



Bahan Kuliah IF4020 Kriptografi

Sertifikat Digital

Oleh: Rinaldi M

Program Studi Teknik Informatika
STEI-ITB
2026

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 dengan mekanisme *challenge and response*.

Mekanisme *challenge* dan *response*

- *Client* mengirim *challenge* ke *server* bank berupa string acak (*nonce*) yang panjangnya 128 bit.

  "F37C2412 8F60E0C8 73BFF201 2E9556B1"

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

- Jika *server* asli, tentu ia mengetahui kunci privatnya sendiri. Lalu, *server* mengenkripsi string tersebut dengan kunci privatnya (yang artinya menandatangani pesan) dan mengirimkan cipherteks kepada *client*.

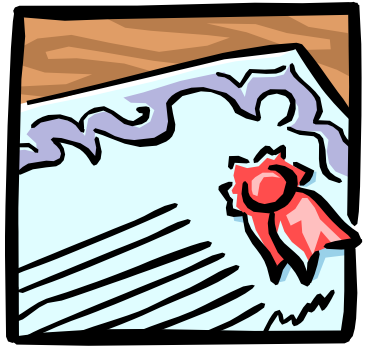
- *Client* kemudian mendekripsi cipherteks dengan kunci publik server. Jika hasilnya sama dengan string acak yang ia kirim, berarti *server* adalah asli.

- Kunci privat bersifat rahasia, hanya diketahui oleh pemilik, tidak dibagi kepada pihak lain, tetapi kunci publik tersedia untuk umum.
- Masalah:
  1. Kunci publik tidak mempunyai suatu kode yang mengidentifikasi pemiliknya.
  2. Kunci publik dapat disalin dan dikirim melalui jaringan.
  3. Penyerang dapat mengganti kunci publik dengan kuncinya sendiri. Penerima sulit memastikan siapa pemilik suatu kunci publik.

- Penyerang 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**.

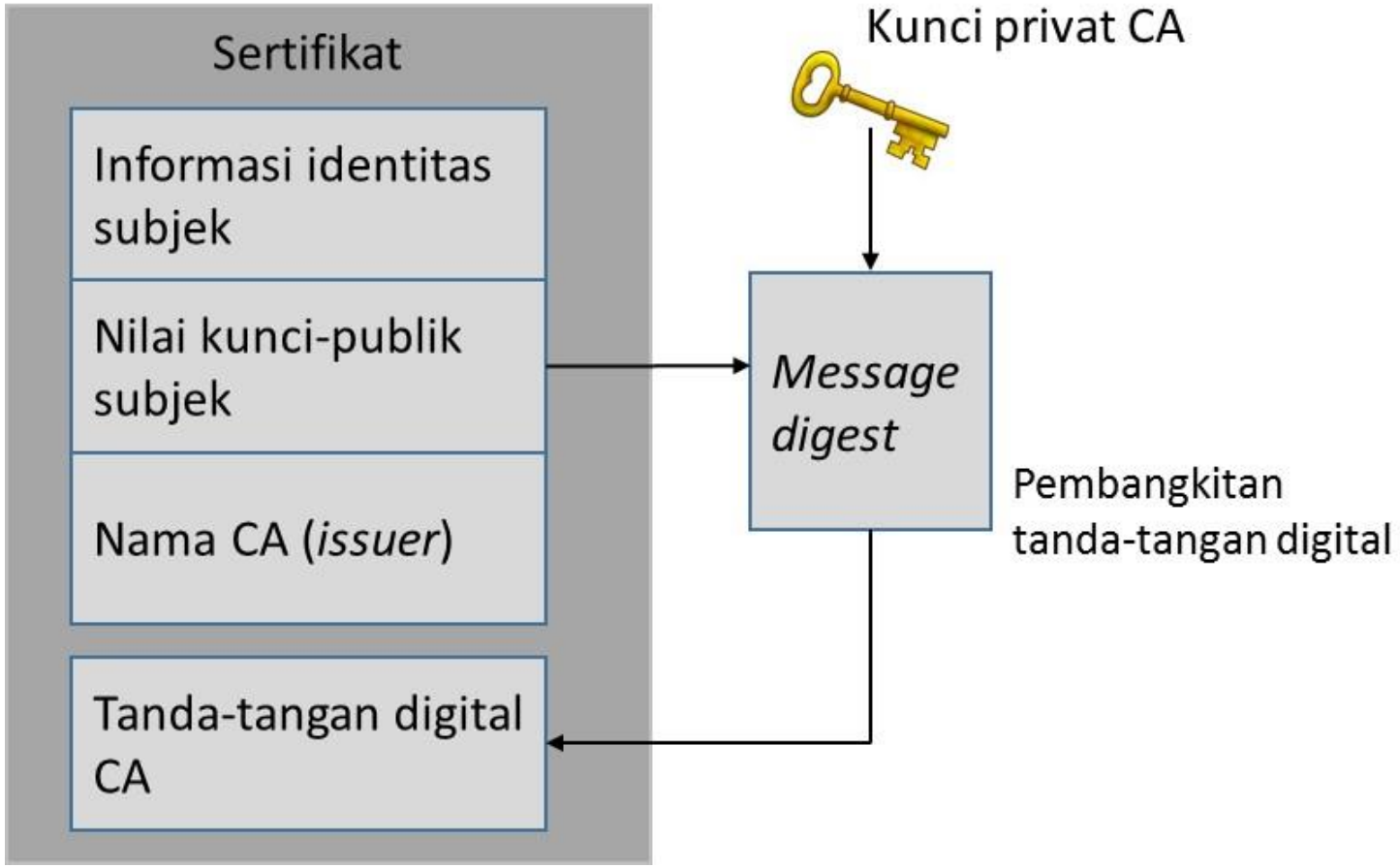
- Sertifikat digital adalah dokumen elektronik yang mengikat kunci publik dengan identitas pemilik kunci.

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

- Sertifikat digital membantu pihak lain membangun kepercayaan saat memeriksa kunci publik.

- 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

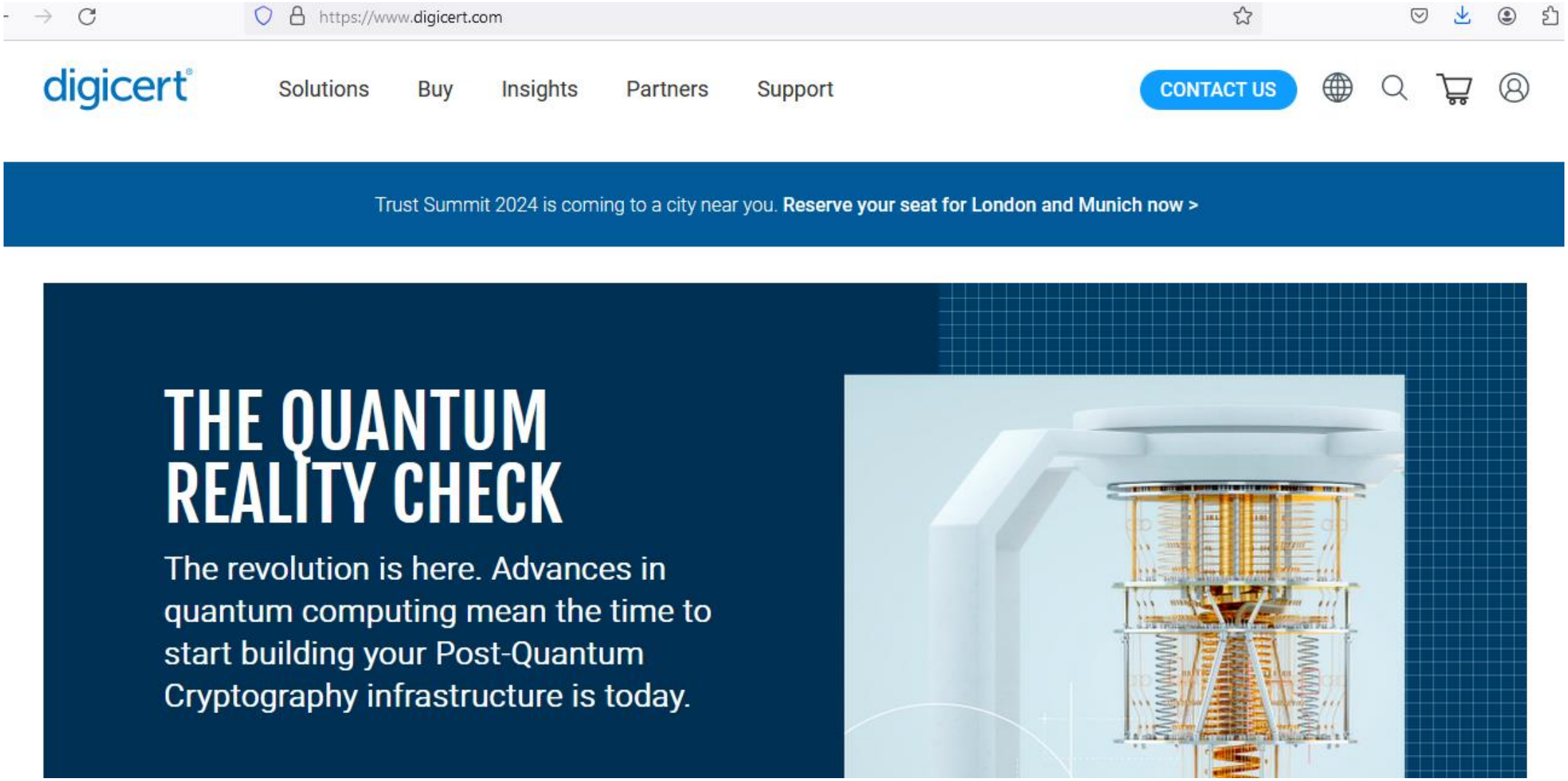


Contoh sebuah sertifikat digital format bebas:

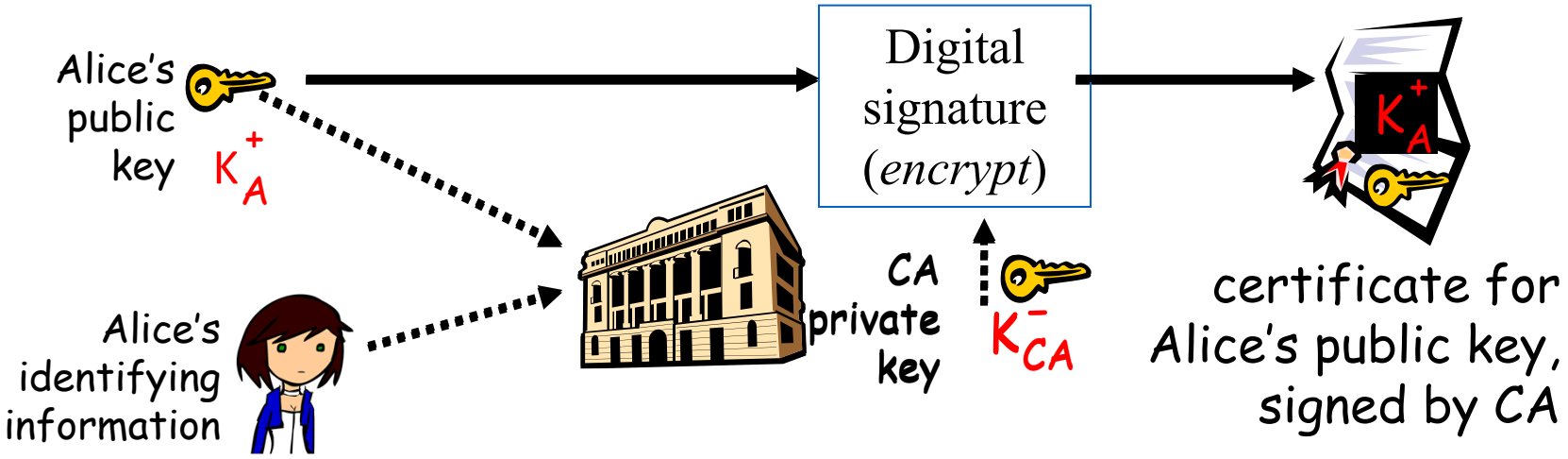


Tanda-tangan CA

- *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

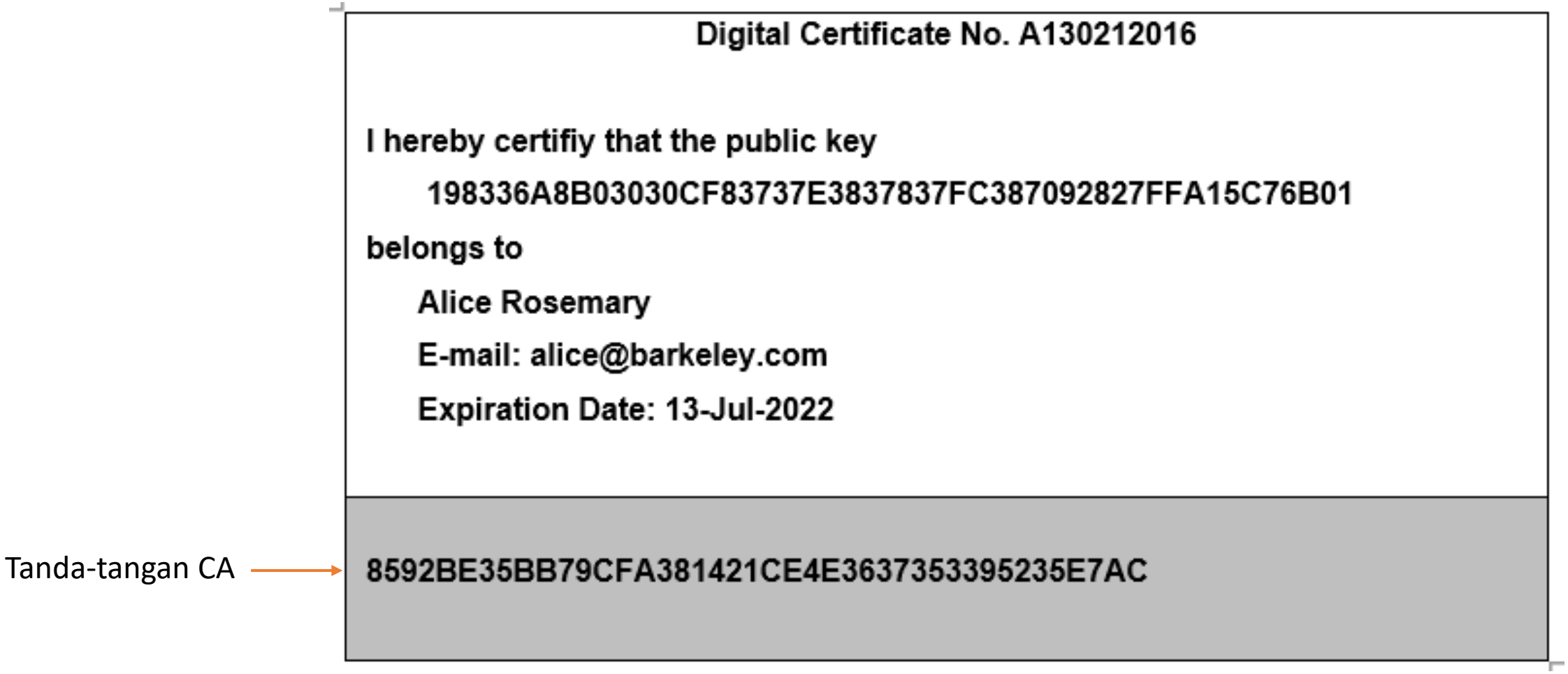
- CA membuat sertifikat digital untuk kunci publik Alice lalu menandatanganinya dengan kunci privat *CA*.

- Caranya:

  1. *CA* membangkitkan nilai *hash* dari kunci publik dan semua informasi terkait identitas pemohon sertifikat. Fungsi *hash* yang digunakan misalnya *SHA-512.*

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

Apa yang dibuktikan oleh sertifikat?

Identitas subjek

Menyatakan identitas atau nama entitas pemilik kunci publik.

Kunci publik

Menyediakan kunci publik dan informasi algoritma yang terkait dengan kunci publik tersebut.

Otorisasi CA

Tanda tangan CA memungkinkan pemeriksa mendeteksi perubahan pada isi sertifikat.

Batas penggunaan

Masa berlaku dan ekstensi membatasi konteks penggunaan sertifikat.

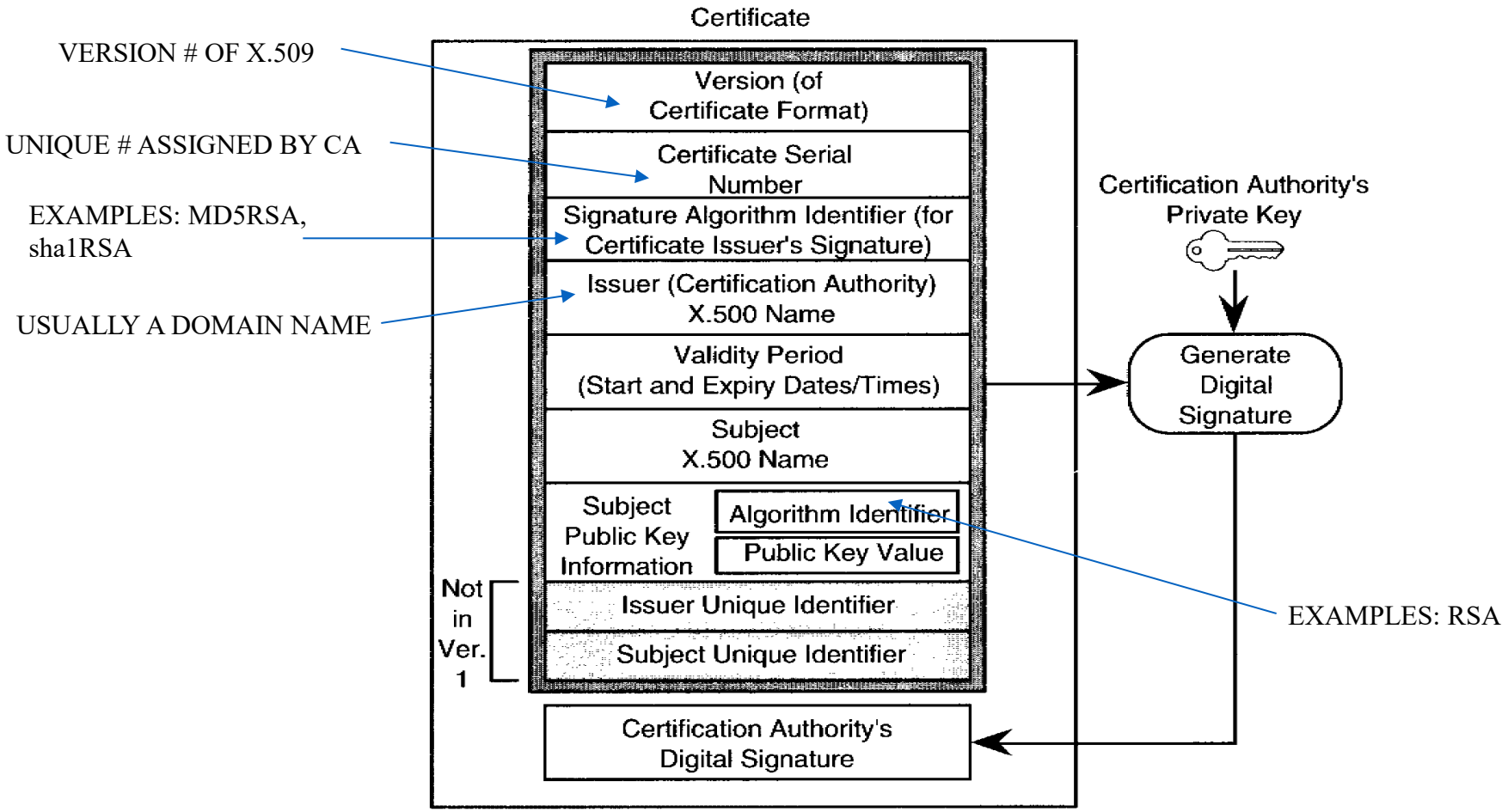
X.509

- Format sertifikat digital yang diterbitkan oleh berbagai CA bisa jadi tidak sama.
- Agar semua sertifikat digital seragam, maka ITU (**International Telecommunication Union)** 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

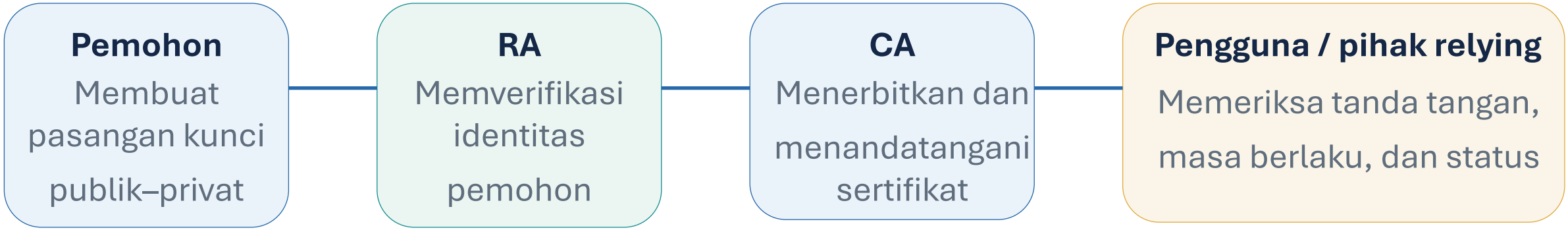


Sumber: MICHAEL I. SHAMOS, Electronic Payment Systems 20-763, Lecture 6 Digital Certificates

Contoh ekstensi penting X.509 v3

Ekstensi	Kegunaan
Subject Alternative Name (SAN)	Nama DNS, alamat IP, atau identitas alternatif yang dilindungi sertifikat.
Key Usage	Membatasi penggunaan kunci, misalnya digitalSignature atau keyEncipherment.
Extended Key Usage (EKU)	Tujuan lebih spesifik, misalnya serverAuth atau clientAuth.
Basic Constraints	Menentukan apakah sertifikat mewakili CA dan batas kedalaman rantai.
Subject Key Identifier / Authority Key Identifier	Membantu mengidentifikasi kunci subjek dan penerbit.
CRL Distribution Points / AIA	Menunjuk lokasi informasi pencabutan atau layanan status sertifikat.

Penerbitan sertifikat digital



Inti proses: identitas diverifikasi → sertifikat diterbitkan → sertifikat didistribusikan → pihak lain memvalidasi.

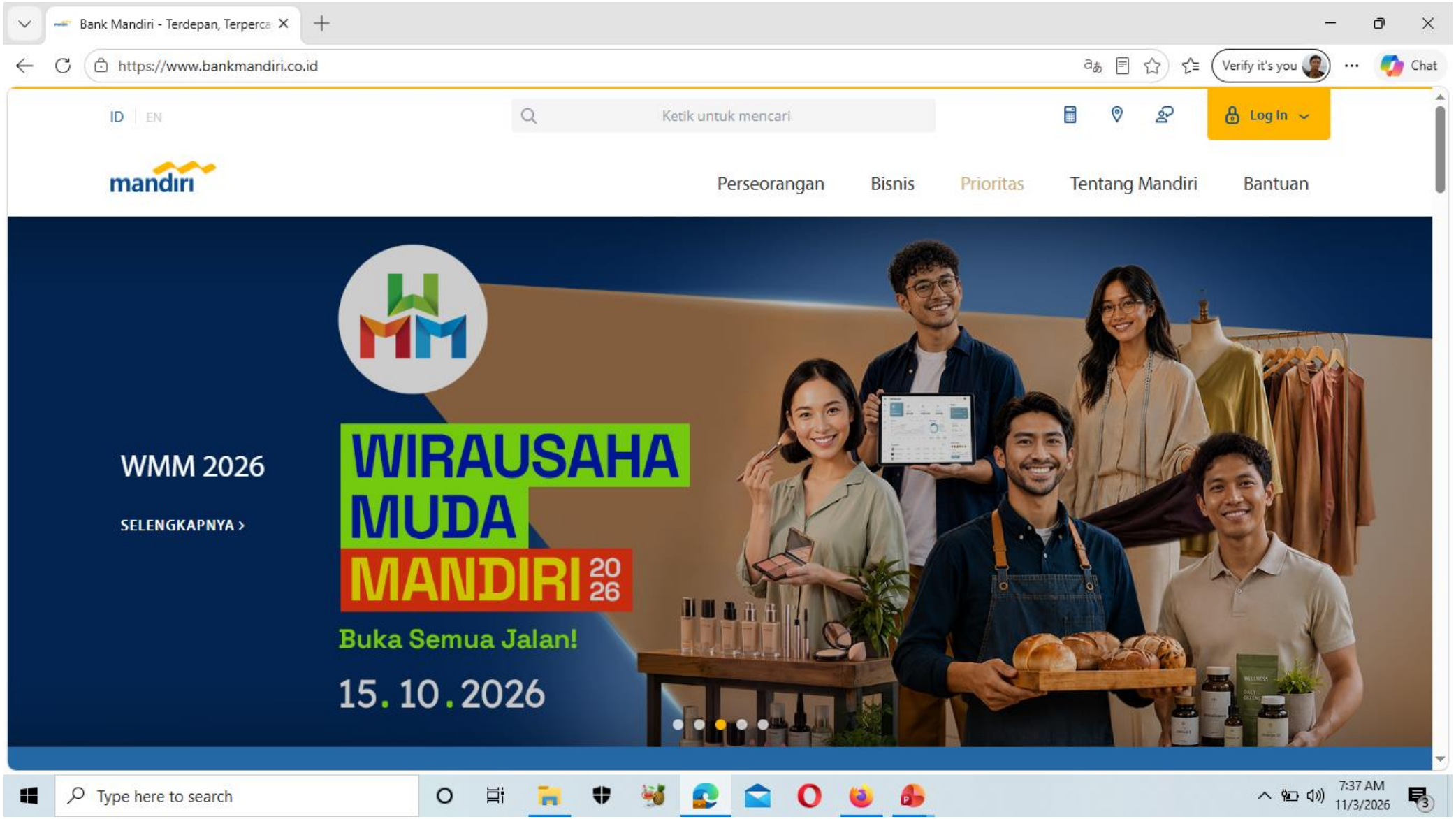
CA = Certification Authority
RA = Registration Authority

Dalam praktik, pembuatan pasangan kunci dapat dilakukan oleh pemohon atau perangkat aman; kunci privat tidak dikirimkan ke CA, hanya kunci public yang dikirim.

Validasi sertifikat oleh penerima

- Memeriksa tanda tangan CA menggunakan kunci publik CA.
- Memeriksa masa berlaku sertifikat dan kecocokan nama/identitas dengan layanan yang diakses.
- Memastikan sertifikat memiliki *Key Usage* yang sesuai.
- Memvalidasi rantai sertifikat hingga *trust anchor* yang dipercaya.
- Memeriksa status pencabutan melalui CRL atau OCSP sesuai kebijakan dan kebutuhan.

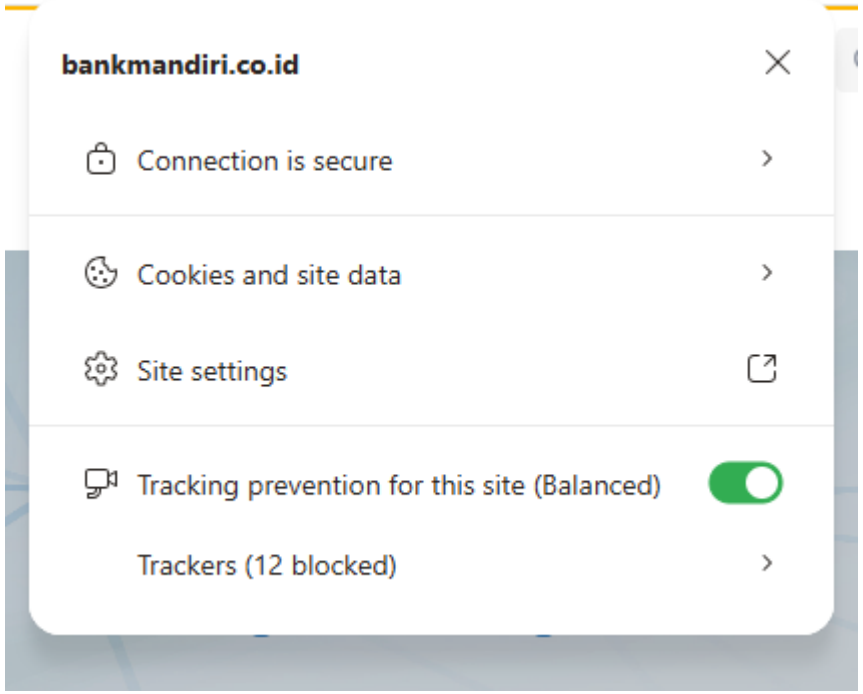
Studi kasus: sertifikat digital untuk server Bank Mandiri *)



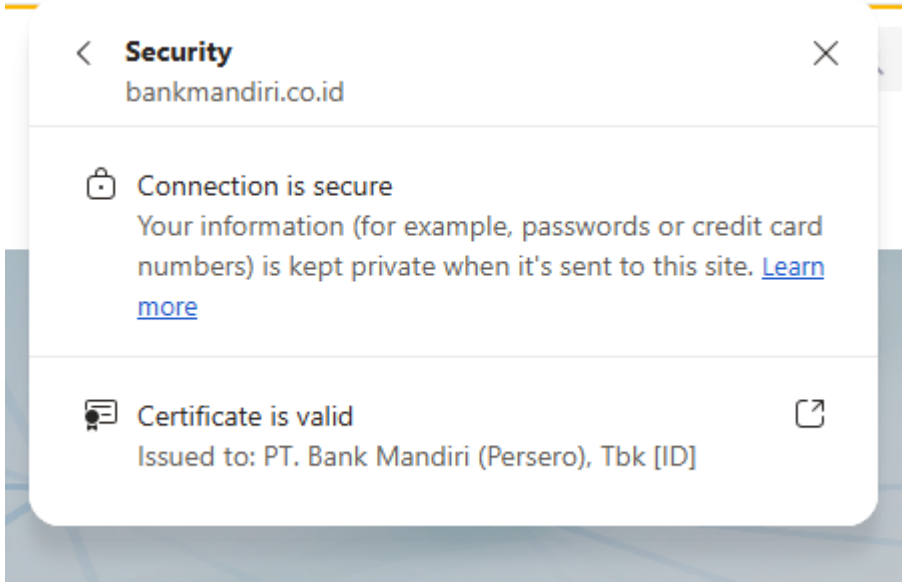
*) Menggunakan browser Microsoft Edge

Klik tanda gambok pada Alamat URL

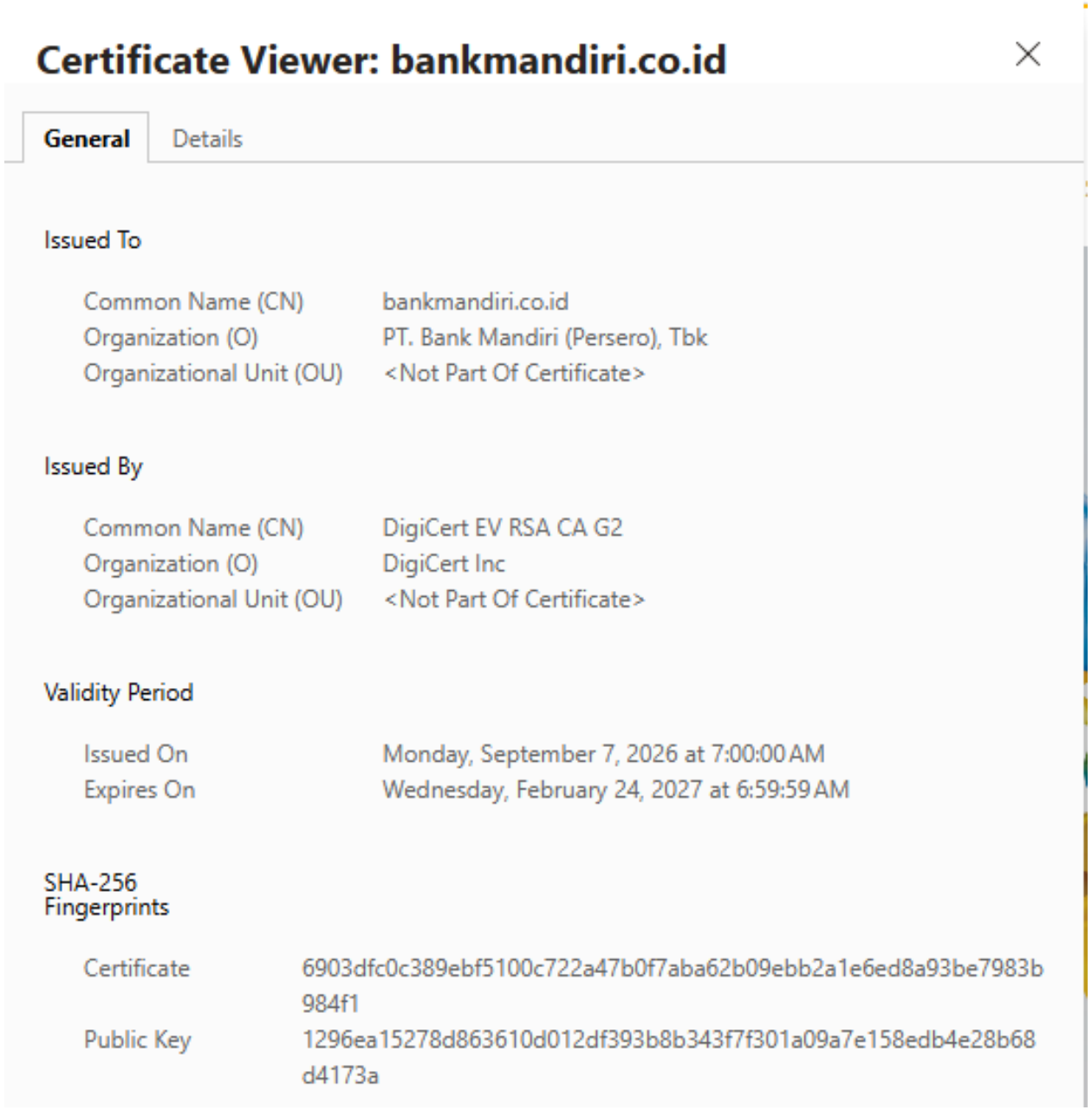




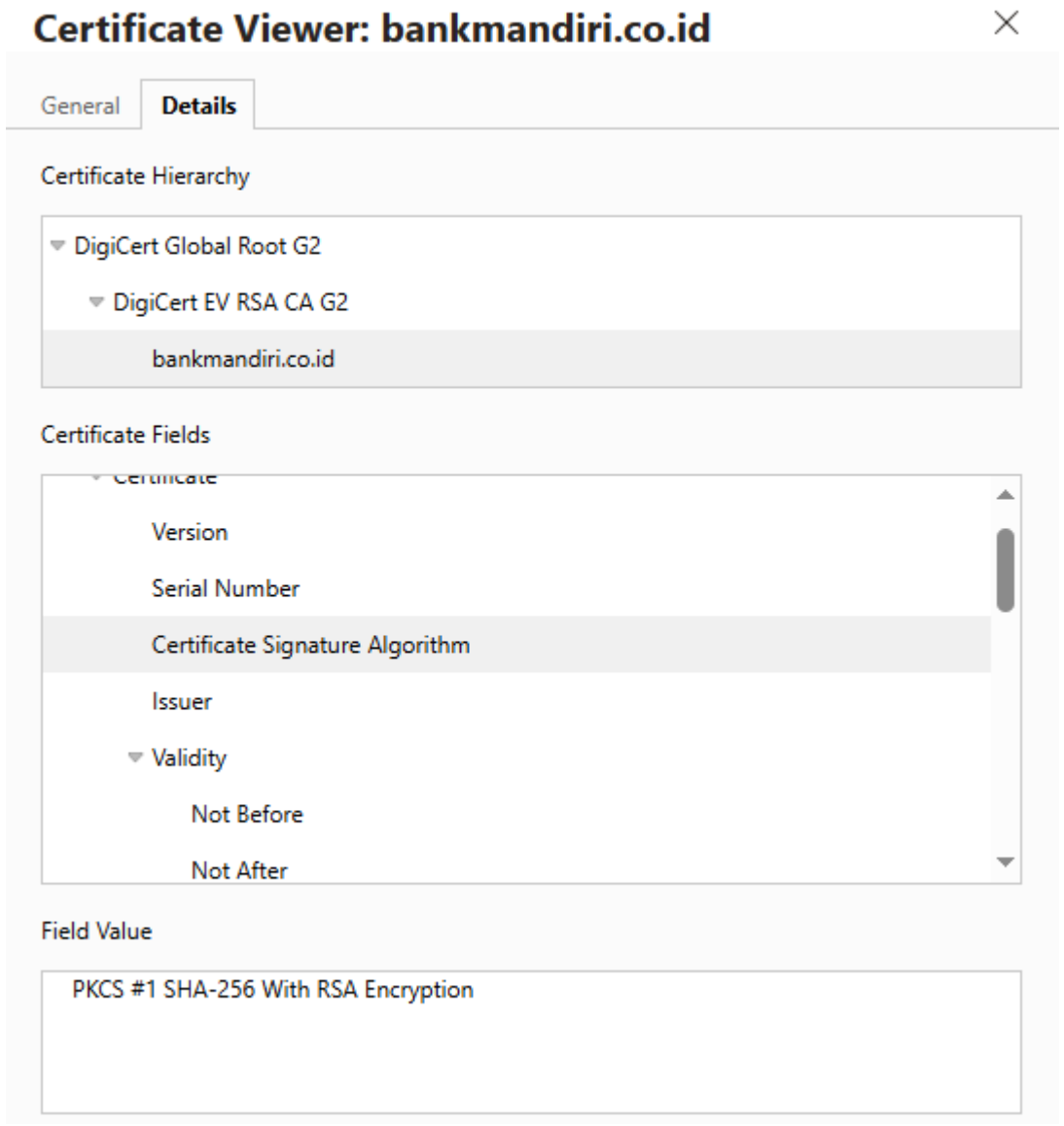
Klik Connection is secure:



Klik icon sertifikat digital:



- Klik details untuk melihat setiap *field*:



Kunci Publik Bank Mandiri:

Modulus (2048 bits):
BD E9 3A 69 8F 72 FD 8E 90 33 42 FD C4 C7 DA 40
0E 36 AF 41 6E 89 81 71 E2 0B FE D4 25 85 17 EA
2C E1 0D 31 A4 44 5F 60 C3 86 63 B1 B5 6C 49 A6
78 B1 81 29 71 DE 10 38 26 CA EE 7F 00 58 11 6B
EB 7D 79 62 41 F1 74 89 31 F7 0E AB 2D B9 A6 18
58 D0 DD B5 28 DF 63 2D 9F 32 1F E2 55 F1 27 99
5A 5D 13 ED 4C E3 88 F9 05 E9 E1 33 15 E6 D9 13
E0 04 07 55 EE 65 B9 E2 15 7C 9E C8 FE BB 91 C6
18 67 32 7D E5 24 6F DF A6 D8 07 EF 82 25 DB D4
EC 33 4E 1F 00 96 25 4F 9A 5C CE 37 52 BF A6 99
DF 76 EB 4E 10 75 CD E7 34 D1 62 99 8A 48 DF 01
D7 D5 3C DA A1 B9 70 BD 36 6C FD 11 E4 6E 93 B2
A1 F4 22 79 54 C7 7A F7 66 3E 2B D3 C3 8A E8 83
14 B8 A0 A1 B3 09 1A 2F 8A 28 37 88 AC 06 D3 2D
E6 49 23 66 3B 8C 43 D5 4B 4D 42 61 80 6C F8 CE
76 75 51 6F BF 90 73 BC F9 D6 0E E5 76 F2 79 DB

Public Exponent (17 bits):
01 00 01

RSA

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

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

Modulus (2048 bits):

```
BD E9 3A 69 8F 72 FD 8E 90 33 42 FD C4 C7 DA 40 0E 36 AF 41 6E 89 81
71 E2 0B FE D4 25 85 17 EA 2C E1 0D 31 A4 44 5F 60 C3 86 63 B1 B5 6C
49 A6 78 B1 81 29 71 DE 10 38 26 CA EE 7F 00 58 11 6B EB 7D 79 62 41
F1 74 89 31 F7 0E AB 2D B9 A6 18 58 D0 DD B5 28 DF 63 2D 9F 32 1F E2
55 F1 27 99 5A 5D 13 ED 4C E3 88 F9 05 E9 E1 33 15 E6 D9 13 E0 04 07
```

n ➡

```
55 EE 65 B9 E2 15 7C 9E C8 FE BB 91 C6 18 67 32 7D E5 24 6F DF A6 D8
07 EF 82 25 DB D4 EC 33 4E 1F 00 96 25 4F 9A 5C CE 37 52 BF A6 99
DF 76 EB 4E 10 75 CD E7 34 D1 62 99 8A 48 DF 01 D7 D5 3C DA A1 B9 70
BD 36 6C FD 11 E4 6E 93 B2 A1 F4 22 79 54 C7 7A F7 66 3E 2B D3 C3 8A
E8 83 14 B8 A0 A1 B3 09 1A 2F 8A 28 37 88 AC 06 D3 2D E6 49 23 66 3B
8C 43 D5 4B 4D 42 61 80 6C F8 CE 76 75 51 6F BF 90 73 BC F9 D6 0E E5
76 F2 79 DB
```

Exponent (17 bits):

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

Tanda-tangan CA
di dalam sertifikat digital

```
02 A0 05 15 45 54 63 AC 97 86 F2 EE DD 1D 8F 5A
40 EF 1F 11 40 AC 5D 2A 5D AC 0D A2 23 FC 63 86
E0 E2 9C 37 CE 10 65 12 03 8C 03 EF F3 C7 38 CC
C3 66 2A 34 C6 68 77 23 A0 3A 8C 4A 55 43 57 88
CB 22 F0 A0 DE 4E 12 95 B6 26 48 78 0F B5 82 E3
36 CE 60 A7 23 CF C3 FE DF 95 1D 5F E1 30 68 05
26 F4 CA C9 A1 31 28 29 41 12 57 2B C9 84 BC CD
F3 8A 1D 9C 6F FA 66 D0 0F 76 9B 28 AC 8F 5A 1A
85 B0 6C 50 B2 FF 21 A1 0E 2D E8 56 45 57 BE 73
B9 FC A8 17 5B 89 6D 30 EE 0C 9A 4C AD F4 27 D8
EE 67 FD 90 90 D7 56 BD 82 19 7C 2D EA 56 72 C3
68 41 36 1A A1 42 61 AD 3C 0C 16 58 39 BA 10 65
0F AA 51 96 7D FE 35 B2 2C 06 97 9B F0 D0 26 0A
76 0A 8C F0 40 DF 81 FE 34 E6 FC F9 CE 9A 5F 15
5D D0 B8 0D D2 6C 26 C6 C6 CF 3A 4B 41 1F 9E FD
B6 0A 58 95 4A 76 61 C8 0B 5C C3 65 C0 0A 0E FC
```

Kunci publik CA:

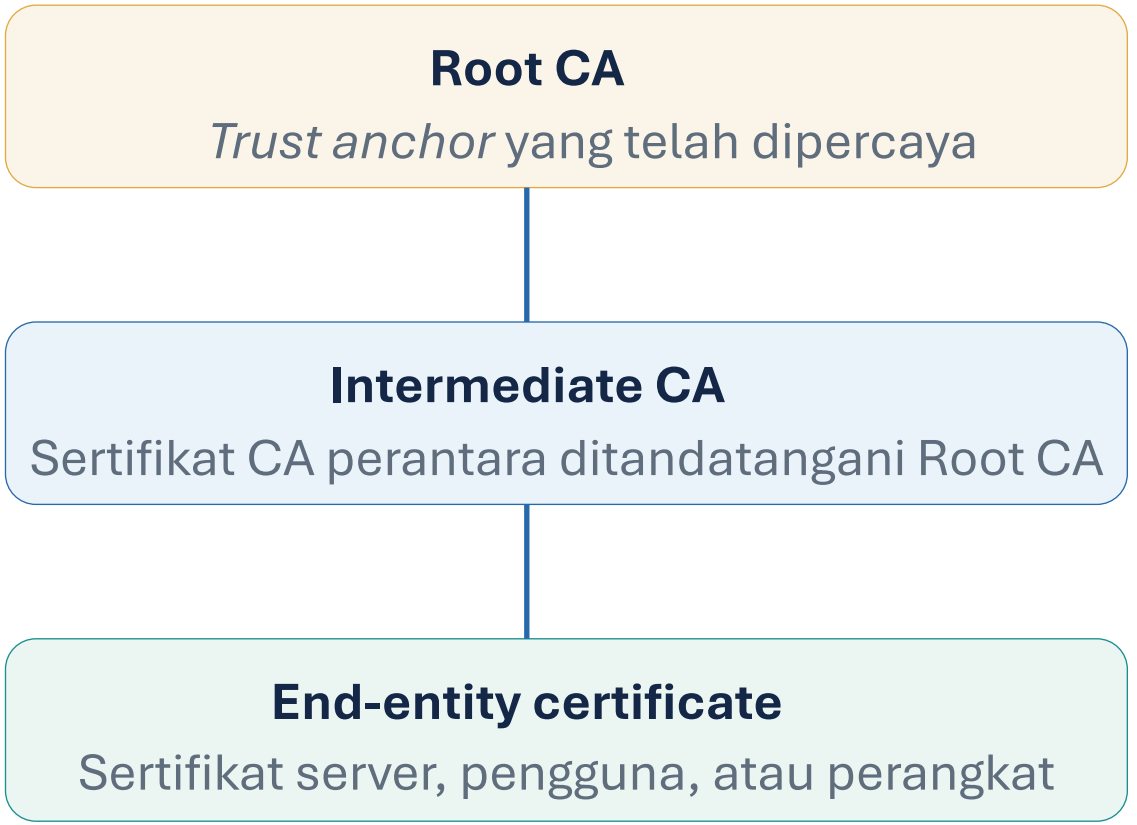
Modulus (2048 bits):

```
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
```

Rantai sertifikat (*certificate chain*)



Setiap sertifikat diverifikasi terhadap penerbitnya; validasi berakhir pada trust anchor yang telah dikonfigurasi.

Rantai sertifikat di dalam Bank Mandiri

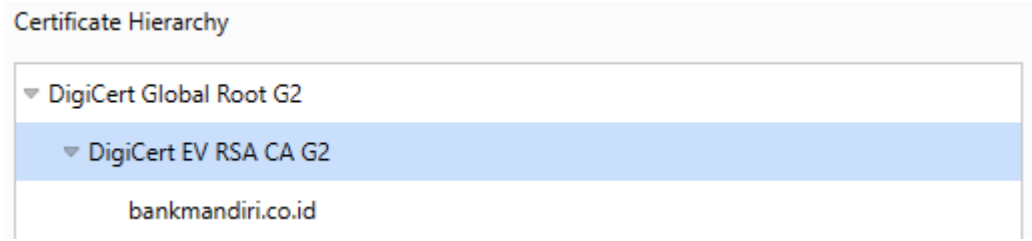


Proses Penggunaan Sertifikat Digital

- 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.

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)

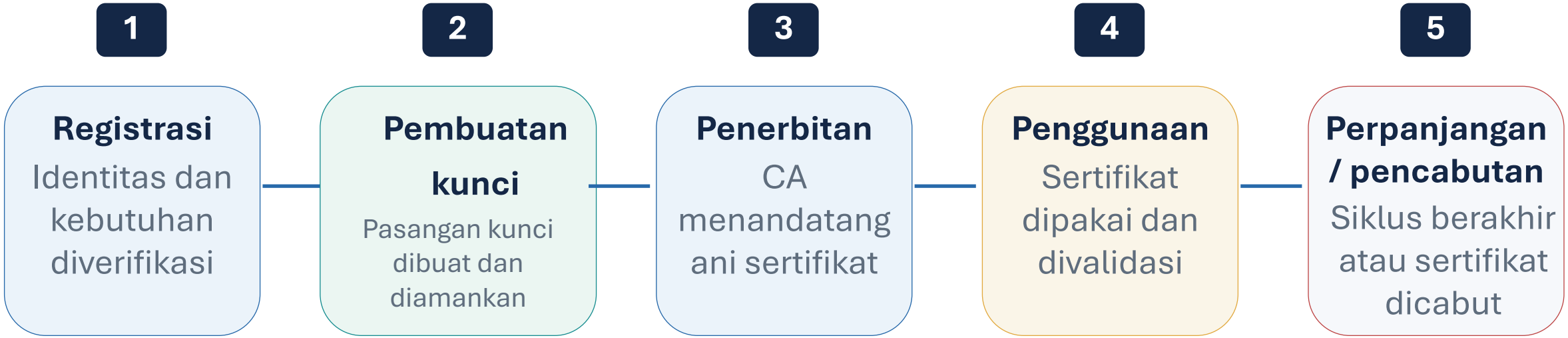
- Sertifikat yang sudah kadaluarsa harus dicabut. Begitu pula sertifikat yang kunci privatnya berhasil diketahui (*revealed*) juga harus dicabut.

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

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

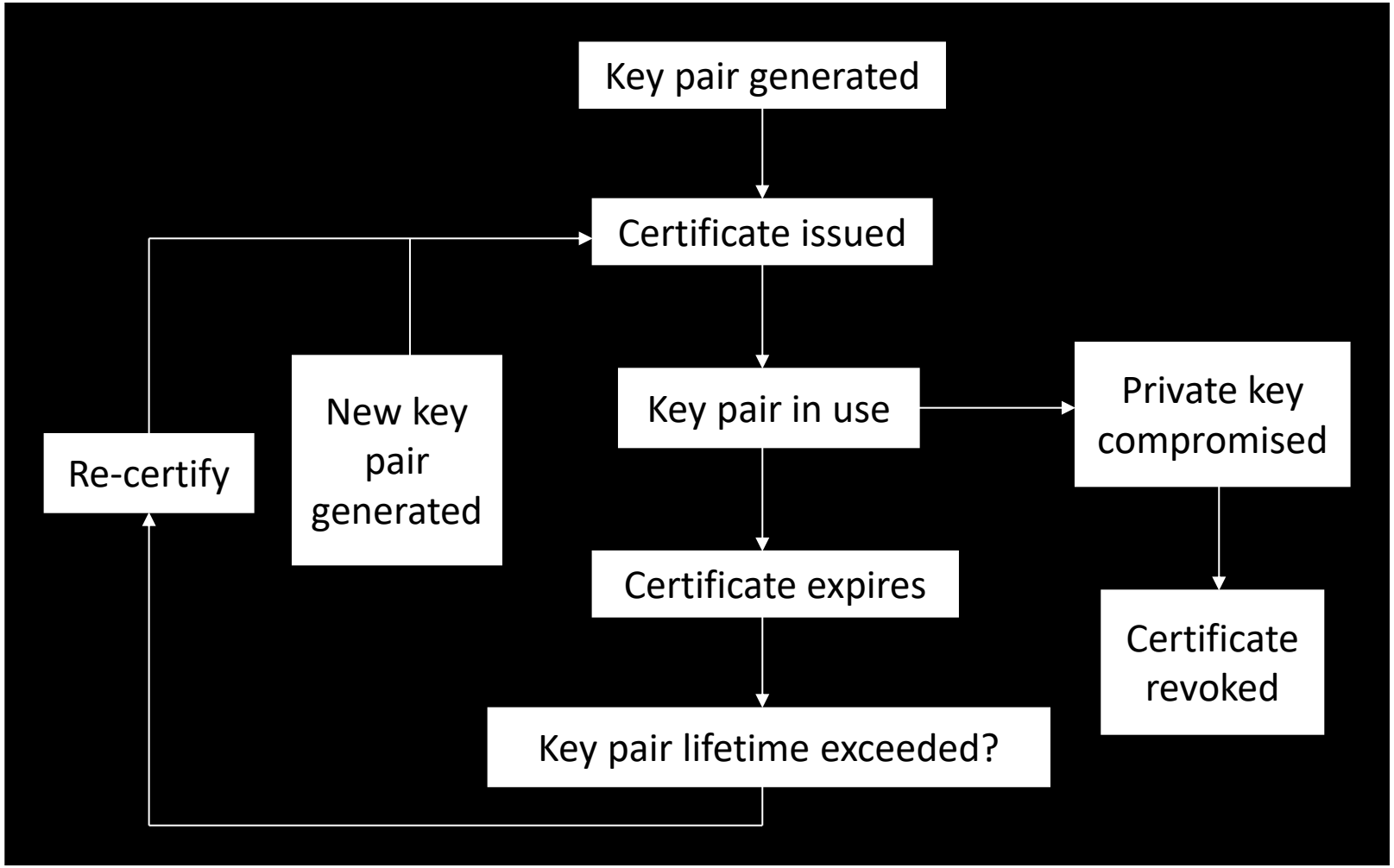
- *Certificate Revocation* List adalah daftar sertifikat yang dicabut. CRL diterbitkan dan ditandatangani oleh CA atau pihak yang berwenang.
- Klien mengunduh CRL dan memeriksa nomor seri sertifikat.

Siklus hidup sertifikat dan kunci



Siklus hidup harus didukung pencatatan, audit, pengelolaan kunci, pembaruan status, dan prosedur pemulihan.

Daur hidup sertifikat digital dan kunci



Dimana Sertifikat Digital Digunakan?

Dalam sejumlah aplikasi internet yang melibatkan:

1. Transport Layer Security (TLS). Protokol komunikasi data yang aman antara *client* dan *server*.
2. Secure Multipurpose Internet Mail Extensions (S/MIME). Standar untuk keamanan email dan *electronic data interchange* (EDI).
3. Secure Electronic Transactions (SET). Protokol untuk keamanan pembayaran elektronik
4. Internet Protocol Secure Standard (IPSec) untuk otentikasi devais di dalam jaringan

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

Contoh penggunaan Sertifikat Digital

HTTPS / TLS

Sertifikat server membantu klien memverifikasi identitas domain dan menegosiasikan koneksi aman.

Email bertanda tangan(S/MIME)

Sertifikat S/MIME dapat mengikat identitas pengirim dengan kunci untuk tanda tangan atau enkripsi email.

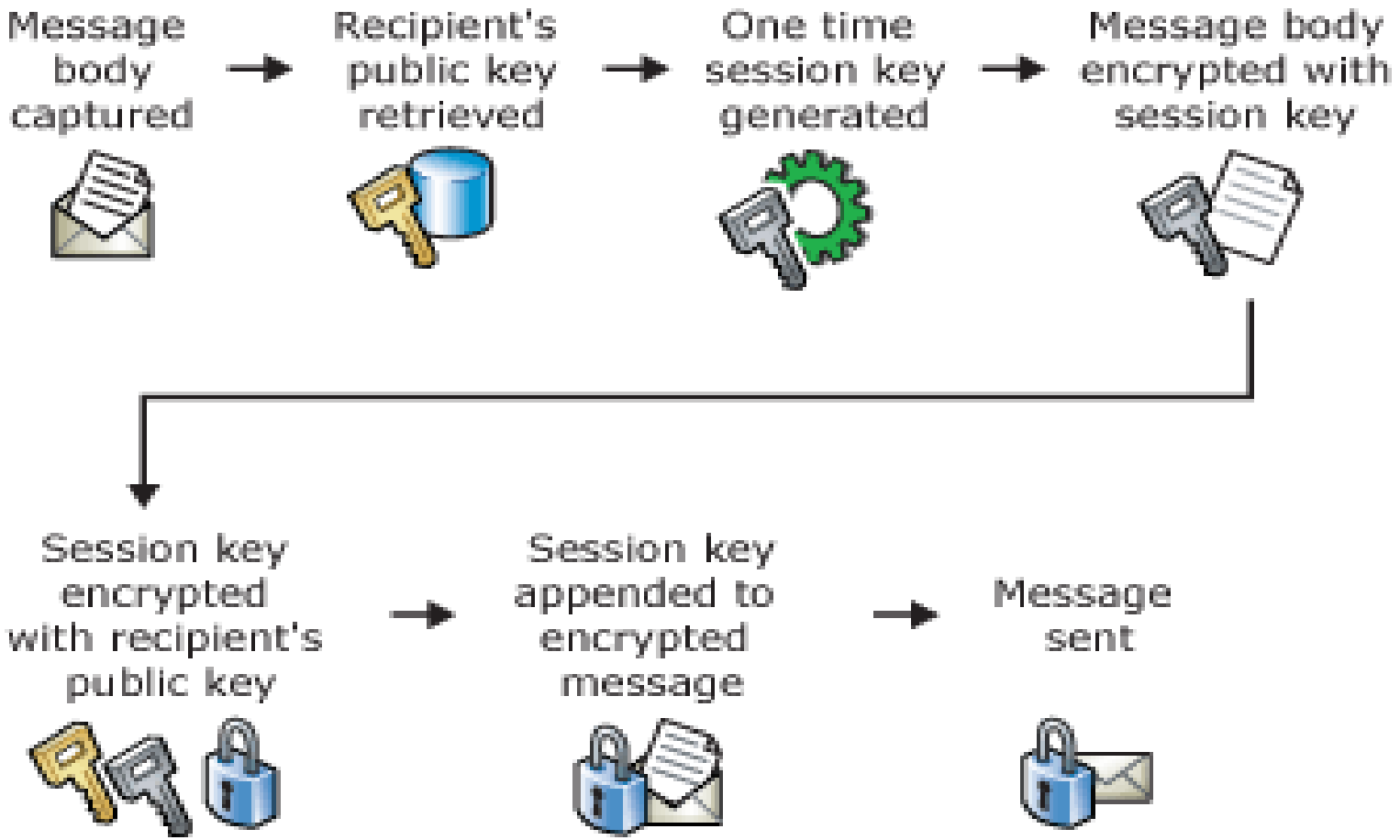
Tanda tangan dokumen

Sertifikat membantu memvalidasi identitas penanda tangan dan integritas dokumen.

Identitas perangkat/IPSec

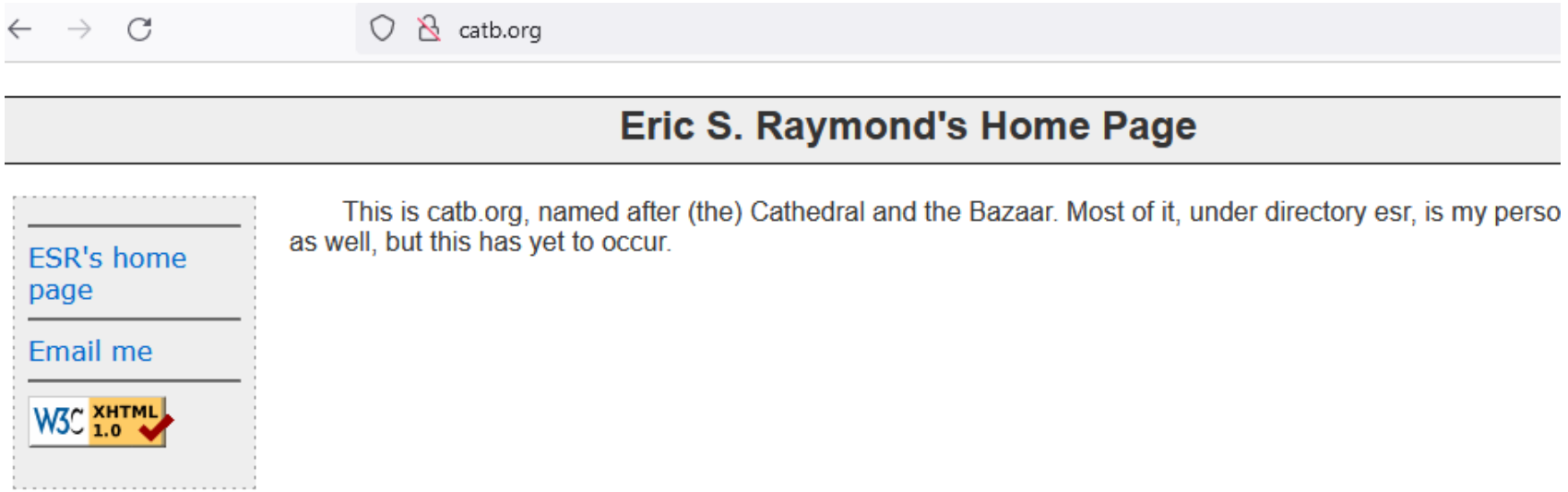
Sertifikat dapat digunakan untuk autentikasi perangkat, layanan, atau pengguna dalam jaringan.

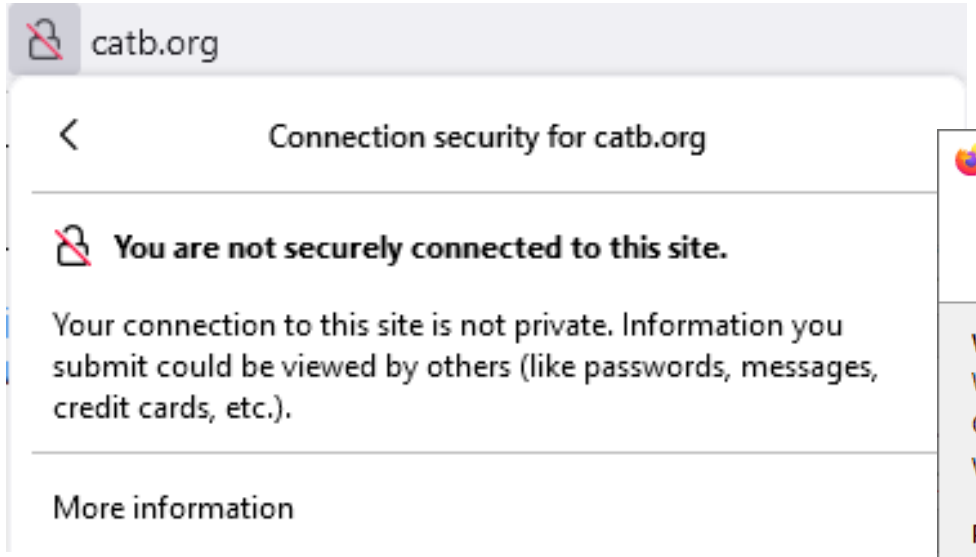
Bagaimana Sertifikat Digital Digunakan untuk Enkripsi Pesan

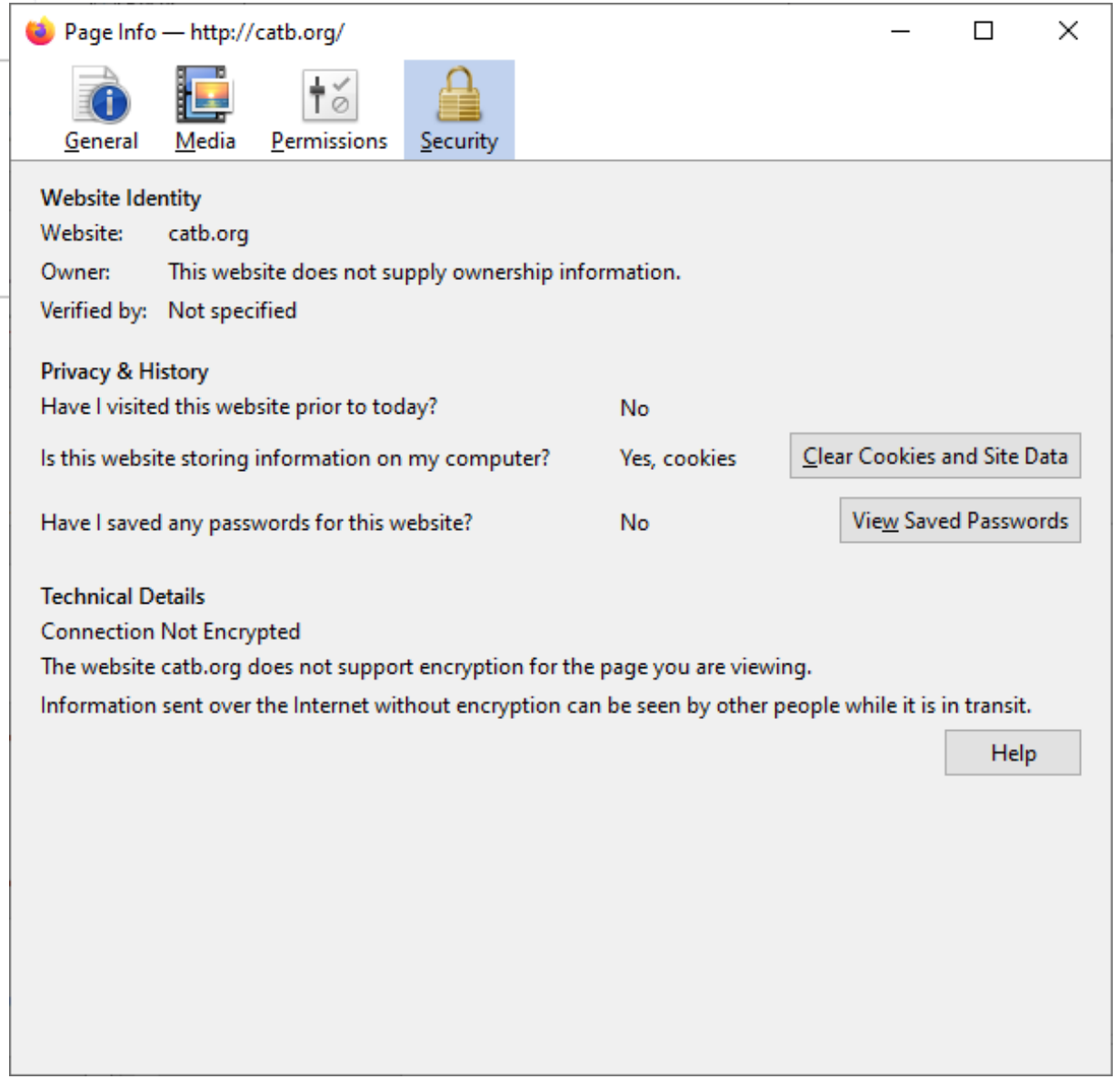


Sumber: **GROUP 11 MEMBERS (**Rackenee Rhule et al, *Digital Certificates*)

- 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