PETUNJUK TEKNIS
VERIFIKASI TANDA TANGAN DIGITAL PADA DOKUMEN PDF

BALAI SERTIFIKASI ELEKTRONIK

"*BUILD TRUST IN ELECTRONIC TRANSACTIONS*"

INFORMASI DOKUMEN

<table>
<tr><td>JUDUL :</td><td>PETUNJUK TEKNIS VERIFIKASI TANDA TANGAN DIGITAL PADA DOKUMEN PDF</td><td>VERSI :</td><td>2.0</td></tr>
<tr><td>NOMOR DOKUMEN :</td><td>306/BS/HK.01.02/11/2022</td><td>KLASIFIKASI :</td><td>BIASA</td></tr>
<tr><td>TANGGAL PEMBUATAN :</td><td>7 Desember 2018</td><td rowspan="2">DIBUAT OLEH :</td><td rowspan="2">Seksi Pemenuhan Teknis Sistem Sertifikasi Elektronik</td></tr>
<tr><td>TANGGAL PERUBAHAN :</td><td>2 Agustus 2022</td></tr>
<tr><td>DIPERIKSA OLEH :</td><td colspan="3">Kepala Seksi Seksi Pemenuhan Teknis Sistem Sertifikasi Elektronik

Ditandatangani secara elektronik oleh:
KEPALA SEKSI PEMENUHAN TEKNIS SISTEM SERTIFIKASI ELEKTRONIK BSRE

Nanang Indarjo, S.E.
Penata Tk. I (III/d)</td></tr>
<tr><td>DISETUJUI OLEH :</td><td colspan="3">Kepala Balai Sertifikasi Elektronik

Ditandatangani secara elektronik oleh:
KEPALA BALAI SERTIFIKASI ELEKTRONIK

Jonathan Gerhard T., S.ST
Penata Tk. I (III/d)</td></tr>
</table>

DAFTAR ISI

DAFTAR ISI.....2
I. PENDAHULUAN.....4
II. PERSIAPAN.....5
III. SIGNING DOKUMEN PDF 7
IV. VERIFIKASI TANDA TANGAN ELEKTRONIK.....12

I. PENDAHULUAN

1. Umum

   Tanda tangan elektronik merupakan tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Format dokumen yang paling populer yang menyediakan mekanisme tanda tangan elektronik adalah PDF (Portable Document Format), yang memungkinkan pengguna untuk bertukar dan melihat dokumen elektronik dengan mudah dan andal, terlepas dari tempat dan waktu. Salah satu format dokumen yang dapat diberikan tanda tangan elektronik adalah PDF. Pdf yang sudah ditanda tangani secara elektronik dapat diverifikasi dengan berbagai macam aplikasi.

   Dalam petunjuk teknis ini akan dibahas bagaimana melakukan verifikasi tanda tangan digital pada dokumen PDF yang sudah ditanda tangani, yaitu menggunakan aplikasi Adobe Acrobat DC, modul verifikasi pada Web, Aplikasi Panter Versi 2.0, Aplikasi Besign dan Openssl.

2. Kebutuhan Teknis

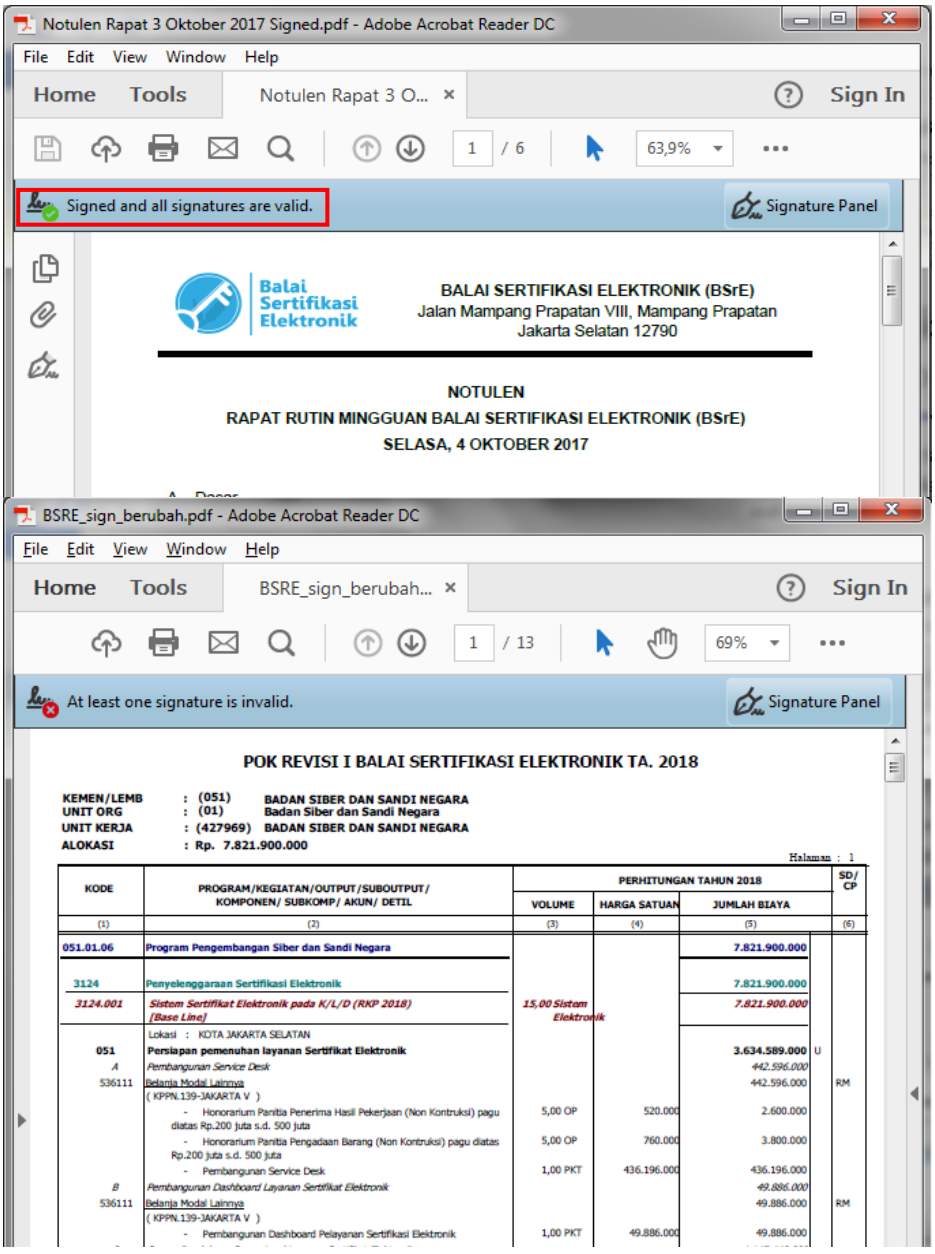
   Aplikasi-aplikasi dan aplikasi pendukung yang akan digunakan untuk verifikasi dokumen PDF pada dokumen petunjuk teknis ini adalah sebagai berikut:

   a. Adobe Acrobat DC
   b. Modul Verifikasi (Browser)
   c. Aplikasi Panter Versi 2.0
   d. Aplikasi Besign (Mobilephone, OS Android)
   e. Terminal atau Command prompt

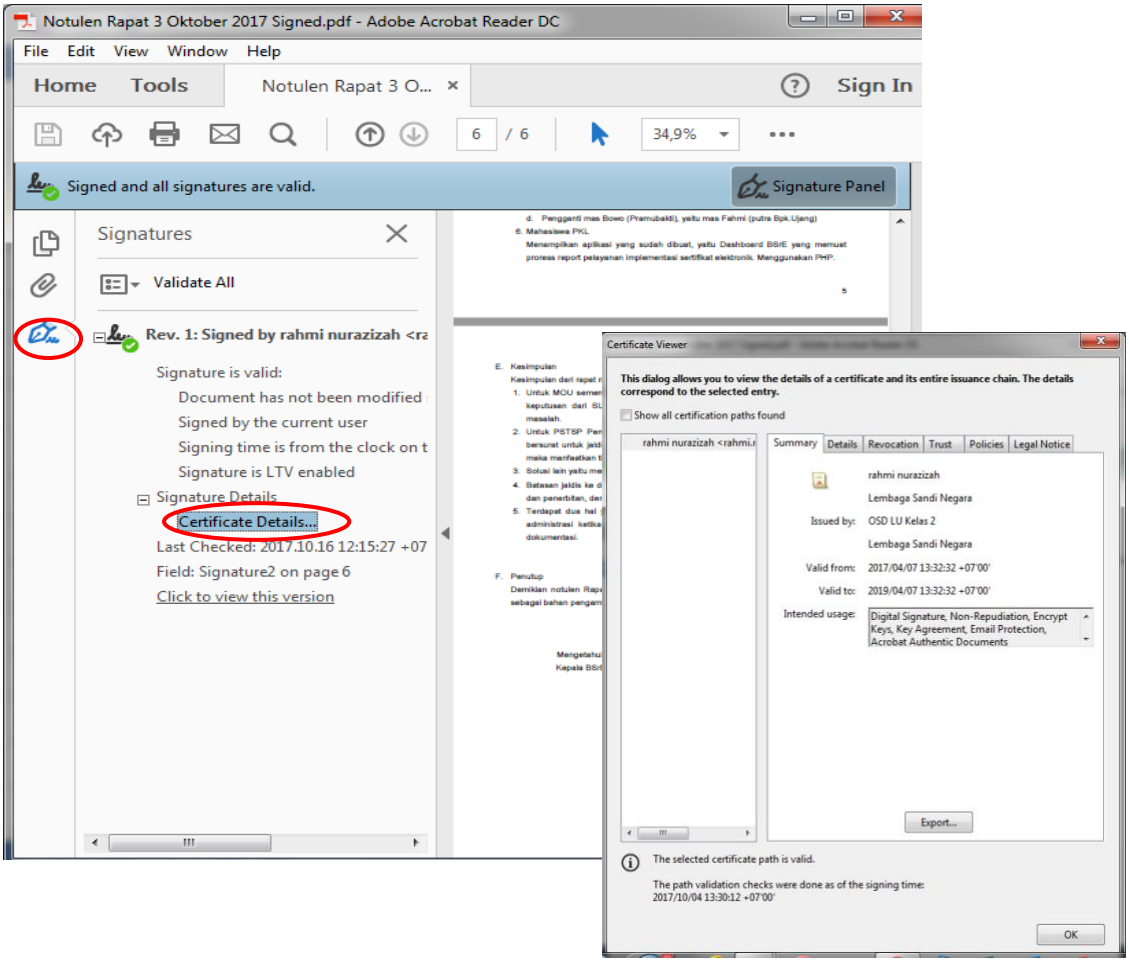
II. VERIFIKASI DENGAN ADOBE ACROBAT DC

Untuk melakukan verifikasi bahwa tanda tangan elektronik valid, maka pastikan komputer terhubung ke internet, dan buka file .pdf yang sudah diberikan tanda tangan elektronik.

1. Buka berkas dokumen PDF yang bertanda tangan digital, Adobe secara otomatis akan melakukan pengecekan tanda tangan elektronik ke server CA. Jika tanda tangan elektronik valid, maka akan diberikan keterangan "**Signed and all signatures are valid**", jika tidak valid maka keterangannya adalah "**At least one signature is invalid**" dengan tanda silang merah **x.**

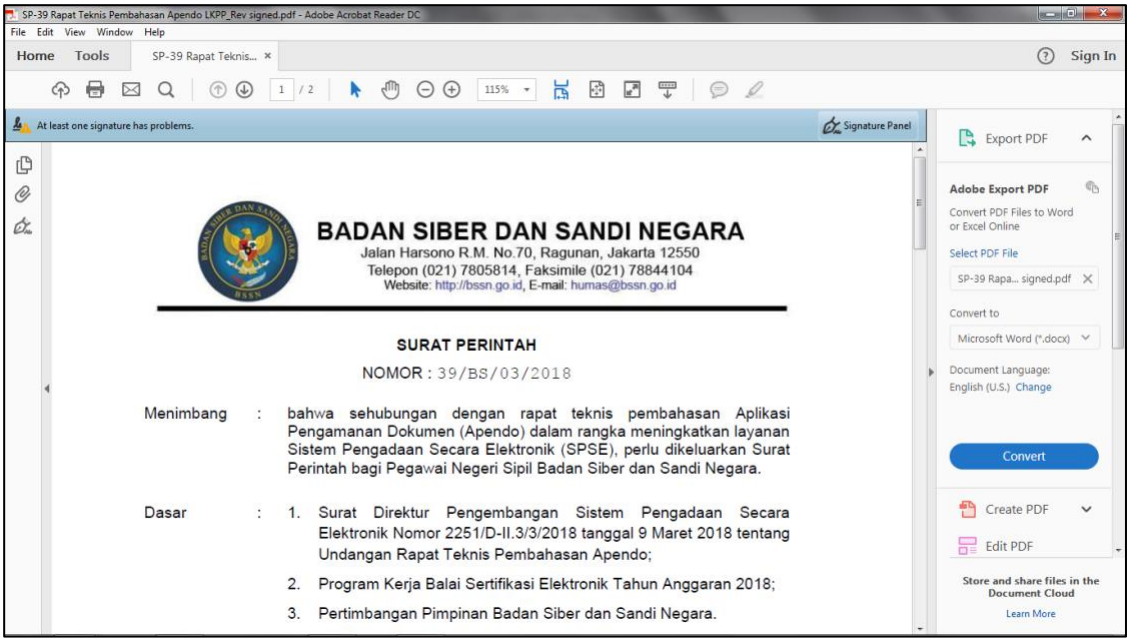


2. Pada tampilan spesimen tanda tangan elektronik dokumen pdf jika ditekan maka Adobe menginformasikan siapa penandatangan, siapa penerbit tanda tangan, waktu, masa valid sertifikat, dll.

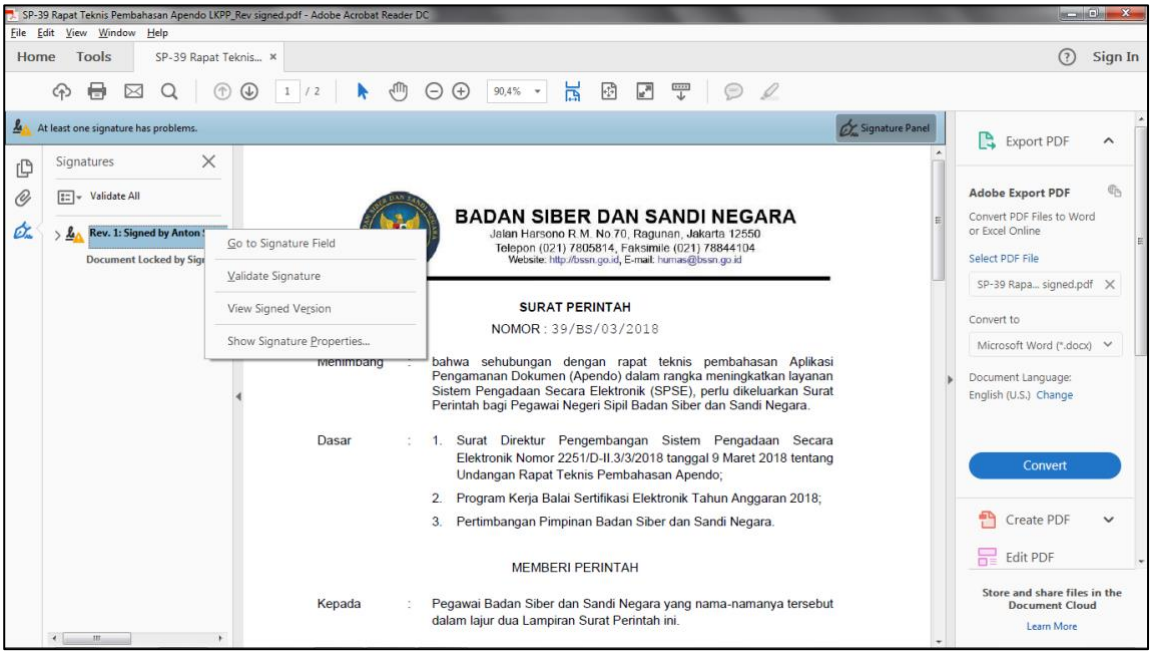


3. Jika dokumen yang ditanda tangani oleh CA (OSD LU KELAS 2) menunjukkan notifikasi berwana kuning. Maka pengguna perlu melakukan trust CA . Langkah – langkah yang perlu dilakukan adalah sebagai berikut:

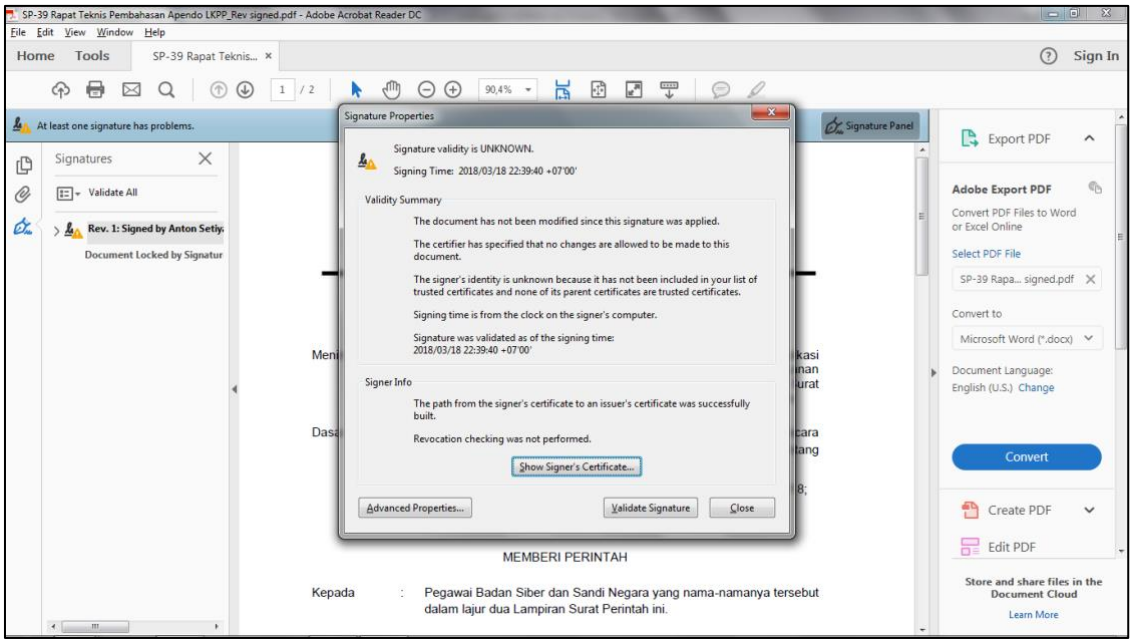
a. Tekan tombol "**Signature Panel**" pada pojok kanan atas Adobe. Adobe akan menampilkan tampilan bar keterangan dokumen.



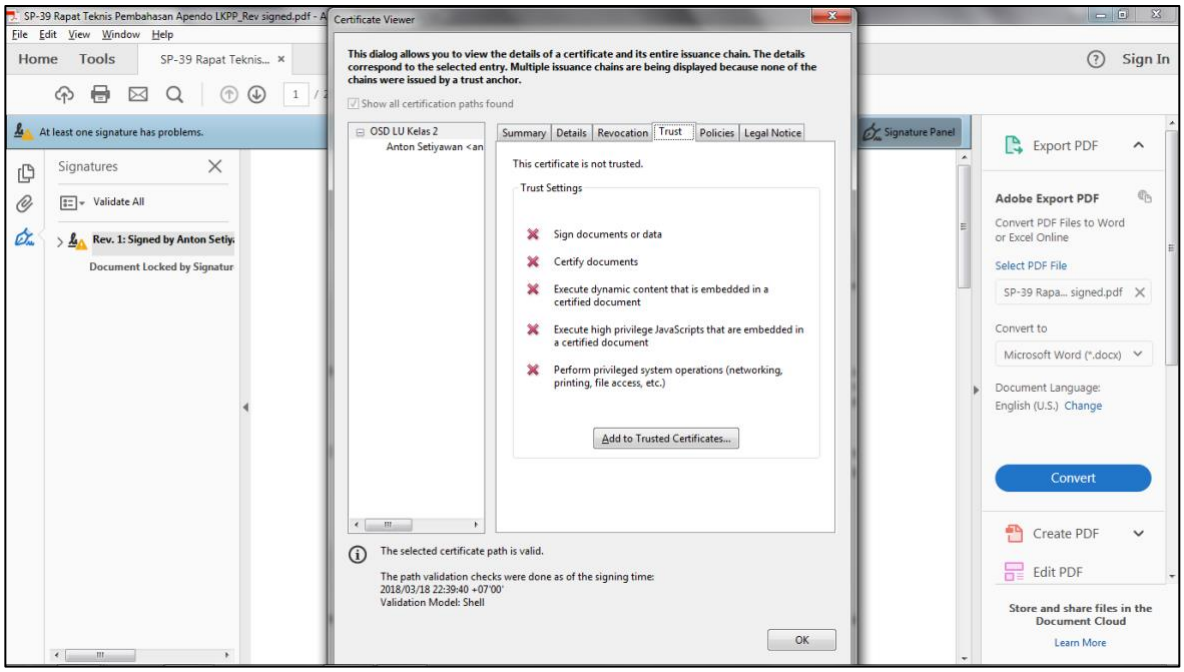
b. Klik kanan pada keterangan penandatangan dokumen. Pilih "**Show Signature Properties**" untuk menampilkan informasi legalitas dokumen.



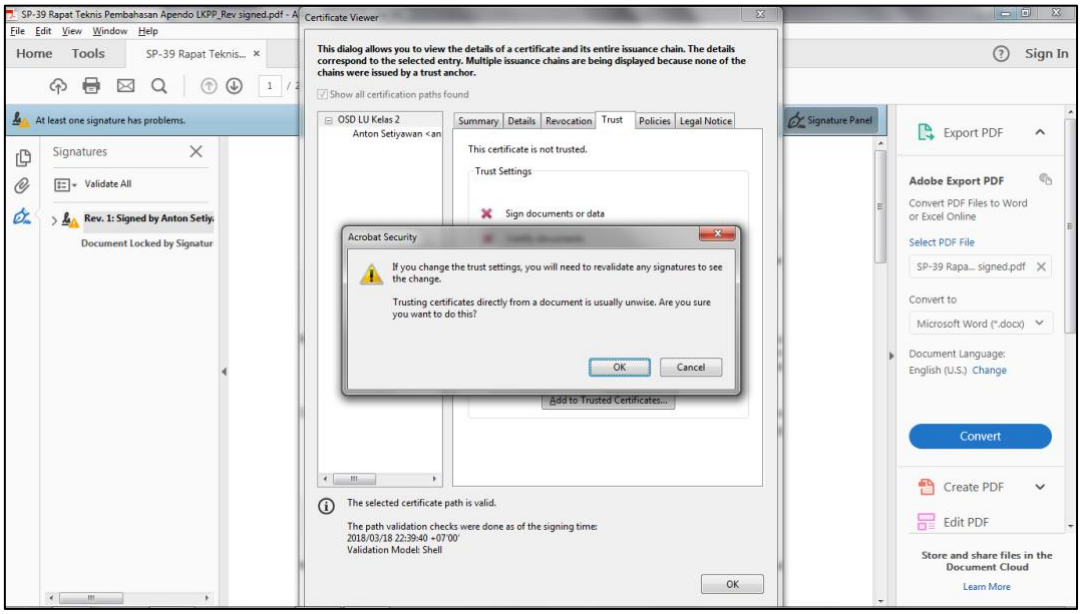
c. Tekan "**Show Signer's Certificate**" untuk menampilkan informasi sertifikat elektronik penandatangan.



d. Tekan "**OSD LU Kelas 2**" untuk memilih Certificate Authority yang akan dipercaya. Kemudian tekan "**Trust**" untuk memproses lebih lanjut dan selanjutnya Tekan "**Add to Trusted Certificates**.." untuk menambahkan CA OSD LU Kelas 2 Sebagai CA terpercaya.



e. Tekan “**OK**” untuk mengkonfirmasi menambahkan CA OSD LU Kelas 2 Sebagai CA terpercaya pada perangkat desktop pengguna.



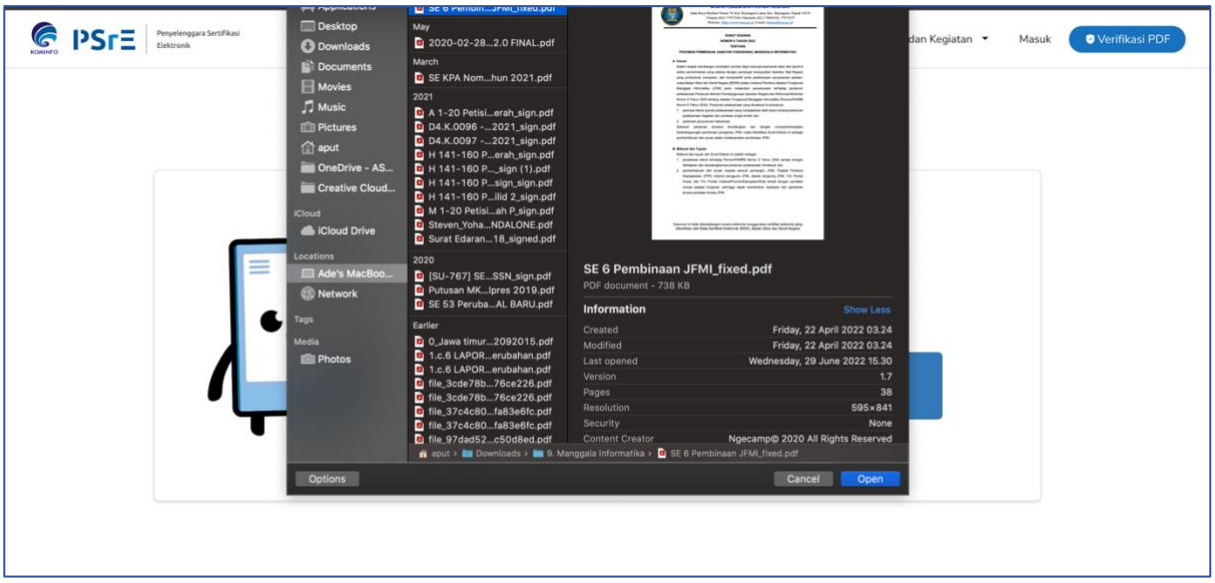
III. VERIFIKASI DENGAN MODUL VERIFIKASI DI WEB

Berikut merupakan langkah – langkah untuk memverifikasi berkas PDF bertanda tangan elektronik pada website.

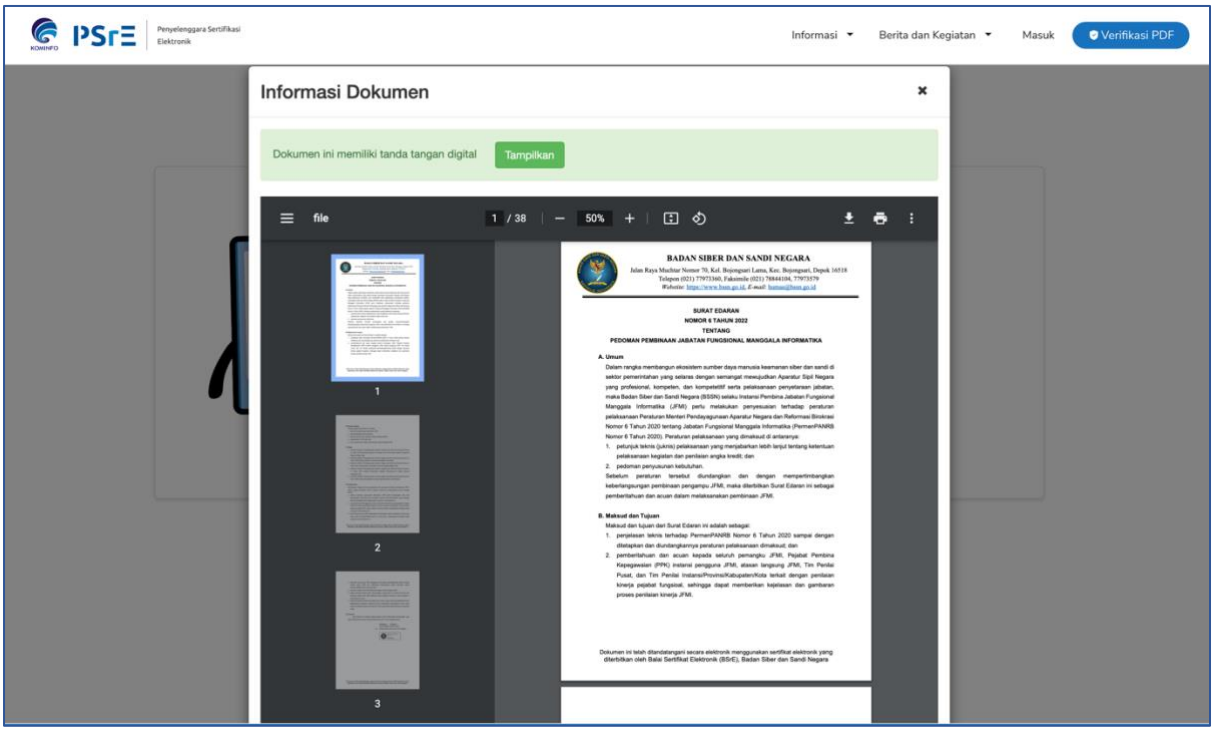
1. Buka website “**tte.kominfo.go.id/verifyPDF**” arahkan pointer mouse pada “**APLIKASI**” tekan “**Unggah Dokumen PDF**”.

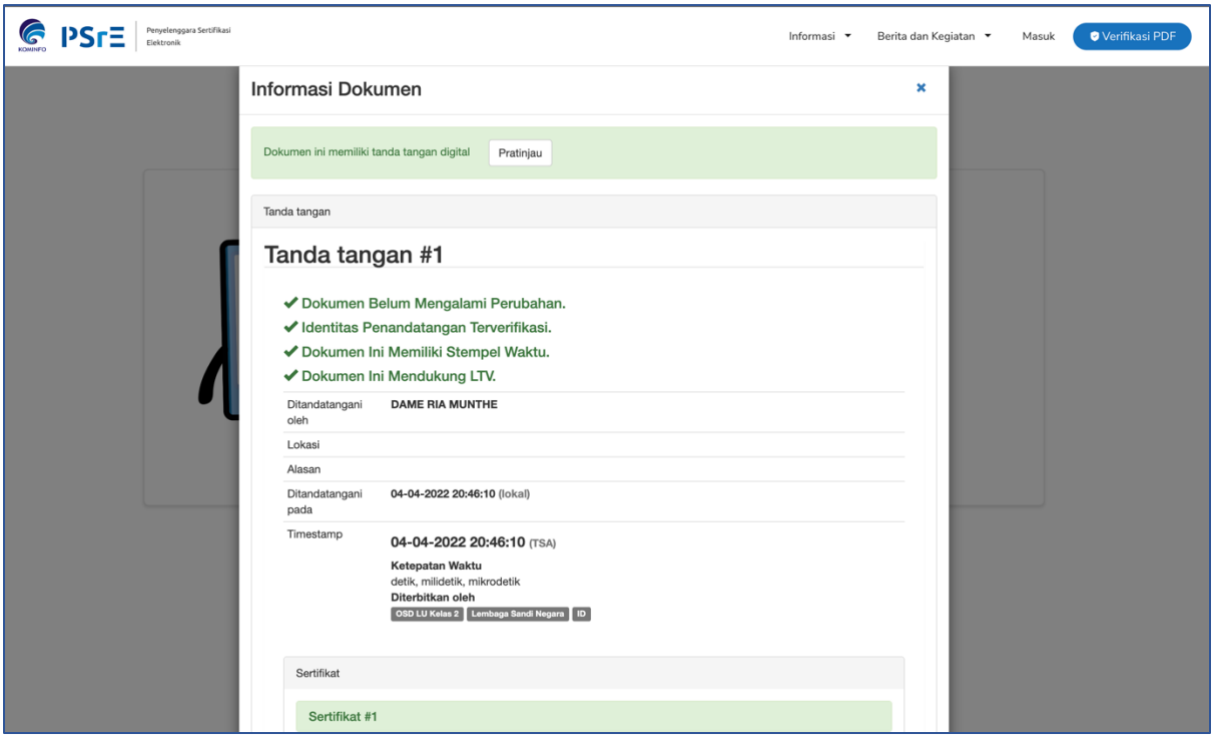


2. Layar menunjukkan halaman browse (file explorer) untuk memilih dokumen PDF yang akan diverifikasi legalitasnya. Pilih dokumen yang akan diverifikasi dengan menekan "**Open".**



3. Akan menampilkan legalitas dokumen PDF bertanda tangan elektronik.

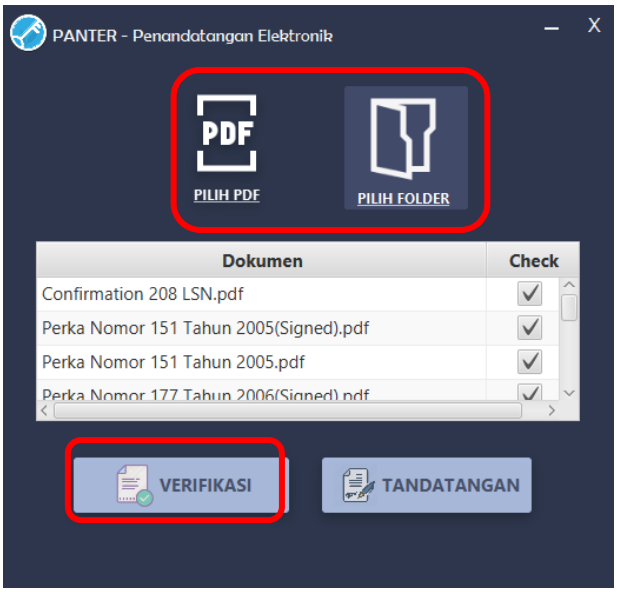



PSrE
Penyelenggara Sertifikasi Elektronik
Informasi
Berita dan Kegiatan
Masuk
Verifikasi PDF
Informasi Dokumen
Dokumen ini memiliki tanda tangan digital
Pratinjau
Tanda tangan
Tanda tangan #1
Dokumen Belum Mengalami Perubahan.
Identitas Penandatangan Terverifikasi.
Dokumen Ini Memiliki Stempel Waktu.
Dokumen Ini Mendukung LTV.
Ditandatangani oleh
DAME RIA MUNTHE
Lokasi
Alasan
Ditandatangani pada
04-04-2022 20:46:10 (lokal)
Timestamp
04-04-2022 20:46:10 (TSA)
Ketepatan Waktu
detik, milidetik, mikrodetik
Diterbitkan oleh
OSD LU Kelas 2
Lembaga Sandi Negara
ID
Sertifikat
Sertifikat #1

IV. VERIFIKASI DENGAN PANTER VERSI 2.0

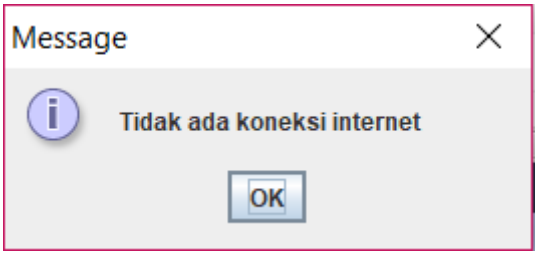
Aplikasi PANTER menyediakan verifikasi dokumen yang ditandatangani secara elektronik, dengan melakukan langkah sebagai berikut :

1. Upload file dokumen yang akan diverifikasi dengan tekan "**PILIH FOLDER**".

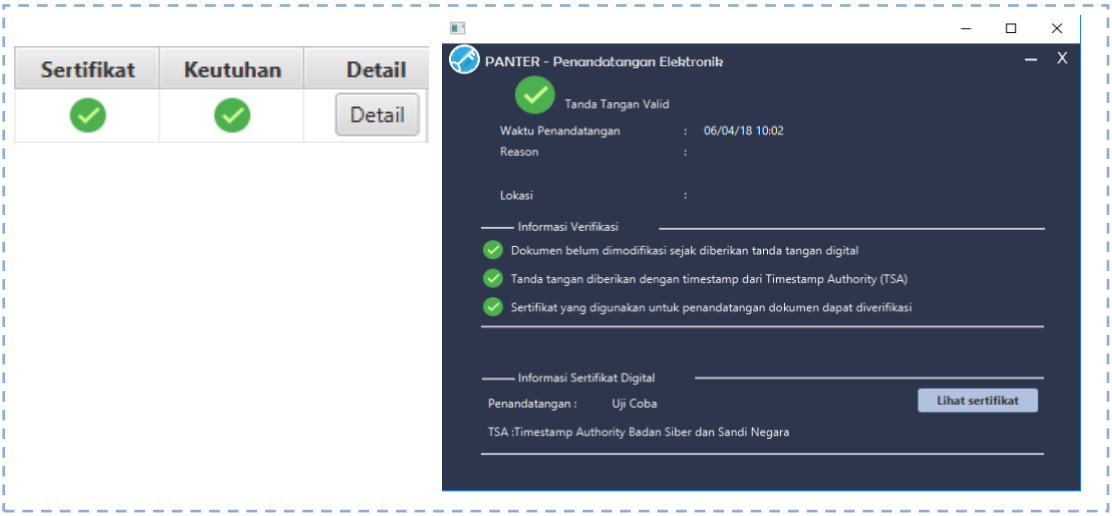


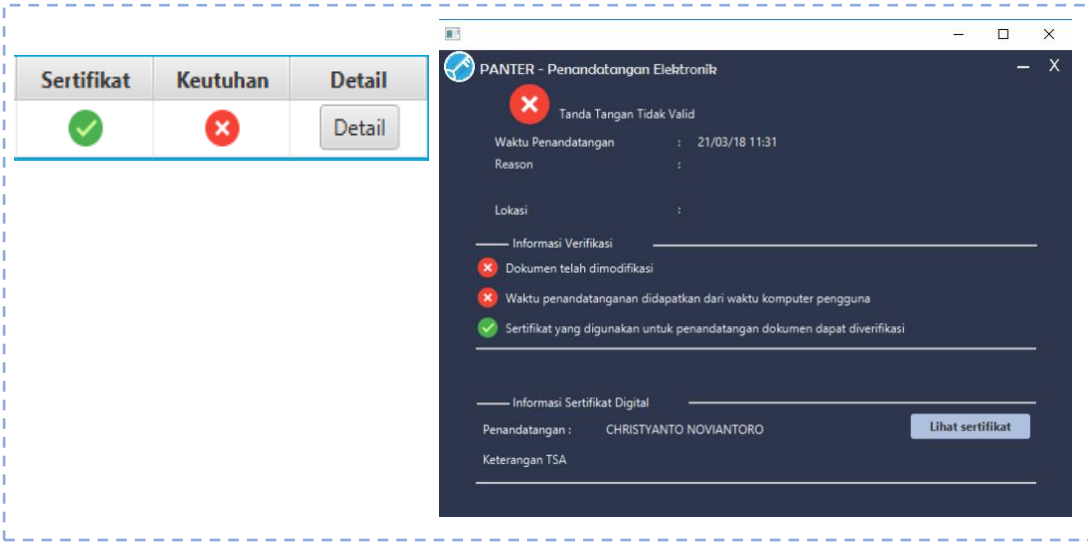
2. Tekan tombol verifikasi, sehingga layar aplikasi akan menampilkan hasil verifikasi seperti pada gambar berikut. Pastikan dokumen yang diverifikasi memiliki sertifikat dan keutuhan yang valid, yang ditunjukan dengan simbol

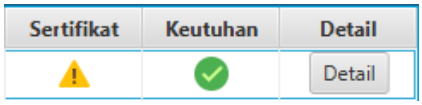
a. Jika komputer tidak terhubung dengan koneksi internet maka akan menampilkan notifikasi sebagai berikut :

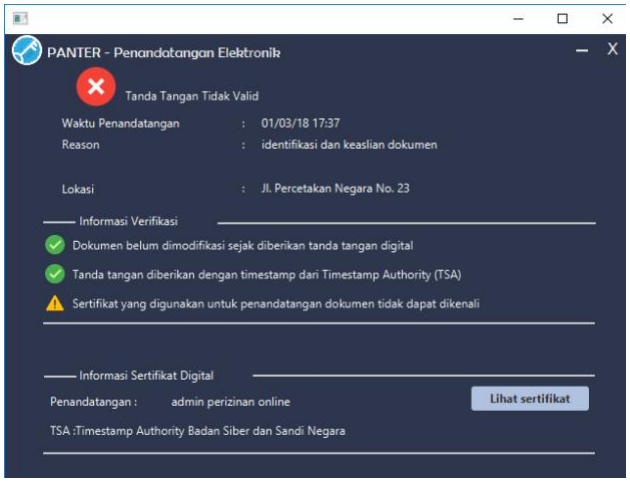


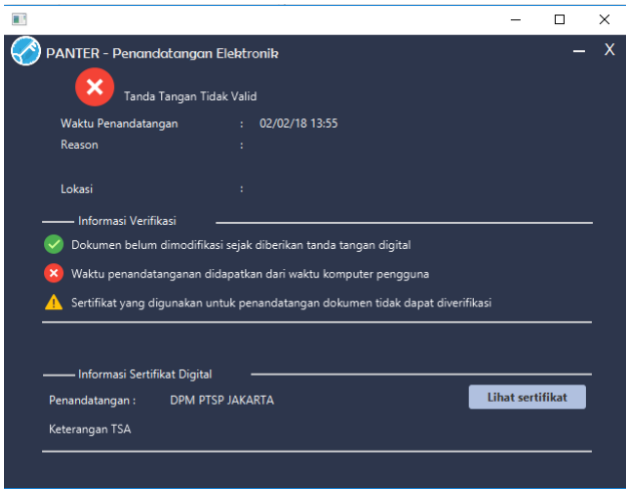
b. Kolom sertifikat dan keutuhan akan menunjukan status dari sertifikat dan keutuhan dokumen. Untuk lebih jelas lagi, tekan tombol detail pada layar aplikasi. Berikut masing-masing symbol :





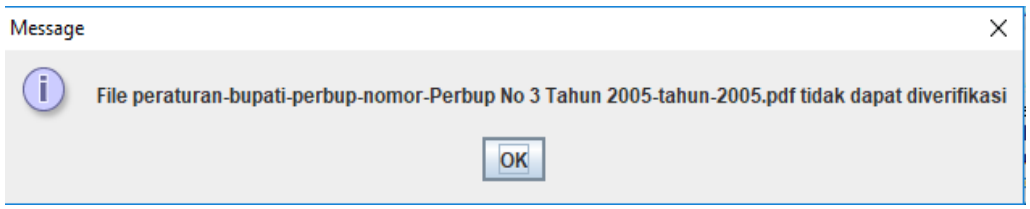








Menyatakan bahwa tidak ada tanda tangan elektronik yang dibubuhkan dalam file dimaksud



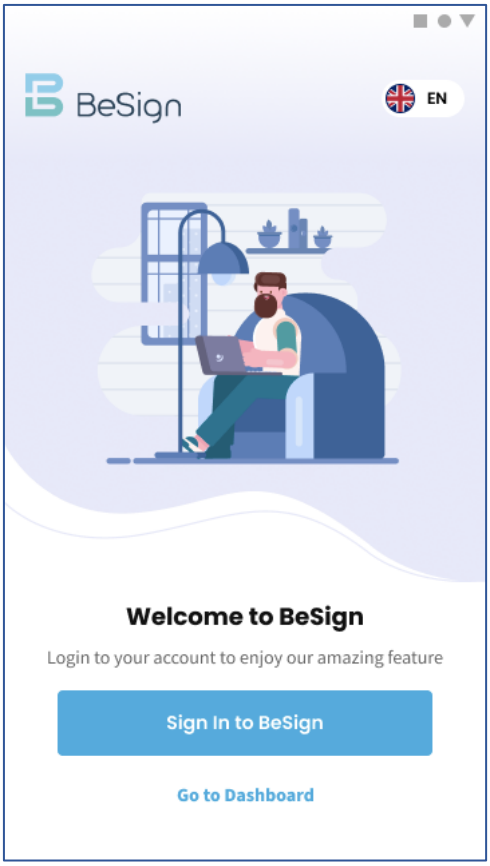
3. Untuk mengetahui lebih rinci informasi sertifikat penandatangan, silahkan klik “**lihat sertifikat**” pada tombol Lihat sertifikat sehingga muncul informasi seperti pada gambar berikut ini :

V. VERIFIKASI DENGAN APLIKASI BESIGN

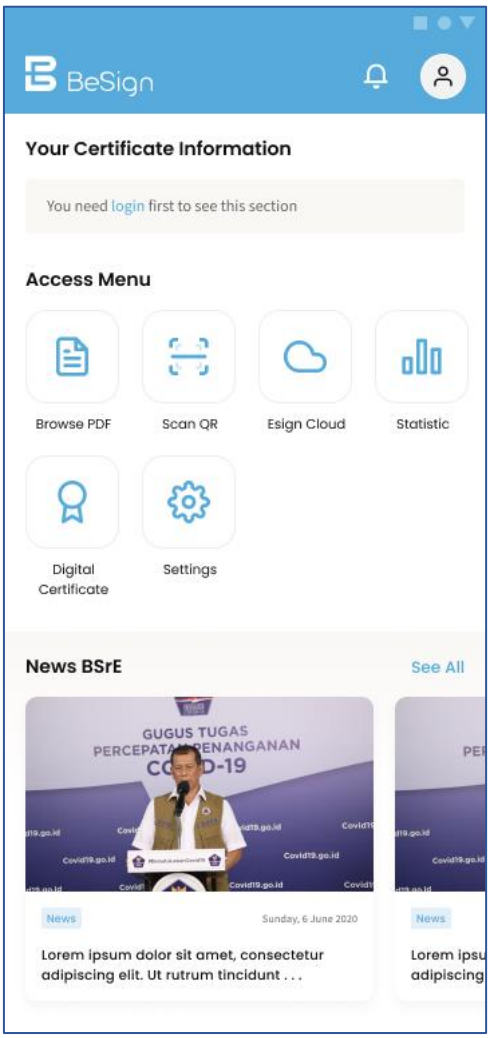
Besign merupakan aplikasi Superapps karya mandiri BSrE pada perangkat smartphone Android dan iOS, yang dapat melakukan manajemen pengguna sertifikat elektronik, tanda tangan elektronik dan verifikasi dokumen bertandatangan elektronik. Aplikasi Besign dapat diunduh pada Google Play Store dan App Store yang tersedia secara bebas.

1. Download aplikasi Besign pada Google Play Store dan Apps Store dengan kata kunci "**Besign**". Pengguna akan ditampilkan aplikasi seperti gambar di samping. Tekan "**INSTALL**" untuk memasang aplikasi pada perangkat smartphone pengguna.

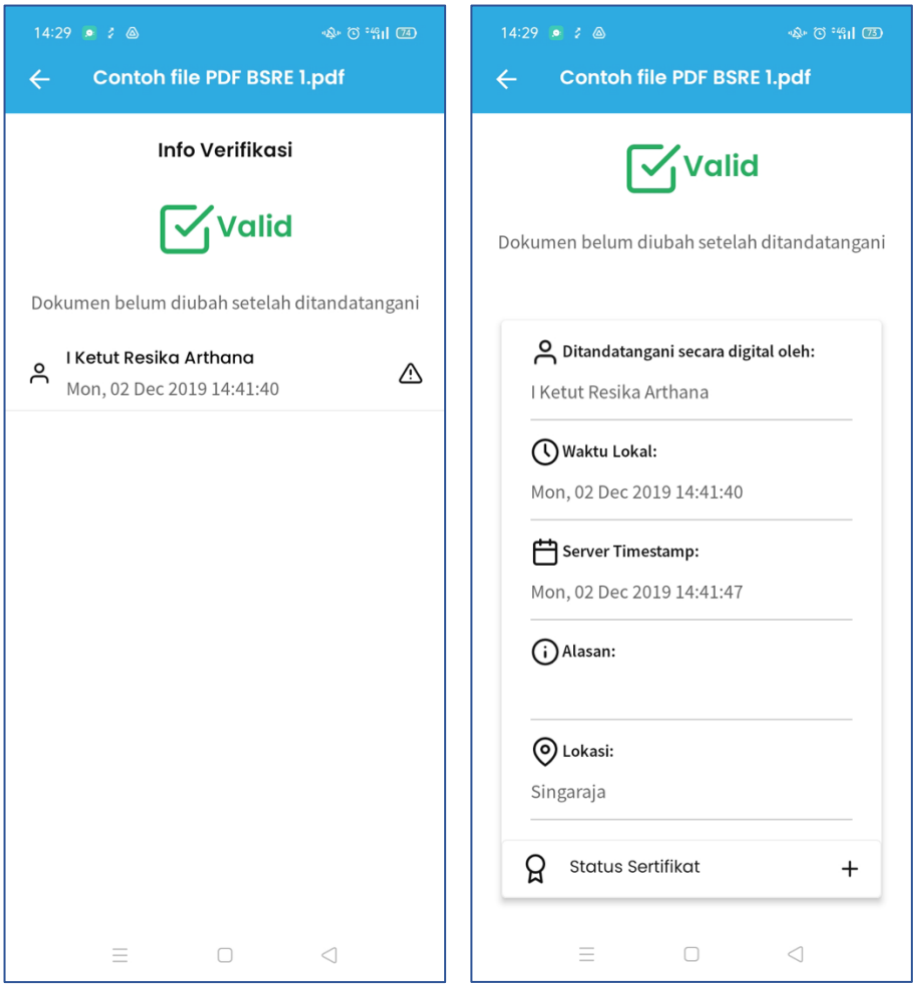
2. Tekan aplikasi Besign untuk membuka aplikasi. Klik "Go To Dashboard" Pengguna juga dapat memilih Bahasa aplikasi pada gambar bendera pada pojok kanan atas.



3. Tekan “**Browser PDF**” untuk melakukan verifikasi dokumen berformat PDF pada smartphone penguna dan pilih dokumen yang akan diverifikasi, atau Tekan “**Scan QR**” untuk melakukan verifikasi salinan dokumen bertanda tangan elektronik yang dicetak.



4. Dokumen yang telah berhasil dibuka akan ditampilkan pada aplikasi Besign. Pada bagian atas terdapat panel “this document contain signatures”, kemudian klik “Show”. Maka akan ditampilkan informasi verifikasi.



VI. VERIFIKASI SERTIFIKAT ELEKTRONIK DENGAN OPENSSL

Verifikasi status sertifikat dapat dilakukan dengan menggunakan OpenSSL, dengan menjalankan perintah berikut

```
openssl ocsp -issuer [certificate_bsre].pem -cert [certificate_pengguna_bsre].pem -text -url [url_ocsp_bsre]
```

```
~ $openssl ocsp -issuer BSRECA.pem -cert aput.pem -text -url https://va.bsre.id/bsrecads/ocsp
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 3824ED41912D49298FF1B4A51104C28AB4A53B20
          Issuer Key Hash: C4F850FECDE7E7D25C0D8C6503FE9B34664D31F9
          Serial Number: 0C364823F0F3ABDFE6DE32999CB4A2E2E1F430DF
    Request Extensions:
        OCSP Nonce:
            0410DBD7C9E210E9CA966E20B676E44B308F
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C83168A5E3843A9539CFAAF8B60384393C14BF60
    Produced At: Aug  2 05:08:54 2022 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 3824ED41912D49298FF1B4A51104C28AB4A53B20
      Issuer Key Hash: C4F850FECDE7E7D25C0D8C6503FE9B34664D31F9
      Serial Number: 0C364823F0F3ABDFE6DE32999CB4A2E2E1F430DF
    Cert Status: good
    This Update: Aug  2 05:08:54 2022 GMT

    Response Extensions:
        OCSP Nonce:
            0410DBD7C9E210E9CA966E20B676E44B308F
    Signature Algorithm: sha256WithRSAEncryption
         aa:7c:70:52:95:3f:ea:48:8f:f5:c6:ed:96:1f:f3:16:44:62:
         f2:a4:31:08:f6:7e:28:2b:be:ce:d4:85:71:45:1a:be:bc:32:
         03:87:f1:94:44:79:7d:09:1e:a7:c6:b4:f1:29:64:fe:2b:05:
         e6:23:3d:f7:f4:11:2d:dd:b4:0f:e8:7d:eb:38:4a:1d:0e:97:
         78:92:35:c9:b9:a1:c5:1e:1f:a6:6a:cc:a9:3a:ed:1d:3d:88:
         d5:84:35:63:88:14:d0:3b:aa:4a:2a:c7:cb:17:9a:ca:8e:dc:
         75:35:16:95:b6:96:7b:bf:80:1a:8d:75:39:c4:10:00:a4:1d:
         8a:93:59:3a:1c:13:f7:c4:7e:f8:7c:00:bc:54:7c:fc:f6:51:
         15:05:2b:aa:85:52:c4:f3:77:a2:8e:ce:fe:e1:9c:02:c9:28:
         1b:21:55:e3:b7:bc:cc:83:39:49:a1:ea:15:ed:b1:45:0a:3d:
         45:74:22:33:82:55:07:67:b2:35:46:c6:c2:44:2f:de:d9:03:
         0d:df:09:c7:04:38:97:29:d3:1c:3c:62:05:2b:d2:b1:0f:73:
         f5:7c:e1:1b:d0:33:da:a9:8d:3f:ed:09:19:4c:07:4e:2e:43:
         67:db:df:45:c1:b2:03:ba:6d:d8:d0:43:16:10:20:54:2e:2c:
         2c:f2:ea:61
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3f:d0:98:98:ea:68:2d:46:aa:7c:a0:f8:b4:ed:a5:d6:1b:6a:3e:30
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=BSRE CA DS G1, O=Balai Sertifikasi Elektronik, C=ID
        Validity
            Not Before: Aug  2 03:10:24 2022 GMT
            Not After : Aug  1 03:10:23 2027 GMT
        Subject: CN=BSrE CA DS - Validation Authority, OU=BSrE OCSP Responder, O=Balai Sertifikasi Elektronik, L=Jakarta Selatan, ST=DKI Jakarta, C=ID
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

```
         c3:fe:60:2a:2c:b8:df:67:76:a6:ca:12:c1:d7:d9:21:6b:72:
         84:ea:26:19:9a:11:e9:c5:29:8c:a9:c8:33:0c:88:29:ad:57:
         e2:22:8c:b0:e1:ac:24:bf:71:e8:6c:5b:5b:79:7e:e2:67:74:
         bc:d2:84:c3:26:0e:f5:a5:a4:43:a0:30:ac:92:b6:35:c0:2e:
         8b:67:b6:20:38:6f:d4:51:a8:bc:3a:08:48:9b:87:95:a5:4f:
         ee:5d:ca:15:ce:e3:3c:5c:f0:50:50:c5:99:a7:70:e6:d1:31:
         52:07:72:cf:26:e0:27:d5:09:57:3a:b8:5d:54:99:f1:77:d9:
         5c:67:ad:2e:23:fc:5b:52:c5:bd:c2:e9:e8:9b:41:88:53:05:
         d0:23:a9:cf:d3:fb:d9:4f:70:8b:1e:15:73:25:bc:17:2b:b4:
         f9:d2:5f:d1:de:94:66:9f:80:14:71:2f:53:f1:25:0e:8a:e4:
         2c:8a:e7:ed:46:2e:59:33:ae:6a:40:b6:b3:e5:cf:55:96:94:
         32:bd:2b:a6:b5:33:1b:65:e8:f0:e2:21:55:53:b1:b3:1a:de:
         af:5d:56:5f:3e:09:4f:7d:5d:c5:6c:39:e6:1c:d3:30:20:4b:
         bf:e8:5a:88:3e:12:23:55:0e:e3:64:65:f4:c1:c7:b3:4e:52:
         cf:64:ac:52:f7:8e:3f:12:5c:8e:b4:7c:93:c6:48:5e:12:e8:
         25:e5:56:fe:28:02:2a:b9:b3:71:ac:7e:36:b6:2a:12:7a:93:
         34:c2:8b:6d:35:66:a0:9c:58:13:1c:7b:97:35:ec:8b:31:22:
         ae:1b:3a:c1:ac:92:42:0e
-----BEGIN CERTIFICATE-----
MIIFETCCAvmgAwIBAgIUP9CYmOpoLUaqfKD4tO2l1htqPjAwDQYJKoZIhvcNAQEL
BQAwTDEWMBQGA1UEAwwNQlNSRSBDQSBEUyBHMTElMCMGA1UECgwcQmFsYWkgU2Vy
dGlmaWthc2kgRWxla3Ryb25pazELMAkGA1UEBhMCSUQwHhcNMjIwODAyMDMxMDI0
WhcNMjcwODAxMDMxMDIzWjCBrjEqMCgGA1UEAwwhQlNyRSBDQSBEUyAtIFZhbGlk
YXRpb24gQXV0aG9yaXR5MRwwGgYDVQQLDBNCU3JFIE9DU1AgUmVzcG9uZGVyMSUw
IwYDVQQKDBxCYWxhaSBTZXJ0aWZpa2FzaSBFbGVrdHJvbmlrMRgwFgYDVQQHDA9K
YWtcnRhIFNlbGF0YW4xFDASBgNVBAgMC0RLSSBKYWtcnRhMQswCQYDVQQGEwJJ
RDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOnh+Z8VAzOAGCXWtB3k
u2/sN7cp1qQ8tMOsOgfkE3Bnfd3xIz4ZHhowWIF07zWK3AFhDQLAaTV6yjSf/rO
G45rbtJn/ObwL81FcYQYoqCUCsd4NB0vCs9kOB4KO/9mnDmPx2KRVCFPcF8OzlkS
D15BAvmBEan29LbVy2dulTcZcC0wBCvZw94JpdqgKofy59S7+gl8x8tyem/VqNP0
axNjBumpMDBMdw6pfT2DPaX8bSHoy1opmx9h3bH0VgFxypm3tAw3E1m9y0tJ+XZz
IHMRMmOzkAVmURCYp+1p8mmr4QV2D7+l/H2UM6owRAoNjdddrd2uApdI2csgIwUrs
Rd8CAwEAAaOBhzCBhDAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFMT4UP7N5+fS
XA2MZQP+mzRmTTH5MA8GCSsGAQUFBzABBQQCBQAwEwYDVR0lBAwwCgYIKwYBBQUH
AwkwHQYDVR0OBBYEFMgxaKXjhDqVOc+q+LYDhDk8FL9gMA4GA1UdDwEB/wQEAwIH
gDANBgkqhkiG9w0BAQsFAAOCAgEArXFe3Wvl/lf3VgM+iUKw+I5OpsBtCFUP4iu7
dW1ZO5l1QHvNm4mpxg+loZAYgw19bjQ+SihBRHNSZHs7vm7G0mU/3kFCFwY/uAbd
2wiwc8aAzU86ytNp/MwhCfx7NJIO/iw5Fv8n45eD+tefequWVJdUqX5cVzJk/RZB
0iDns0fcM476CpCg2IwZ9LMVarXIQ5pUd7ymEJK26XFewabtspWuUG7PWlvrjWss
s8nzBn7VctE/Myc0BbnV9t8vbeSN6eYPNp9Bw/5gKiy432d2psoSwdfZIWtyhOom
GZoR6cUpjKnIMwyIKa1X4iKMsOGsJL9x6GxbW3l+4md0vNKEwyYO9aWkQ6AwrJK2
NcAui2e2IDhv1FGovDoISJuHlaVP713KFc7jPFzwUFDFmadw5tExUgdyzybgJ9UJ
Vzq4XVSZ8XfZXGetLiP8W1LFvcLp6JtBiFMF0COpz9P72U9wix4VcyWBFyu0+dJf
0d6UZp+AFHEvU/ElDorkLIrn7UYuWTOuakC2s+XPVZaUMr0rprUzG2Xo8OIhVVOx
sxrer11WXz4JT31dxWw55hzTMCBLv+haiD4SI1UO42Rl9MHHs05Sz2SsUveOPxJc
jrR8k8ZIXhLoJeVW/igCKrmzcax+NrYqEnqTNMKLbTVmoJxYExx7lzXsizEirhs6
waySQg4=
-----END CERTIFICATE-----
Response Verify Failure
4598834688:error:27069065:OCSP routines:OCSP_basic_verify:certificate verify error:crypto/ocsp/ocsp_vfy.c:93:Verify error:unable to get local issuer certificate
4598834688:error:27069065:OCSP routines:OCSP_basic_verify:certificate verify error:crypto/ocsp/ocsp_vfy.c:93:Verify error:self signed certificate in certificate chain
aput.pem: good
        This Update: Aug  2 05:08:54 2022 GMT
~ $
```

VII. TABEL RUJUKAN VERIFIKASI

Dalam operasionalnya dapat ditemukan perbedaan hasil verfikasi yang disebabkan perbedaan penggunaan library verifikasi pada aplikasi.

	Adobe	Website	Panter	Besign	Kesimpulan
Hasil Verifikasi	✅	✅	✅	✅	✅
	❌	✅	✅	✅	✅
	✅	❌	✅	❌	✅
	✅	✅	❌	✅	✅
	❌	❌	❌	❌	❌

-SELESAI-

Jika terjadi kendala silahkan menghubungi kami di:
BALAI SERTIFIKASI ELEKTRONIK

JL.Mampang Prapatan VIII No.27 Tegal Parang, Mampang Prapatan, Jakarta Selatan

(021) 7900534

info.bsre@bssn.go.id