Téken pake Téken Aja!

By Djelas Tandatangan Bersama

PT. DJELAS TANDATANGAN BERSAMA

PANDUAN VERIFIKASI TANDA TANGAN ELEKTRONIK TERSERTIFIKASI DAN VERIFIKASI SERTIFIKAT ELEKTRONIK

Nomor	006/LGL-DTB/PJN/II/2021
Versi	3.0
Tanggal	28 Desember 2023
Jenis Dokumen	Publik

28 Desember 2023

Chief Operating Officer

Rony Tanrim

Keterangan Revisi Dokumen

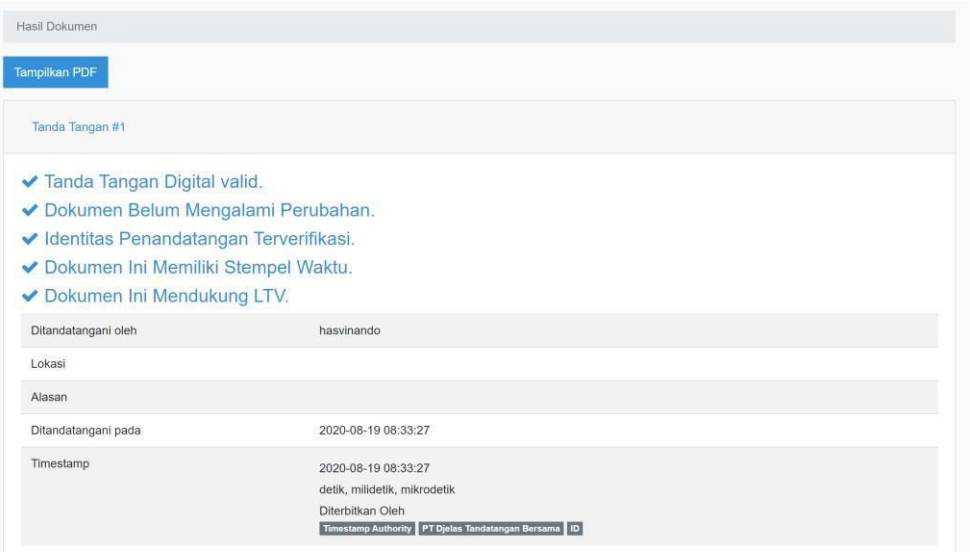
Revisi	Tgl.	Penjelasan perubahan	Dibuat oleh	Disetujui oleh
1.0	**24-02- 2021**	**Edisi perdana**	**Legal**	**COO**
2.0	**30-10- 2022**	• **Review Dokumen secara berkala**	**CTO** **Legal**	**COO**
3.0	**28-12- 2023**	• **Review Dokumen secara berkala Perubahan Logo**	**CTO** **Legal**	**COO**

1. Verifikasi melalui web verify.djelas.id

A. Buka situs https://verify.djelas.id , kemudian seret berkas pdf ke kotak bergaris putus-putus atau klik untuk memilih file di explorer, kemudian klik “Unggah”

B. Jika berkas memiliki tanda tangan elektronik tersertifikasi maka setelah pengunggahan selesai akan muncul tampilan seperti pada gambar berikut.

- Verifikasi Tanda Tangan Elektronik

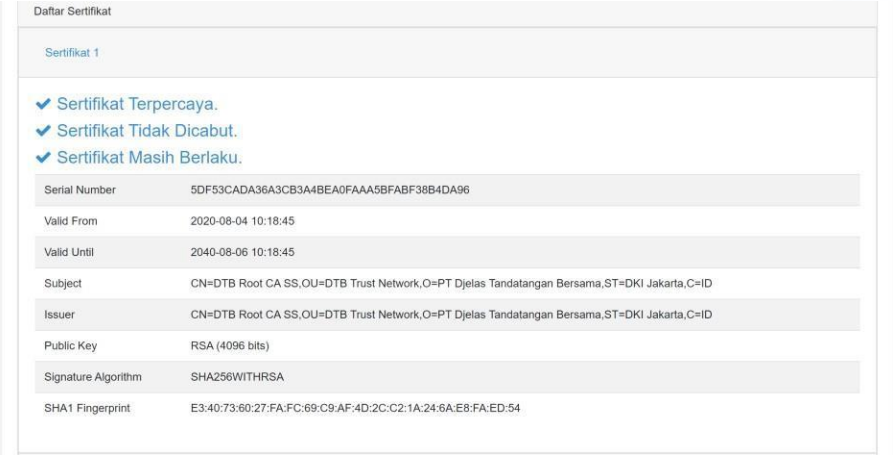


- **Tanda Tangan Digital Valid** artinya tanda tangan digital pada dokumen ini dinilai valid
- **Dokumen Belum Mengalami Perubahan** artinya isi dokumen tersebut belum pernah diubah sejak dokumen tersebut ditandatangani (Integritas dokumen).
- **Identitas Penanda Tangan Terverifikasi** artinya sertifikat elektronik yang berisi identitas

  Penanda Tangan yang sudah diverifikasi oleh DTB dan sertifikat elektroniknya belum kadaluarsa dan tidak pernah dicabut (*revoke*).
- **Dokumen Ini Memiliki Stempel Waktu** artinya waktu penandatanganan mengacu
- pada *Timestamp server* yang disepakati, bukan terhadap waktu komputer lokal.
- **Dokumen Ini Mendukung LTV** artinya sertifikat elektronik yang digunakan untuk membuat tanda tangan elektronik tersebut menggunakan fitur Long-Term Validation (LTV), dengan tujuan agar tanda tangan elektronik tetap dapat diverifikasi meskipun masa berlaku sertifikat elektroniknya sudah habis.

- Verifikasi Sertifikat

- Sertifikat RCA



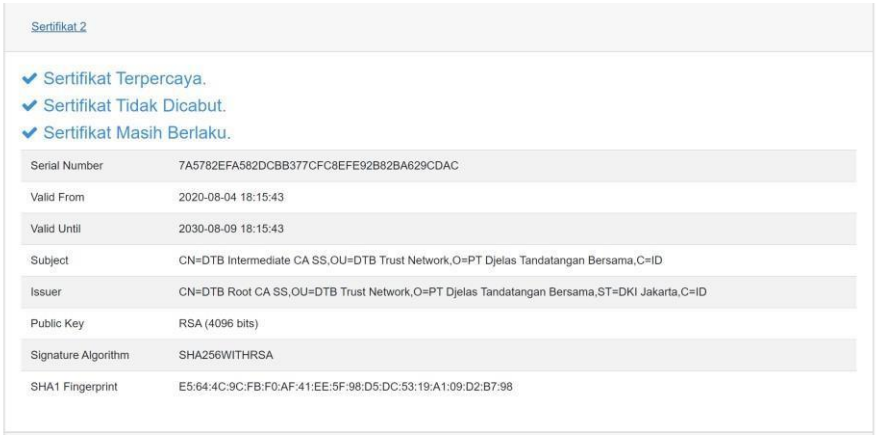
Daftar Sertifikat

Sertifikat 1

✔ Sertifikat Terpercaya.
✔ Sertifikat Tidak Dicabut.
✔ Sertifikat Masih Berlaku.

Serial Number	5DF53CADA36A3CB3A4BEA0FAAA5BFABF38B4DA96
Valid From	2020-08-04 10:18:45
Valid Until	2040-08-06 10:18:45
Subject	CN=DTB Root CA SS,OU=DTB Trust Network,O=PT Djelas Tandatangan Bersama,ST=DKI Jakarta,C=ID
Issuer	CN=DTB Root CA SS,OU=DTB Trust Network,O=PT Djelas Tandatangan Bersama,ST=DKI Jakarta,C=ID
Public Key	RSA (4096 bits)
Signature Algorithm	SHA256WITHRSA
SHA1 Fingerprint	E3:40:73:60:27:FA:FC:69:C9:AF:4D:2C:C2:1A:24:6A:E8:FA:ED:54

- Sertifikat ICA

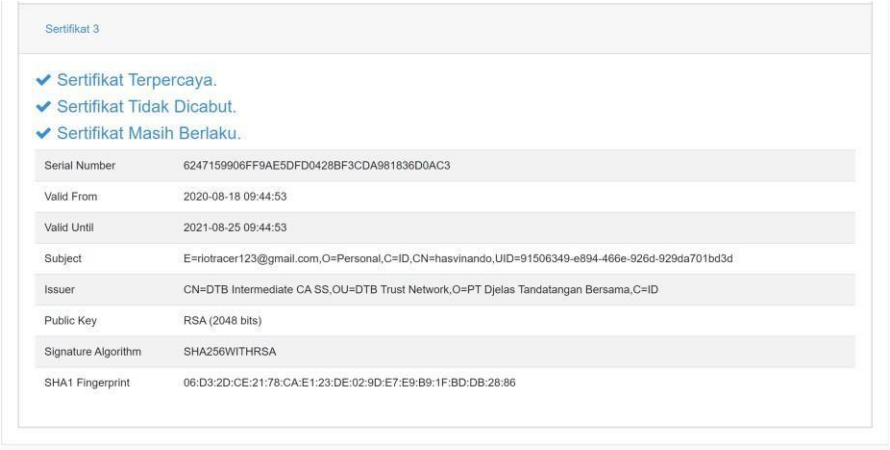


Sertifikat 2

✔ Sertifikat Terpercaya.
✔ Sertifikat Tidak Dicabut.
✔ Sertifikat Masih Berlaku.

Serial Number	7A5782EFA582DCBB377CFC8EFE92B82BA629CDAC
Valid From	2020-08-04 18:15:43
Valid Until	2030-08-09 18:15:43
Subject	CN=DTB Intermediate CA SS,OU=DTB Trust Network,O=PT Djelas Tandatangan Bersama,C=ID
Issuer	CN=DTB Root CA SS,OU=DTB Trust Network,O=PT Djelas Tandatangan Bersama,ST=DKI Jakarta,C=ID
Public Key	RSA (4096 bits)
Signature Algorithm	SHA256WITHRSA
SHA1 Fingerprint	E5:64:4C:9C:FB:F0:AF:41:EE:5F:98:D5:DC:53:19:A1:09:D2:B7:98

- Sertifikat Entity



Sertifikat 3

✔ Sertifikat Terpercaya.
✔ Sertifikat Tidak Dicabut.
✔ Sertifikat Masih Berlaku.

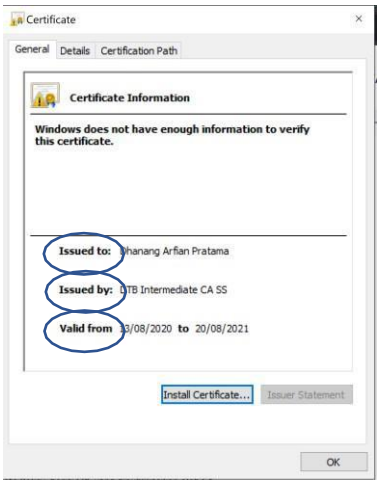
Serial Number	6247159906FF9AE5DFD0428BF3CDA981836D0AC3
Valid From	2020-08-18 09:44:53
Valid Until	2021-08-25 09:44:53
Subject	E=riotracer123@gmail.com,O=Personal,C=ID,CN=hasvinando,UID=91506349-e894-466e-926d-929da701bd3d
Issuer	CN=DTB Intermediate CA SS,OU=DTB Trust Network,O=PT Djelas Tandatangan Bersama,C=ID
Public Key	RSA (2048 bits)
Signature Algorithm	SHA256WITHRSA
SHA1 Fingerprint	06:D3:2D:CE:21:78:CA:E1:23:DE:02:9D:E7:E9:B9:1F:BD:DB:28:86

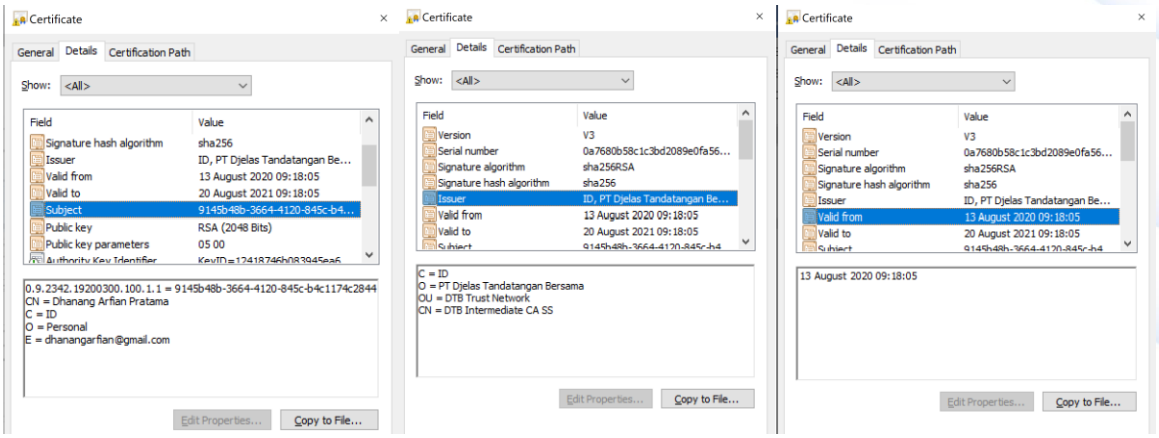
Keterangan rinci sertifikat:

- **Sertifikat Terpercaya** maksudnya adalah sertifikat elektronik diterbitkan oleh DTB
- **Sertifikat Tidak Dicabut** maksudnya adalah sertifikat elektronik yang digunakan untuk menandatangani tidak pernah dicabut (revoke).
- **Sertifikat Masih Berlaku** adalah sertifikat elektronik yang belum kadaluwarsa saat
- digunakan untuk menandatangani dokumen.
- Keterangan rinci sertifikat:
  - Serial: nomor serial unik sertifikat a elektronik
  - Validitas: masa berlaku sertifikat elektronik
  - Subject :
    - E : Alamat email pemilik sertifikat elektronik
    - O : Organization. Organisasi pemilik sertifikat elektronik.
    - C : Country. Negara dari pemilik sertifikat elektronik.
    - CN : Common Name. Nama pemilik sertifikat elektronik
  - Issuer :
    - CN : Common Name. Nama pemilik sertifikat elektronik
    - OU : Organization Unit. Berisi unit organisasi pemilik sertifikat
    - O : Organization. Organisasi pemilik sertifikat elektronik.
    - C : Country. Negara dari pemilik sertifikat elektronik.
  - Public Key: Algoritma yang digunakan untuk pembuatan pasangan kunci
  - Signature Algorithm: Algoritma yang digunakan untuk melakukan *hashing* terhadap Dokumen Elektronik dan Tanda Tangan Elektronik
  - SHA-1 Fingerprint: Nilai *hash* dari sertifikat elektronik

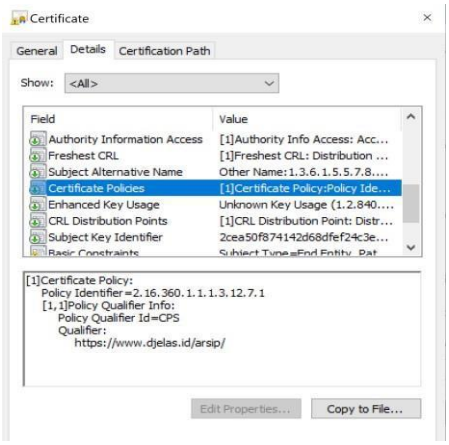
Selain dari tampilan web, sertifikat juga dapat diunduh dan diverifikasi

- Unduh sertifikat dari web cp.djelas.id
- Buka sertifikat dengan double click
- Attribute pada sertifikat sebagai berikut :
  a) Issued to / Subject, adalah pemilik dari sertifikat, contoh : Dhanang Afrian Pratama.
  b) Issued by, adalah CA yang mengeluarkan sertifikat, contoh : DTB Intermediate CA SS
  c) Valid From - To -, adalah Masa berlaku sertifikat.

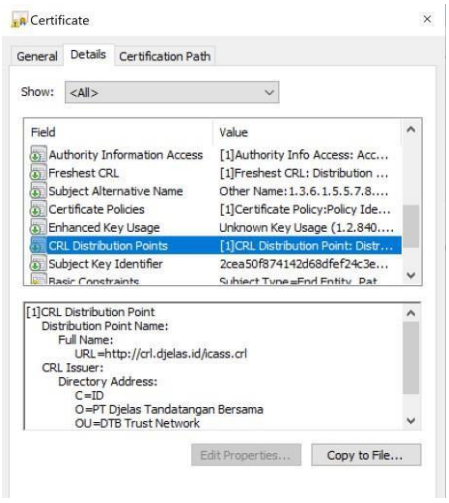




- Sertifikat Policy, berisi CPS yang dipublikasikan oleh CA.

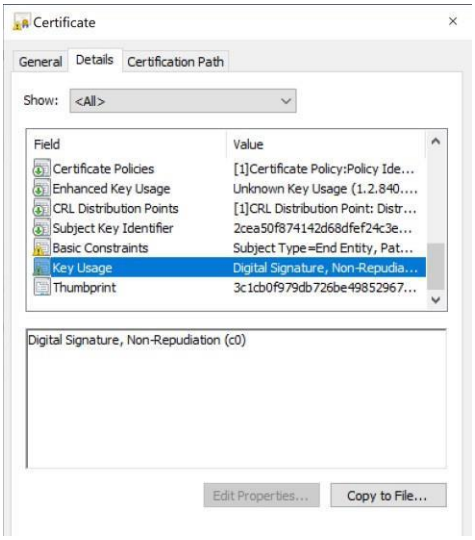


- CRL Distribution Point, Sertifikat Revoke List dimana daftar sertifikat yang sudah dicabut.



- Key Usage, adalah peruntukan dari Sertifikat yang dikeluarkan, contoh nya untuk Digital

Signature / Document Signing.



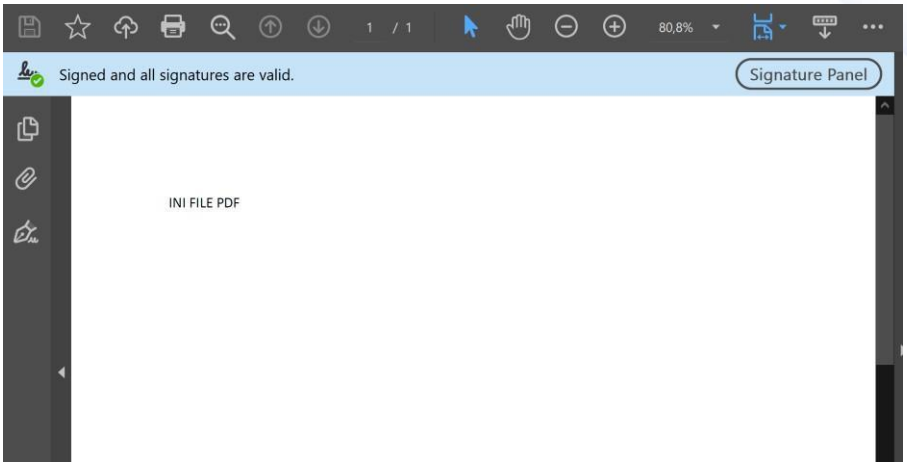
Catatan:
Setiap sertifikat dapat dilihat detailnya menggunakan pdf Adobe Reader atau membuka file.crt pada
Windows. Informasi yang perlu diperiksa di antaranya :

- Tanda tangan penerbit;
- Parameter kebijakan;
- Parameter penggunaan;
- Periode validitas;
- Informasi pencabutan atau pembekuan;
- Batas tanggung jawab penggunaan sertifikat

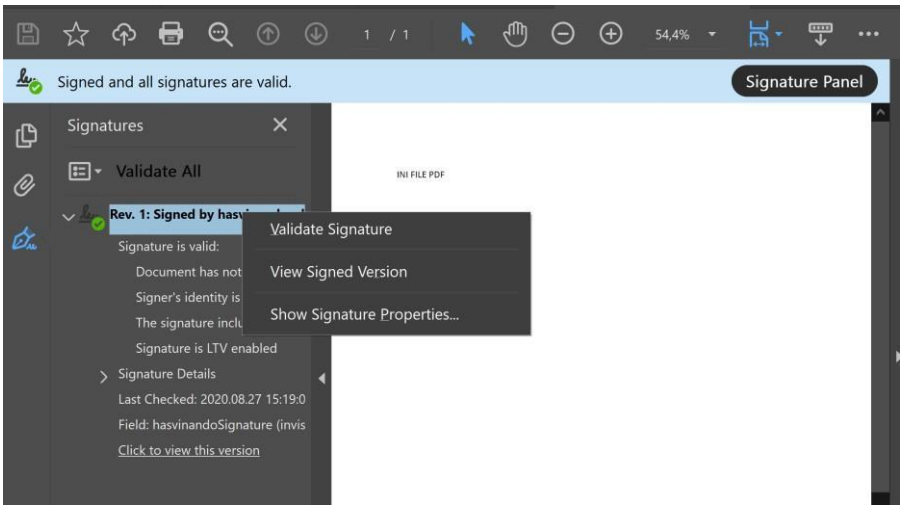
2. Verifikasi sertifikat menggunakan aplikasi Adobe Reader

A. Buka file dokumen menggunakan aplikasi Adobe Reader

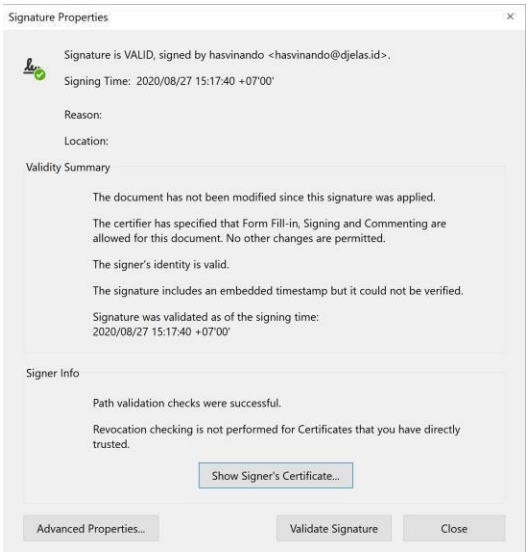
B. Adobe Reader akan secara otomatis memeriksa validitas tanda tangan Ketika file dibuka. Tanda tangan akan dianggap valid jika kontennya tidak dirubah, serta sertifikat elektroniknya terpercaya (trusted) dan masih berlaku. Jika tanda tangan valid, akan muncul tampilan "Signed and all signatures are valid" seperti pada gambar



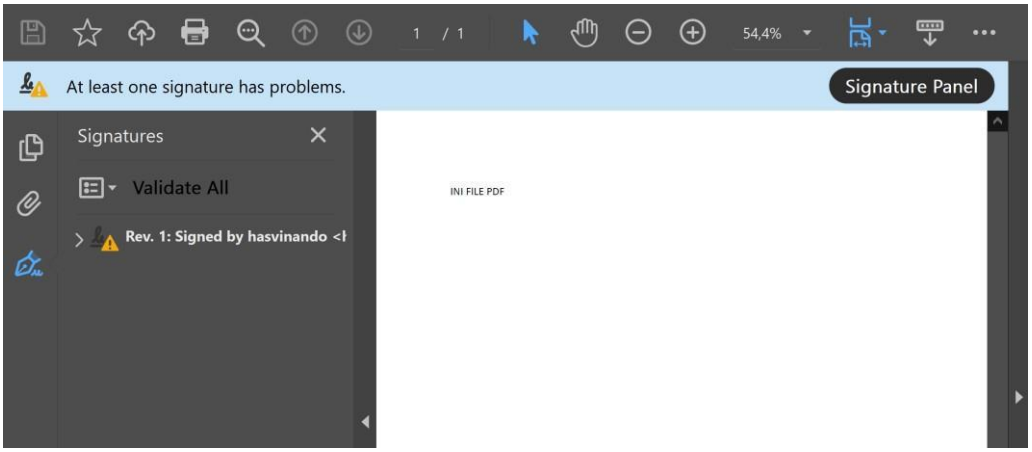
C. Untuk melihat detail tanda tangan, bisa dilakukan dengan mengklik Signature Panel, lalu klik kanan pada signature, kemudian pilih "Show Signature Properties"



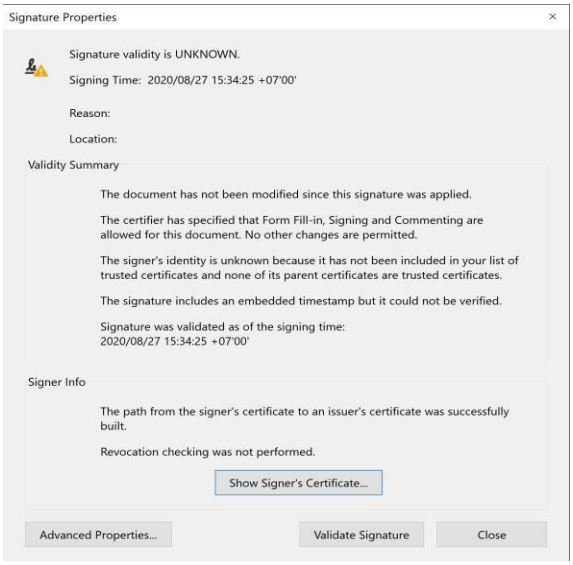
PT Djelas Tandatangan Bersama
Jl. Bangka Raya No. 21, Pela Mampang,
Jakarta Selatan 12720



D. Jika verifikasi dilakukan menggunakan Adobe Reader, ada kemungkinan bahwa sertifikat elektronik belum dikenali oleh Adobe Reader sehingga saat dilakukan verifikasi sebagaimana yang dijelaskan di atas, akan muncul keterangan Signature Validity is UNKNOWN seperti pada gambar di bawah.



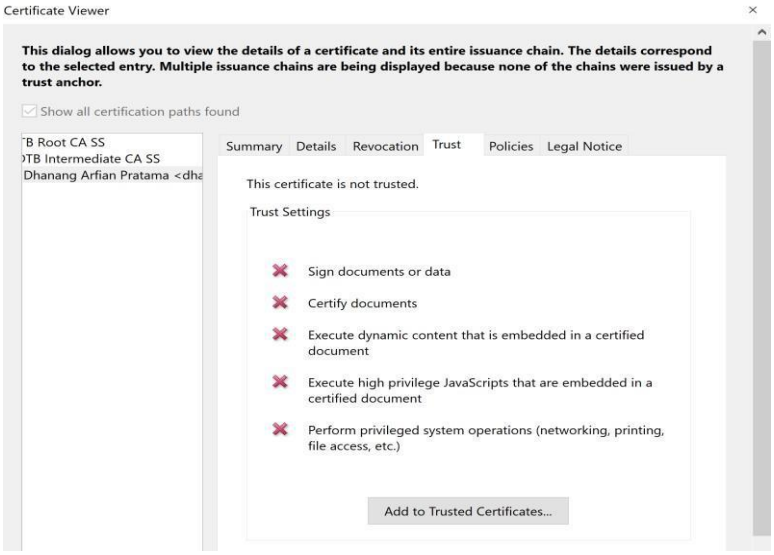
PT Djelas Tandatangan Bersama
Jl. Bangka Raya No. 21, Pela Mampang,
Jakarta Selatan 12720



Ini dikarenakan identitas yang terdapat di sertifikat elektronik belum masuk ke daftar trusted sertifikat di komputer dimana Adobe Reader di-install. Alasan lainnya adalah sertifikat induk dari sertifikat elektronik belum dikenali sebagai trusted sertifikat .

Oleh karena itu, sertifikat harus ditambahkan secara manual ke komputer. Hal ini bisa dilakukan dengan langkah-langkah berikut:

1. Pada Signature Properties ,klik “Show Signer’s Sertifikat” , pilih tab Trust , lalu klik Add to Trusted Sertifikats. Namun perlu dipastikan bahwa sertifikat induk tersebut memang sudah Anda percaya.



2. Setelah klik OK, lalu klik “Validate Signature” pada Signature Properties.
3. Selesai, tanda tangan telah tersetifikasi.