Workshop Honeynet Project
2019

# PEMANFAATAN SERTIFIKAT DIGITAL UNTUK GENERASI MILENIAL

Yon Handri, SST, MM, CISA
Balai Sertifikasi Elektronik

cnnindonesia.com/teknologi/20190807182227-185-419288/milenial-jadi-sasaran-empuk-p...

CNN Indonesia

Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya Hidup CNN TV

Home > Teknologi > Berita Teknologi Informasi

# Milenial Jadi Sasaran Empuk Peretasan

CNN Indonesia | Kamis, 08/08/2019 08:15 WIB

Bagikan :

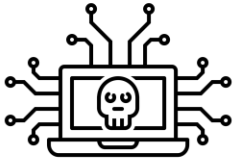
# OUTLINE

- Crypto Magic dengan Standar Kriptografi
- Tantangan 5 Detik Tanda Tangan Digital
- Akses HTTPS di Sosmed dan Online Shopping Aman?
- Aplikasi Kamu Asli, Bajakan atau Jebakan Batman?
- Email ini dijamin 100% Asli bukan Phising

# CRYPTO MAGIC
# DENGAN STANDAR KRIPTOGRAFI

# KARAKTERISTIK SERANGAN SIBER

**Jenis Serangan**



**Mekanisme**

**Aspek Keamanan**

| Man in the middle attacks | Phishing | Rogue software /downloads | Unpatched vulnerabilities | Targeted attacks (APTs) |
|---|---|---|---|---|
| Sertifikat digital SSL Palsu | Tanpa tanda tangan digital dan enkripsi | Code Signing dengan Sertifikat digital palsu | Cookies tidak diamankan , akses kontrol lemah | Konfigurasi keamanan di bawah standar |

**KRITOGRAFI**

**SERTIFIKAT DIGITAL**

Kerahasiaan, autentikasi, integritas data, nir-sangkal dan ketersediaan

# CRYPTOGRAPHY IS EVERYWHERE

GSM

3G

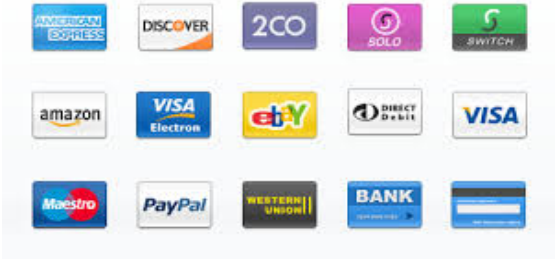










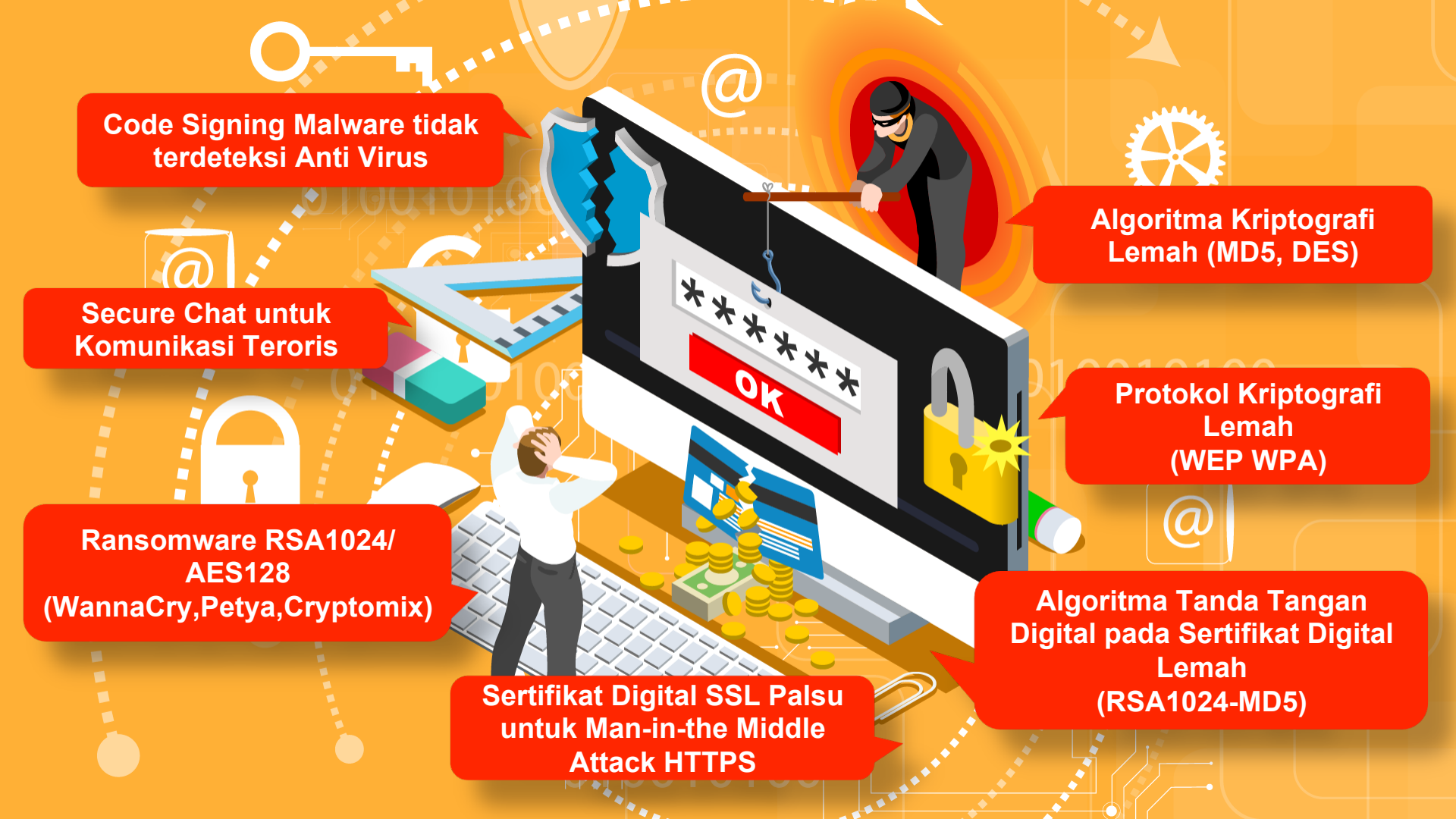







# STANDAR KRIPTOGRAFI

| Date | Minimum of Strength | Symmetric Algorithms | Factoring Modulus | Discrete Logarithm | | Elliptic Curve | Hash (A) | Hash (B) |
|---|---|---|---|---|---|---|---|---|
| | | | | Key | Group | | | |
| (Legacy) | 80 | 2TDEA* | 1024 | 160 | 1024 | 160 | SHA-1** | |
| 2016 - 2030 | 112 | 3TDEA | 2048 | 224 | 2048 | 224 | SHA-224<br>SHA-512/224<br>SHA3-224 | |
| 2016 - 2030 & beyond | 128 | AES-128 | 3072 | 256 | 3072 | 256 | SHA-256<br>SHA-512/256<br>SHA3-256 | SHA-1 |
| 2016 - 2030 & beyond | 192 | AES-192 | 7680 | 384 | 7680 | 384 | SHA-384<br>SHA3-384 | SHA-224<br>SHA-512/224 |
| 2016 - 2030 & beyond | 256 | AES-256 | 15360 | 512 | 15360 | 512 | SHA-512<br>SHA3-512 | SHA-256<br>SHA-512/256<br>SHA-384<br>SHA-512<br>SHA3-512 |


Code Signing Malware tidak terdeteksi Anti Virus
Secure Chat untuk Komunikasi Teroris
Ransomware RSA1024/ AES128 (WannaCry,Petya,Cryptomix)
Sertifikat Digital SSL Palsu untuk Man-in-the Middle Attack HTTPS
Algoritma Kriptografi Lemah (MD5, DES)
Protokol Kriptografi Lemah (WEP WPA)
Algoritma Tanda Tangan Digital pada Sertifikat Digital Lemah (RSA1024-MD5)
******
Ok

# CRYPTO MAGIC BEGINS….

- Standar Kriptografi : Hash Function MD5
- Konsep : Perubahan 1 bit akan merubah nilai Hash
- Contoh :
  - “Jemput Aku Jam 8” → 90917202FCFEA7385D45710C27C0928C
  - “Jemput Aku Jam 9” → 38071F394BDFB5673584DE79468FE9AA
- Tools : MD5Checker

# SIM SALABIM.. PILIHAN KAMU ADALAH...

# TANTANGAN 5 DETIK
# TANDA TANGAN DIGITAL

File Edit View Window Help

LAMPIRAN KEPUTUSAN REKTOR UNIVERSITAS INDONESIA NOMOR 660 /SK/R/UI/2019 TENTANG TARIF UANG KULIAH TUNGGAL (UKT) BAGI MAHASISWA PROGRAM SARJANA (S1) KELAS REGULER UNIVERSITAS INDONESIA ANGKATAN TAHUN AKADEMIK 2019/2020

**Tarif Uang Kuliah Tunggal (UKT) Bagi Mahasiswa Program Sarjana (S1) Kelas Reguler Universitas Indonesia Angkatan Tahun Akademik 2019/2020**

I. Tarif Uang Kuliah Tunggal Biaya Operasional Pendidikan Berkeadilan (BOP-B) adalah sebagai berikut (dalam rupiah):

| Kelas | Rumpun Sains Teknologi dan Kesehatan (IPA) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. 5.000.000 |
| 6 | >5.000.000 s.d. 6.500.000 |
| 7 | >6.500.000 s.d. <7.500.000 |
| 8 | 7.500.000 |

| Kelas | Rumpun Sosial Humaniora (IPS) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. <5.000.000 |
| 6 | 5.000.000 |

File Edit View Window Help

LAMPIRAN KEPUTUSAN REKTOR UNIVERSITAS INDONESIA NOMOR 660 /SK/R/UI/2019 TENTANG TARIF UANG KULIAH TUNGGAL (UKT) BAGI MAHASISWA PROGRAM SARJANA (S1) KELAS REGULER UNIVERSITAS INDONESIA ANGKATAN TAHUN AKADEMIK 2019/2020

**Tarif Uang Kuliah Tunggal (UKT) Bagi Mahasiswa Program Sarjana (S1) Kelas Reguler Universitas Indonesia Angkatan Tahun Akademik 2019/2020**

I. Tarif Uang Kuliah Tunggal Biaya Operasional Pendidikan Berkeadilan (BOP-B) adalah sebagai berikut (dalam rupiah):

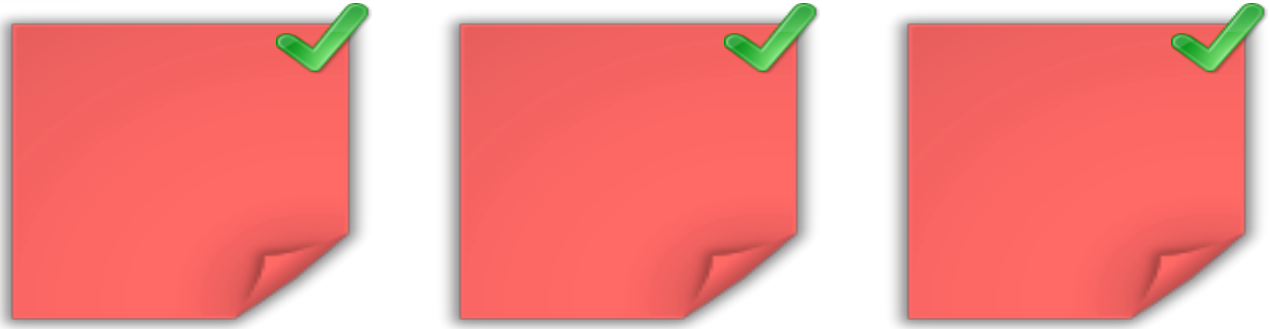
| Kelas | Rumpun Sains Teknologi dan Kesehatan (IPA) |
|---|---|
| 1 | 0 s.d. 700.000 |
| 2 | >700.000 s.d. 1.200.000 |
| 3 | >1.200.000 s.d. 2.700.000 |
| 4 | >2.700.000 s.d. 4.200.000 |
| 5 | >4.200.000 s.d. 5.200.000 |
| 6 | >5.200.000 s.d. 6.700.000 |
| 7 | >6.700.000 s.d. <7.700.000 |
| 8 | 7.500.000 |

| Kelas | Rumpun Sosial Humaniora (IPS) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. <5.000.000 |
| 6 | 5.000.000 |

**MANA DOKUMEN ASLI?**

# TTE TIDAK TERSERTIFIKASI (SCAN)

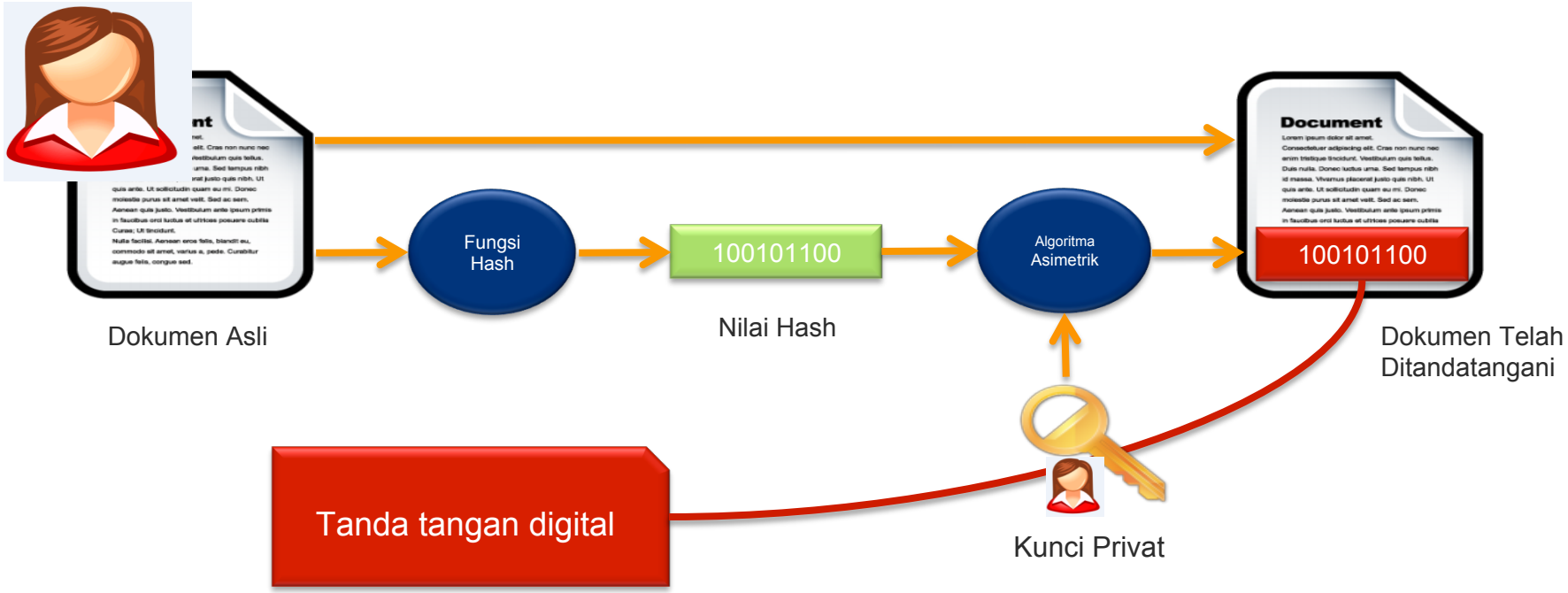
Dokumen Asli



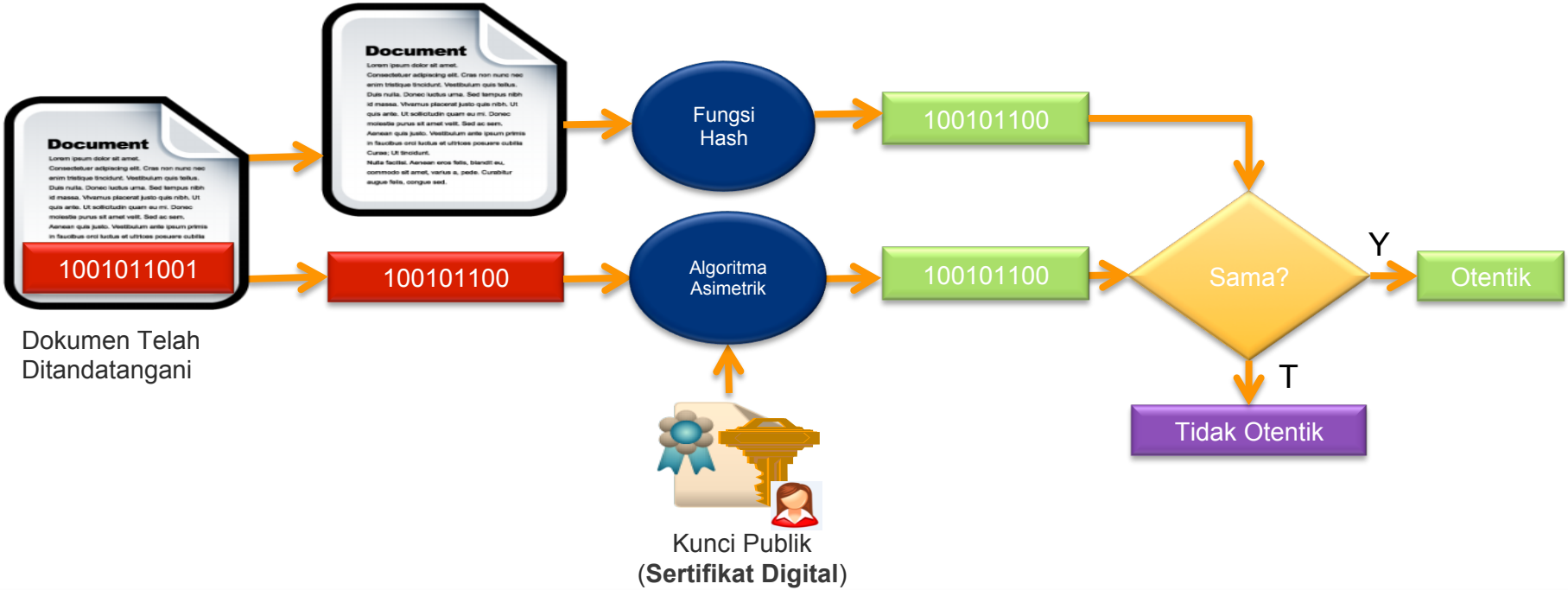
Dokumen Palsu

Pihak tidak bertanggung jawab dapat menggunakan **tanda tangan elektronik** untuk **memalsukan dokumen** sehingga sulit dibuktikan ke**asli**annya

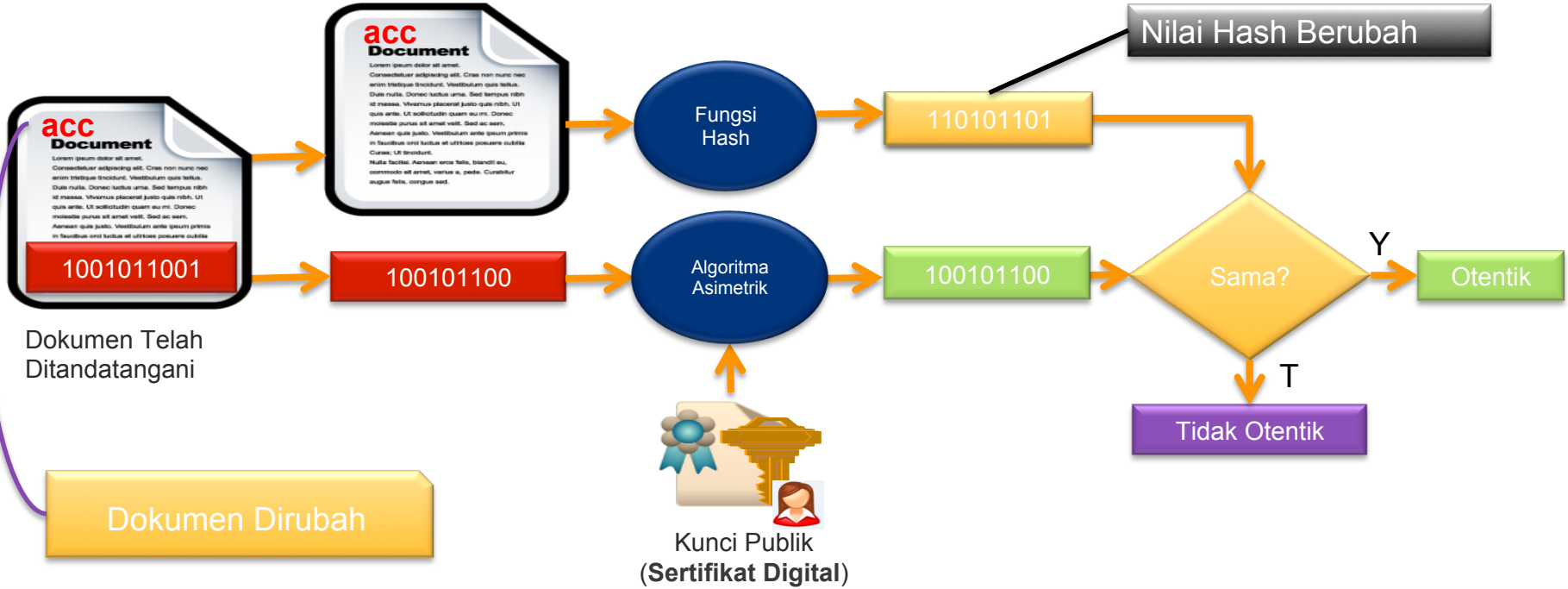
# PROSES PENANDATANGANAN



# PROSES VERIFIKASI (1)



# PROSES VERIFIKASI (2)



# TTE TERSERTIFIKASI (TT DIGITAL)


Dokumen Asli


Dokumen Palsu

**Tanda tangan digital** bersifat **unik** untuk setiap dokumen yang ditandatangani sehingga **sulit** untuk dipalsukan (di-copy) ke dokumen lainnya

Signed and all signatures are valid. Signature Panel

LAMPIRAN KEPUTUSAN REKTOR UNIVERSITAS INDONESIA NOMOR 660 /SK/R/UI/2019 TENTANG TARIF UANG KULIAH TUNGGAL (UKT) BAGI MAHASISWA PROGRAM SARJANA (S1) KELAS REGULER UNIVERSITAS INDONESIA ANGKATAN TAHUN AKADEMIK 2019/2020

**Tarif Uang Kuliah Tunggal (UKT) Bagi Mahasiswa Program Sarjana (S1) Kelas Reguler Universitas Indonesia Angkatan Tahun Akademik 2019/2020**

I. Tarif Uang Kuliah Tunggal Biaya Operasional Pendidikan Berkeadilan (BOP-B) adalah sebagai berikut (dalam rupiah):

| Kelas | Rumpun Sains Teknologi dan Kesehatan (IPA) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. 5.000.000 |
| 6 | >5.000.000 s.d. 6.500.000 |
| 7 | >6.500.000 s.d. <7.500.000 |
| 8 | 7.500.000 |

| Kelas | Rumpun Sosial Humaniora (IPS) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. <5.000.000 |
| 6 | 5.000.000 |

At least one signature is invalid. Signature Panel

LAMPIRAN KEPUTUSAN REKTOR UNIVERSITAS INDONESIA NOMOR 660 /SK/R/UI/2019 TENTANG TARIF UANG KULIAH TUNGGAL (UKT) BAGI MAHASISWA PROGRAM SARJANA (S1) KELAS REGULER UNIVERSITAS INDONESIA ANGKATAN TAHUN AKADEMIK 2019/2020

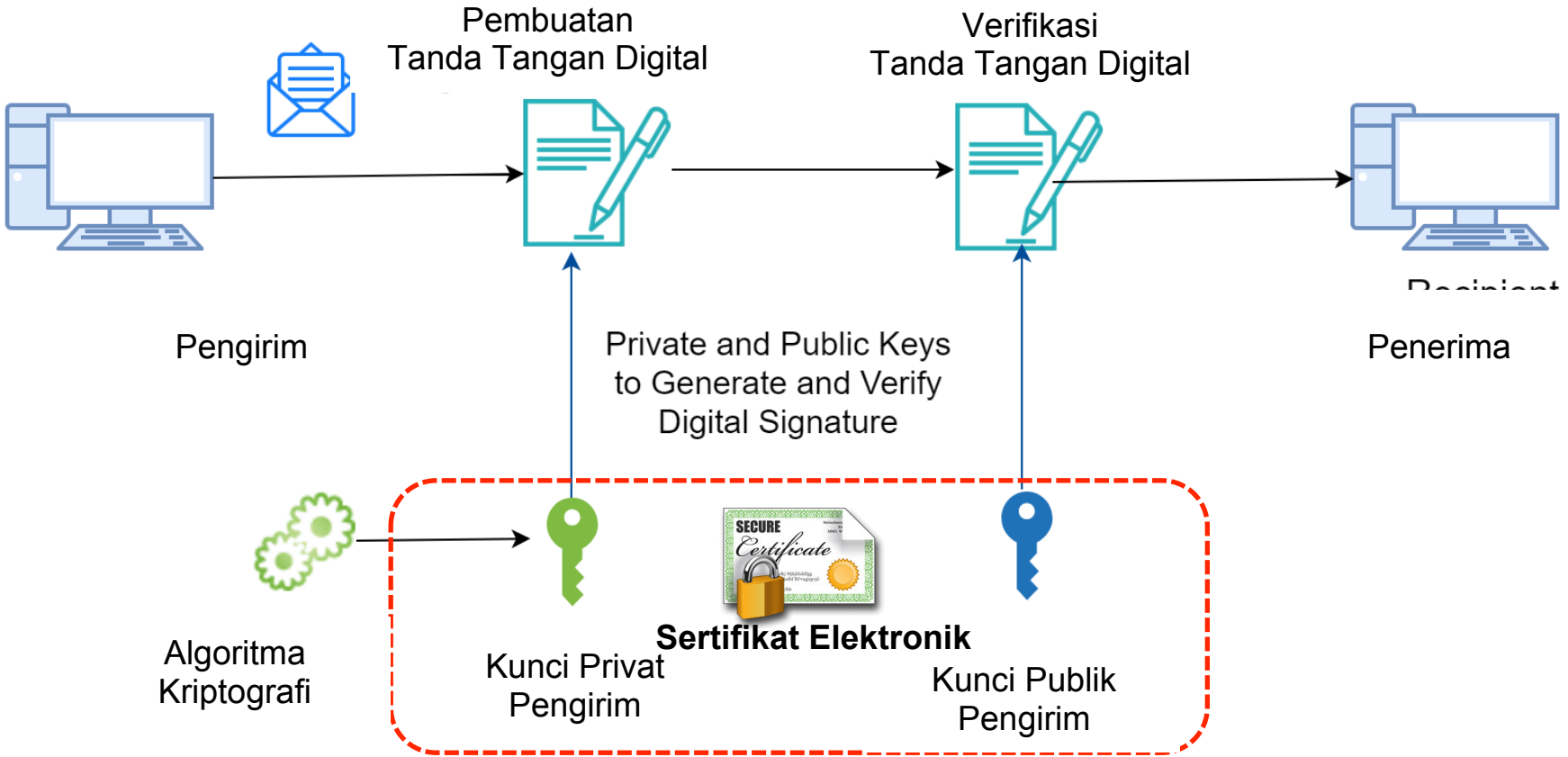
**Tarif Uang Kuliah Tunggal (UKT) Bagi Mahasiswa Program Sarjana (S1) Kelas Reguler Universitas Indonesia Angkatan Tahun Akademik 2019/2020**

I. Tarif Uang Kuliah Tunggal Biaya Operasional Pendidikan Berkeadilan (BOP-B) adalah sebagai berikut (dalam rupiah):

| Kelas | Rumpun Sains Teknologi dan Kesehatan (IPA) |
|---|---|
| 1 | 0 s.d. 700.000 |
| 2 | >700.000 s.d. 1.200.000 |
| 3 | >1.200.000 s.d. 2.700.000 |
| 4 | >2.700.000 s.d. 4.200.000 |
| 5 | >4.200.000 s.d. 5.200.000 |
| 6 | >5.200.000 s.d. 6.700.000 |
| 7 | >6.700.000 s.d. <7.700.000 |
| 8 | 7.500.000 |

| Kelas | Rumpun Sosial Humaniora (IPS) |
|---|---|
| 1 | 0 s.d. 500.000 |
| 2 | >500.000 s.d. 1.000.000 |
| 3 | >1.000.000 s.d. 2.500.000 |
| 4 | >2.500.000 s.d. 4.000.000 |
| 5 | >4.000.000 s.d. <5.000.000 |
| 6 | 5.000.000 |

# Teknologi Tanda Tangan Digital



# DEFINISI SERTIFIKAT ELEKTRONIK

| Name | Date modi... | Type | Size |
|---|---|---|---|
| botan.dll | 06/12/201... | Application extens... | 1.785 KB |
| ca.pem | 05/04/201... | Privacy Enhanced ... | 2 KB |
| EKO YON HANDRI.crt | 07/04/201... | Security Certificate | 2 KB |
| EKO YON HANDRI.p12 | 07/04/201... | Personal Informati... | 4 KB |
| EKO YON HANDRI-csr.pem | 07/04/201... | Privacy Enhanced ... | 2 KB |
| EKO YON HANDRI-priv.pem | 07/04/201... | Privacy Enhanced ... | 2 KB |
| libbz2.dll | 25/10/201... | Application extens... | 118 KB |
| libeay32.dll | 24/01/201... | Application extens... | 1.328 KB |
| libeay32MD.dll | 27/01/201... | Application extens... | 1.310 KB |
| LOCK 1.0.exe | 201... | Application | 1.218 KB |
| openssl.exe | 201... | Application | 502 KB |
| QtCore4.dll | 06/10/201... | Application extens... | 2.538 KB |
| QtGui4.dll | 27/06/201... | Application extens... | 8.381 KB |
| QtNetwork4.dll | 27/06/201... | Application extens... | 1.029 KB |

EKO YON HANDRI (198305212003121005_Proteksi Email dan Tanda Tangan Digital)

**EKO YON HANDRI (198305212003121005_Proteksi Email dan Tanda Tangan Digital)**
Issued by: OSD LU Kelas 2
Expires: Wednesday, March 17, 2021 at 08:49:37 Western Indonesia Time
This certificate is valid

▶ Trust
▼ Details

Subject Name
Description 198305212003121005_Proteksi Email dan Tanda Tangan Digital
Email Address yon.handri@bssn.go.id
Common Name EKO YON HANDRI
Organizational Unit Balai Sertifikasi Elektronik
Organization Badan Siber dan Sandi Negara
Locality Jakarta Selatan
State/Province DKI Jakarta
Country ID

**Identitas Pemilik**

Issuer Name
Common Name OSD LU Kelas 2
Organization Lembaga Sandi Negara
Country ID

**Penerbit**

Serial Number 4132709044706344333
Version 3

Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )
Parameters none

Not Valid Before Monday, March 18, 2019 at 08:49:37 Western Indonesia Time
Not Valid After Wednesday, March 17, 2021 at 08:49:37 Western Indonesia Time

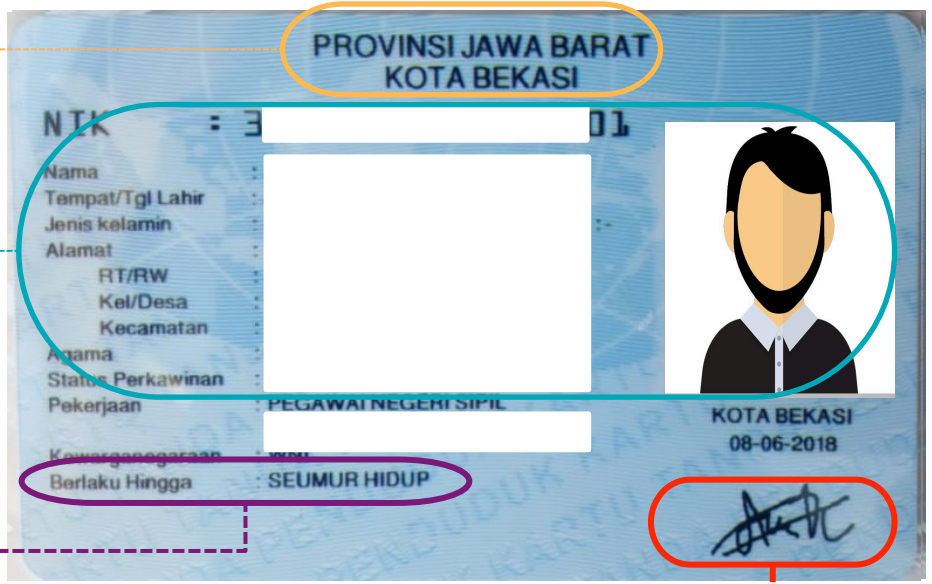
**Masa Berlaku**

Public Key Info
Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )
Parameters none
Public Key 256 bytes : BE 29 E4 A8 23 33 0A 87 ...
Exponent 65537
Key Size 2048 bits
Key Usage Verify, Wrap, Derive

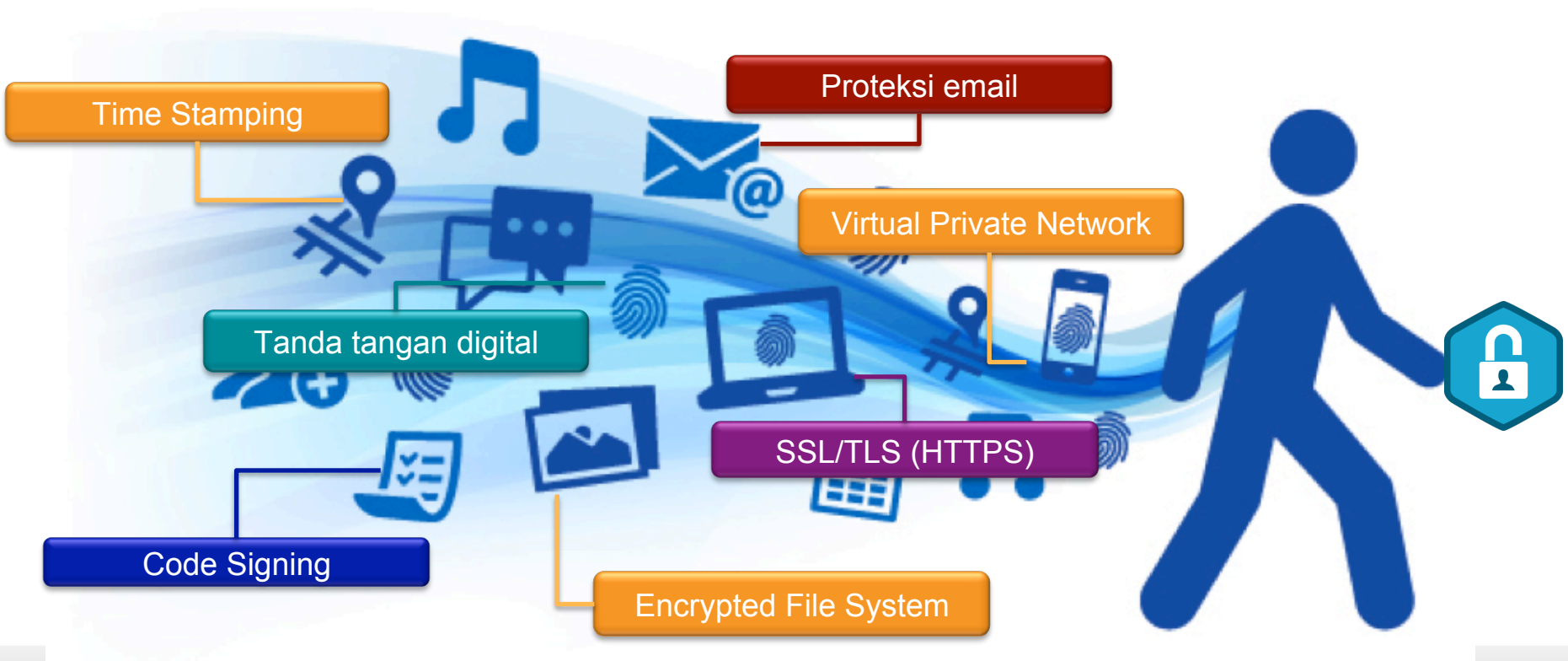
Signature 256 bytes : 3D 35 AB A9 03 83 A9 53 ...

**Tanda Tangan**

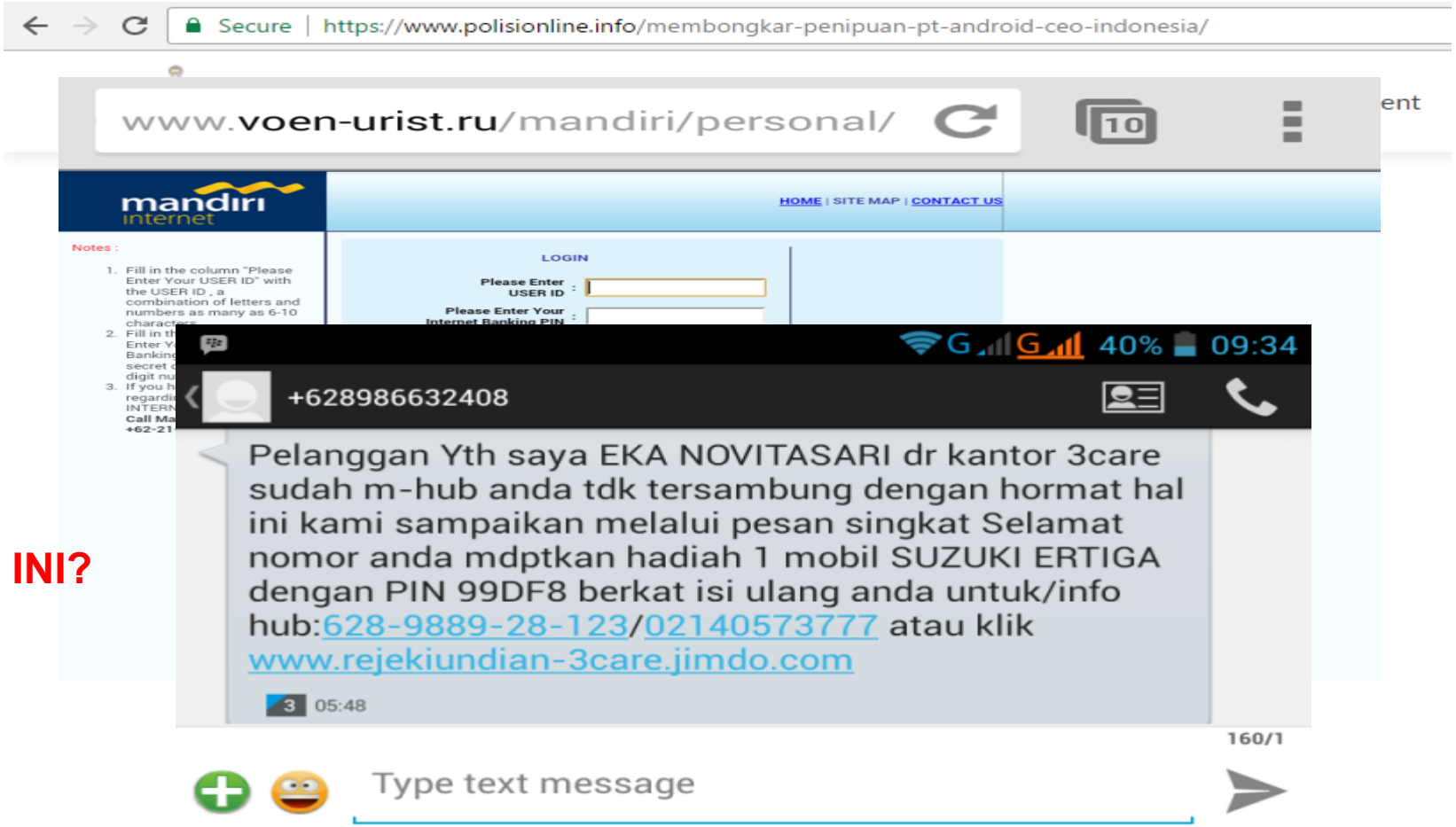
SHA256
RSA-2048



# KEGUNAAN SERTIFIKAT DIGITAL



# AKSES HTTPS DI SOSMED DAN ONLINE SHOPPING AMAN?


Secure | https://www.polisionline.info/membongkar-penipuan-pt-android-ceo-indonesia/
www.voen-urist.ru/mandiri/personal/
mandiri internet
HOME | SITE MAP | CONTACT US
LOGIN
Please Enter USER ID :
Please Enter Your Internet Banking PIN :
Notes :
1. Fill in the column "Please Enter Your USER ID" with the USER ID , a combination of letters and numbers as many as 6-10 characters
2. Fill in the column "Please Enter Your Internet Banking PIN" with the secret code of 6 digit numbers
3. If you have any questions regarding INTERNET BANKING please Call Ma... +62-21...
40% 09:34
+628986632408
Pelanggan Yth saya EKA NOVITASARI dr kantor 3care sudah m-hub anda tdk tersambung dengan hormat hal ini kami sampaikan melalui pesan singkat Selamat nomor anda mdptkan hadiah 1 mobil SUZUKI ERTIGA dengan PIN 99DF8 berkat isi ulang anda untuk/info hub:628-9889-28-123/02140573777 atau klik www.rejekiundian-3care.jimdo.com
05:48
160/1
Type text message

**MAU KLIK INI?**

# How does HTTPS work: SSL explained

*This presumes that SSL has already been issued by SSL issuing authority.*

*3. Website Records found. Going to the Host Web Server.*

*4. Requesting Secure SSL connection from Website Host.*


*2. Check DNS records for IP address to find website host.*

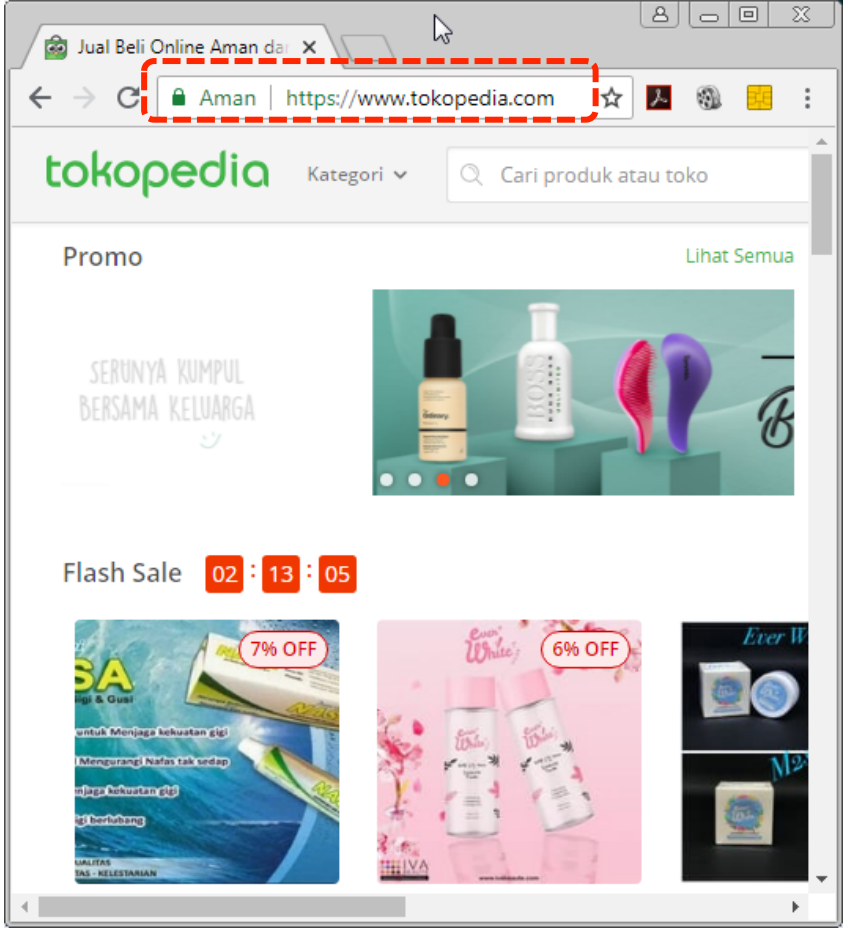
*5. Host responds with valid SSL certificate.*




*1. User accessing secure site.*

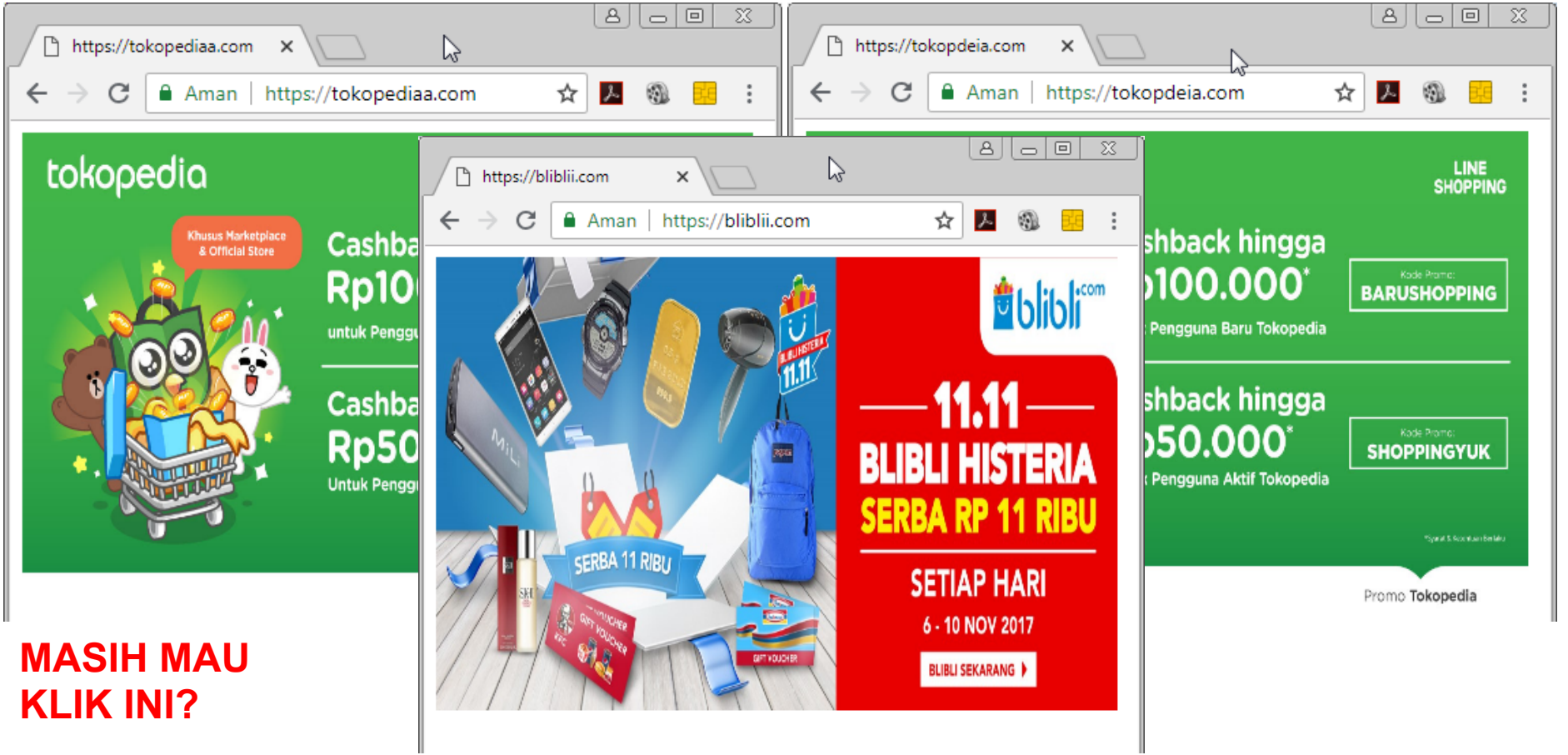
*6. Secure connection is now established. Transferred data is encrypted.*


www.voen-urist.ru/mandiri/personal/
mandiri internet
HOME | SITE MAP | CONTACT US
Notes :
1. Fill in the column "Please Enter Your USER ID" with the USER ID , a combination of letters and numbers as many as 6-10 characters
2. Fill in the column "Please Enter Your Internet Banking PIN" with the secret code number , 6 digit number
3. If you have any questions regarding MANDIRI INTERNET, please contact Call Mandiri at 14000 or +62-21-5299-7777.
LOGIN
Please Enter USER ID :
Please Enter Your Internet Banking PIN :
Please Enter Your Email :
Please Enter Your Phone Number :
RESET
SEND
Use Token PIN Mandiri for financial transaction
Norton SECURED powered by VeriSign
ABOUT SSL CERTIFICATES
New User / Re-registration
Please click here to activate your Mandiri Internet services.
Forgot USER ID / PIN LOGIN?
Please click here for the activation.
My Security
For your security, please keep your User ID and Internet Banking PIN for yourself. Do not tell your User ID and PIN to anyone, including bank personnel. Bank Mandiri will never ask for those information, either through e-mail, printed mail, SMS or any other method. If your receive such e-mail, printed mail or SMS asking for your User ID and PIN, please notify us immediately at mandiri call 14000 or (+6221) 5299 7777
Situs Palsu
Menggunakan Sertifikat Digital Server Authentication
Situs Asli
PT. BANK MANDIRI (PERSERO) TBK. [ID] https://ib.bankmandiri.co.id/retail/Login.do?a
Apl
Folder baru
Dev
Save to Mendel...
mandiri internet
HOME | SITE MAP | CONTACT US
Notes :
1. Fill in the column "Please Enter Your USER ID" with the USER ID , a combination of letters and numbers as many as 6-10 characters
2. Fill in the column "Please Enter Your Internet Banking PIN" with the secret code number , 6 digit number
3. If you have any questions regarding MANDIRI INTERNET, please contact Call Mandiri at 14000 or +62-21-5299-7777.
LOGIN
Please Enter USER ID :
Please Enter Your Internet Banking PIN :
RESET
SEND
Use Token PIN Mandiri for financial transaction
Norton SECURED powered by VeriSign
ABOUT SSL CERTIFICATES
New User / Re-registration
Please click here to activate your Mandiri Internet services.
Forgot USER ID / PIN LOGIN?
Please click here for the activation.
My Security
For your security, please keep your User ID and Internet Banking PIN for yourself. Do not tell your User ID and PIN to anyone, including bank personnel. Bank Mandiri will never ask for those information, either through e-mail, printed mail, SMS or any other method. If your receive such e-mail, printed mail or SMS asking for your User ID and PIN, please notify us immediately at mandiri call 14000 or (+6221) 5299 7777


**HTTPS**

- meningkatkan kepercayaan transaksi / pertukaran informasi
- menjaga informasi sensitif selama proses pengiriman data melalui Internet dengan cara dienkripsi
- Jaminan dengan adanya sertifikat digital yang diterbitkan pihak terpercaya (CA)




**MASIH MAU KLIK INI?**

# APLIKASI KAMU ASLI, BAJAKAN ATAU JEBAKAN BATMAN?

- mod_fcgid
- mod_ftp

**Related Projects**

- Apache Traffic Server
- Tomcat
- APR

**Miscellaneous**

- Contributors
- Sponsors
- Sponsorship


- Security and official patches
- Other files
- Files for Microsoft Windows

**Apache mod_fcgid FastCGI module for Apache HTTP Server released as 2.3.9** **2013-10-08**

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the release of version 2.3.9 of mod_fcgid, a FastCGI implementation for Apache HTTP Server versions 2.2 and 2.4. This version of mod_fcgid is a security release.

For information about this module subproject, see the mod_fcgid module project page.

- Source as gzip with LF line endings: mod_fcgid-2.3.9.tar.gz [ PGP ] [ MD5 ] [ SHA1 ]
- Source as bz2 with LF line endings: mod_fcgid-2.3.9.tar.bz2 [ PGP ] [ MD5 ] [ SHA1 ]
- Win32, Netware or OS/2 Source with CR/LF line endings: mod_fcgid-2.3.9-crlf.zip [ PGP ] [ MD5 ] [ SHA1 ]

Checksum Nilai Hash

**Apache FTP module for Apache HTTP Server released as 0.9.6-beta** **2008-10-08**

The Apache HTTP Server Project is pleased to announce the release of Apache FTP module for Apache HTTP Server, version 0.9.6 as beta.

**Download WinMD5 (only 249KB):**

WinMD5 Freeware Download

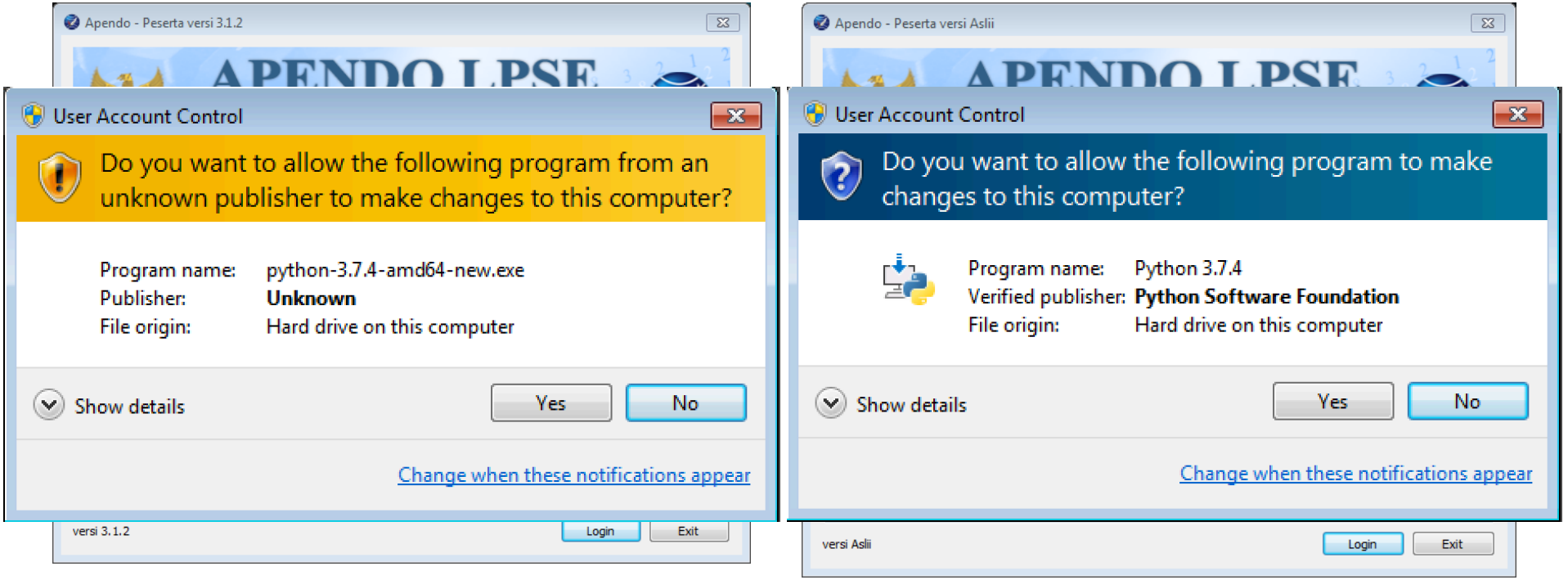
WinMD5Free.zip MD5: 73f48840b60ab6da68b03acd322445ee

WinMD5Free.exe MD5: 944a1e869969dd8a4b64ca5e6ebc209a

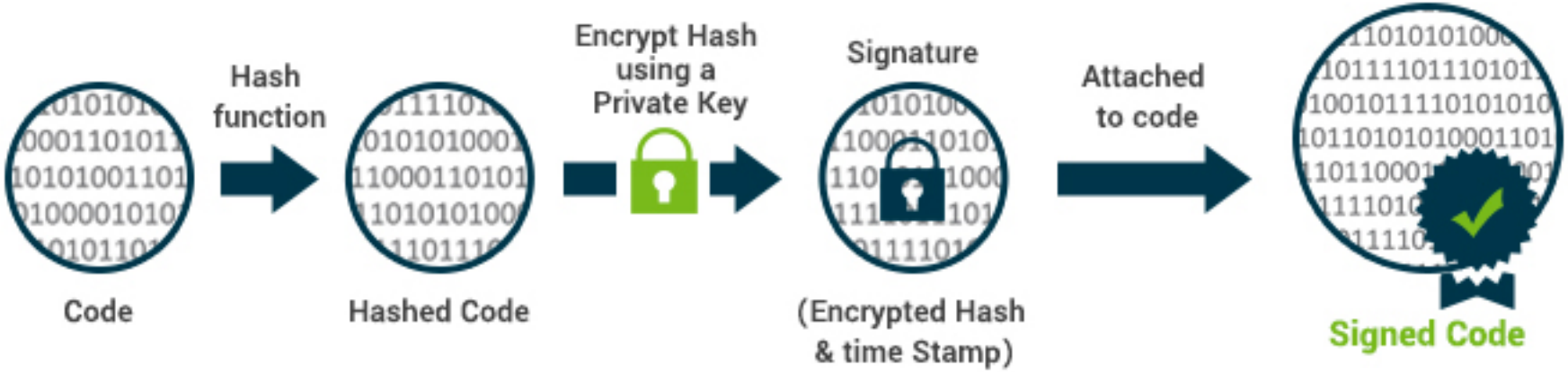
Checksum Nilai Hash

You may simply download it, then unzip and put the exe to any folder on your hard drive, and start to use. No installation is required. The download does not contain any virus, spyware, adware or malware.

# MANAKAH APLIKASI RESMI?



# CODE SIGNING



# APA MANFAATNYA SIH?

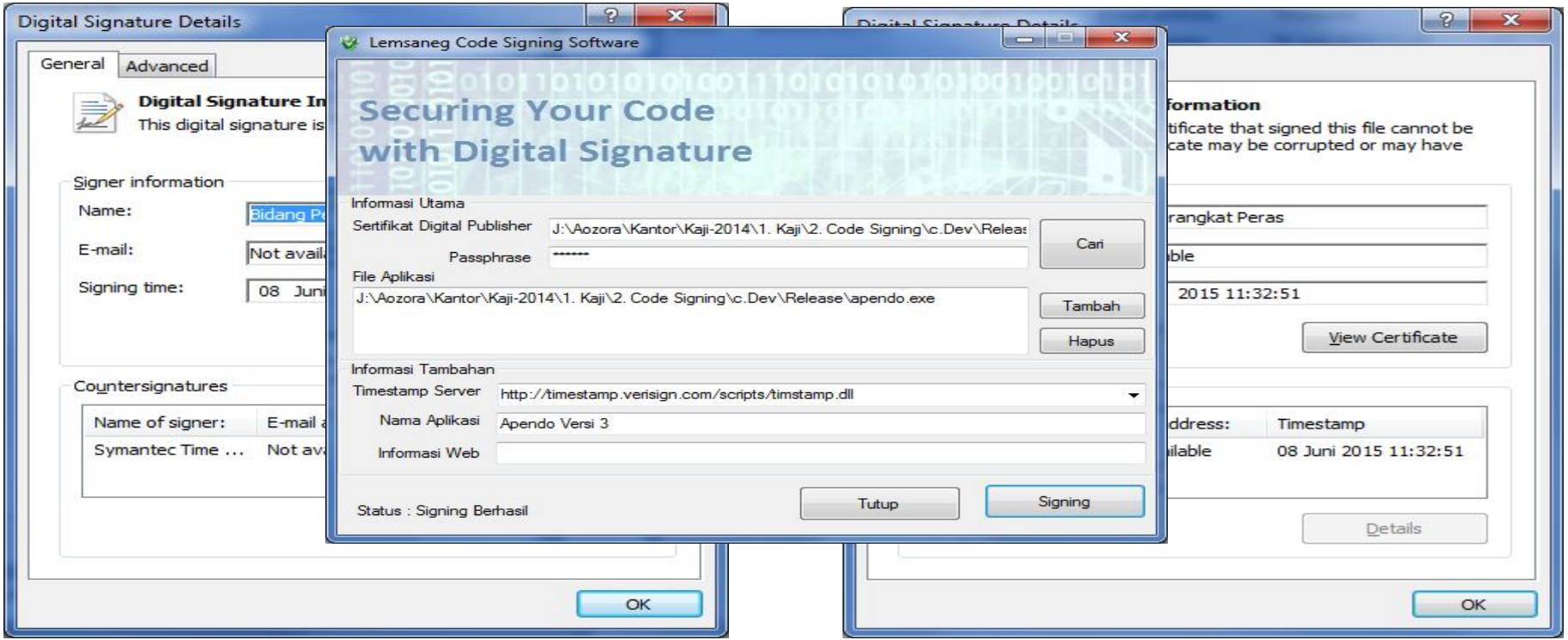

## Developer

- Membangun kepercayaan bagi *publisher* terhadap *end user*
- Menjadikan Aplikasi yang dibuat sulit untuk dipalsukan

## End User

- mengkonfirmasi bahwa *software* benar berasal dari *publisher sebenarnya*
- memverifikasi bahwa software tersebut tidak dimanipulasi sejak ditanda tangani

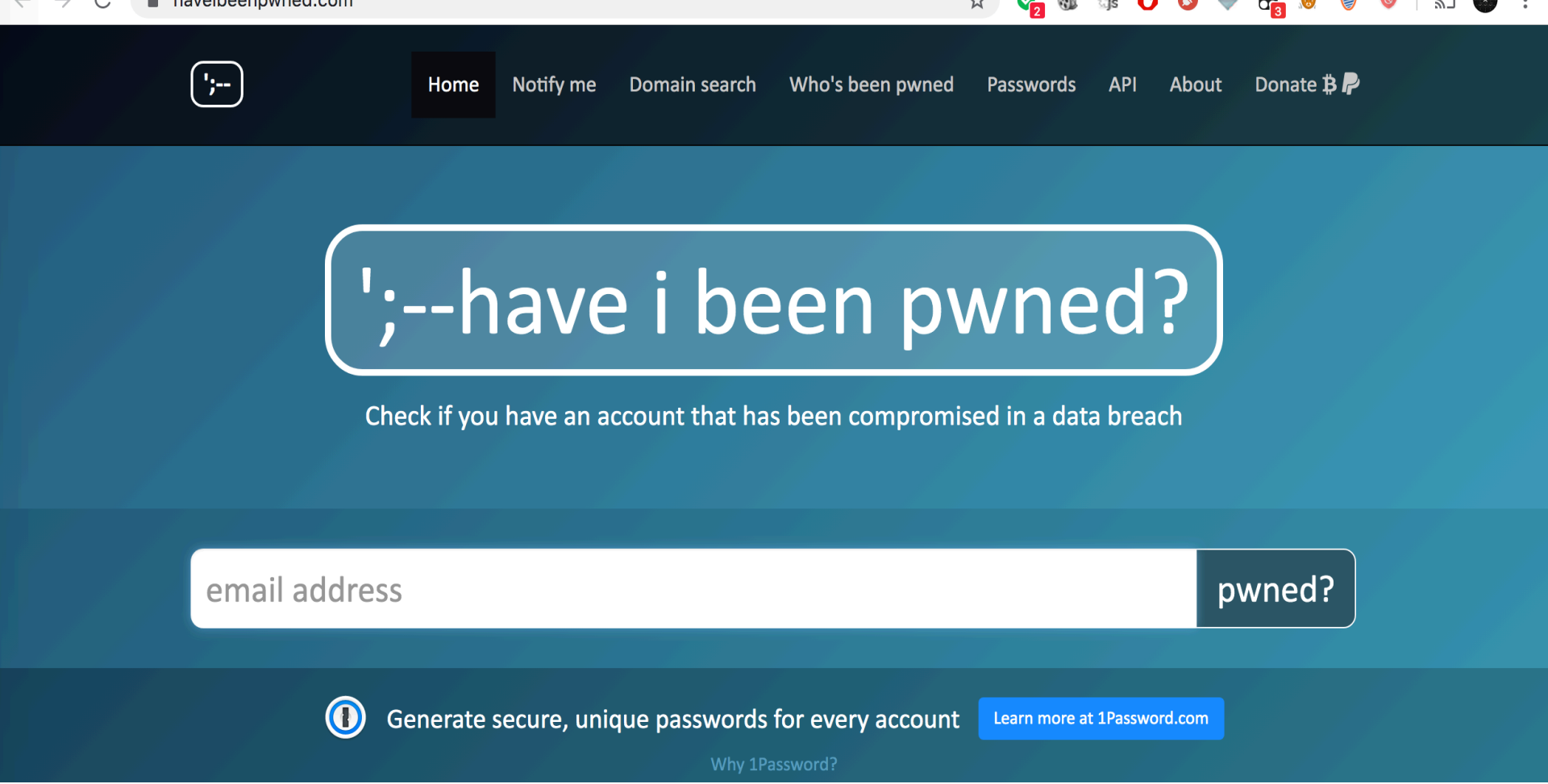
# CODE SIGNING



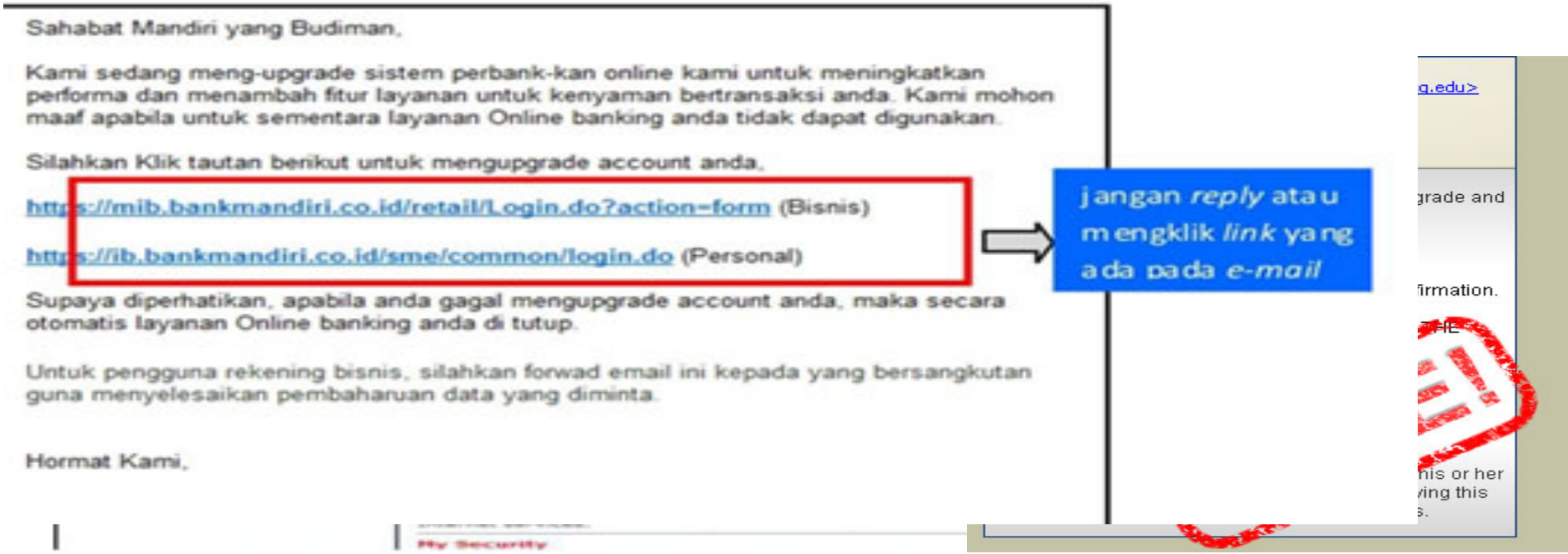
# ASLI, BAJAKAN ATAU ....


**Kita Buktikan....**

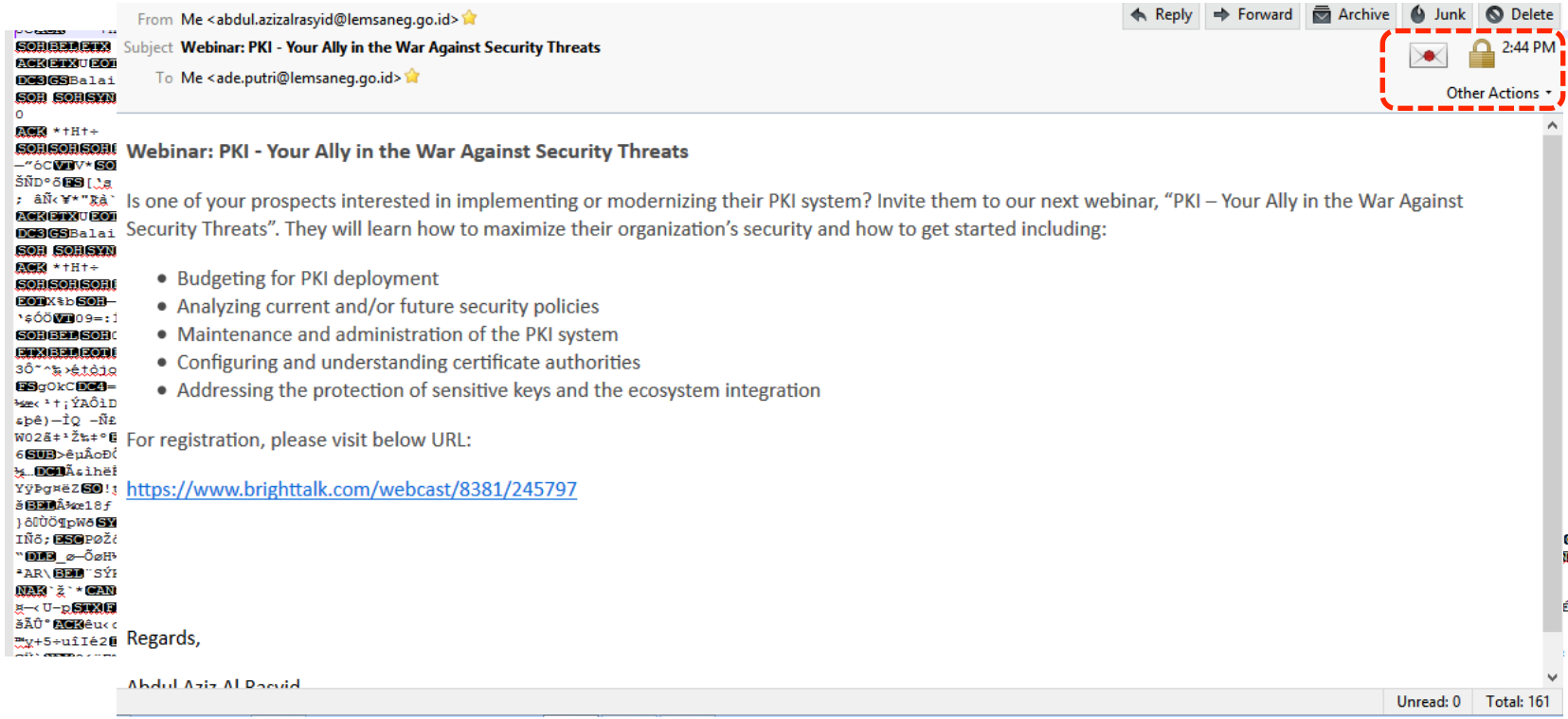
# EMAIL INI DIJAMIN 100% ASLI
# BUKAN PHISING


haveibeenpwned.com
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?

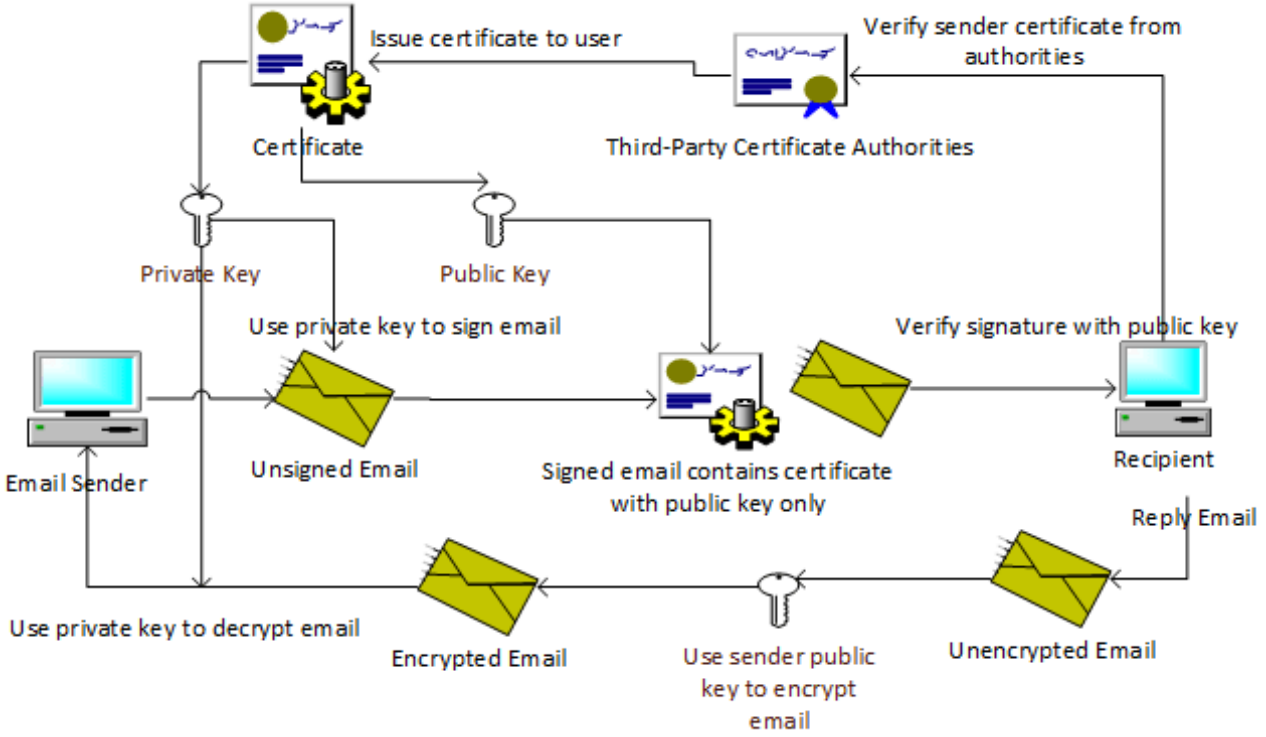
# PERNAH SEPERTI INI?



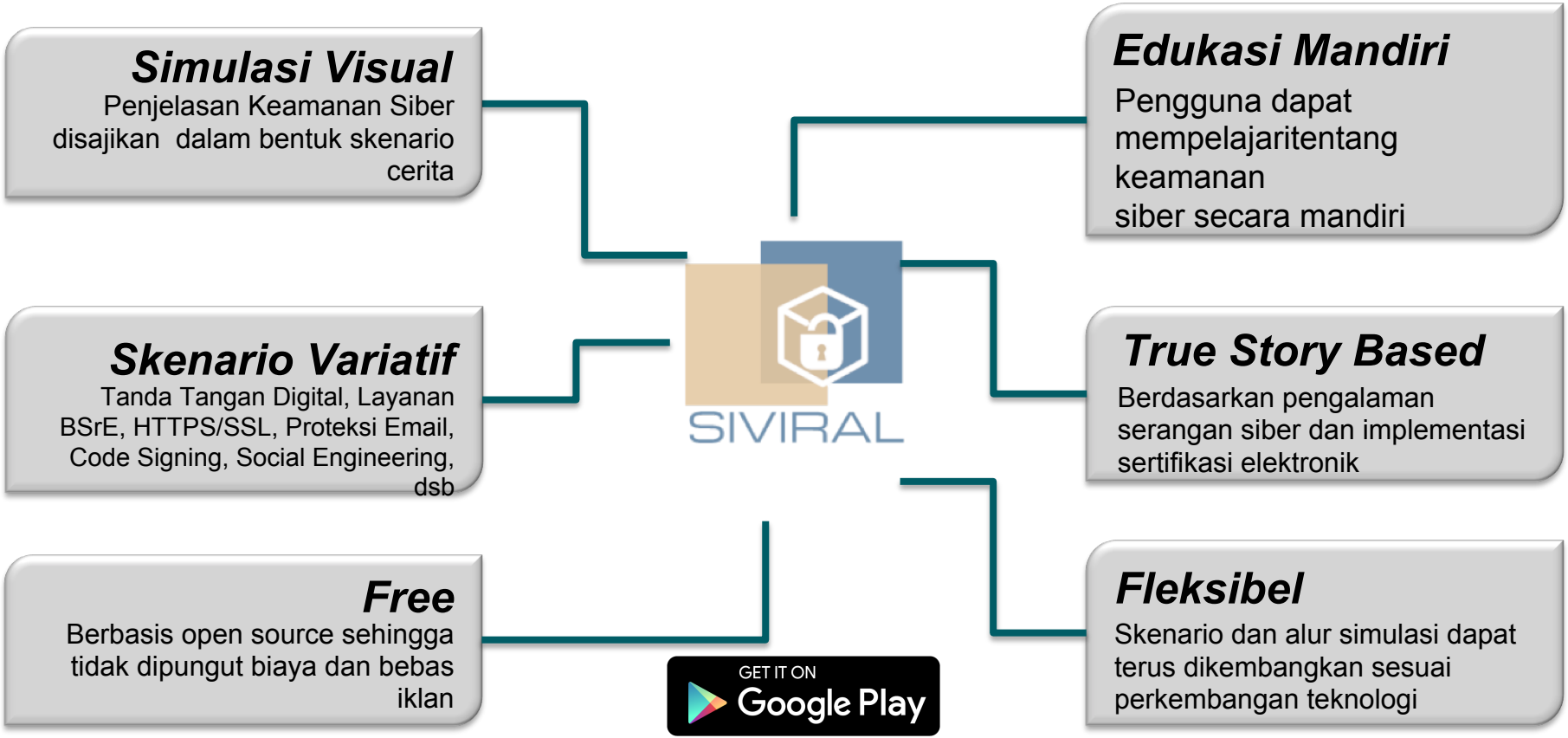
# PROTEKSI EMAIL



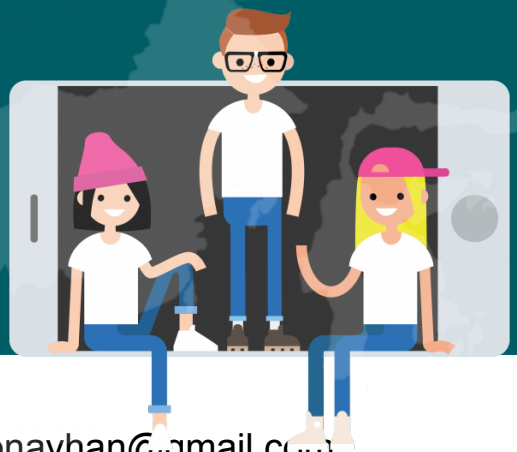
# HOW TO


Issue certificate to user
Verify sender certificate from authorities
Certificate
Third-Party Certificate Authorities
Private Key
Public Key
Use private key to sign email
Verify signature with public key
Email Sender
Unsigned Email
Signed email contains certificate with public key only
Recipient
Reply Email
Use private key to decrypt email
Encrypted Email
Use sender public key to encrypt email
Unencrypted Email

# GAME EDUKASI KEAMANAN SIBER



# TERIMA KASIH




yonavhan@gmail.com

08115 595 044

@yonavhan

snahvalabs