

PT DIGITAL TANDA TANGAN ASLI

PANDUAN VERIFIKASI TANDA TANGAN ELEKTRONIK TERSERTIFIKASI DAN VERIFIKASI SERTIFIKAT ELEKTRONIK

No Dokumen : IT-SOP-56-00

No Revision : 00

4 April 2022 Administrator CP Front-End

Bilal Abudan



Daftar Isi

Verifikasi melalui web	. 3
Verifikasi tanpa web	. 6
Verifikasi sertifikat menggunakan aplikasi Adobe Reader	. 9

Verifikasi melalui web

A. Buka situs <u>https://tte.kominfo.go.id/verifyPDF</u>, 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

Dokumen ini memiliki tar	nda tangan digital Pratinjau
Tanda tangan	
Tanda tang	an #1
A Dakuman Da	lum Mangalami Basubaban
✓ Identitas Pen	iant mengalarin rerubahan. Iandatangan Terverifikasi
Dokumen Ini	Memiliki Stempel Waktu
✓ Dokumen Ini	Mendukung LTV.
Ditandatangani oleh	Bilal Abudan
Lokasi	Jakarta
Alasan	I approve this document
Ditandatangani pada	04-04-2022 15:20:24 (lokal)
Timestamp	04-04-2022 15:20:24 (T SA)
	Ketepatan Waktu detik, mikrodetik Diterbitkan oleh DTACA PT Digital Tandalangan Asii ID
Sertifikat	
Sertifikat #1	
Sertifikat #2	
Sertifikat #3	

 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 DTA dan sertifikat elektroniknya belum kadaluarsa dan tidak pernah dicabut.
- 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 #1 Sertifikat Terpercaya Sertifikat Tidak Dicabut Sertifikat Masih Berlaku 6EBB7C44A8E962AE Serial Validitas 28-08-2018 11:55 - 23-08-2038 11:55 🗸 Subject CN=Root CA Indonesia DS G1,O=Kementerian Komunikasi dan Informatika,C=ID Self Signed Issuer CN=Root CA Indonesia DS G1,O=Kementerian Komunikasi dan Informatika,C=ID Public Key RSA (4096 bits) Algoritma TTD SHA256WITHR SA SHA-1 7B:83:61:5A:8B:B9:87:69:E9:C2:1A:1B:AC:39:C8:74:58:49:FA:E6 Fingerprint
 - Sertifikat RootCA

o Sertifikat IntermediaryCA

Sertifikat #2	
 ✓ Sertifikat T ✓ Sertifikat T ✓ Sertifikat N 	Terpercaya Tidak Dicabut Masih Berlaku
Serial	0888A72F7AE3604B
Validitas	22-12-2021 09:54 - 20-12-2031 09:54 🖌
Subject	C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA
Issuer	CN=Root CA Indonesia DS G1,O=Kementerian Komunikasi dan Informatika,C=ID
Public Key	RSA (4096 bits)
Algoritma TTD	SHA256WITHR SA
SHA-1 Fingerprint	60:53:60:79:AF:E8:E1:1B:55:31:34:B0:41:CD:7A:5B:4B:0B:F1:23

o Sertifikat Entity

 ✓ Sertifikat Terpercaya ✓ Sertifikat Tidak Dicabut ✓ Sertifikat Tidak Dicabut ✓ Sertifikat Masih Berlaku Serial 3B9C7A15CEE8E57D50DE13EDE62A95133740878A Validitas 31-01-2022 14:44 - 31-01-2023 14:44 ✓ Subject E=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal Abudan Issuer C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA Public Key RSA (2048 bits) Algoritma TTD SHA256WITHRSA SHA-1 6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76 	Sertifikat #3	
Serial3B9C7A15CEE8E57D50DE13EDE62A95133740878AValiditas31-01-2022 14:44 - 31-01-2023 14:44 ✓SubjectE=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal AbudanIssuerC=ID,O=PT Digital Tandatangan Asli,CN=DTA CAPublic KeyRSA (2048 bits)Algoritma TTDSHA256WITHRSASHA-16A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	 ✓ Sertifikat 1 ✓ Sertifikat 1 ✓ Sertifikat 1 	Ferpercaya Fidak Dicabut Masih Berlaku
Validitas31-01-2022 14:44 - 31-01-2023 14:44 ✓SubjectE=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal AbudanIssuerC=ID,O=PT Digital Tandatangan Asli,CN=DTA CAPublic KeyRSA (2048 bits)Algoritma TTDSHA256WITHRSASHA-16A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Serial	3B9C7A15CEE8E57D50DE13EDE62A95133740878A
SubjectE=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal AbudanIssuerC=ID,O=PT Digital Tandatangan Asli,CN=DTA CAPublic KeyRSA (2048 bits)Algoritma TTDSHA256WITHRSASHA-16A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Validitas	31-01-2022 14:44 - 31-01-2023 14:44 🖍
Issuer C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA Public Key RSA (2048 bits) Algoritma TTD SHA256WITHRSA SHA-1 6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Subject	E=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal Abudan
Public Key RSA (2048 bits) Algoritma TTD SHA256WITHRSA SHA-1 6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Issuer	C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA
Algoritma TTD SHA256WITHRSA SHA-1 6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Public Key	RSA (2048 bits)
SHA-1 6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76	Algoritma TTD	SHA256WITHRSA
Fingerprint	SHA-1 Fingerprint	6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76

Keterangan rinci sertifikat:

- Sertifikat Terpercaya maksudnya adalah sertifikat elektronik diterbitkan oleh DTA
- 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

Verifikasi tanpa web

- Unduh sertifikat dari detail sertifikat yang ada di dokumen yang sudah ditandatangan
- Buka sertifikat dengan double click
- Attribute pada sertifikat sebagai berikut :
 - a) Issued to / Subject, adalah pemilik dari sertifikat, contoh : Pandu Septian Gumilar.
 - b) Issued by, adalah CA yang mengeluarkan sertifikat, contoh : DTA Intermediate CA SS
 - c) Valid From To -, adalah Masa berlaku sertifikat.



General Details Certification Pat	h	General Details Certification Pa	th	×	General Details Certification Pa	sth	>
Show: <all></all>	~	Show: <all></all>	~		Show: <all></all>	~	
Field Soure Valid from Valid to Subject Public key parameters Authority Key Identifier The Authority Key Identifier	Value D. Dida Jakarta, PT Digital Tan Tuesday, September 22, 2020 Vechesday, September 29, 2 Status, September 29, 2 Status, September 29, 2 Status, September 29, 2 (Horizon, September 29, 2 (Horizon, September 29, 2 (Horizon, September 29, 2 (Horizon, September 29, 2) (Hori	Field Version Scraia number Signature adjorithm Signature hash adjorithm Valid from Valid from Valid from	Value V3 216c0b2fc45fbe55c63ea7496 sha256R5A sha255 10, DKI Jakarta, PT Digtal Tan Tuesday, September 22, 2020 Wednesday, September 23, 2 a 1068101.2635.41hc-bfc-1.43	<	Field Version Signature algorithm Signature hash algorithm Issue Valid from Valid from Sightmert	Value V3 216:0b2fc45fbe55c63ea7496 sha256R5A sha256 D, OKI Jakarta, PT Digital Tan Tuesday, September 22, 202 Wednesday, September 29, 2 01068.013.4635.41bc-/sfr-1-3	< · · · · · · · · · · · · · · · · · · ·
0.9.2342.19200300.100.1.1 = 91 CN = Pandu Septan Gumilar C = ID O = Personal E = pandusg404@gmail.com	1968 103-8635-41bc-bfc1-43b08561d62f	C = ID S = DKI Jakarta O = PT Digital Tandatangan Asik OU = DTA Trust Network CN = DTA EV Intermediate CA Si	5		Tuesdøy, September 22, 2020 :	1: 16:02 PM	
1	Gdt Properties Copy to File		Edit Properties Copy to File.	ж		Edit Properties Copy to File.	

• Sertifikat Policy, berisi CPS yang dipublikasikan oleh CA.



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

Show:	<all></all>	~	
Field	bject Alternative Name ertificate Policies	Value Other Name: 1.3.6. 1.5.5.7.8 [1]Certificate Policy:Policy Ide	^
SL	RL Distribution Points Ibject Key Identifier	[1]CRL Distribution Point: Distr 5fbd75e0cb5faa555ab6c1dca	
Ba Ke	asic Constraints ey Usage numbprint	Subject Type=End Entity, Pat Digital Signature, Non-Repudia 1b5dfe333f5b99f70d0231ca7	~
[1]CRL Disi	. Distribution Point tribution Point Name: Full Name: URL=http://crl.digitaltar Issuer: Directory Address:	ndatanganasli.com/icass.crl	^
	C=ID S=DKI Jakarta O=PT Digital Tandatang	an Asli	~

• Key Usage, adalah peruntukan dari Sertifikat yang dikeluarkan, contoh nya untuk Digital Signature / Document Signing.

how:	<all></all>	~	
Field	bject Alternative Name ertificate Policies XL Distribution Points bject Key Identifier wis Construinte	Value Other Name: 1.3.6.1.5.5.7.8 [1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr Stid 75e0cb5faa55ab6c1dca	^
Ba	ISIC CONSU dints	Subject Type=End Entity, Pat	
Ba Ke	ey Usage numbprint	Subject Type == End Entity, Pat Digital Signature, Non-Repudia 1b5dfe333f5b99f70d0231ca7	v
Ba Ke	signature, Non-Repudiati	Subject i type=tend britty, Pat., Digital Signature, Non-Reputal, 1b5dfe333f5b99f70d0231ca7	v
Digital :	y Usage umbprint Signature, Non-Repudiati	Subject i type=izho Entroy, Pac Digital Signature, Non-Repuda 1b5dfe333f5b99f70d0231ca7 on (c0)	v

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

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"



Signature	Properties	\times
<u>k</u> o	Signature is VALID, signed by Pandu Septian Gumilar <pandusg404@gmail.com>.</pandusg404@gmail.com>	
	Signing Time: 2020/09/29 16:31:51 +07'00'	
	Reason:	
	Location:	
Validit	ty Summary	
	The document has not been modified since this signature was applied.	
	The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.	
	The signer's identity is valid.	
	The signature includes an embedded timestamp but it could not be verified.	
	Signature was validated as of the signing time: 2020/09/29 16:31:51 +07'00'	
Signe	r Info	
	Path validation checks were successful.	
	Revocation checking is not performed for Certificates that you have directly trusted.	
	Show Signer's Certificate	
Adv	Validate Signature Close	

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.



ignature	Properties
	Signature validity is UNKNOWN.
<u> 140</u>	Signing Time: 2020/09/29 16:31:51 +07'00'
	Reason:
	Location:
Validi	y Summary
	The document has not been modified since this signature was applied.
	The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.
	The signer's identity is unknown because it has not been included in your list of trusted certificates and none of its parent certificates are trusted certificates.
	The signature includes an embedded timestamp but it could not be verified.
	Signature was validated as of the signing time: 2020/09/29 16:31:51 +07'00'
Signe	r Info
	The path from the signer's certificate to an issuer's certificate was successfully built.
	Revocation checking was not performed.
	Show Signer's Certificate
Adv	anced Properties Validate Signature Close

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