Bahan Kuliah IF4020 Kriptografi

Sertifikat Digital

Oleh: Rinaldi Munir

Program Studi Teknik Informatika
STEI-ITB
2023

Pengantar

- 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 kunci privat dan publik: untuk otentikasi server, Client perlu mengotentikasi apakah server yang dituju merupakan server yang valid.

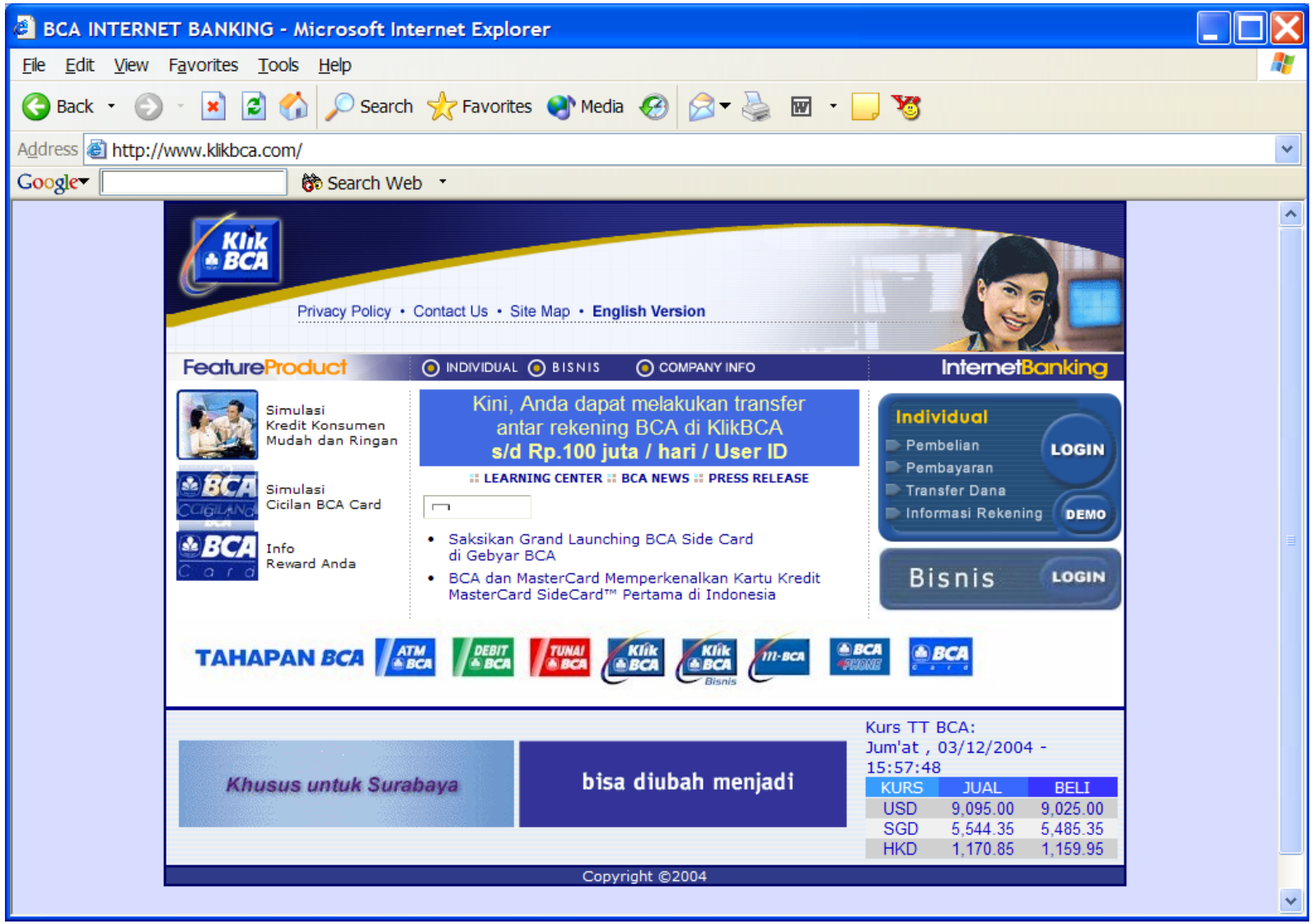
- Kunci privat bersifat rahasia, hanya diketahui oleh pemilik, tidak dibagi kepada pihak lain, tetapi kunci publik tersedia untuk umum.

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

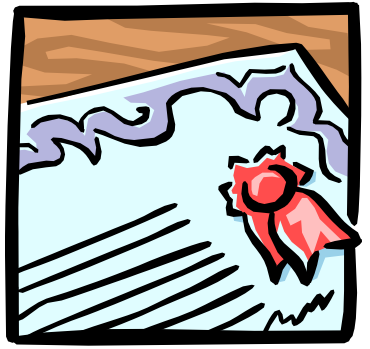
- Pihak lain dapat menyalahgunakan kunci publik yang bukan miliknya untuk *impersonation attack* .

- Kasus *impersonation attack atau phising* yang pernah terjadi di Indonesia tahun 2001: peniruan *website* BCA.

www.kilkbca.com
www.clikbca.com
www.klickbca.com
www.klikbac.com



Sertifikat Digital



- Karena kunci publik tersedia secara publik, maka kunci publik perlu disertifikasi dengan memberikan **sertifikat digital**.

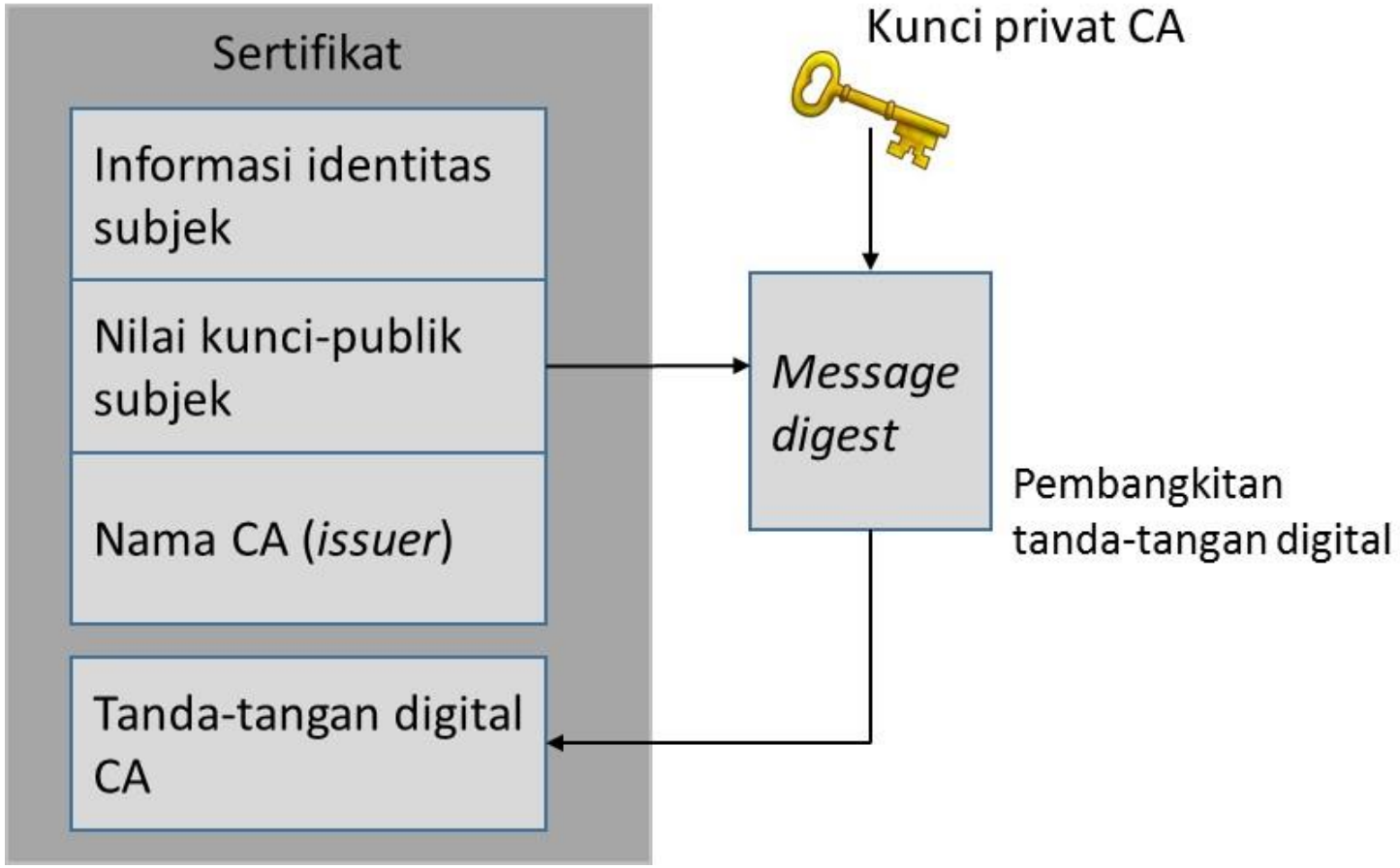
- Sertifikat digital adalah dokumen digital yang mengikat kunci publik dengan informasi pemiliknya.

- Sertifikat digital dikeluarkan (*issued*) oleh pemegang otoritas sertifikasi yang disebut *Certification Authority* atau *CA*. Sertifikat digital ditandatangani oleh CA.

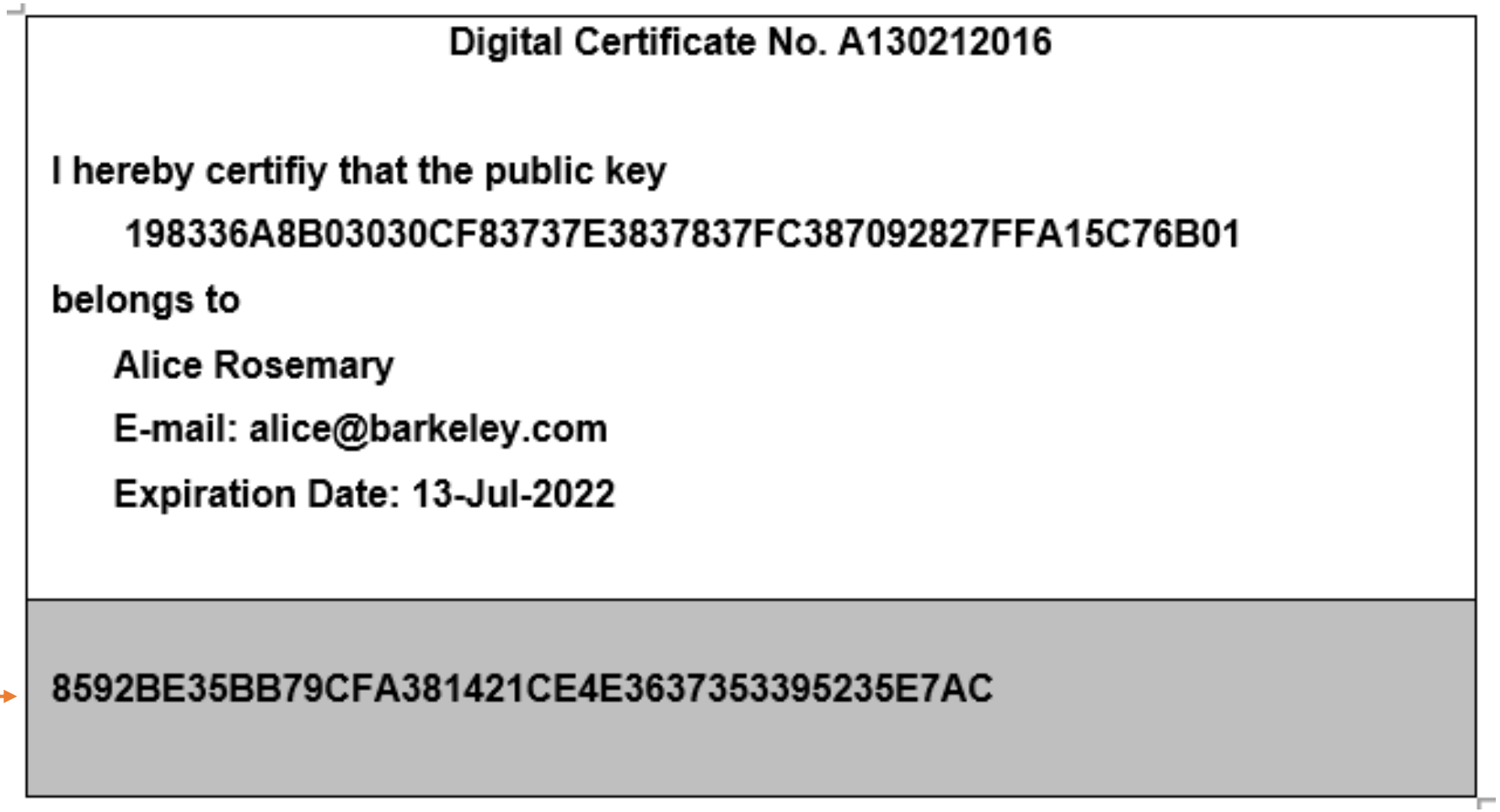
- Sertifikat digital mempunyai fungsi yang sama seperti SIM atau paspor.

- Informasi minimal di dalam sertifikat digital:
  1. identitas subjek (perusahaan/individu pemilik kunci publik)
  2. kunci publik si subjek
  3. nama *CA* (*issuer*)
  4. tanda tangan *CA* (*issuer*)

- Selain itu ditambahkan informasi lain seperti nomor seri sertifikat, waktu kadaluarsa, dan lain-lain

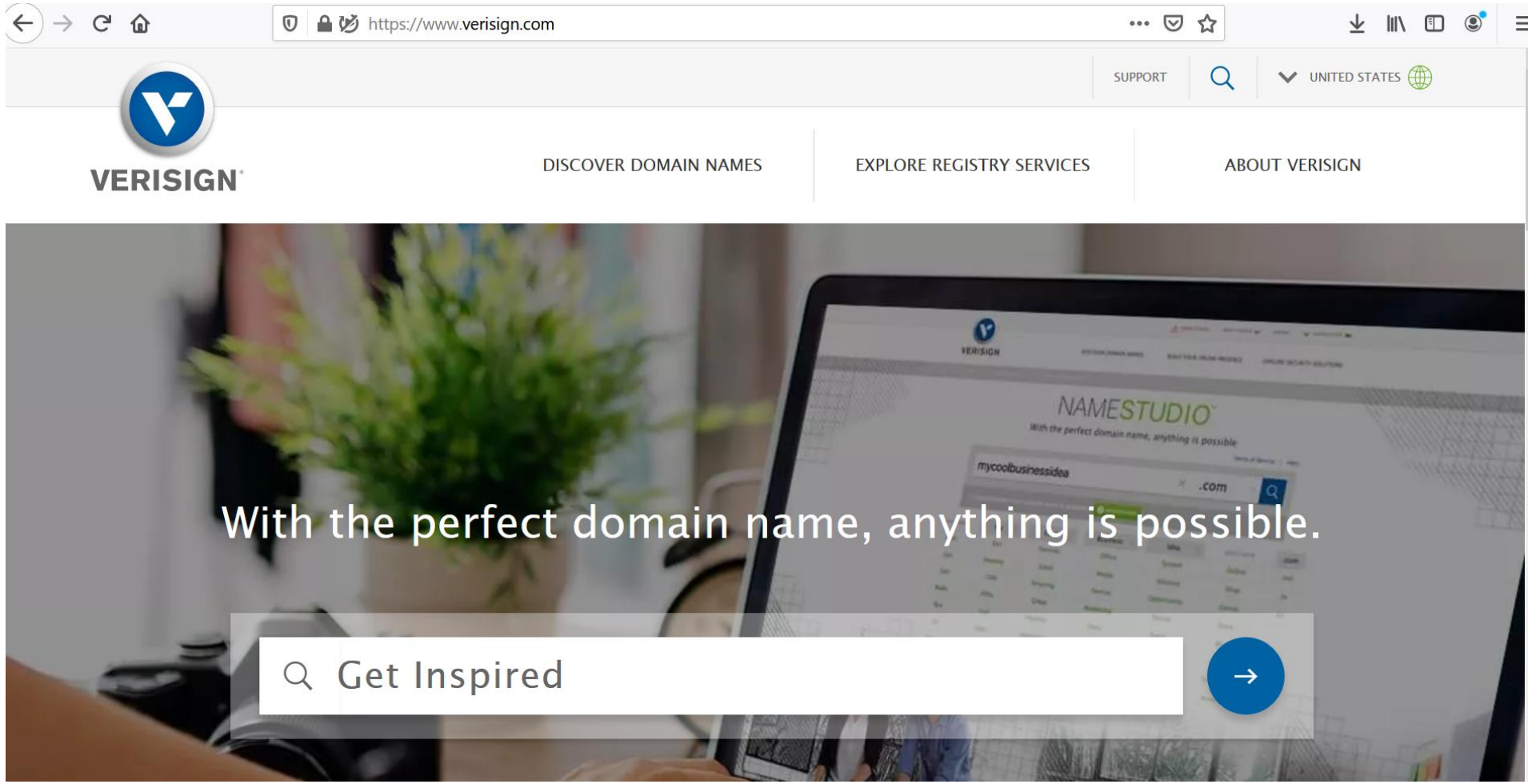


Contoh sebuah sertifikat digital:

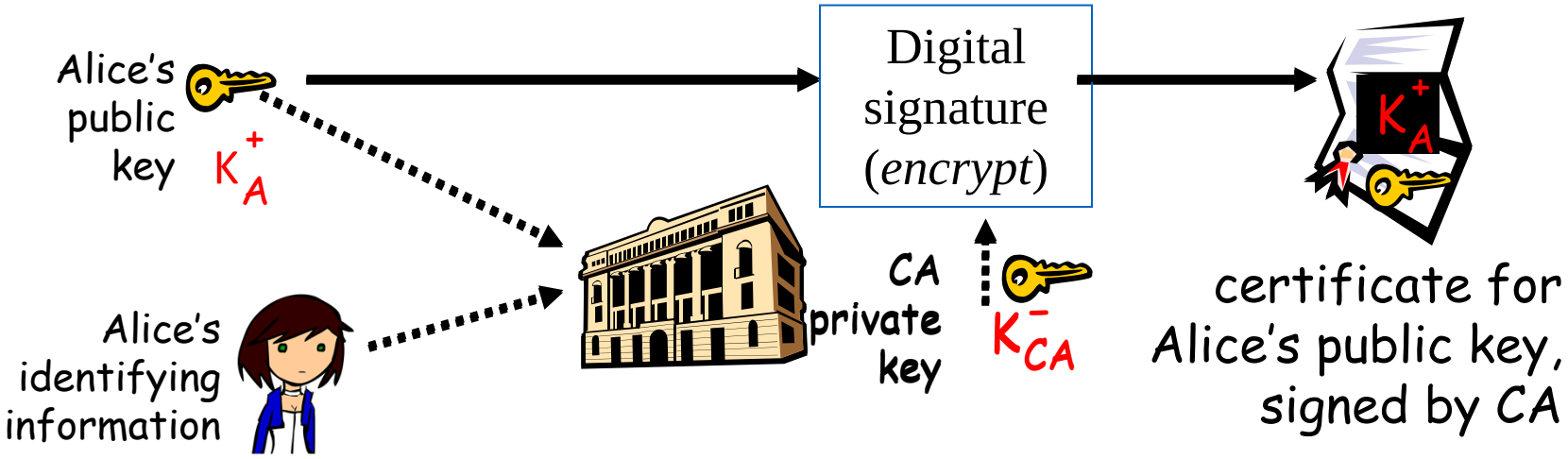


Tanda-tangan CA →

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



Proses Mendapatkan Sertifikat Digital



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

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

  198336A8B03030CF83737E3837837FC3870928 27FFA15C76B01

- CA membuat sertifikat digital untuk kunci publik Alice 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.

Contoh 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*.

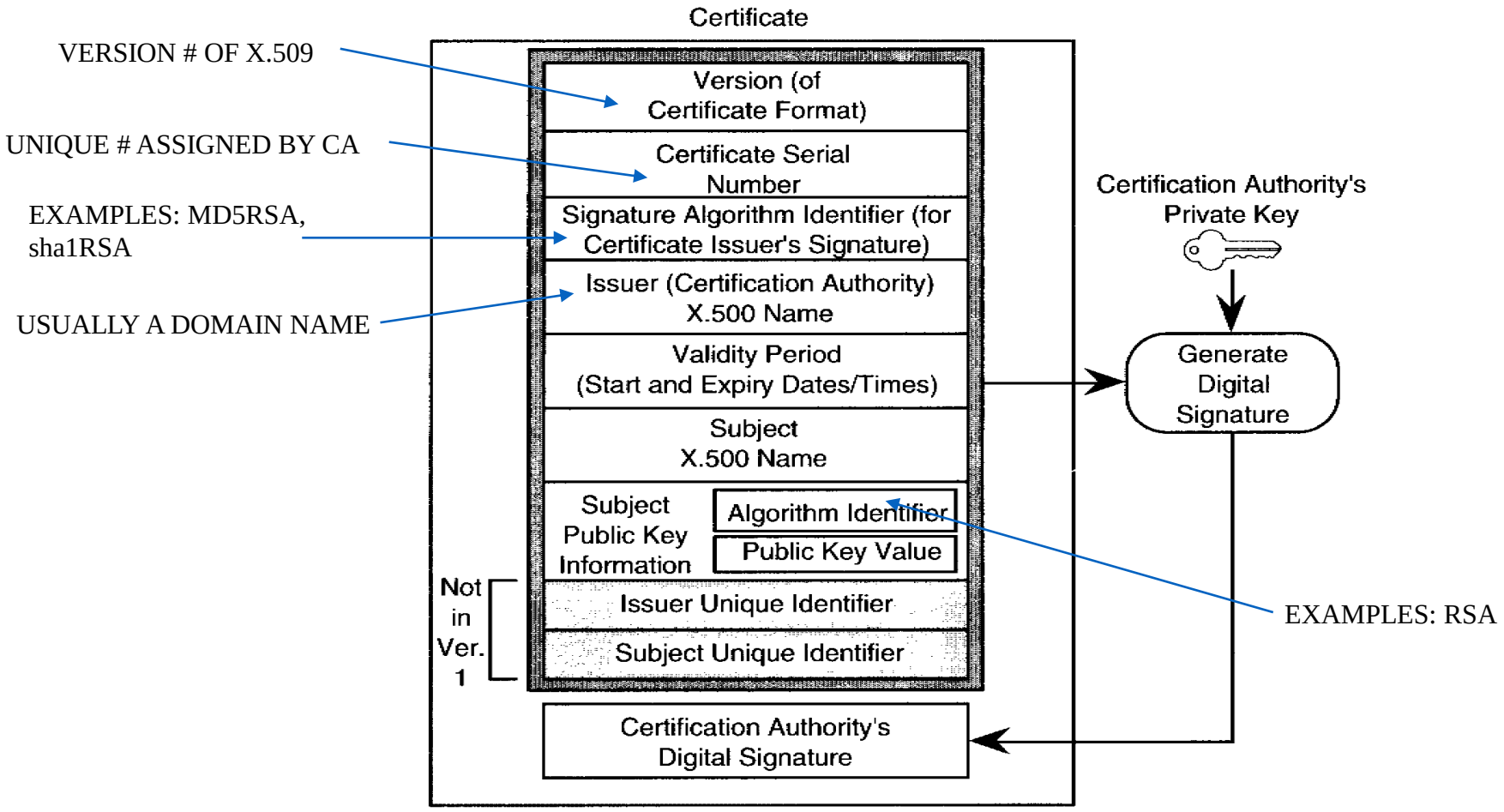
X.509

- Format sertifikat digital yang diterbitkan oleh berbagai CA tidak sama.
- Agar semua sertifikat digital 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 digital standard *X*.509

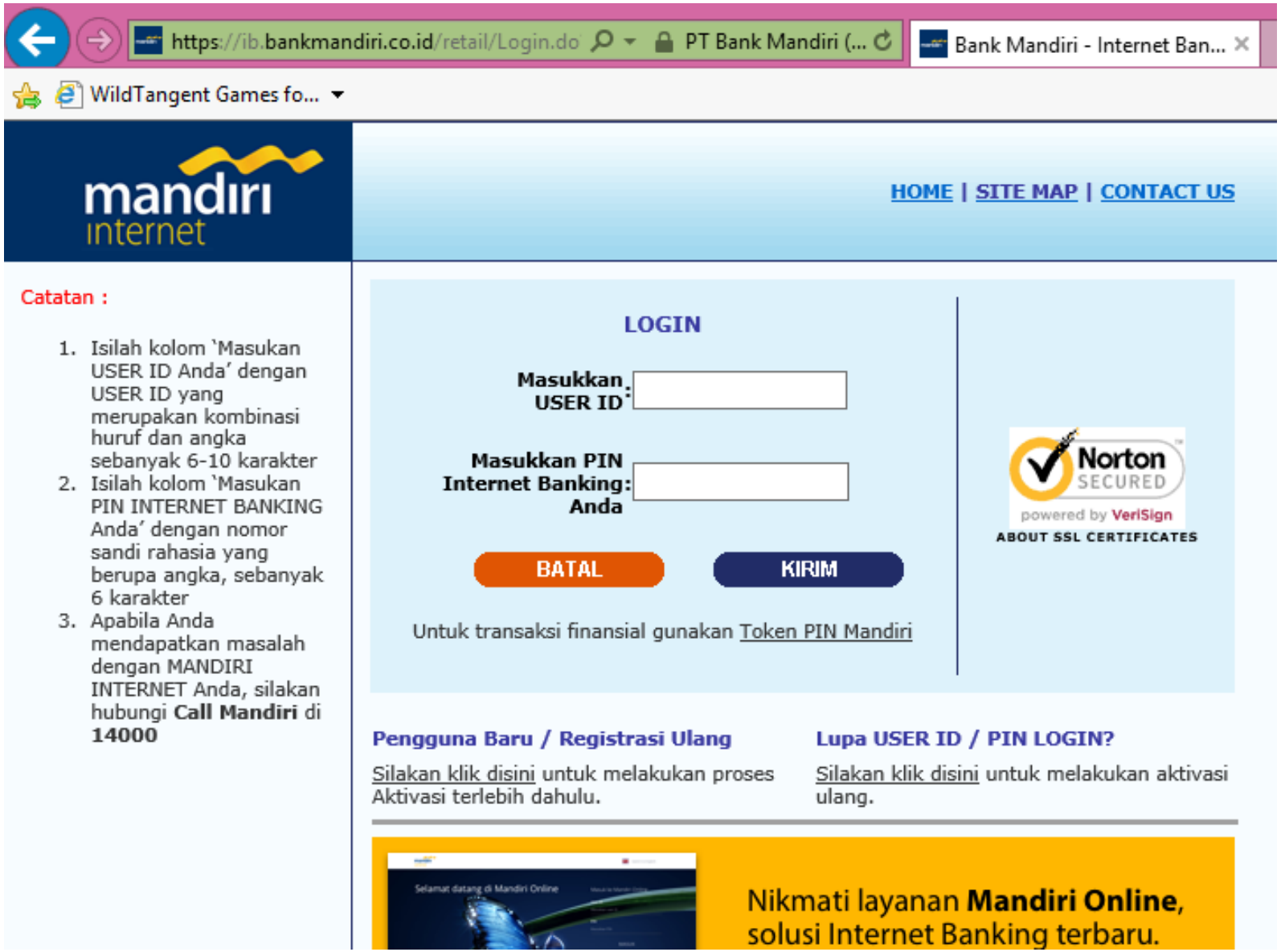
Field	Arti
Version	Versi X.509
Serial Number	Nomor ini plus nama CA secara unik digunakan untuk mengidentifikasi sertifikat
Certificate Signature Algorithm	Algoritma yang digunakan untuk tanda-tangan digital. Contoh: MD5RSA, SHA1RSA
Issuer	Nama CA yang mengeluarkan sertifikat digital. Biasanya nama domain.
Validity period	Waktu awal dan akhir periode valid
Subject name	Entitas (individu atau organisasi) yang disertifikasi
Subject Public Key Info	Kunci publik subjek dan algoritma kriptografi kunci-publik yang digunakan (misalnya RSA).
Issuer ID	ID opsional yang secara unik mengidentifikasi certificate's issuer.
Subject ID	ID opsional yang secara unik mengidentifikasi certificate's subject
Extensions	Banyak ekstensi yang telah didefinisikan (opsional).
Signature	Tanda-tangan digital (ditandatangani dengan kunci privat CA).
Signature algorithm	Algoritma tanda-tangan digital yang digunakan.

Sertifikat Digital X.509 Versi 2

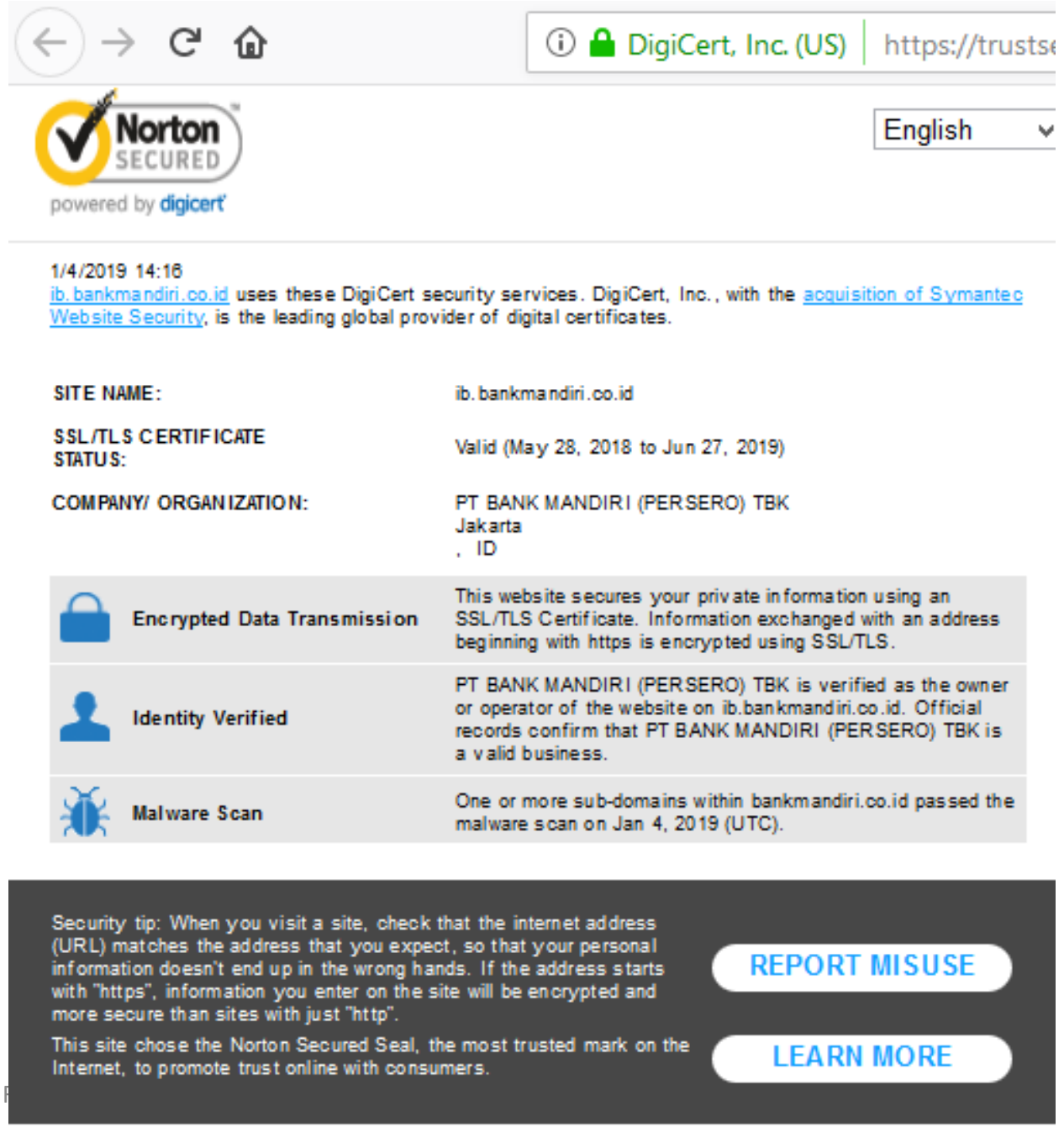


Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

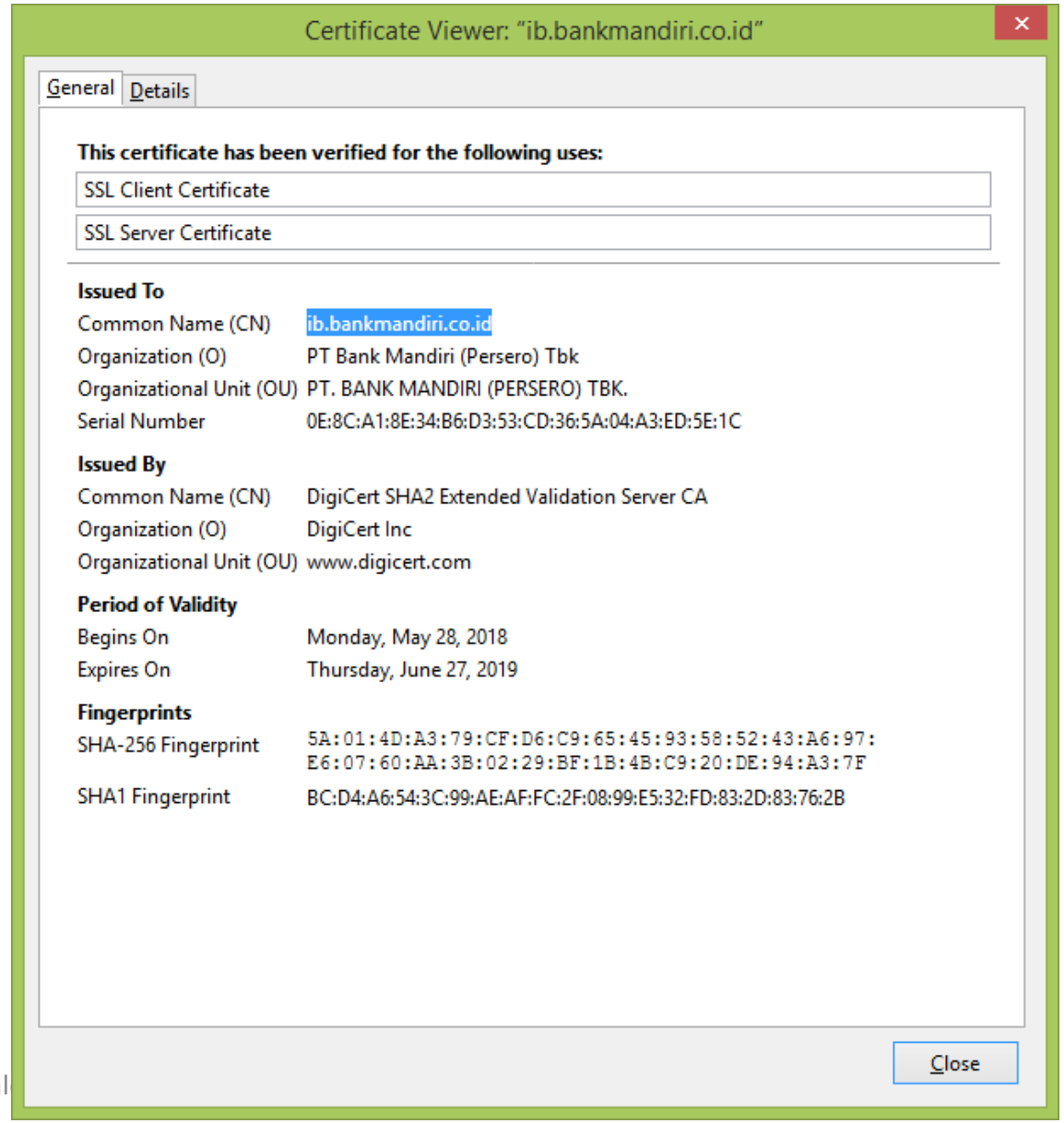
Studi kasus: sertifikat digital untuk server Bank Mandiri



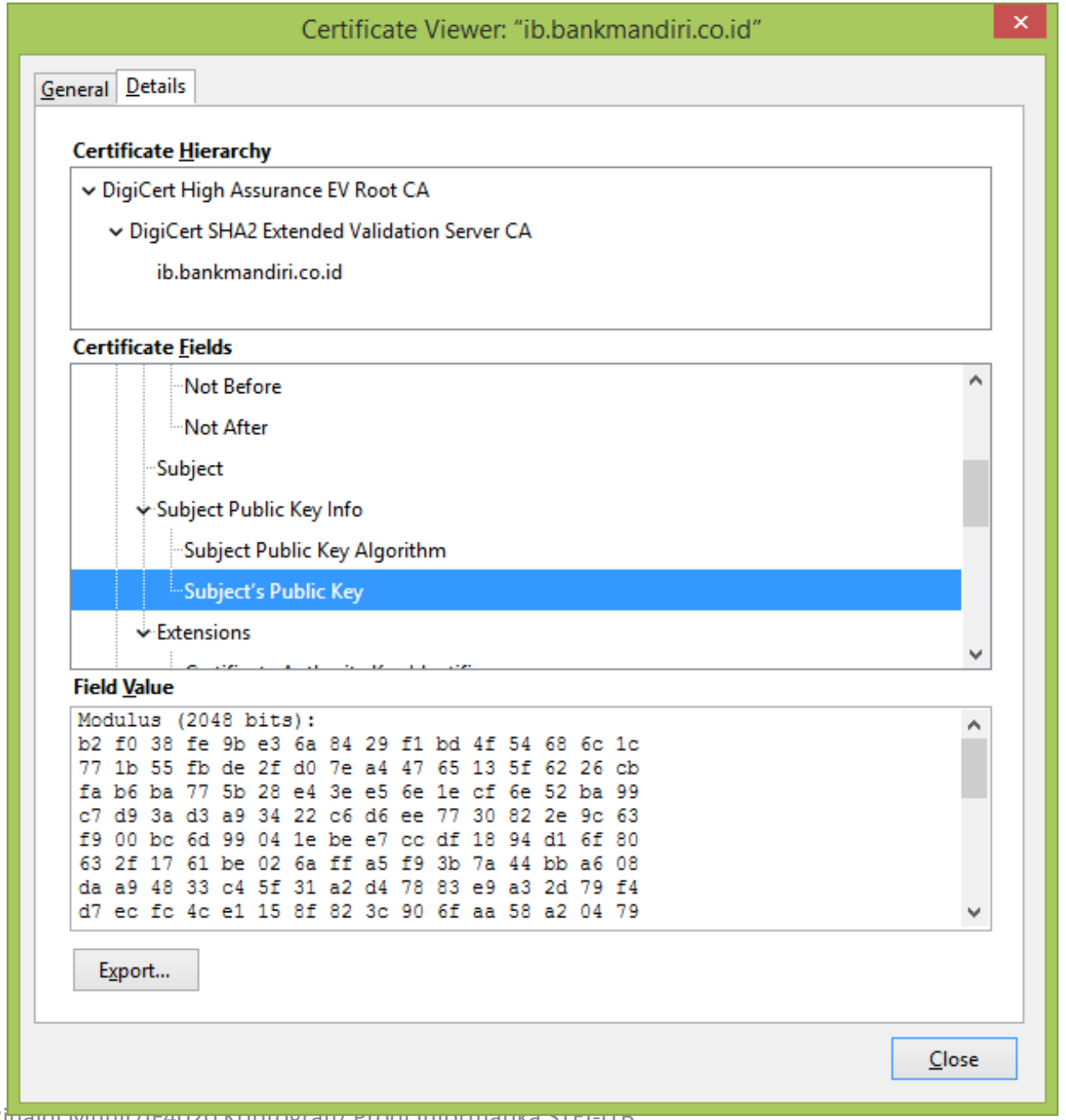
Pernyataan bahwa situs Bank Mandiri adalah situs yang aman untuk transaksi *e-bank*



Informasi umum sertifikat Digital server Bank Mandiri



Melihat kunci publik *server* situs Bank Mandiri



RSA

Enkripsi: $c = m^e \bmod n$

Dekripsi: $m = c^d \bmod n$

Modulus (2048 bits):

```
b2 f0 38 fe 9b e3 6a 84 29 f1 bd 4f 54 68 6c 1c 77 1b 55 fb de 2f d0 7e a4 47 65 13 5f
62 26 cb fa b6 ba 77 5b 28 e4 3e e5 6e 1e cf 6e 52 ba 99 c7 d9 3a d3 a9 34 22 c6 d6 ee
77 30 82 2e 9c 63 f9 00 bc 6d 99 04 1e be e7 cc df 18 94 d1 6f 80 63 2f 17 61 be 02 6a
```

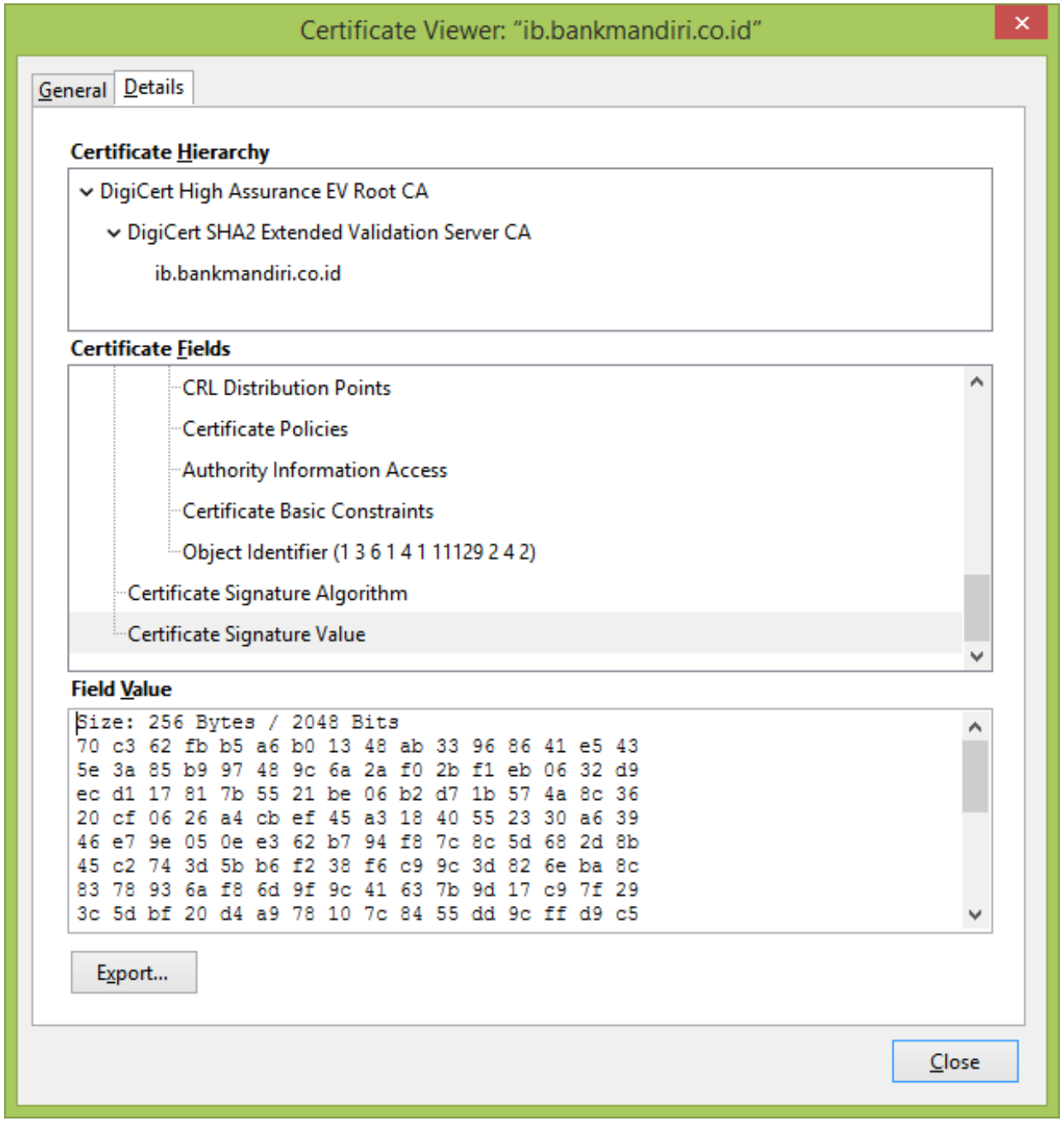
n ➡

```
ff a5 f9 3b 7a 44 bb a6 08 da a9 48 33 c4 5f 31 a2 d4 78 83 e9 a3 2d 79 f4 d7 ec fc 4c
e1 15 8f 82 3c 90 6f aa 58 a2 04 79 74 c3 f4 da 87 68 1c 9e f6 50 9f be 74 34 2e 8c 4b
f4 ba 62 71 cc af 48 eb ef 99 95 2a 49 8f f9 8e dd e5 cc ec 7b 05 4e 7e 6d 73 95 5a 61
84 88 0b b2 4d b9 31 a4 c5 62 cf b2 7d ed d1 35 75 9d 4b d2 f9 34 95 a9 55 aa 33 ce 90
72 10 97 74 79 50 a3 ed d5 cb 71 0e 3a f2 3a 1a b8 03 ea cf 31 ce 7a 12 9c 68 2f 32 8f
59 66 28 b8 d9 e1 05 af 0e bd af 5d bf 62 f3 16 b4 d8 e5 b0 a2 54 09 df
```

Kunci publik (exponent)(24 bits):

e ➡ **65537**

Tanda-tangan CA
di dalam sertifikat digital



Tanda-tangan digital dari CA:

```
Size: 256 Bytes / 2048 Bits
70 c3 62 fb b5 a6 b0 13 48 ab 33 96 86 41 e5 43 5e 3a 85 b9 97 48
9c 6a 2a f0 2b f1 eb 06 32 d9 ec d1 17 81 7b 55 21 be 06 b2 d7 1b
57 4a 8c 36 20 cf 06 26 a4 cb ef 45 a3 18 40 55 23 30 a6 39 46 e7
9e 05 0e e3 62 b7 94 f8 7c 8c 5d 68 2d 8b 45 c2 74 3d 5b b6 f2 38
f6 c9 9c 3d 82 6e ba 8c 83 78 93 6a f8 6d 9f 9c 41 63 7b 9d 17 c9
7f 29 3c 5d bf 20 d4 a9 78 10 7c 84 55 dd 9c ff d9 c5 d2 79 9d 8c
45 68 fa 06 c7 f1 d8 84 76 4e d4 f0 d3 a8 55 94 35 a6 9c 3e 9d 32
61 3d 9b 3c 80 7b 2b 06 68 af 97 7d d5 37 68 bd 6b 91 5b e0 e1 0c
a0 42 75 f8 09 34 99 61 16 5d fd 0e 8c 6e 8c 55 47 50 84 f6 d2 ac
e3 dd 54 f4 90 89 fc 05 e6 70 38 9b d5 73 0f ff 4b 9d a4 d3 44 c8
d1 ce 24 42 8f e5 54 e9 86 6b 13 a2 ab 85 16 7d 74 48 f4 64 7a 83
4f b7 fc fa 63 4f af e1 65 f8 10 e4 db 8b
```

Proses Penggunaan Sertifikat Digital

- Misalkan pemilik kunci publik (individu, server, dsb) sudah memiliki sertifikat digital atas kunci publiknya.
- 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 (ada di dalam sertifikat digital).
- Penerima pesan dapat meminta verifikasi sertifikat digital tersebut melalui repositori CA yang tersedia secara publik.
- Repositori CA melaporkan status sertifikat si pengirim pesan.

Proses Verifikasi Sertifikat Digital

- Carilah kunci publik CA yang mengeluarkan sertifikat tersebut. (pada contoh Bank Mandiri, klik digicert)

- Gunakan kunci kunci publik CA untuk mendekripsi tanda-tangan digital di dalam sertifikat.

- Bandingkan hasil dekripsi dengan nilai hash dari sertifikat digital. Jika sama, berarti sertifikat digital tersebut asli.

Memverifikasi Pemilik Sertifikat Digital

- Bagaimana memastikan situs Bank Mandiri adalah benar, bukan situs bank palsu?

- Caranya: menggunakan teknik *challenge* dan *response.*

- *Client* memberikan *challenge*, *server* memberi respon.

Mekanisme *challenge* dan *response*

- *Client* mengirim *challenge* ke *server* Bank Mandiri berupa string acak yang panjangnya 128 bit.

  "F37C2412 8F60E0C8 73BFF201 2E9556B1"

- *Client* meminta *server* Bank Mandiri untuk mengenkripsi string tersebut dengan menggunakan kunci privatnya.

- Jika *server* Bank Mandiri asli, tentu ia mengetahui kunci privatnya. Lalu, *server* Bank Mandiri mengenkripsi string tersebut dengan kunci privatnya dan mengirimkan cipherteksnya kepada *client*.

- *Client* kemudian mendekripsi cipherteks dengan kunci publik yang terdapat di dalam sertifikat. Jika hasilnya sama dengan string acak yang ia kirim, berarti *server* Bank Mandiri adalah asli.

Jenis-jenis sertifikat digital

1. Server Certificates

2. Personal Certificates

3. Organization Certificates

4. Developer Certificates

Batas Kadaluarsa Sertifikat Digital

- 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.

CRL (*Certificate Revocation List*)

- 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.

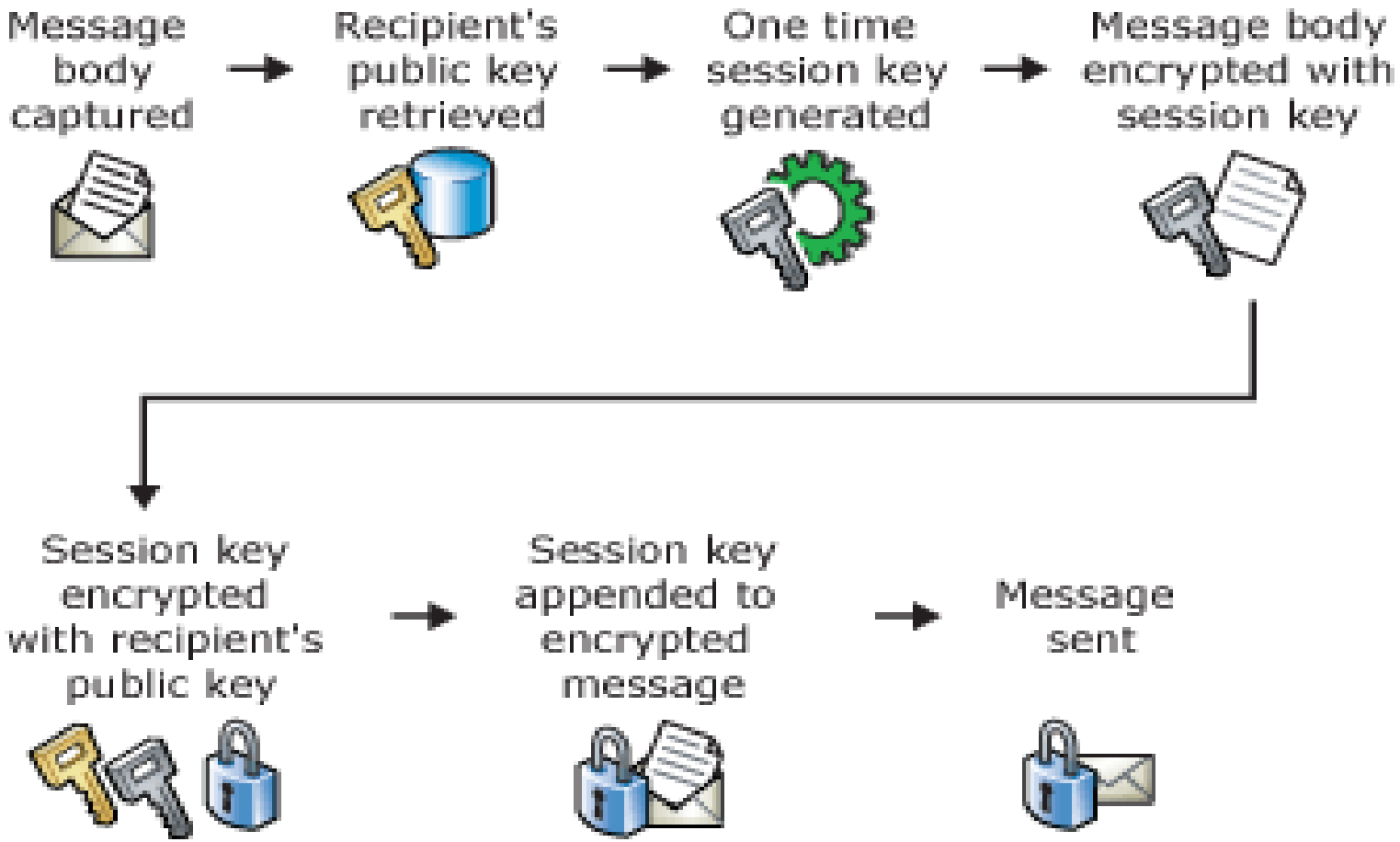
Dimana Sertifikat Digital Digunakan?

- **Dalam sejumlah aplikasi Internet yang melibatkan:**

1. Secure Socket Layer (SSL) dikembangkan oleh *Netscape Communications Corporation*
2. Secure Multipurpose Internet Mail Extensions (S/MIME) Standar untuk keamanan email dan *electronic data interchange* (EDI).
3. Secure Electronic Transactions (SET) protocol untuk keamanan pembayaran elektronik
4. Internet Protocol Secure Standard (IPSec) funtuk otentikasi devais di dalam jaringan

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

Bagaimana Sertifikat Digital Digunakan untuk Enkripsi Pesan



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

SELAMAT BELAJAR