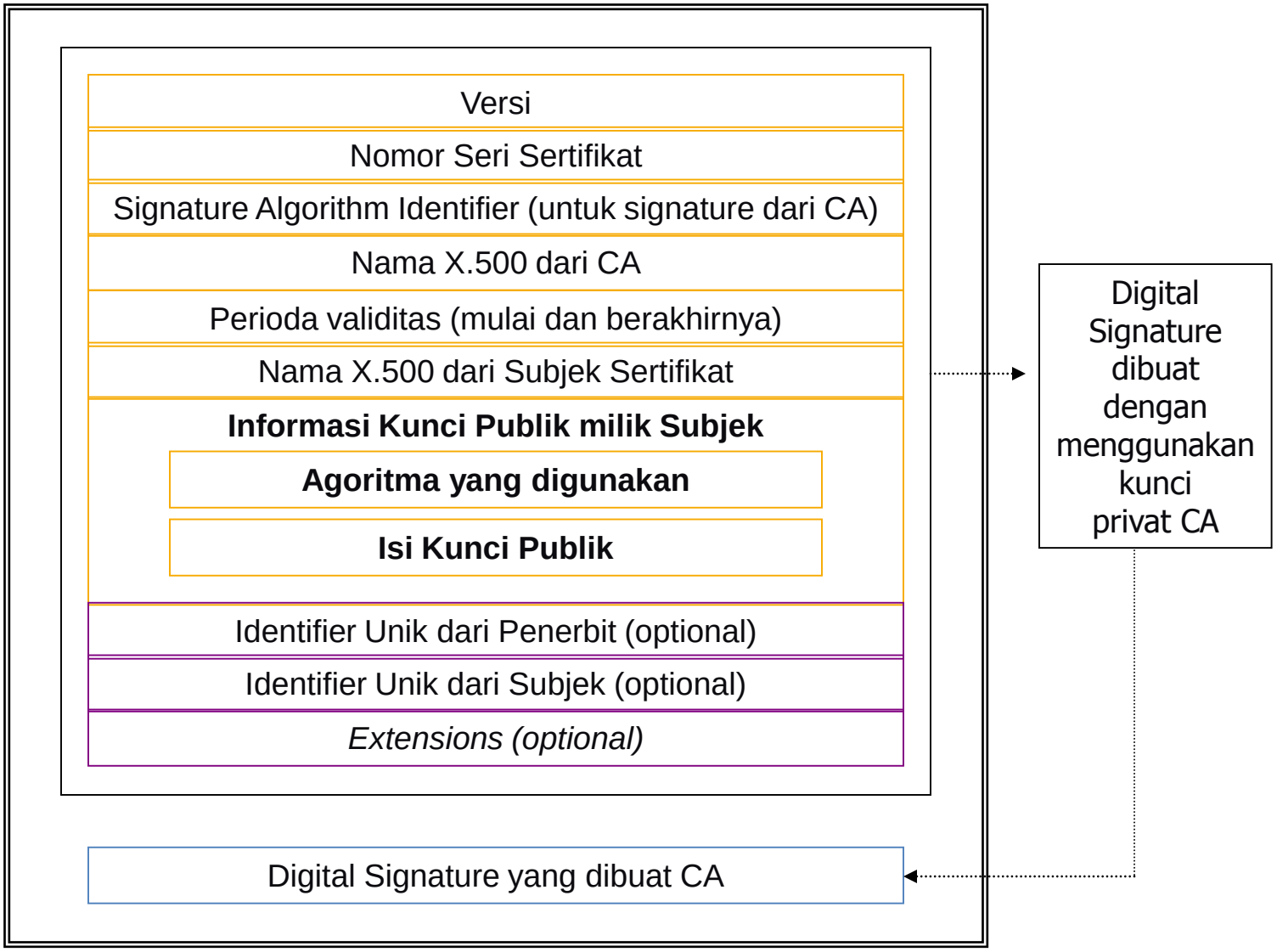
Field	Arti
Version	Versi X.509
Serial Number	Nomor ini plus nama *CA* secara unik digunakan untuk mengidentifikasi sertifikat
Signature Algorithm	Algoritma yang digunakan untuk menandatangani sertifikat.
Issuer	Nama pemberian X.509 untuk *CA*
Validity period	Waktu awal dan akhir periode valid
Subject name	Entitas (individu atau organisasi) yang disertifikasi
Public Key	Kunci publik subjek dan *ID* dari algoritma yang menggunakannya.
Issuer ID	*ID* opsional yang secara unik mengidentifikasi *certificate's issuer*.
Subject ID	*ID* opsional yang secara unik mengidentifikasi *certificate's subject*
Extensions	Bayak ekstensi yang telah didefinisikan.
Signature	Tanda-tangan sertifikat (ditandatangani dengan kunci privat CA).

Sertifikat Digital X.509 Versi 2



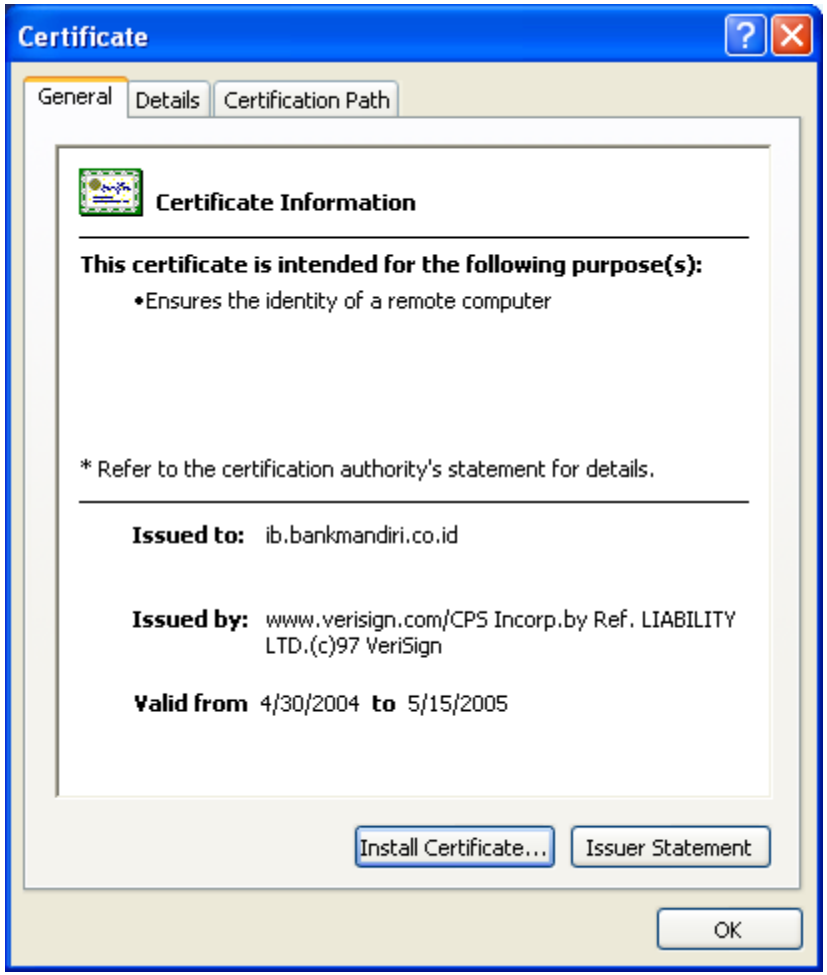
Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

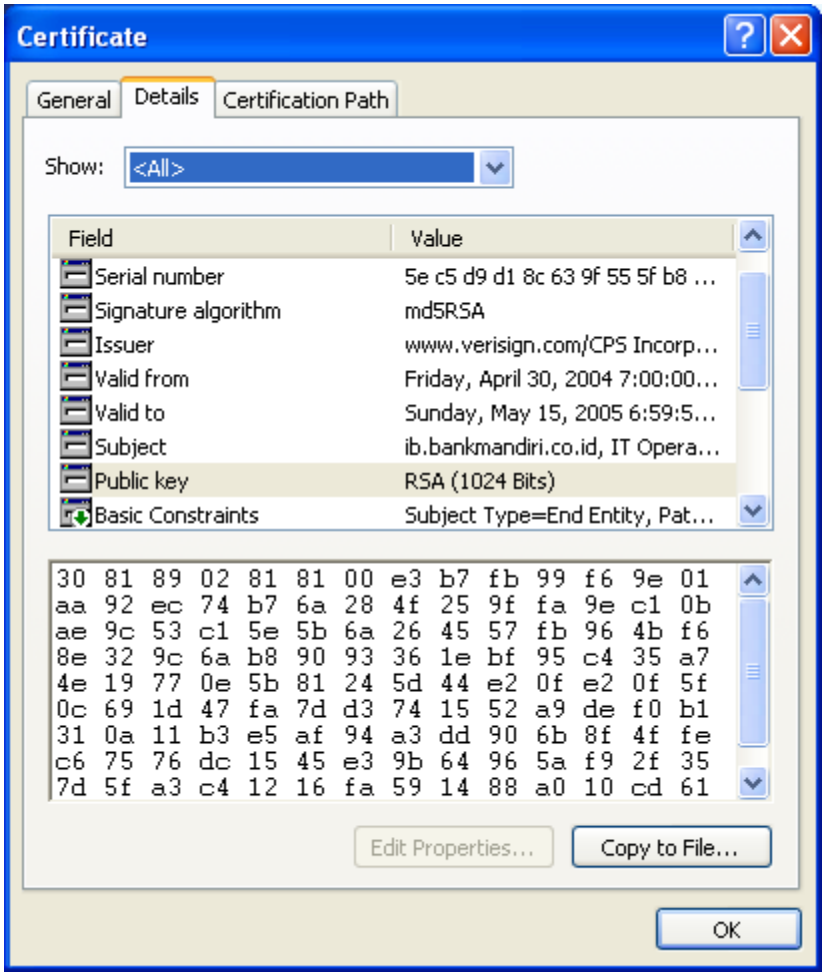
Sertifikat Digital X.509 versi 3 (*)



*) Sumber: http://budi.paume.itb.ac.id

Contoh sertifikat digital:

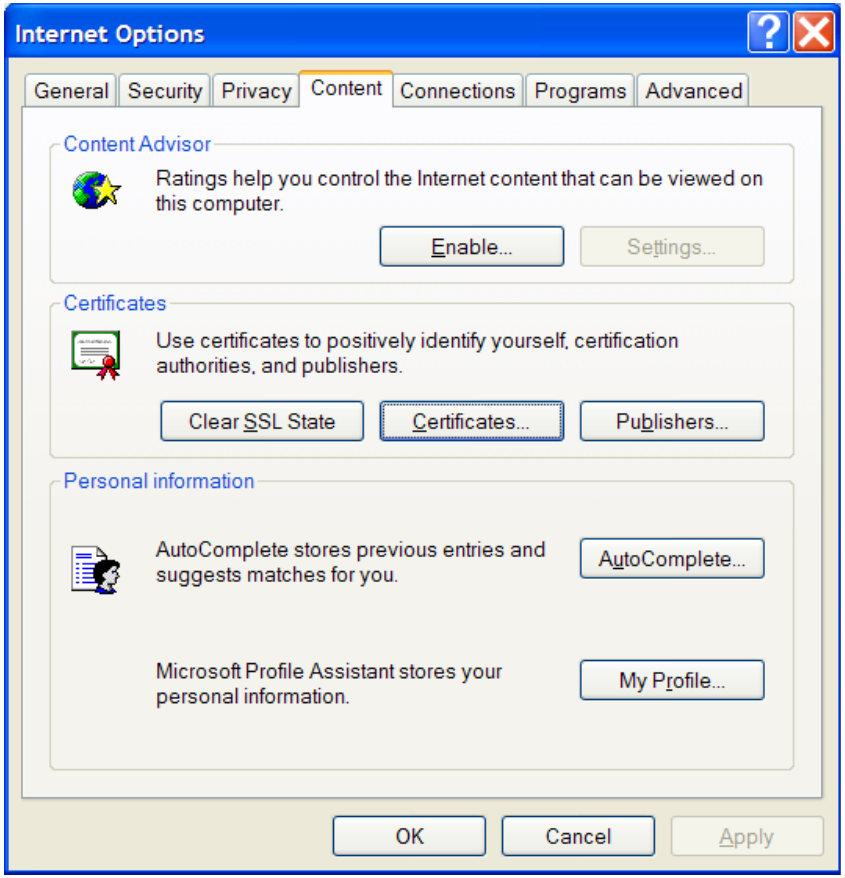




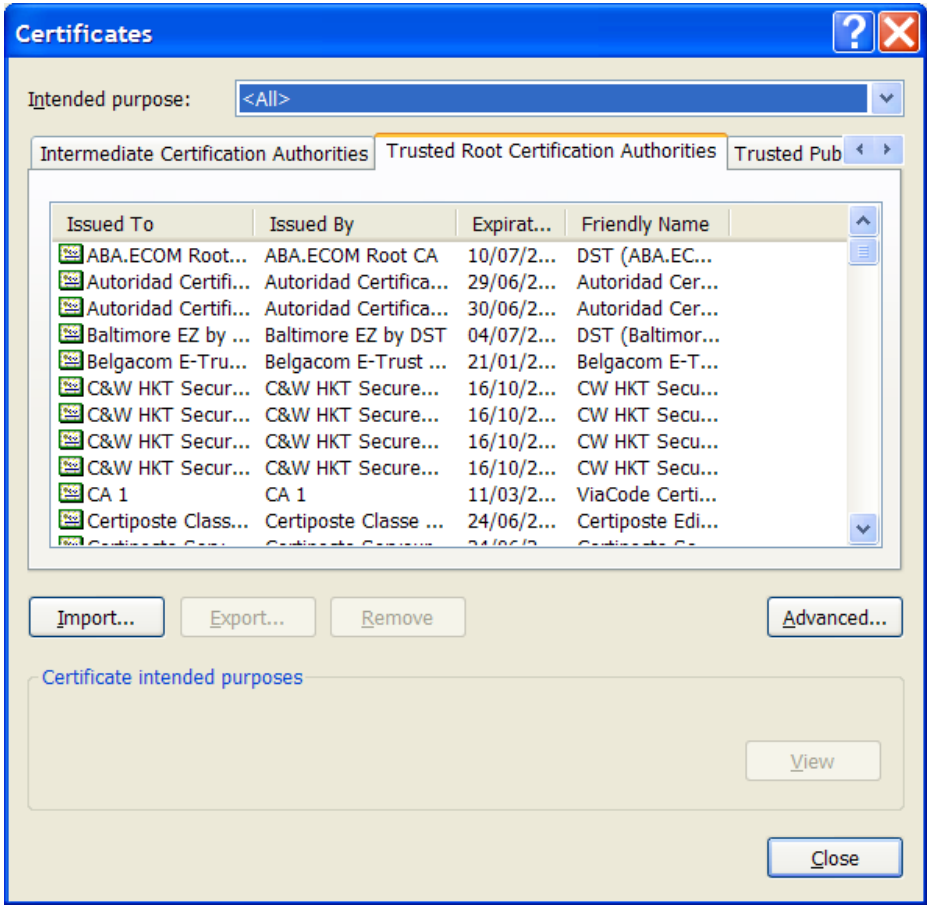
*) Sumber: http://budi.paume.itb.ac.id

- Untuk melihat *CA* dan sertifikat digitalnya yang yang telah dipasang di dalam *Internet Explorer* (*IE*), pilih:

  Tools → *Internet Options* → *Contents*



- Kemudian, klik tab:
- *Certificates → Trusted Root Certification Authorities*



- Adanya atribut waktu kadualarsa pada sertifikat digital dimaksudkan agar pengguna mengubah kunci publik (dan kunci privat pasangannya) secara periodik.

- Makin lama penggunaan kunci, makin besar peluang kunci diserang dan dikriptanalisis. Jika pasangan kunci tersebut diubah, maka sertifikat digital yang lama harus ditarik kembali (*revoked*).

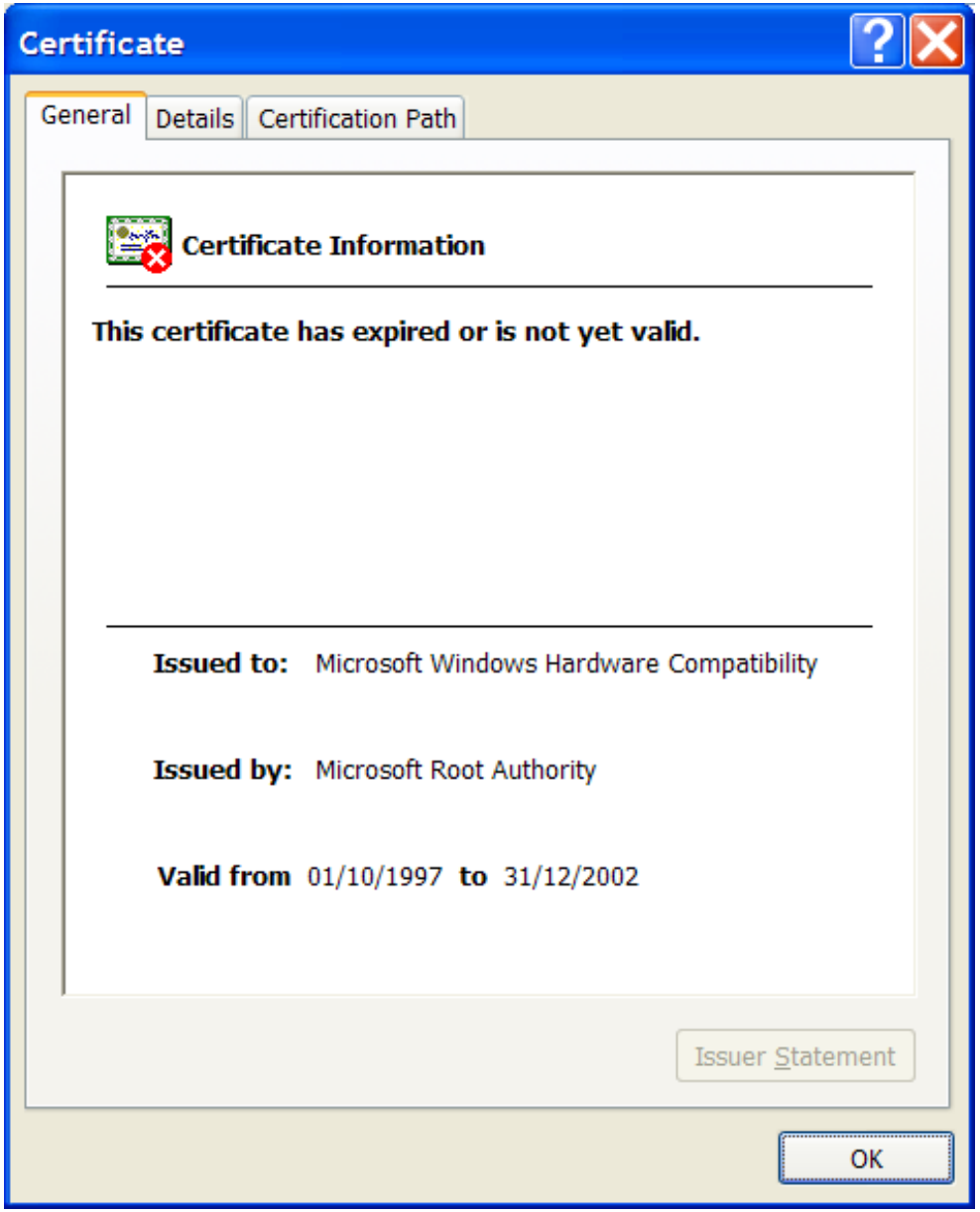
- Pada sisi lain, jika kunci privat berhasil diketahui pihak lain sebelum waktu kadualarsanya, sertifikat digital harus dibatalkan dan ditarik kembali, dan pengguna harus mengganti pasangan kuncinya.

- Bagaimana *CA* memberitahu ke publik bahwa sertifikat digital ditarik?

- Caranya: *CA* secara periodik mengeluarkan *CRL* (*Certificate Revocation List*) yang berisi nomor seri sertifikat digital yang ditarik.

- Sertifikat digital yang sudah kadaluarsa otomatis dianggap sudah tidak sah lagi dan ia juga dimasukkan ke dalam *CRL*.

- Dengan cara ini, maka *CA* tidak perlu memberitahu perubahan sertifikat digital kepada setiap orang.


Certificate
General
Details
Certification Path
Certificate Information
This certificate has expired or is not yet valid.
Issued to: Microsoft Windows Hardware Compatibility
Issued by: Microsoft Root Authority
Valid from 01/10/1997 to 31/12/2002
Issuer Statement
OK

Types of Digital Certificates

- There are four main types of digital certificates :-
  - Server Certificates
  - Personal Certificates
  - Organization Certificates
  - Developer Certificates

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Server Certificates

- Allows visitors to exchange personal information such as credit card numbers, free from the threat of interception or tampering.
- Server Certificates are a must for building and designing e-commerce sites as confidential information is shared between clients, customers and vendors.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Personal Certificates

- Personal Certificates allow one to authenticate a visitor's identity and restrict access to specified content to particular visitors.
- Personal Certificates are perfect for business to business communications such as offering suppliers and partners controlled access to special web sites for updating product availability, shipping dates and inventory management.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Organization & Developer Certificates

- Organization Certificates are used by corporate entities to identify employees for secure e-mail and web-based transaction.

- Developer Certificates prove authorship and retain integrity of distributed software programs e.g. installing a software on a computer system in most instances requires what is called a “serial key”

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Why are they Used?

There are four(4) main uses:

1. Proving the Identity of the sender of a transaction

2. Non Repudiation – the owner of the certificate cannot deny partaking in the transaction

3. Encryption and checking the integrity of data - provide the receiver with the means to encode a reply.

4. Single Sign-On - It can be used to validate a user and log them into various computer systems without having to use a different password for each system

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

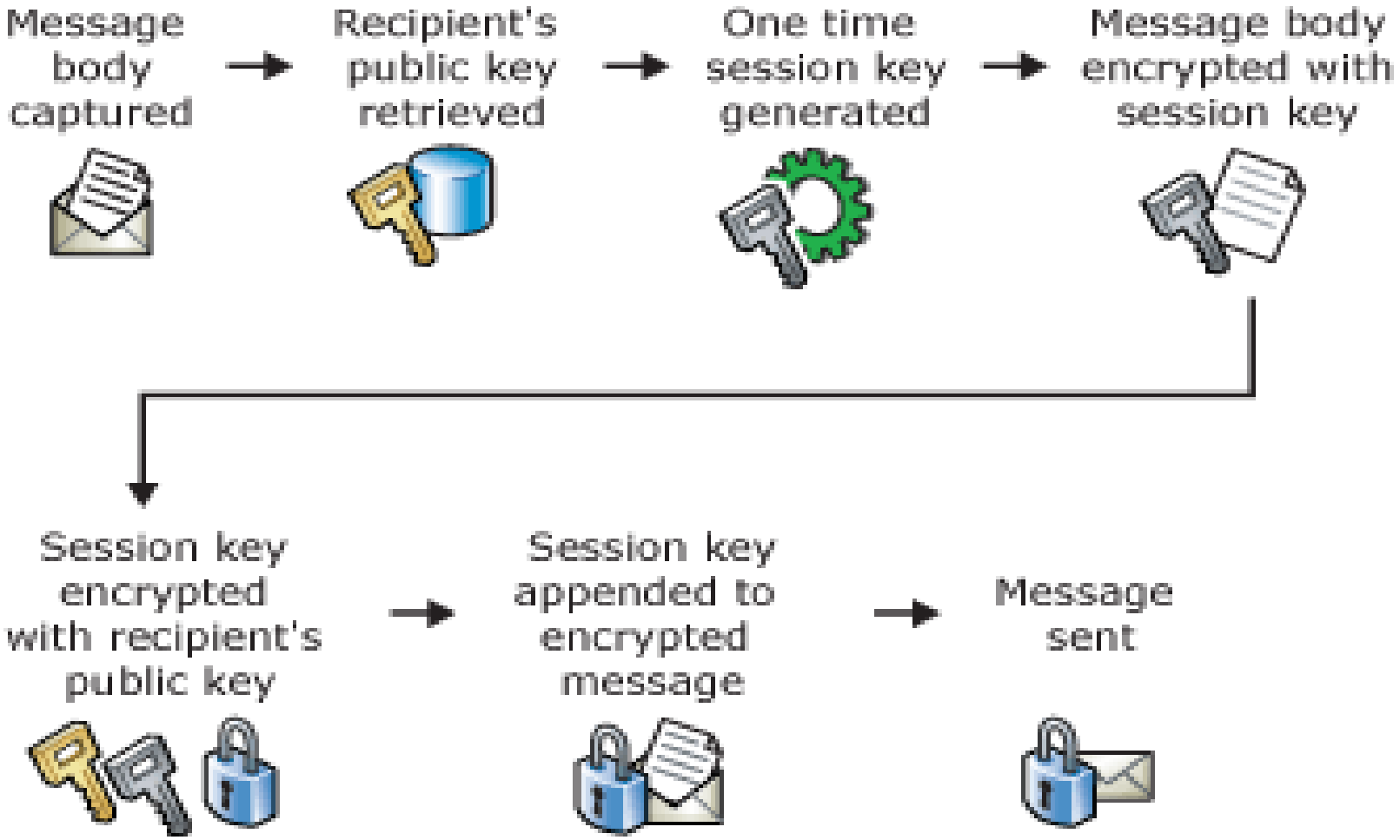
Where are Digital Certificates Used?

- **In a number of Internet applications that include:**

1. Secure Socket Layer (SSL) developed by Netscape Communications Corporation
2. Secure Multipurpose Internet Mail Extensions (S/MIME) Standard for securing email and electronic data interchange (EDI).
3. Secure Electronic Transactions (SET) protocol for securing electronic payments
4. Internet Protocol Secure Standard (IPSec) for authenticating networking devices

Sumber: **GROUP 11 MEMBERS** (Rackenee Rhule et al, *Digital Certificates*)

How Digital Certificates are Used for Message Encryption



Sumber: **GROUP 11 MEMBERS** (Rackenee Rhule et al, *Digital Certificates*)

Why do I need a Digital Certificate?

- Virtual malls, electronic banking and other electronic services are a commonplace offering service from the luxury of one's home. One's concern about privacy and security may prevent you from taking advantage of the luxury; this is where digital certificate comes in.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Why do I need a Digital Certificate?

- Encryption alone is not enough as it provides no proof of the identity of the sender of the encrypted information. Used in conjunction with Encryption, Digital Certificates provides a more complete security solution, assuring the identity of all the parties involved in a transaction.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Advantages of Digital Certificates

- Decrease the number of passwords a user has to remember to gain access to different network domains.

- They create an electronic audit trail that allows companies to track down who executed a transaction or accessed an area.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Do Digital Certificates Have Vulnerabilities?

- One problem with a digital certificate is where it resides once it is obtained.
- The owner's certificate sits on his computer, and it is the sole responsibility of the owner to protect it.
- If the owner walks away from his computer, others can gain access to it and use his digital certificate to execute unauthorized business.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Do Digital Certificates Have Vulnerabilities?

- The best way to address the vulnerabilities of digital certificates is by combining them with biometric technology, as that confirms the actual identity of the sender, rather than the computer.

Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

Public Key Infrastructure (*PKI*)

- Luasnya penggunaan kriptografi kunci-publik di dalam Internet membutuhkan sebuah infrastruktur yang menyediakan layanan terintegrasi untuk membuat, menyimpan, memverifikasi, dan membuang sertifikat digital.

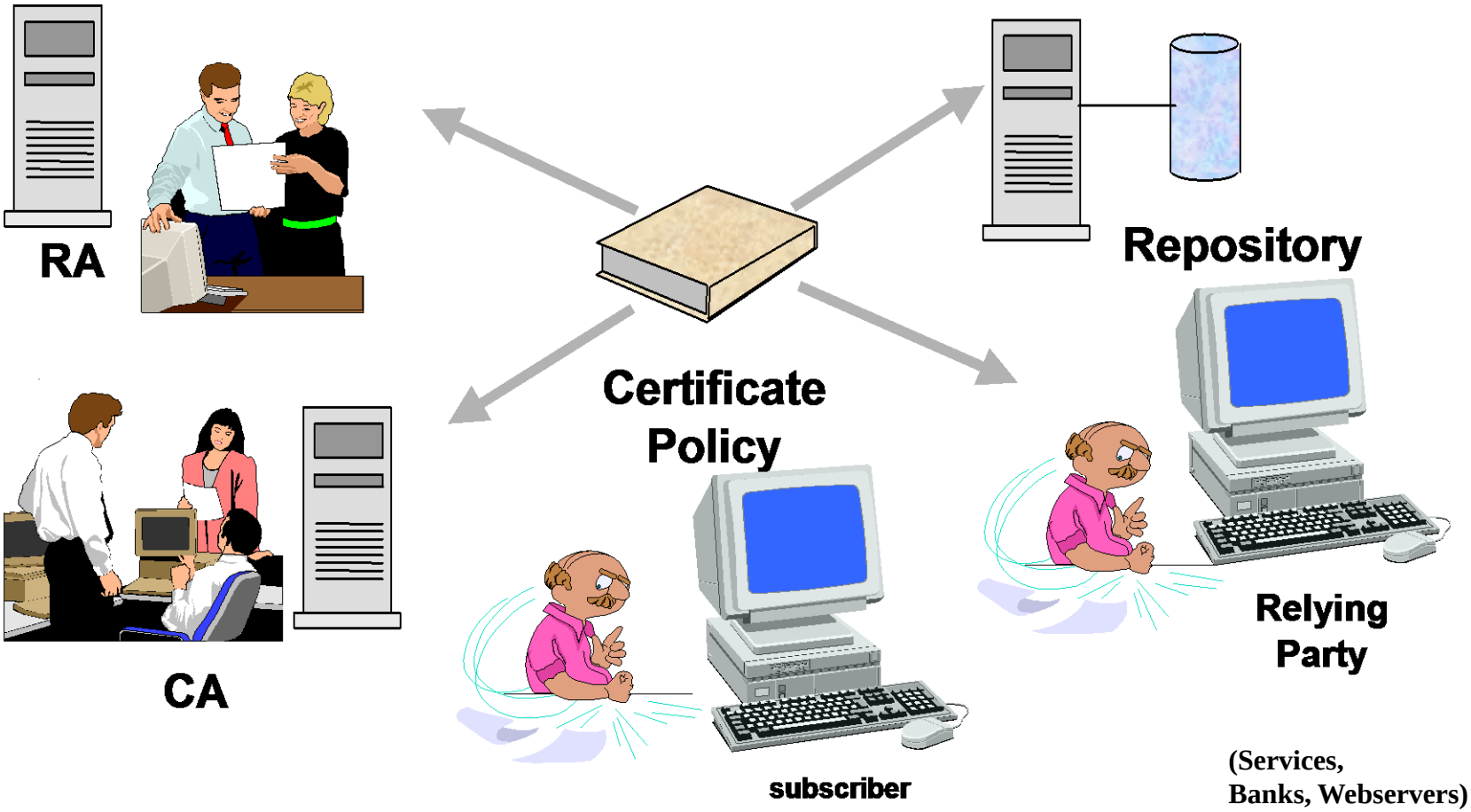
- Infrastruktur tersebut juga mengatur CA dan membuat kebijakan.

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

- PKI adalah sekumpulan *hardware*, *software*, orang, kebijakan, dan prosedur yang dibutuhkan untuk membuat, mengelola, mendistribusikan, menyimpan, dan membuang sertifkat digital.

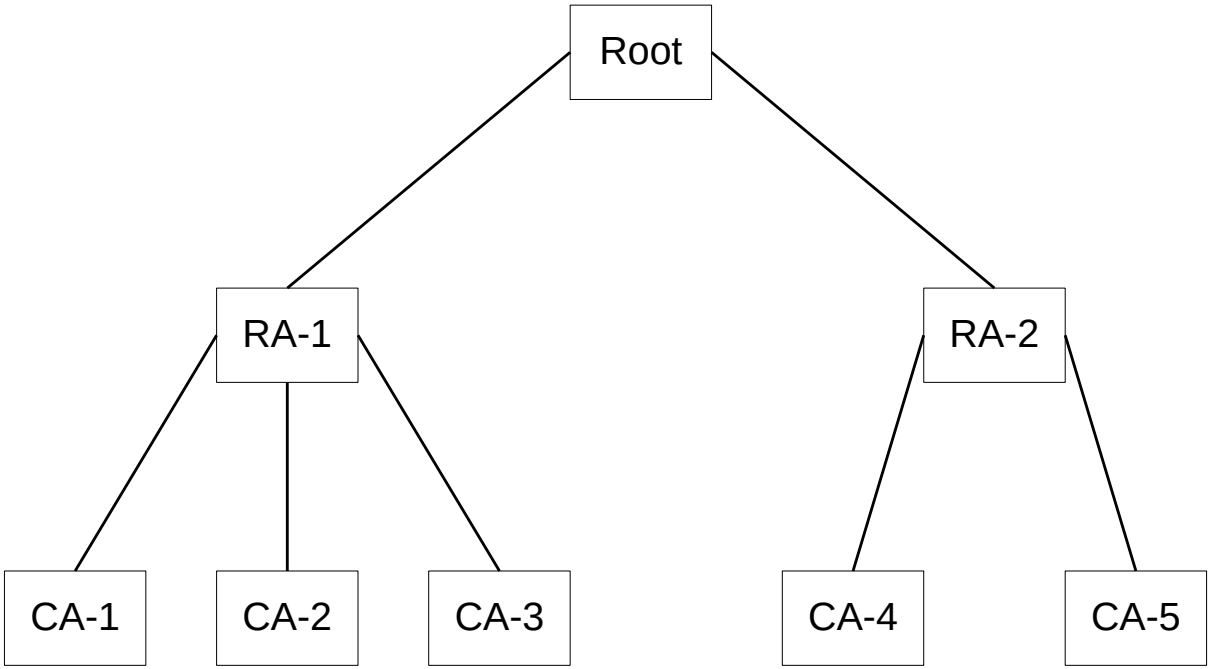
- *PKI* terdiri atas komponen-komponen:
  - CA yang menerbitkan dan memverifikasi sertifikat digital
  - RA (Registration Authority) yang memverifikasi identitas pengguna yang meminta informasi dari CA
  - Repositori (menyimpan sertifikat digital dan *CRL*)
  - Aturan/kebijakan (*policy*)

Enterprise PKI



Sumber gambar: Ravi Mukkamala, Department of Computer Science
Old Dominion University Norfolk, Virginia, USA , *Public Key Infrastructure: A Tutorial*

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



Hirarkhi *CA* di dalam *PKI*

- Aras ke-nol adalah *root*. *Root* merupakan *root certificate authority*, yang mana adalah *Internet Policy Registration Authority* (*IPRA*).

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

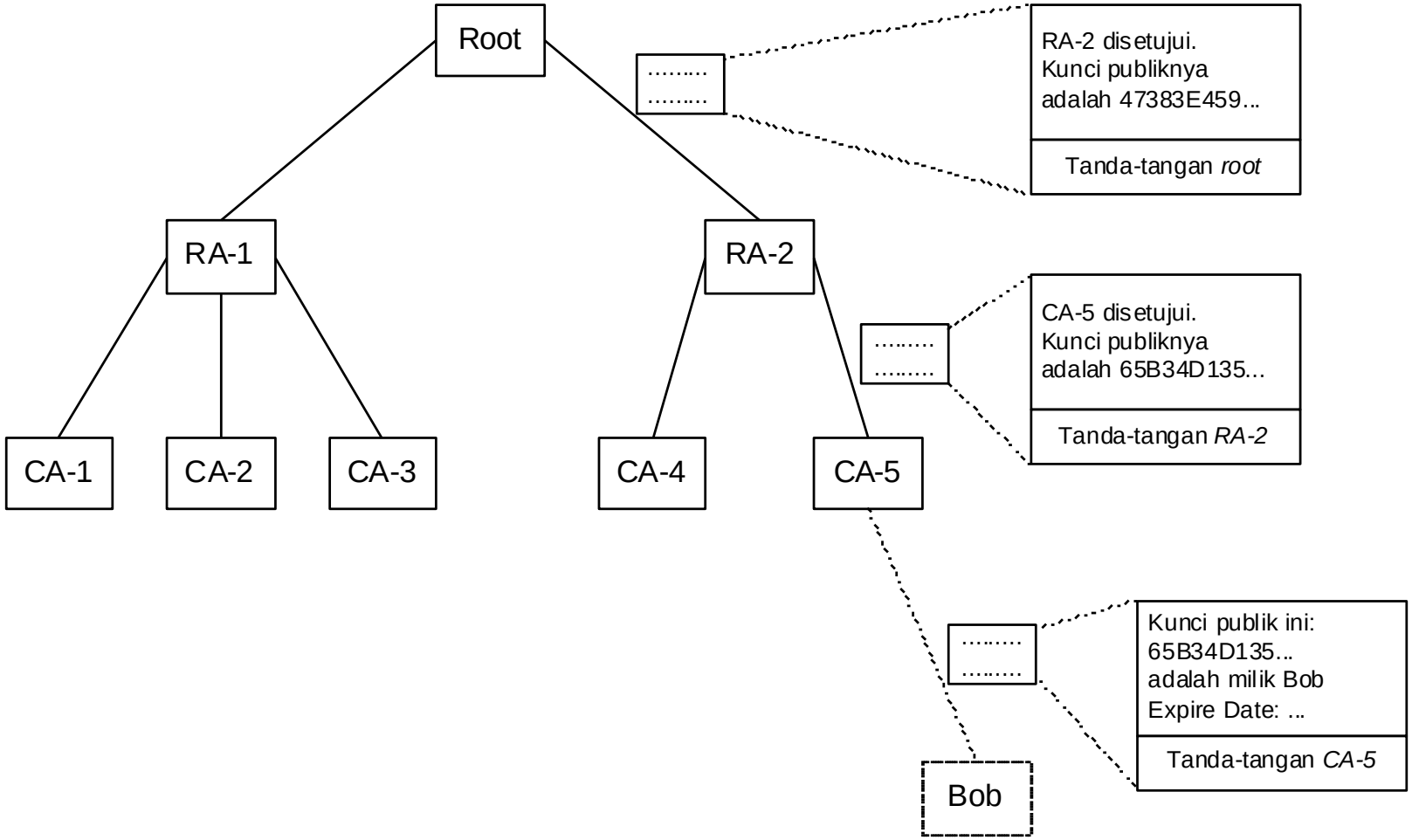
- *CA* aras satu disebut *RA* (*Regional Authorities*), yang bertindak sebagai *policy creation authority*, yaitu oganisasi yang membuat kebijakan untuk memperoleh sertifikat digital.

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

- *RA* menandatangai sertifikat digital untuk *CA* di bawahnya dengan menggunakan kunci privat *RA*.

- *CA* menandatangani sertifikat digital untuk individu atau organisasi dengan mengguankan kunci privat *CA*.

- *CA* bertanggung jawab untuk otentikasi sertifikat digital, sehingga *CA* harus memeriksa informasi secara hati-hati sebelum mengeluarkan sertifikat digital. Gambar 23.5 memperlihatkan rantai sertifikat di dalam *PKI*.



Gambar 23.5 Contoh rantai sertifikat digital

- Verifikasi sertifikat digital dilakukan dari daun menuju akar (*root*).

- Rantai sertifikat yang menuju ke *root* disebut *chain of trust* atau *certification path*.

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 Directory Server product is said to support 50 million objects and process 5,000 queries a second; Secure E-Commerce, which allows a company or extranet manager to manage digital certificates; and Meta-Directory, which can connect all corporate directories into a single directory for security management

Sumber: Wikipedia

Wireless PKI

- *Wireless PKI* (*WPKI*) adalah protokol keamanan yang dispesifikasikan untuk transmisi nirkabel (*wireless*).

- Seperti *PKI*, *WPKI* mengotentikasi pengguna dengan sertifikat digital dan mengenkripsi pesan dengan kriptografi kunci-publik.

- *CA* WPKI melibatkan Certicom (www.certicom.com) dan RSA (www.rsasecurity.com).