Bahan Kuliah IF4020 Kriptografi

Sertifikat Digital

Oleh: Rinaldi Munir

Program Studi Teknik Informatika
STEI-ITB
2024

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.

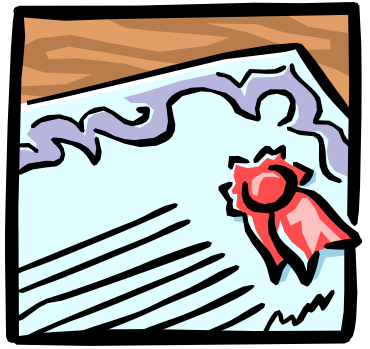
- Kunci privat bersifat rahasia, hanya diketahui oleh pemilik, tidak dibagi kepada pihak lain, tetapi kunci publik tersedia untuk umum.

- 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.

Sertifikat Digital



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

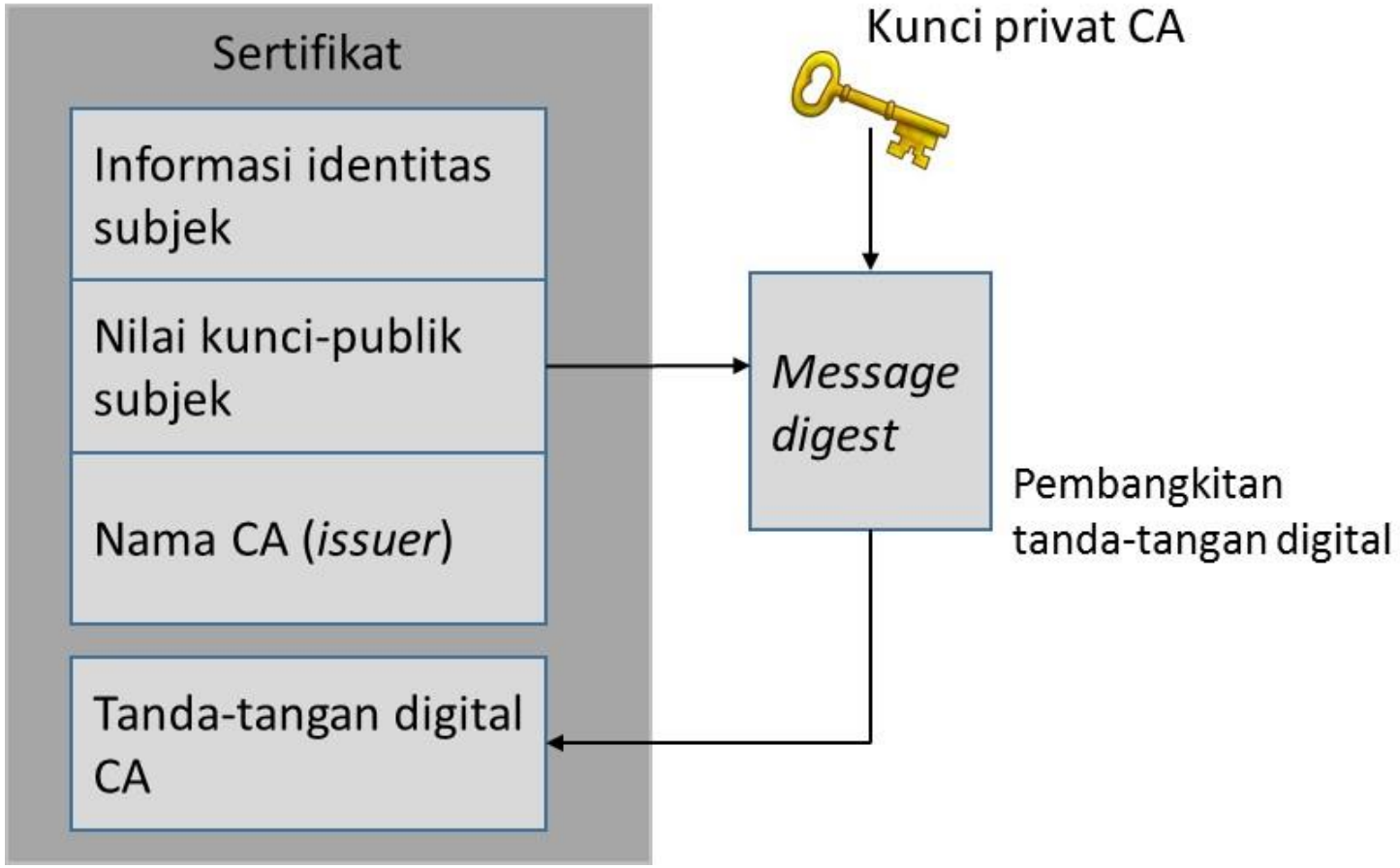
- Sertifikat digital adalah dokumen digital yang mengikat kunci publik dengan informasi pemiliknya.

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

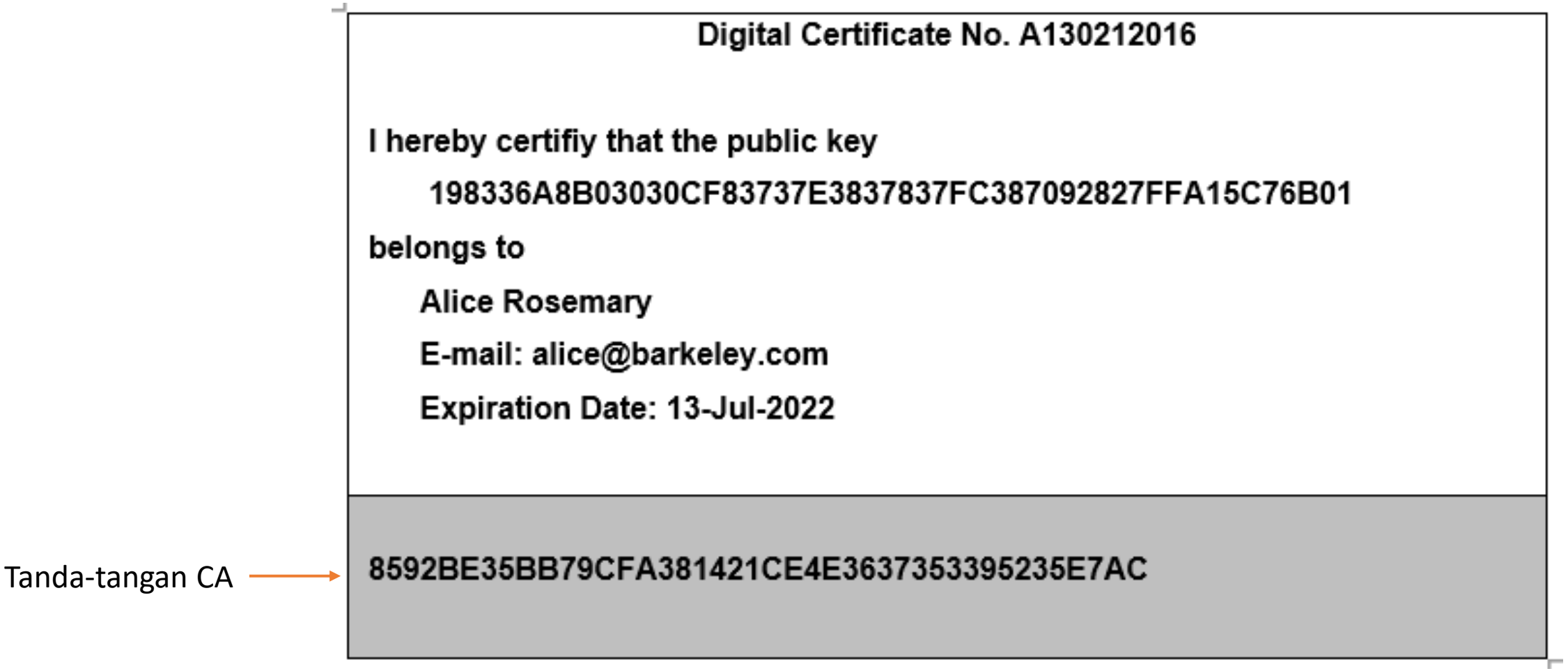
- Sertifikat digital mempunyai fungsi yang sama seperti SIM atau paspor.

- 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*)

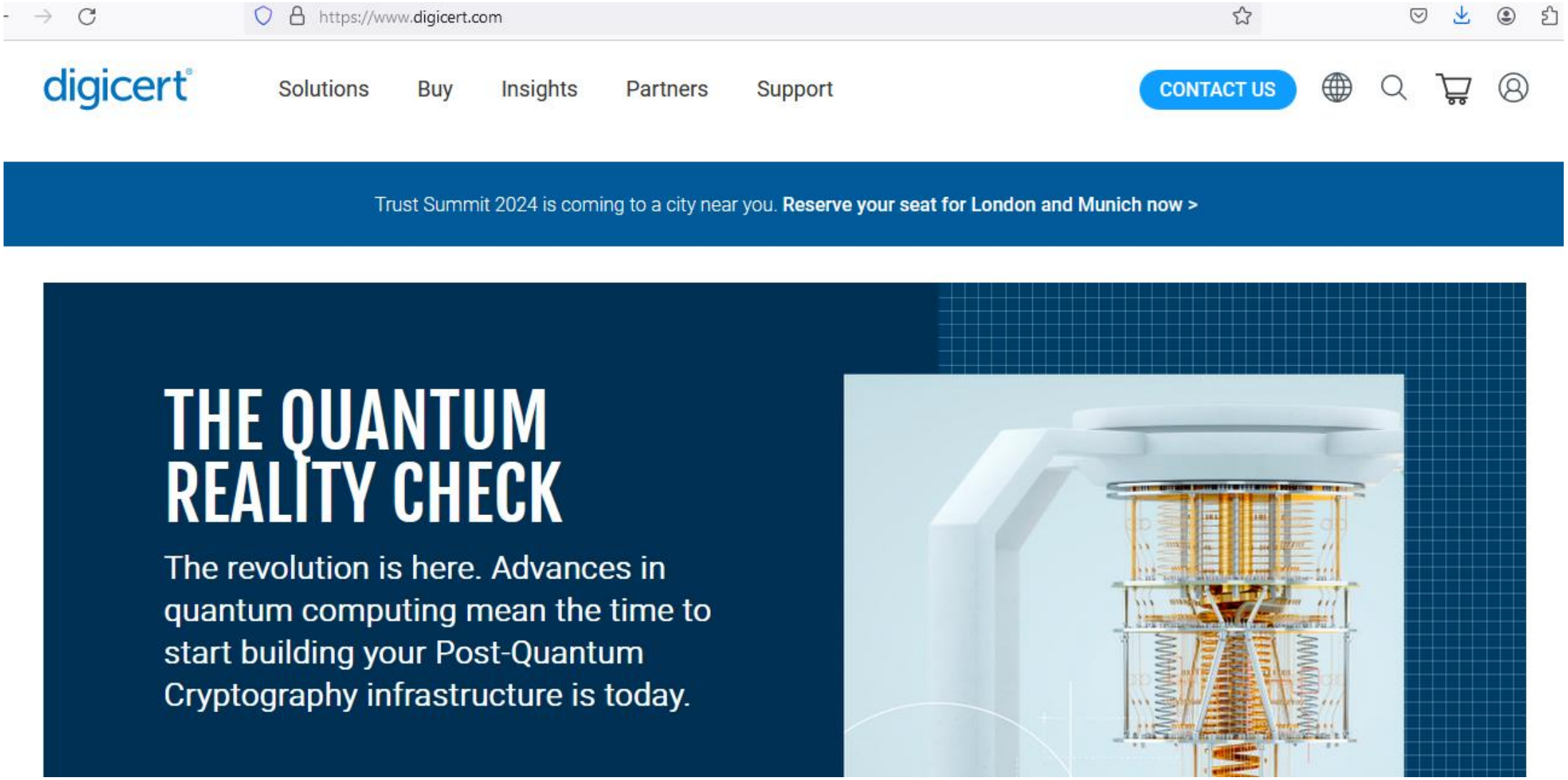
- Selain itu ditambahkan informasi lain seperti nomor seri sertifikat, waktu kadaluarsa, dan lain-lain



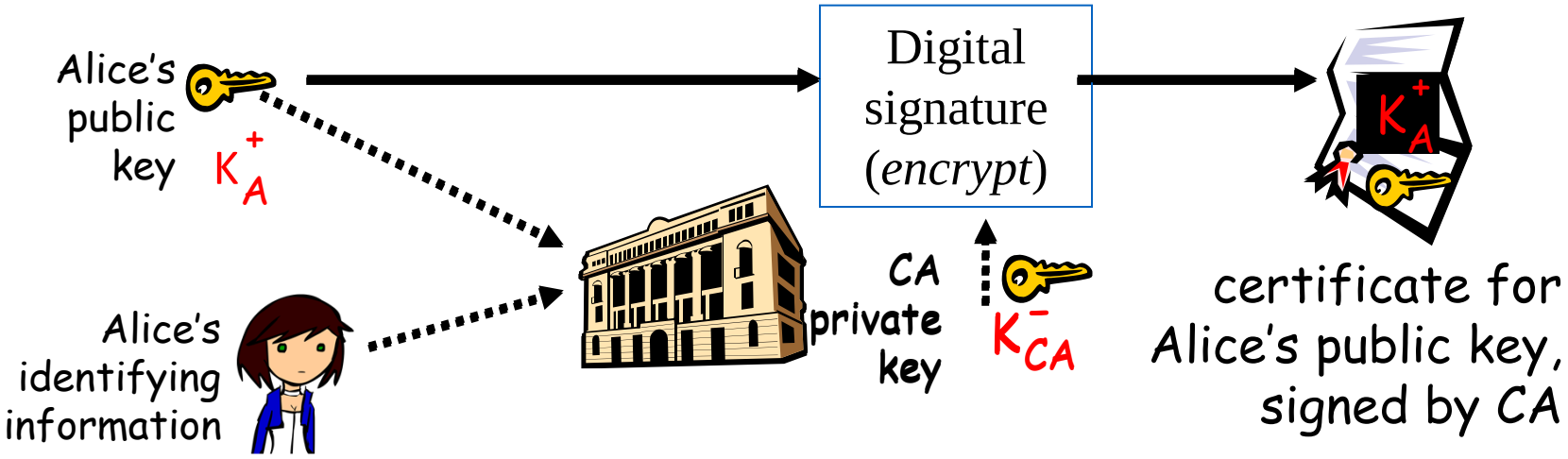
Contoh sebuah sertifikat digital:



- *CA* biasanya adalah bank atau institusi institusi yang terpercaya.
- Contoh CA terkenal: *Digicert* (www.digicert.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

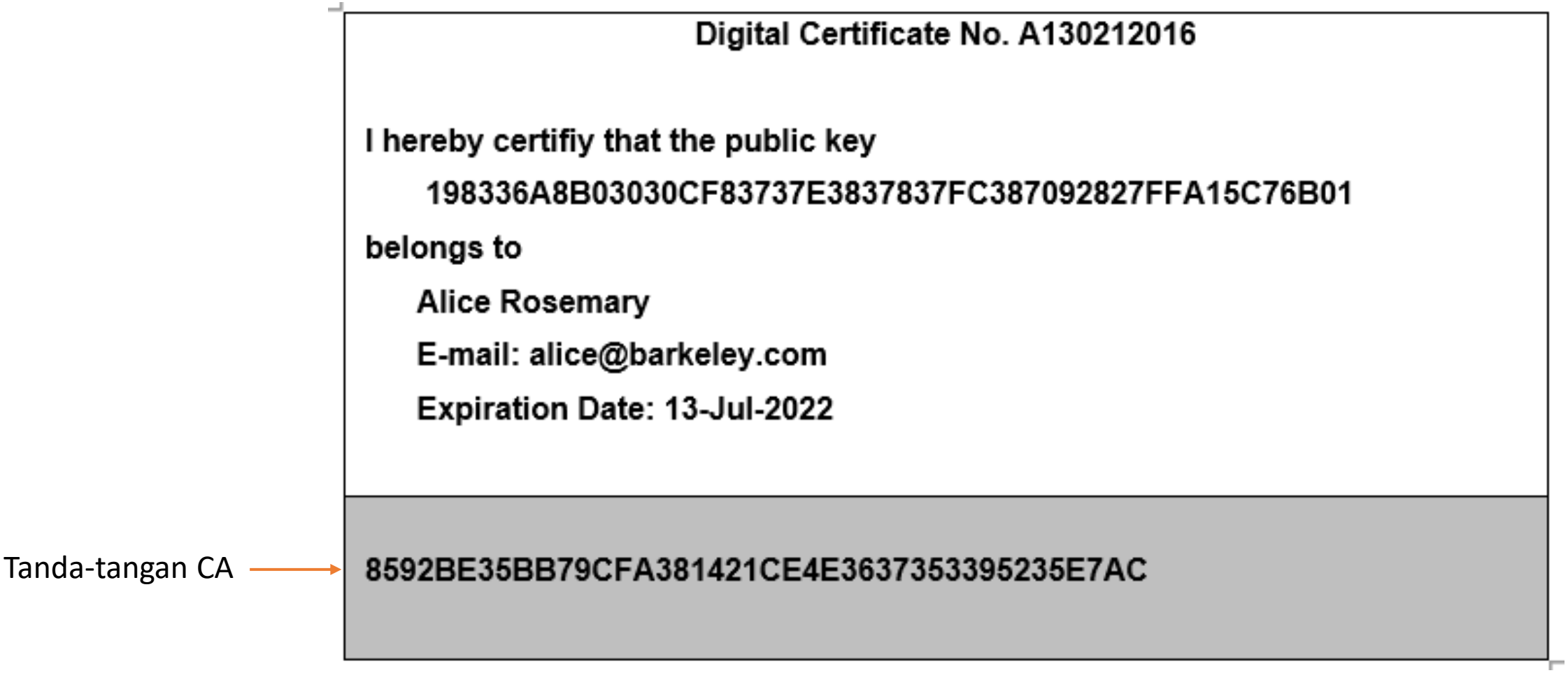
- CA membuat sertifikat digital untuk kunci publik Alice lalu menandatanganinya dengan kunci privat *CA*.

- 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 sertifikat digital yang dikeluarkan oleh CA untuk Alice:



- 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*.

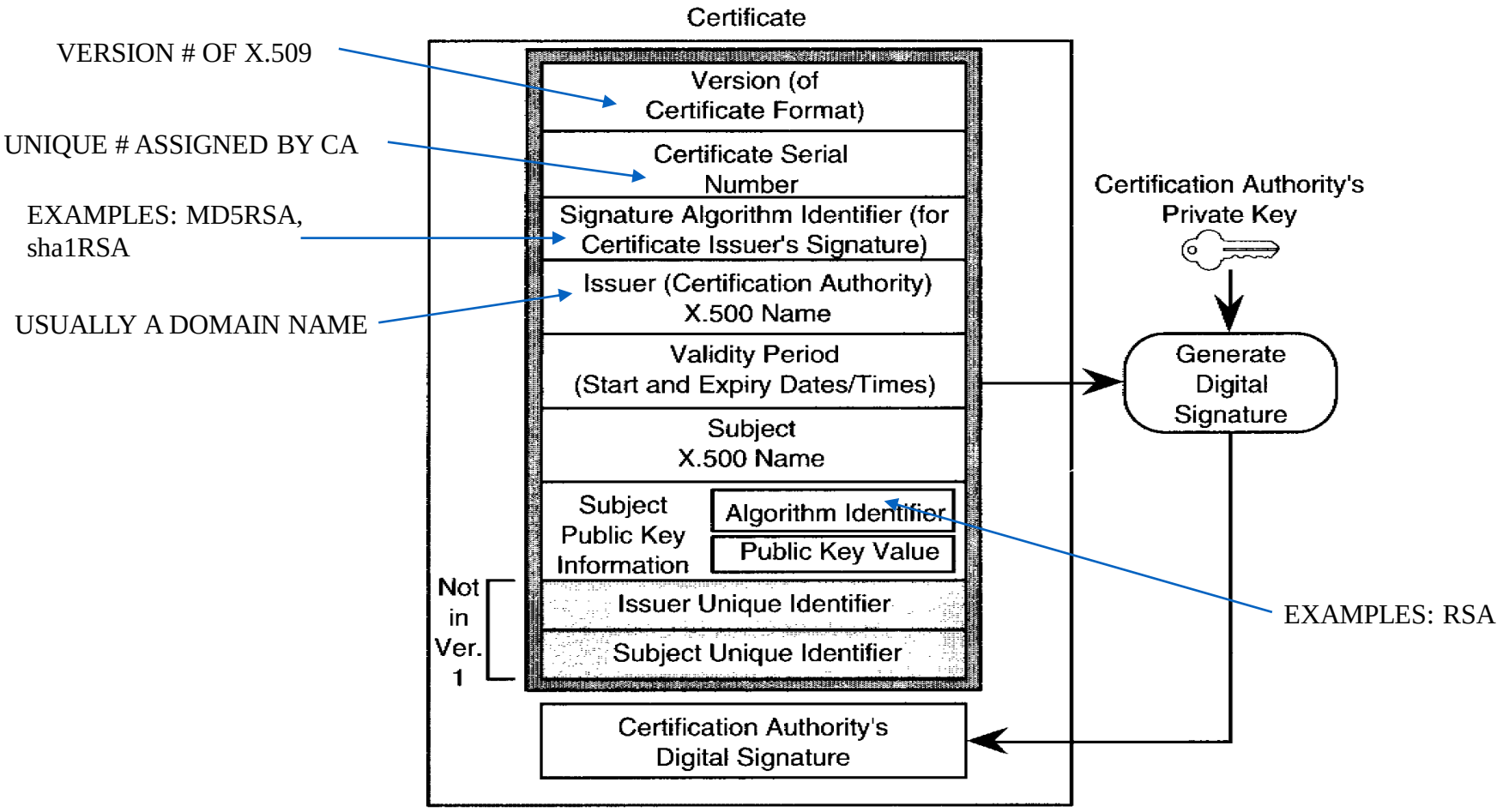
X.509

- 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

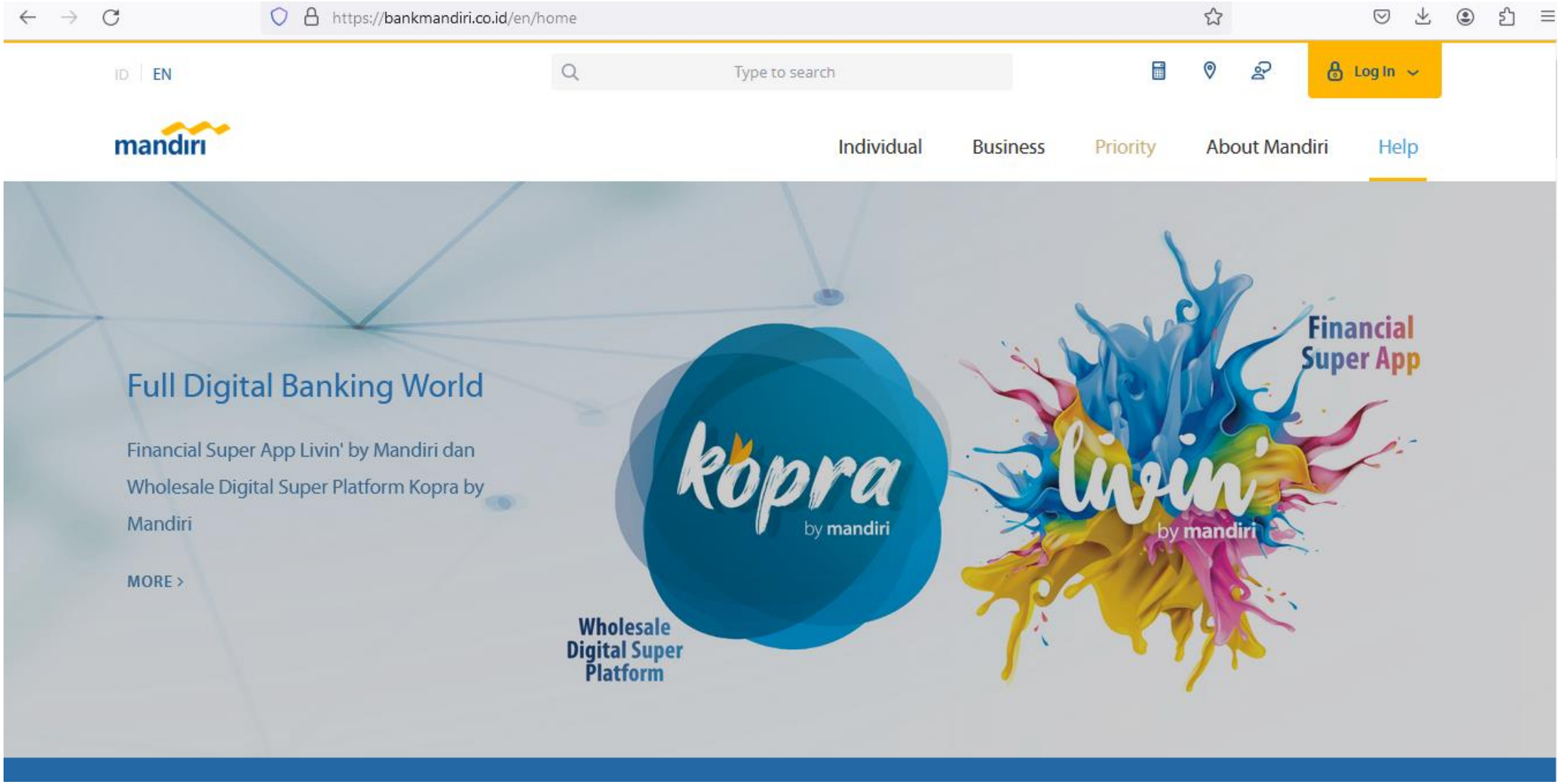
Field	Arti
Version	Versi X.509
Serial Number	Nomor ini plus nama CA secara unik digunakan untuk mengidentifikasi sertifikat
Certificate Signature Algorithm	Algoritma yang digunakan untuk tanda-tangan digital. Contoh: MD5RSA, SHA1RSA
Issuer	Nama CA yang mengeluarkan sertifikat digital. Biasanya nama domain.
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



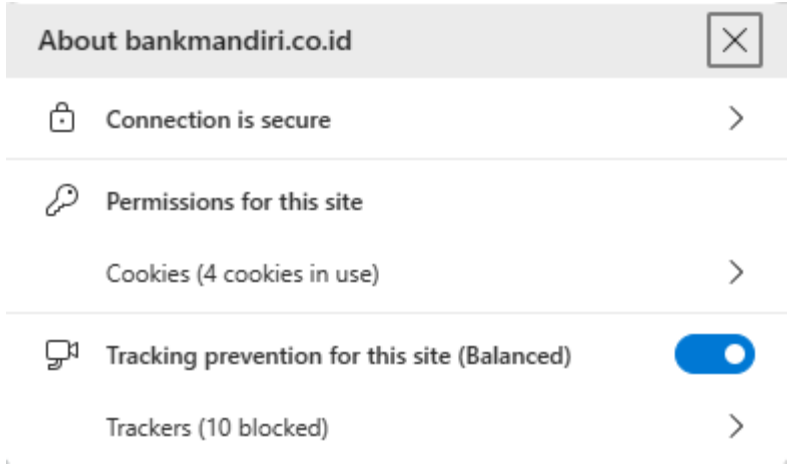
Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

Studi kasus: sertifikat digital untuk server Bank Mandiri *)

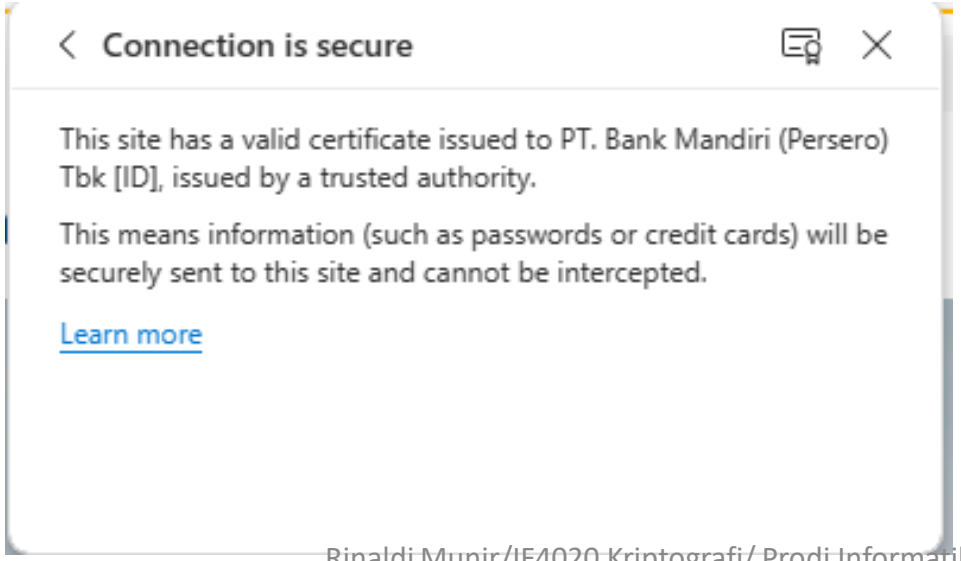


*) Menggunakan browser Microsoft Edge

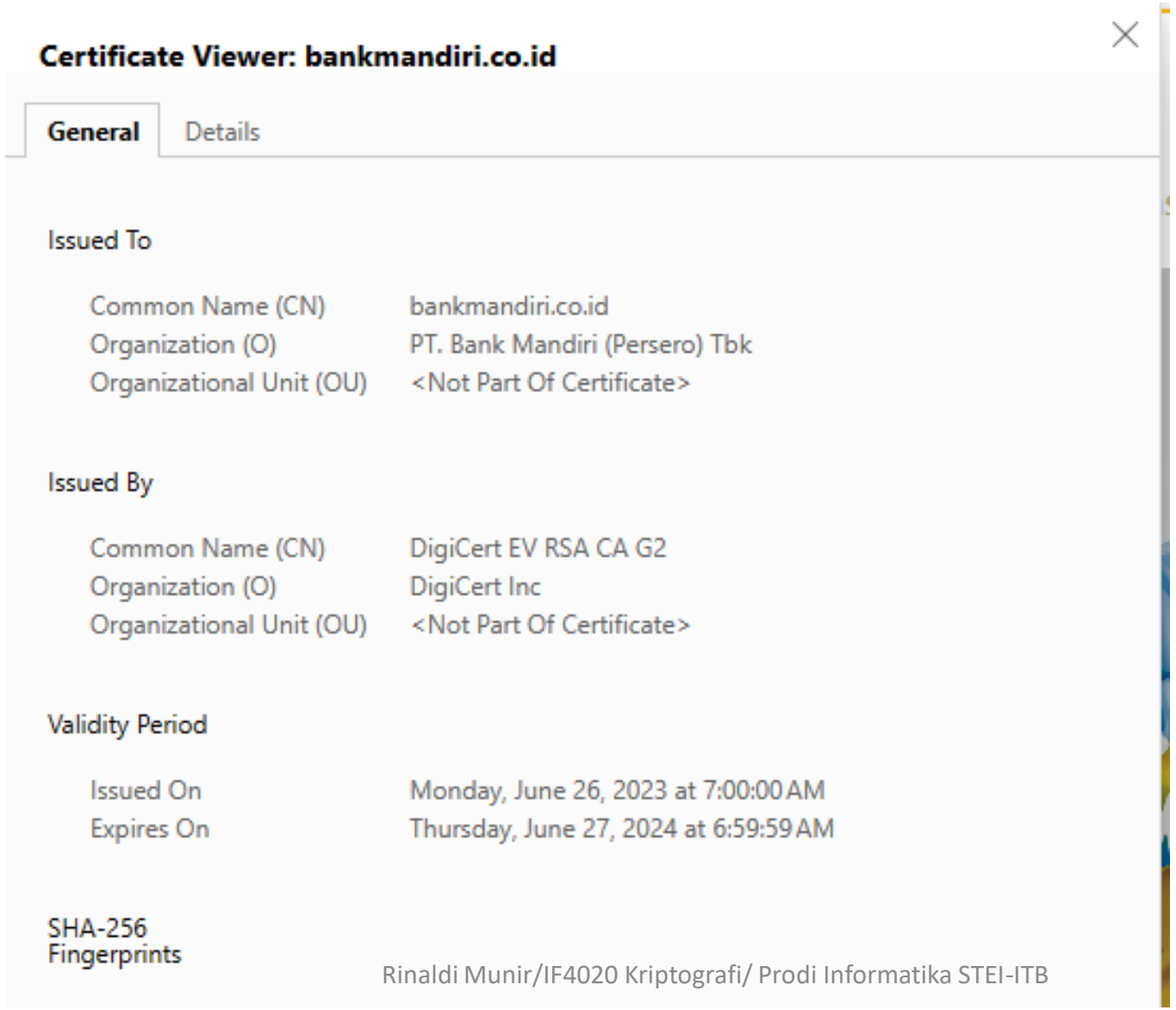
Klik tanda gambok pada Alamat URL



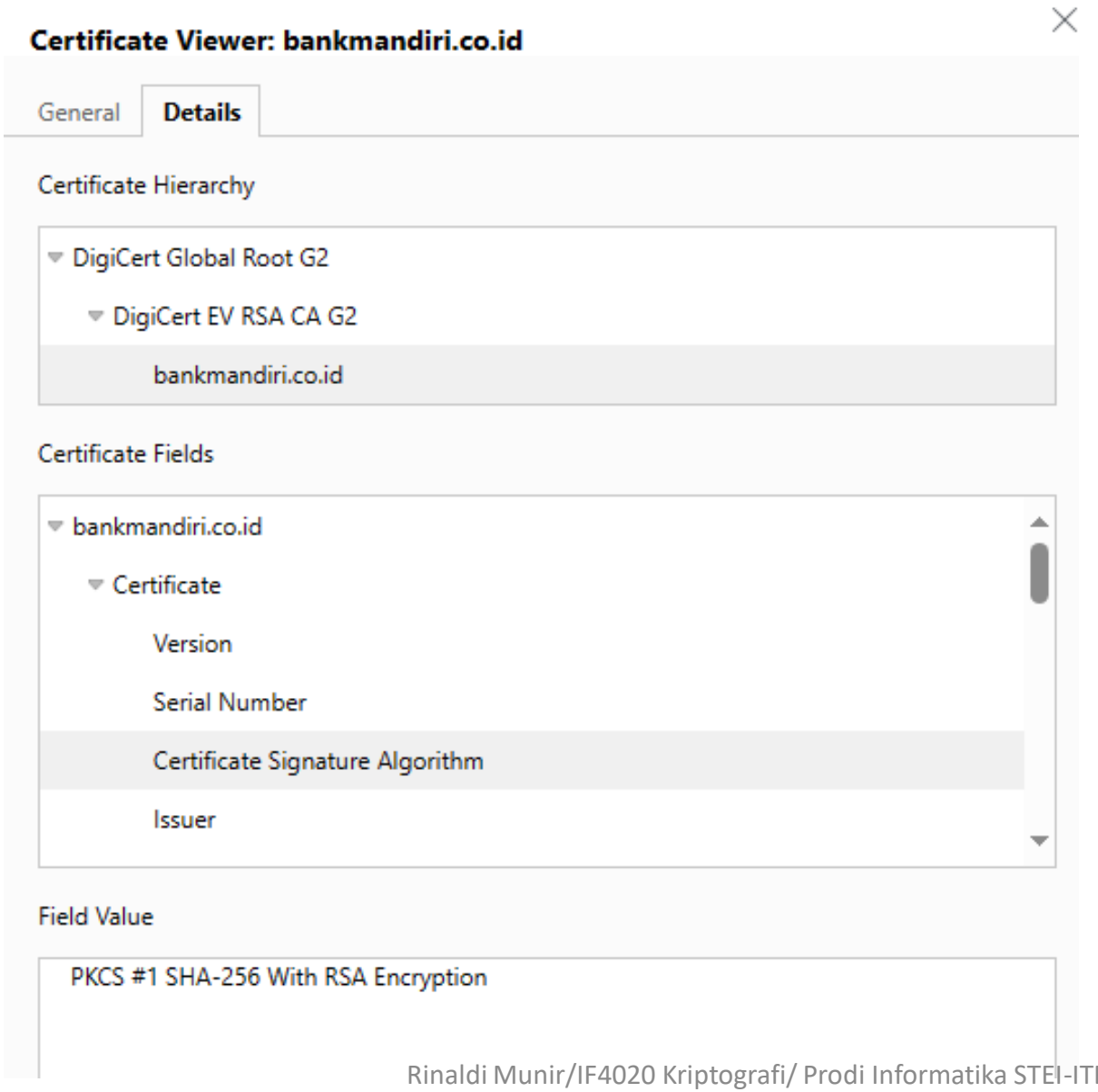
Klik Connection is secure:



Klik icon sertifikat digital:



- Klik details untuk melihat setiap *field*:



Modulus (2048 bits):
D1 2F 92 05 23 F2 A3 C8 7D 91 11 B0 5F 48 C3 4E 8E AA B2 21 68 90 1C
69 D9 E6 68 53 C1 D4 D6 E6 C2 04 A4 AA 65 15 F7 8A 75 C5 D3 84 D4
FC 55 2F 72 E9 82 CC D4 62 F7 80 DA 3A 4C 70 2A 37 75 4F DE 38 33 FC
09 F2 21 38 D4 B8 EF 51 FD FC FA A0 21 61 32 F0 47 B4 2E 0F 3B AA 18
EF 7C 97 0F 4C 1F E3 67 88 08 BA E7 16 2A AF 73 D3 F7 50 2A 13 FD 9E
CB 7E 63 A8 6D 00 D0 7F D3 0B 6F 71 41 4A 10 F2 A9 DA 76 E7 5A 49
0E 77 04 9C 27 D6 3D FA 32 38 17 DB 3D 2B 8D 65 69 BC 54 17 D3 45
9F 99 95 0A CD 67 A0 A7 39 42 74 62 B5 6D 15 0B 06 AA 3A C9 F3 E3
3D E3 42 95 BE 92 5D 37 87 73 A4 E7 61 76 C1 62 7F C0 00 DE 83 DE 61
89 CD 7F 2C D1 90 EB 3B 61 DD D4 51 97 B3 D7 DE 3E 9E BE EE 50 9E
77 7F 5C 3F 33 EA DD 11 E3 3B 93 B1 43 8D 2A A0 D8 25 0B 56 86 7F
DD BA 40 5F 39 55 22 82 9B

Public Exponent (17 bits):
01 00 01

RSA

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

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

Modulus (2048 bits):

D1 2F 92 05 23 F2 A3 C8 7D 91 11 B0 5F 48 C3 4E 8E AA B2 21 68 90 1C 69 D9 E6 68 53 C1 D4 D6 E6 C2 04 A4 AA 65 15 F7 8A 75
C5 D3 84 D4 FC 55 2F 72 E9 82 CC D4 62 F7 80 DA 3A 4C 70 2A 37 75 4F DE 38 33 FC 09 F2 21 38 D4 B8 EF 51 FD FC FA A0 21 61
32 F0 47 B4 2E 0F 3B AA 18 EF 7C 97 0F 4C 1F E3 67 88 08 BA E7 16 2A AF 73 D3 F7 50 2A 13 FD 9E CB 7E 63 A8 6D 00 D0 7F D3

n ➡ 0B 6F 71 41 4A 10 F2 A9 DA 76 E7 5A 49 0E 77 04 9C 27 D6 3D FA 32 38 17 DB 3D 2B 8D 65 69 BC 54 17 D3 45 9F 99 95 0A CD 67
A0 A7 39 42 74 62 B5 6D 15 0B 06 AA 3A C9 F3 E3 3D E3 42 95 BE 92 5D 37 87 73 A4 E7 61 76 C1 62 7F C0 00 DE 83 DE 61 89 CD
7F 2C D1 90 EB 3B 61 DD D4 51 97 B3 D7 DE 3E 9E BE EE 50 9E 77 7F 5C 3F 33 EA DD 11 E3 3B 93 B1 43 8D 2A A0 D8 25 0B 56 86
7F DD BA 40 5F 39 55 22 82 9B

Exponent (17 bits):

e ➡ **010001 (dalam hexadecimal, dalam decimal = 65537)**

Tanda-tangan CA
di dalam sertifikat digital

42 9B B7 04 DE 1E 3D 51 8B 65 71 23 42 F4 2E 84
64 D5 0D 8D D5 79 AF F0 1C 0D AC 40 BF C5 E8 E5
C2 68 63 2E D4 36 20 33 58 AB DD 62 63 62 4D 64
BF 72 1A 4B 0C A5 3C 32 17 52 A8 07 B8 6C C3 F6
34 CD 7E D2 A3 8E 67 1F DE 08 5B BA 89 34 B1 8B
0D E3 6D B1 33 2C 29 F4 A4 71 EC 45 EF C3 7A 18
60 C7 35 17 92 42 99 71 23 C7 5E F2 37 F5 EA C1
98 3C 56 28 DF C8 67 73 63 FE 3B 8E 04 8F BD F9
BE 71 55 E5 0F 80 25 0F E6 70 7F 3A 90 C6 62 1F
0A 99 F5 72 93 5F 45 3D 53 44 E0 CA 92 63 B5 DE
7D B3 94 C8 05 33 A9 7D 6C 8F D8 A9 F4 89 75 87
8E 83 3A 52 F8 ED 7D 75 D1 68 99 5D A7 6C 5C 79
59 2A F9 6E 95 B1 93 B8 4A 04 39 27 E4 08 15 A8
66 D7 21 09 E7 EF D5 9B 87 67 5B B2 5B B8 94 BC
4D 70 13 AC 6C 0F D5 9B A8 DC 68 FE 14 11 35 F8
AA 6C 72 58 C8 99 2F 24 56 C7 B8 C5 94 3D 67 3E

Kunci publik CA:

Modulus (2048 bits):
AD 1E 66 CC 7F 9D E4 EB 7F 83 17 27 3D 11 D9 F2
53 20 37 CD F0 0C 14 02 EE E1 CB 88 08 D2 FA 7B
3B C2 C0 00 7C 76 87 76 DB 7F CC 25 FA 91 8C 4B
16 89 2B D7 DF 0C 30 83 EB 71 6A A8 50 6A 13 D7
93 9A 8D D1 92 04 21 96 EE 79 6B 4E 0B B1 74 4B
70 AE 9C AE 40 4E 3B 47 63 76 89 F2 6E 68 6B 7C
6A ED 06 A6 2F 6D 16 AD C5 E9 E4 BF 44 A0 E1 FA
E1 46 5E 30 62 1E 1D 9D 6D 0B 39 54 46 85 BB 75
1B 94 35 F7 39 BD 0A A3 25 AB B2 E5 51 D0 04 FB
A7 77 6B 9F BE A6 97 C6 72 75 8B 99 B1 15 11 C2
C7 3C 09 DB 97 EF E2 29 AB 90 A5 09 54 D4 C8 BE
C0 40 67 8C 4E 6D 2B C4 3B EF C9 DA 5E 71 7E 0E
C7 9D 40 9E CD 12 2F 9B 42 8A 27 4C 71 33 F6 BC
9E 11 C5 07 B9 04 EF EE 70 29 6B FC C2 A9 EB 39
95 79 F5 A4 CB 38 2D 92 77 49 58 1B 91 32 E3 F9
16 C1 A2 FF EE 8B 04 D7 B6 40 44 59 AC 2F 64 7F

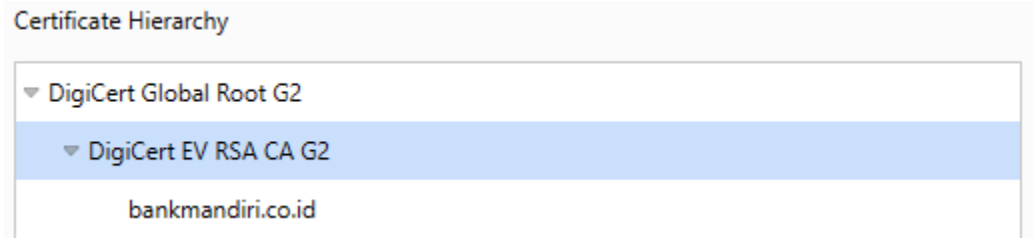
Public Exponent (17 bits):
01 00 01

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 EV RSA CA G2)



- 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*)

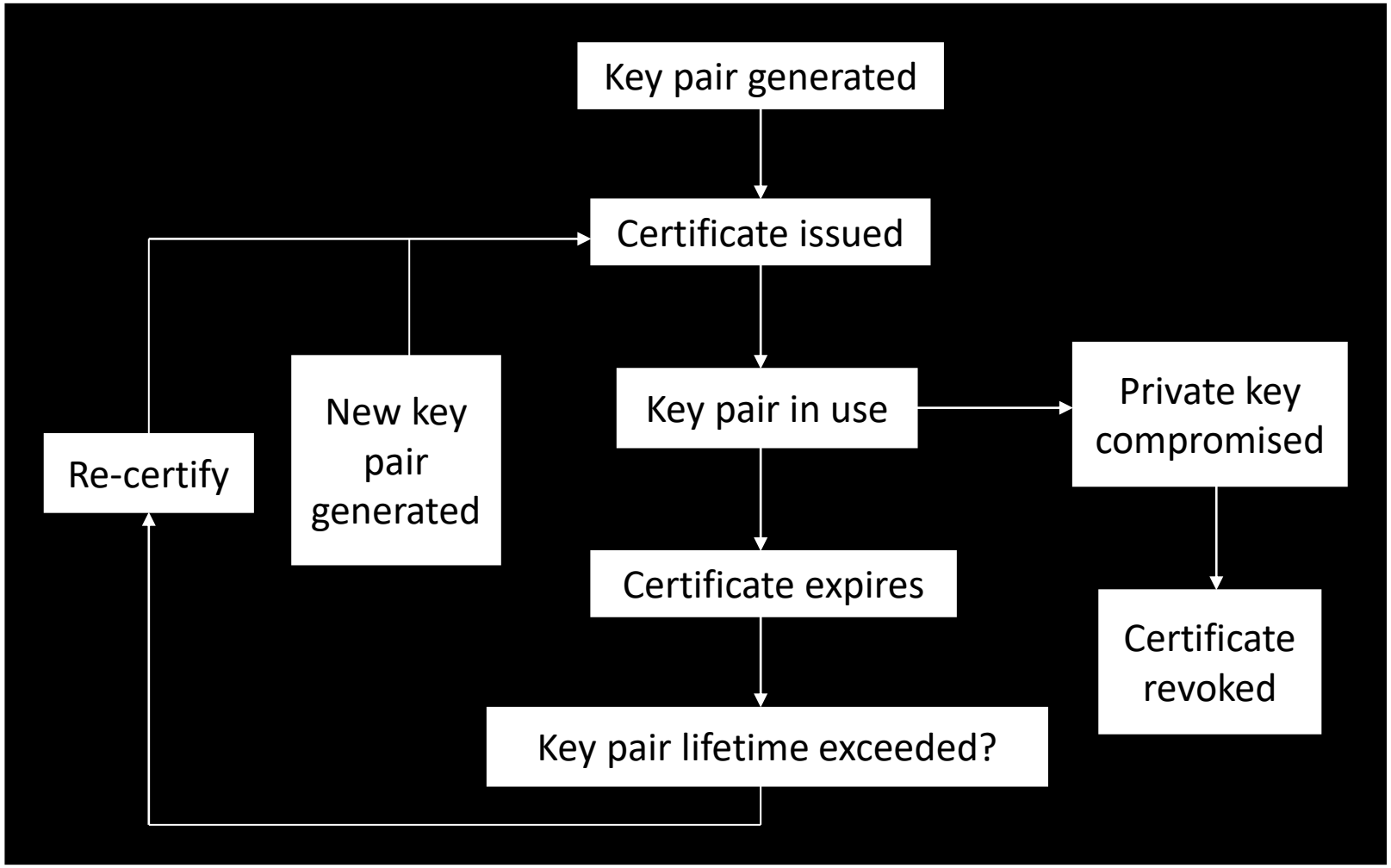
- Bagaimana *CA* memberitahu ke publik bahwa sertifikat digital ditarik?

- 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.

Daur hidup sertifikat digital



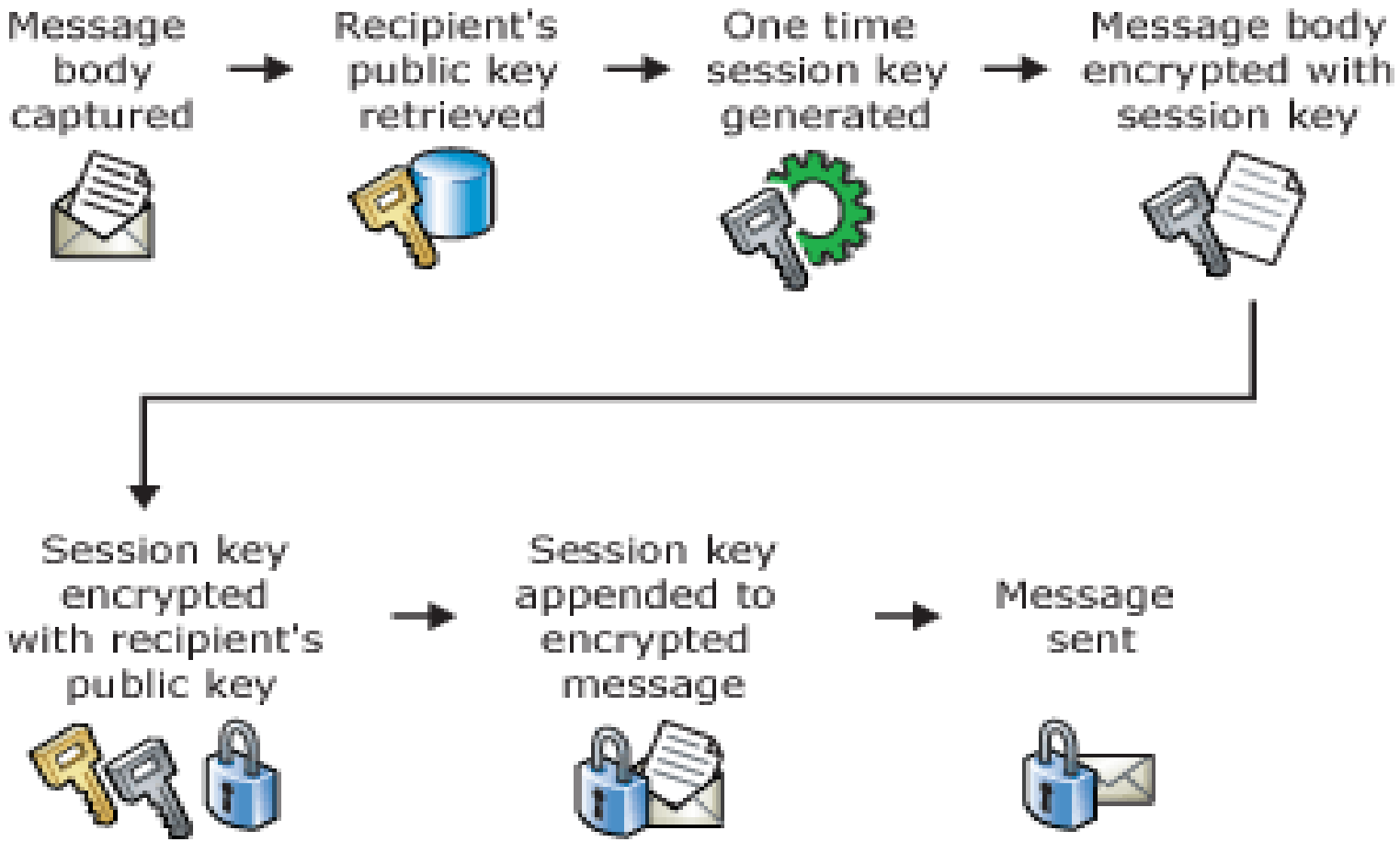
Dimana Sertifikat Digital Digunakan?

- **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

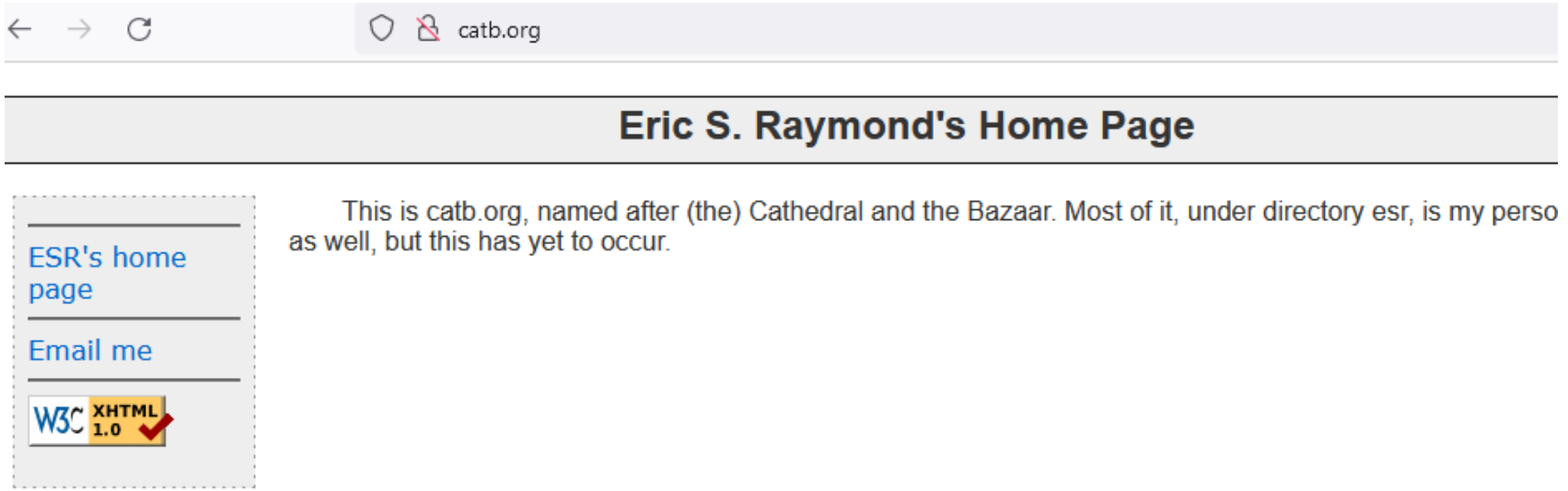
Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

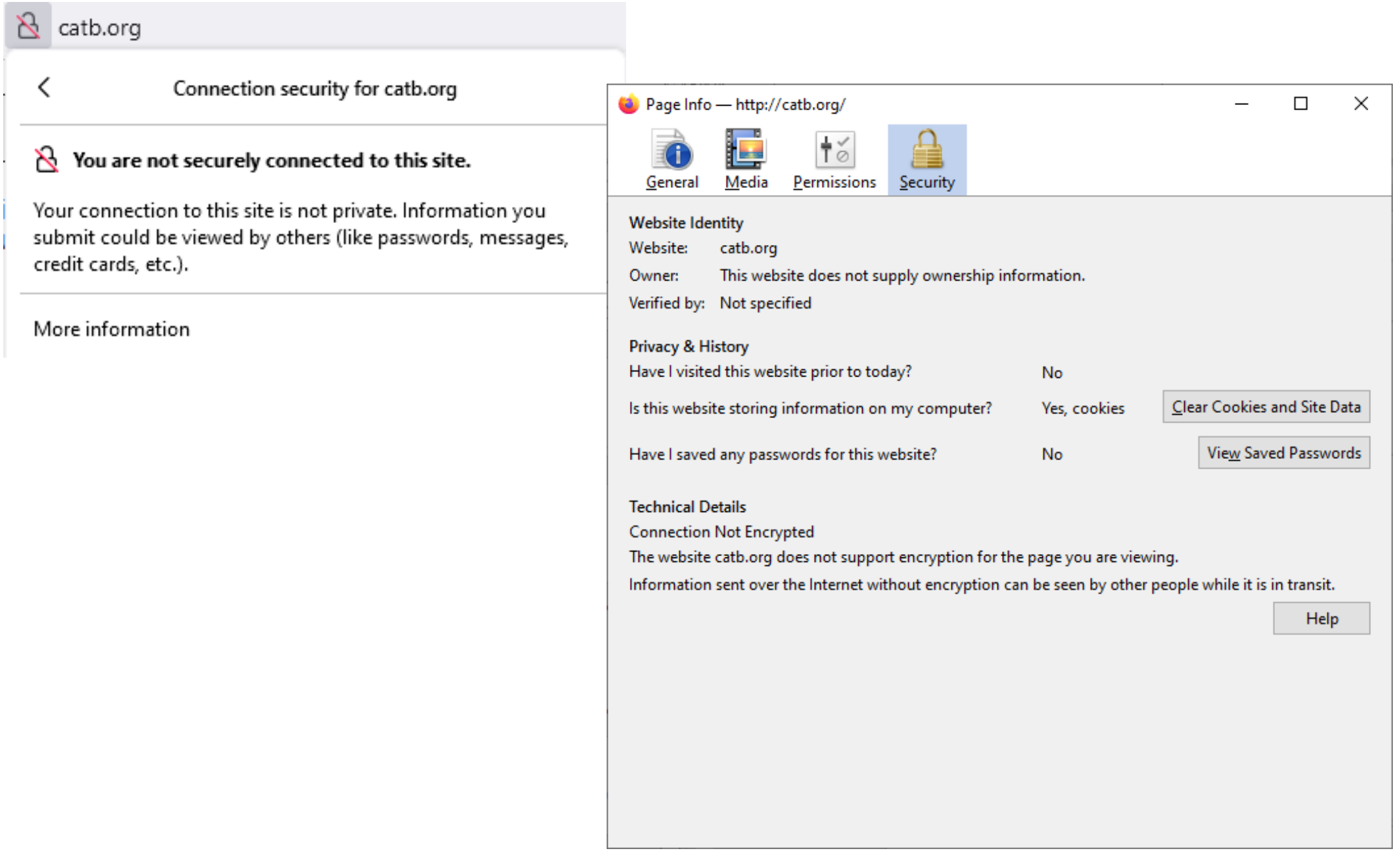
Bagaimana Sertifikat Digital Digunakan untuk Enkripsi Pesan



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

- Contoh webserver yang tidak memiliki sertifikat digital:




catb.org
Connection security for catb.org
You are not securely connected to this site.
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).
More information
Page Info — http://catb.org/
General
Media
Permissions
Security
Website Identity
Website: catb.org
Owner: This website does not supply ownership information.
Verified by: Not specified
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Not Encrypted
The website catb.org does not support encryption for the page you are viewing.
Information sent over the Internet without encryption can be seen by other people while it is in transit.
Help

SELAMAT BELAJAR