



Balai
Sertifikasi
Elektronik

PETUNJUK TEKNIS PENGGUNAAN API E-SIGN CLIENT SERVICE

BALAI SERTIFIKASI ELEKTRONIK
“BUILD TRUST IN ELECTRONIC TRANSACTIONS”

INFORMASI DOKUMEN

JUDUL :	PETUNJUK TEKNIS PENGGUNAAN API ESIGN CLIENT SERVICE	VERSI :	2.0
TANGGAL PEMBUATAN :	Januari 2024	DIBUAT OLEH :	Tim Dukungan Aplikasi
DIPERIKSA OLEH :	<p style="text-align: center;">Ketua Tim Dukungan Aplikasi</p> 		
DISETUJUI OLEH :	<p style="text-align: center;">Kepala Balai Sertifikasi Elektronik</p> 		

CATATAN VERSI DOKUMEN

Nomor	Tanggal	Direvisi oleh	Keterangan
1	Desember 2020	Andreyanto Pratama, S.Tr.TP	Pembuatan Petunjuk Teknis Penggunaan API Esign Client Service
2	Januari 2024	Diah Mulya Pitaloka, A.Md.	Pembaruan Petunjuk Teknis Penggunaan API Esign Client Service Versi 2.0

DAFTAR ISI

1. PENDAHULUAN.....	1
1.1. SKEMA.....	1
2. LISENSI.....	2
3. PRASYARAT.....	3
3.1. PERSIAPAN SERVER ESIGN CLIENT.....	3
3.2. INSTALASI SERVER ESIGN CLIENT.....	3
4. PEMBUATAN CREDENTIAL.....	4
5. API SERVICE VERSION 1.....	7
5.1. AUTHORIZATION.....	7
5.2. SIGN PDF.....	7
5.3. API DOWNLOAD (SIGNED) DOCUMENT.....	15
5.4. VERIFY PDF.....	15
6. API SERVICE VERSION 2.....	18
6.1. AUTHORIZATION.....	18
6.2. API SIGN.....	18
6.3. API REQUEST SIGN TOTP.....	24
6.4. API REQUEST SEAL ACTIVATION TOTP.....	25
6.5. API REQUEST SEAL OTP.....	28
6.6. API SEAL PDF.....	29
6.7. CHECK STATUS USER.....	31
6.8. REGISTRASI USER.....	33
6.9. VERIFY PDF.....	34

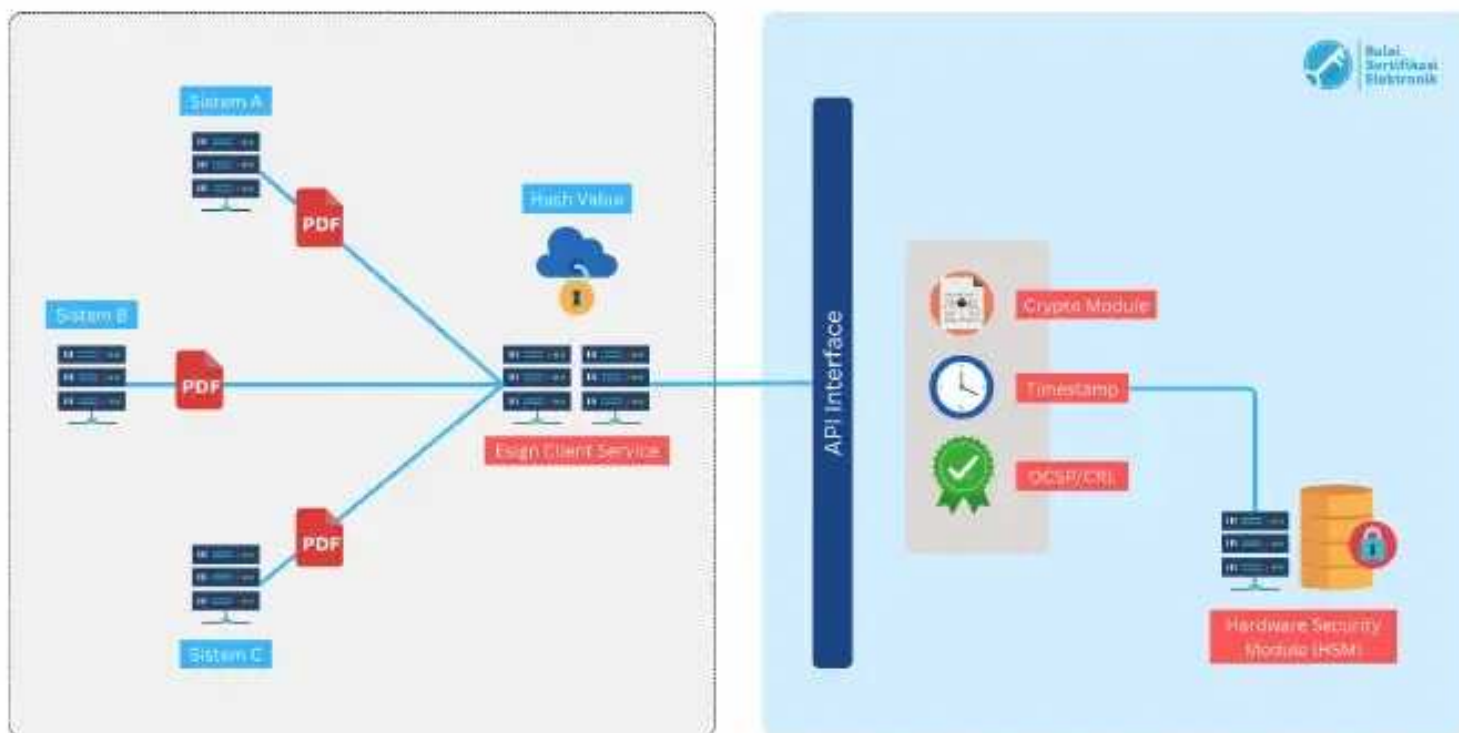
1. PENDAHULUAN

Esign Client Service adalah aplikasi penghubung antara Sistem Informasi yang dimiliki pengguna dengan Sistem Penandatanganan Elektronik berbasis cloud milik

Balai Sertifikasi Elektronik (BSrE). Pengguna dapat menggunakan Esign Client Service untuk mengembangkan sistem transaksi elektronik yang membutuhkan tanda tangan elektronik.

1.1. SKEMA

Secara umum, peran Esign Client Service sebagai penghubung sistem dalam transaksi menggunakan Sertifikat Elektronik dapat digambarkan sebagai berikut:



Esign Client Service yang terpasang di server sisi pengguna akan menghitung nilai *hash* dokumen yang akan ditandatangani lalu mengirimkannya ke Esign BSrE. Pada Esign BSrE, nilai hash tersebut akan diolah menjadi nilai *signature* yang kemudian akan dikirimkan kembali ke Esign Client Service untuk disematkan pada dokumen. Esign Client Service dapat digunakan oleh lebih dari satu sistem/aplikasi. Setiap sistem/aplikasi yang akan menerapkan tanda tangan elektronik dapat menggunakan REST API yang disediakan oleh Esign Client Service telah diinstal pada jaringan local instansi pengguna.

2. LISENSI

Esign Client Service dirilis dengan hak cipta oleh BSR E Badan Siber dan Sandi Negara (BSSN), yang artinya produk ini tidak dapat digunakan tanpa izin dari BSR E-BSSN. Saat ini Esign Client Service diperuntukkan bagi sistem informasi yang dibangun oleh instansi pemerintah.

3. PRASYARAT

3.1. PERSIAPAN SERVER ESIGN CLIENT

Sebelum menggunakan Esign Client Service, pengguna harus mempersiapkan terlebih dahulu server yang akan menjadi tempat di mana Esign Client Service akan dipasangkan. Terdapat dua server yang harus dipersiapkan, yaitu untuk lingkungan pengembangan (*Development Environment*) dan untuk lingkungan sistem sedang aktual berjalan (*Production Environment*). Server setidaknya memiliki spesifikasi minimum sebagai berikut:

1. OS: CentOS 7 2009
2. RAM: 8 GB
3. Processor: 4 Core
4. HDD: 50 GB
5. Jaringan: Koneksi Internet; Port 80, 443, 22

Selain spesifikasi minimum seperti di atas, terdapat beberapa alamat yang harus dimasukkan ke dalam *whitelist* untuk menunjang kelancaran instalasi dan penggunaan Esign Client Service. Alamat tersebut antara lain:

1. <https://api-bsre.bssn.go.id> (*production*)
2. <https://registry-bsre.bssn.go.id> (*development dan production*)
3. mail.bssn.go.id (*production dan development*)

3.2. INSTALASI SERVER ESIGN CLIENT

Instalasi Esign Client Service dapat dilakukan dengan menghubungi kontak yang tersedia pada dukungan teknis di dokumen ini. Setelah instalasi selesai, Esign Client Service dapat diakses dengan memasukkan alamat `http://{IP Server Esign Client}`.

4. PEMBUATAN CREDENTIAL

Kredensial digunakan sebagai otentikasi dari Sistem Informasi milik pengguna kepada Esign Client Service. Pembuatan kredensial dapat dilakukan dengan mengakses Esign Client Service melalui peramban ke alamat `http://{IP Server Esign Client}/login`, maka akan menampilkan halaman seperti di bawah ini.



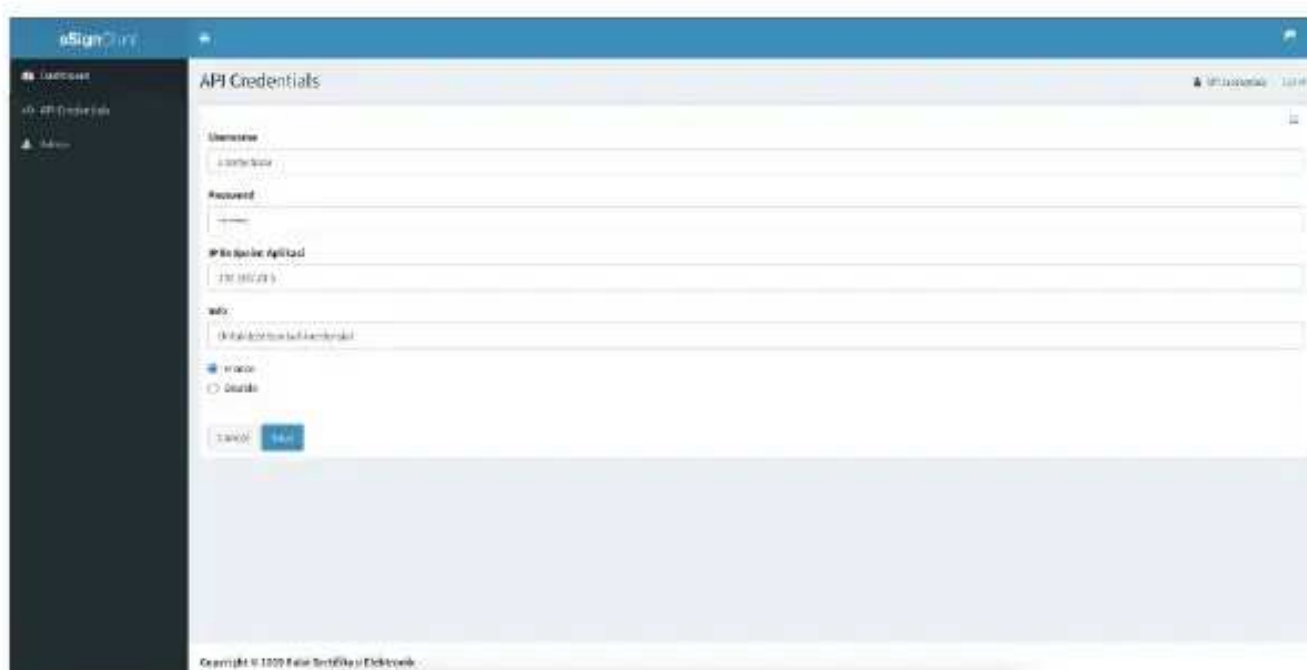
Untuk masuk ke halaman berikutnya, secara *default* dapat menggunakan *username* admin dan *password* qwerty. *Password* dapat diganti sesuai dengan keinginan pengguna. Setelah berhasil login, akan muncul halaman dashboard seperti berikut.



Terdapat dua menu di sini yaitu Dashboard dan API Credentials. Halaman Dashboard berfungsi untuk memantau jumlah aplikasi yang terhubung dengan API Esign Client Service.



Sedangkan halaman API Credentials berfungsi untuk melihat kredensial aplikasi apa saja yang terhubung dengan API Esign Client Service dan menambahkan kredensial baru. Untuk menambahkan kredensial baru, dapat dilakukan dengan klik tombol "Tambah API".



Pada halaman kredensial ada beberapa kolom yang harus diisi oleh pengguna, yaitu Username, Password, IP Endpoint/Aplikasi yang akan dipasangkan kredensial, Informasi singkat mengenai aplikasi, dan status kredensial apakah akan diizinkan (Enable) atau tidak diizinkan (Disable).

Setelah memenuhi kolom isian, kredensial dapat disimpan dengan menekan tombol Save.



Pada Kredensial yang sudah disimpan, terdapat dua aksi untuk mengelola data yaitu edit dan delete. Aksi edit digunakan untuk mengubah data Kredensial yang sudah dibuat, sementara aksi delete digunakan untuk menghapus data Kredensial.

Kredensial yang sudah ditambahkan ini akan digunakan saat melakukan hit API Esign Client Service.

5. API SERVICE VERSION 1

Application Programming Interface (API) Esign Client Service adalah antarmuka yang digunakan untuk melakukan komunikasi antara sistem pengguna dengan Esign BSR.E. API ini dapat diakses menggunakan Aplikasi Penguji API seperti Postman, Insomnia dan sebagainya.

Pada versi 1 ini, ada tiga endpoint utama yang dapat digunakan untuk implementasi tanda tangan elektronik, yaitu Sign PDF, Download Signed Document, dan Verify. Namun sebelum dijelaskan lebih lanjut, pengguna harus mengetahui komponen apa saja yang tersedia di Esign Client Service.

5.1. AUTHORIZATION

Sebelum mengakses endpoint, pengguna harus mengisi terlebih dahulu otorisasi yang berfungsi sebagai pemberian hak akses penggunaan. Tipe otorisasi yang digunakan adalah Basic Auth yang diisi dengan username dan password aplikasi. Kedua kredensial ini bisa didapatkan dari halaman admin Esign Client Service.

Header

Tipe	Content
Basic Auth	base64(username:password)

5.2. SIGN PDF

Endpoint ini berfungsi untuk membubuhkan tanda tangan elektronik pada dokumen. Terdapat dua tipe tanda tangan untuk endpoint ini, yaitu *visible* (menggunakan visualisasi), dan *invisible* (tidak menggunakan visualisasi).

Endpoint

Method	URL
POST	/api/sign/pdf

Parameter (Visualisasi dengan Spesimen Kustom)

Type	Params	Values
POST	file	file (.pdf)
POST	imageTTD	file (.jpg)
POST	nik	string
POST	passphrase	string
POST	tampilan	string (visible)
POST	page	number
POST	image	boolean (true)
POST	tag_koordinat	string
POST	xAxis	number
POST	yAxis	number
POST	width	number
POST	height	number

Parameter (Visualisasi dengan QR Code)

Type	Params	Values
POST	file	file (.pdf)
POST	nik	string
POST	passphrase	string
POST	tampilan	string (visible)
POST	page	number
POST	image	boolean (false)
POST	linkQR	string
POST	tag_koordinat	string
POST	xAxis	number
POST	yAxis	number
POST	width	number
POST	height	number

Parameter (Tanpa Visualisasi)

Type	Params	Values
POST	file	file (.pdf)
POST	nik	string
POST	passphrase	string
POST	tampilan	string (invisible)

Dari daftar parameter di atas, berikut adalah penjelasan masing-masing parameter.

1. File

File merupakan parameter yang diisi dengan dokumen yang akan ditandatangani. Dokumen yang dapat diunggah adalah dokumen dengan format PDF. Parameter ini wajib diisi oleh pengguna.

2. NIK

NIK merupakan parameter yang diisi dengan Nomor Induk Kependudukan milik pengguna yang akan membubuhkan tanda tangan elektronik. Parameter ini diisi dengan format string dan alfanumerik yang terdiri dari 16 digit. Parameter ini wajib diisi oleh pengguna.

3. Passphrase

Passphrase merupakan parameter yang diisi dengan kata kunci milik pengguna. Parameter ini diisi menggunakan format string dan wajib diisi oleh pengguna.

4. Tampilan

Parameter ini berfungsi untuk mengatur tampilan spesimen tanda tangan. Ada dua tipe pada parameter ini, yaitu *visible* dan *invisible*.

Jika pengguna ingin menampilkan visualisasi tanda tangan elektronik, maka parameter ini diisi dengan isian *visible*. Sedangkan jika pengguna tidak ingin menampilkan visualisasi apapun, parameter bisa diisi dengan *invisible*.

5. Image

Parameter image digunakan untuk menentukan tipe spesimen sebagai visualisasi. Parameter ini memiliki dua isian, yaitu `true` dan `false`.

Jika pengguna ingin membubuhkan spesimen kustom, parameter ini dapat diisi `true`. Jika diisi `false`, maka parameter `linkQR` wajib diisi. Penggunaan parameter `linkQR` akan dijelaskan pada poin berikutnya.

6. ImageTTD

Image TTD merupakan parameter yang isianya masih terkait dengan parameter Image di atas. Jika parameter Image diisi dengan `true`, maka spesimen visualisasi TTE harus diunggah. Parameter ini dapat menerima gambar dalam bentuk JPG, JPEG, atau PNG.

7. LinkQR

Selain ImageTTD, parameter ini juga terkait dengan parameter Image. Jika pada parameter Image diisi dengan `false`, maka parameter ini dapat diisi dengan link yang akan dituju. Parameter ini berfungsi untuk menghasilkan QR code yang akan mengarah ke alamat tertentu.

8. Halaman

Parameter ini wajib diisi jika tipe visualisasi yang akan dibubuhkan adalah `visible`, parameter ini berfungsi untuk meletakkan spesimen visualisasi di awal atau akhir halaman.

9. Page

Parameter ini wajib diisi jika visualisasi yang akan dibubuhkan adalah `visible`, parameter ini berfungsi untuk meletakkan spesimen visualisasi di halaman yang ditentukan oleh pengguna. Parameter ini diisi dengan nomor halaman pada dokumen.

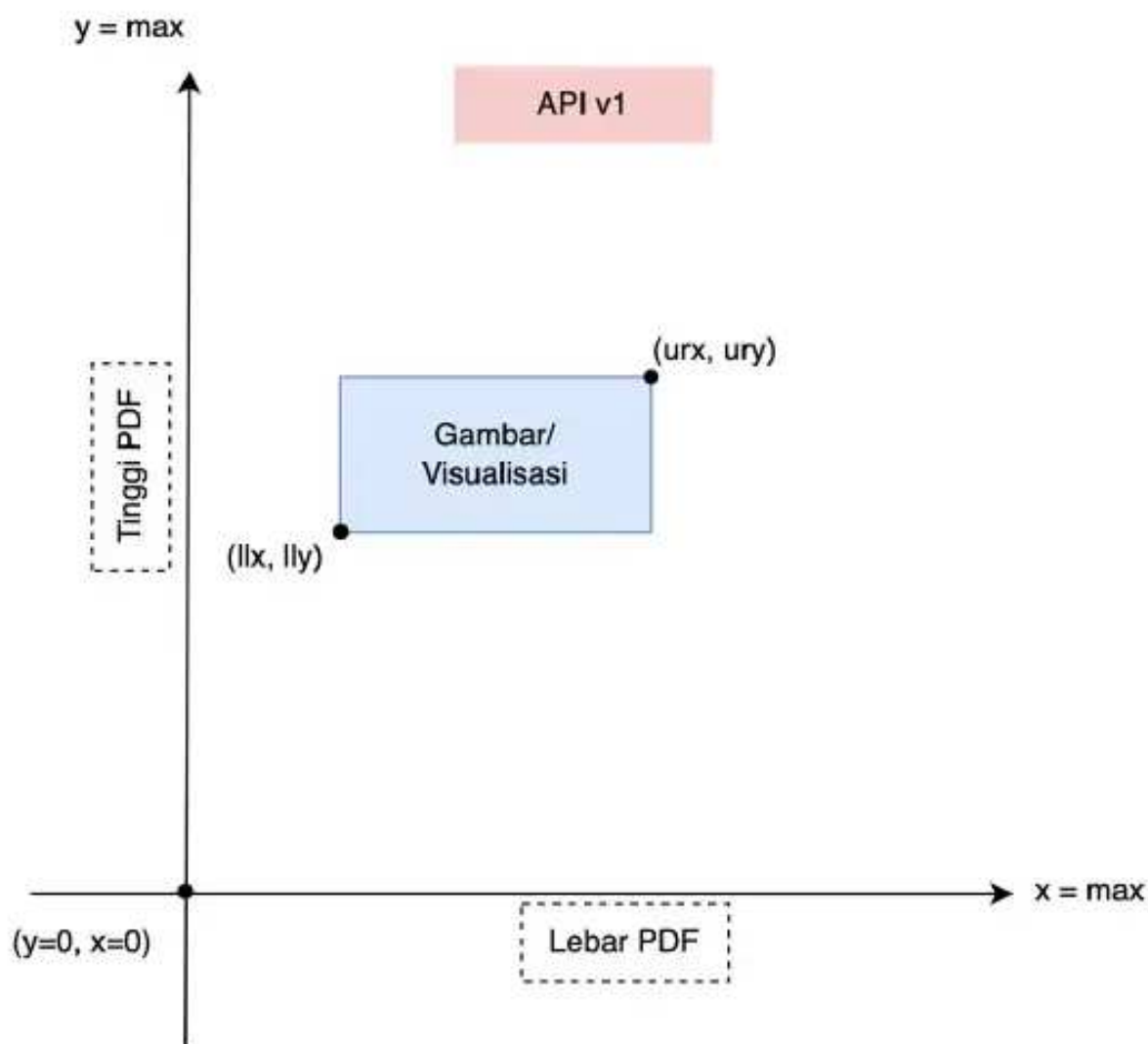
10. Xaxis

Parameter ini digunakan untuk menentukan titik koordinat secara horizontal di mana visualisasi akan dipasang. Penggunaan parameter ini diisi bersamaan dengan parameter `yAxis`. Parameter ini wajib diisi jika pengguna menggunakan parameter `page` atau halaman dan tipe visualisasi yang akan dibubuhkan adalah `visible`.

11. Yaxis

Parameter ini digunakan untuk menentukan titik koordinat secara vertikal di mana visualisasi akan dipasang. Penggunaan parameter diisi bersamaan dengan parameter `xAxis`. Parameter ini wajib diisi jika pengguna menggunakan parameter `page` atau halaman dan tipe visualisasi yang dibubuhkan adalah `visible`.

Kedua parameter ini (`xAxis` dan `yAxis`) adalah salah satu dari dua metode penentuan posisi visualisasi. Sebagai gambaran bagaimana parameter ini terkait untuk menentukan koordinat visualisasi dapat dilihat pada ilustrasi di bawah ini.



12. Width

Parameter ini digunakan untuk menentukan lebar spesimen visualisasi yang akan ditampilkan di dalam dokumen. Parameter ini diisi dalam bentuk angka dengan satuan pixel, dan wajib diisi untuk tipe visualisasi *visible*.

13. Height

Parameter ini digunakan untuk menentukan tinggi spesimen visualisasi yang akan ditampilkan dalam dokumen. Parameter ini diisi dalam bentuk angka dengan satuan pixel, dan wajib diisi untuk tipe visualisasi *visible*.

14. Tag_koordinat

Tag koordinat merupakan parameter yang berfungsi sebagai penanda posisi di mana spesimen akan diletakkan. Berbeda dengan koordinat visualisasi, tag koordinat hanya memerlukan sebuah karakter khusus (misal: # atau \$) yang dibubuhkan ke dalam dokumen.

15. Reason (Opsional)

Parameter ini digunakan jika pengguna ingin memasukkan catatan saat melakukan tanda tangan. Catatan ini akan muncul sebagai properti yang melekat pada tanda tangan. Penggunaan parameter ini bersifat opsional.

16. Location (Opsional)

Parameter ini dapat diisi dengan lokasi tempat di mana tanda tangan dibubuhkan (misal: Jakarta, Jayapura, dll). Penggunaan parameter ini juga bersifat opsional.

17. Text (Opsional)

Seperti dua parameter sebelumnya (*reason* dan *location*), penggunaan parameter ini juga bersifat opsional. Parameter ini digunakan untuk menambahkan teks sesuai keinginan pengguna.


Contoh

Berikut adalah contoh penggunaan API Sign Service 1

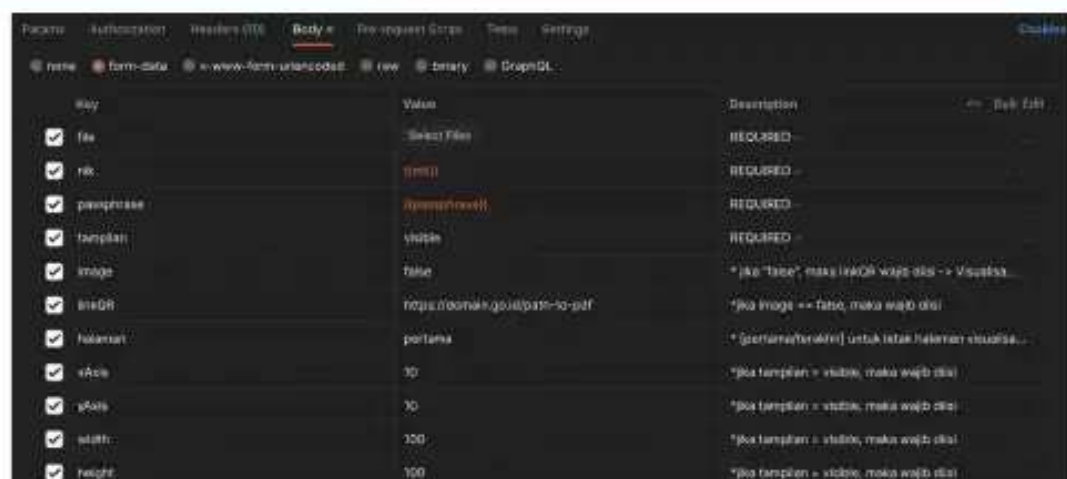
a. Visualisasi Invisible

Tipe	FORM
POST	


b. Visualisasi Visible Koordinat

Tipe	FORM
POST	

c. Visualisasi linkQR

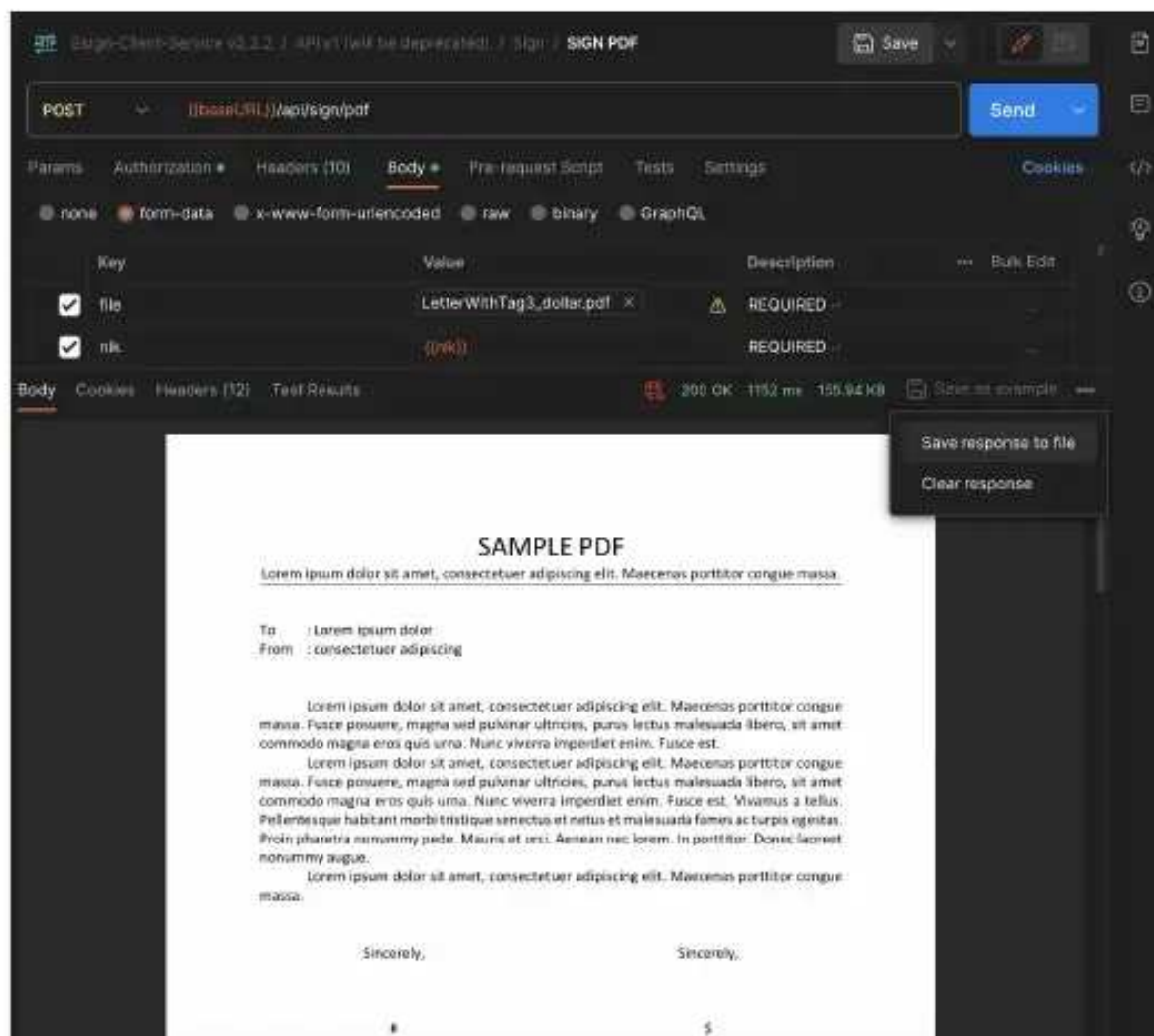
Tipe	FORM
POST	

d. Visualisasi Tag Koordinat

Tipe	FORM
POST	

Setelah memasukkan daftar parameter di atas, ada beberapa response yang dapat diterima oleh pengguna. Bergantung dari berhasil atau tidaknya transaksi yang dilakukan.

Jika proses berhasil, maka respon akan menampilkan dokumen yang sudah ditandatangani.



Pengguna dapat menyimpan hasil dokumen tersebut dengan klik tombol option dan memilih `save response to file`, lalu menyimpannya dalam bentuk `.pdf`.

5.3. API DOWNLOAD (SIGNED) DOCUMENT

Endpoint ini berfungsi untuk mengunduh dokumen yang sudah ditandatangani. Dokumen hanya bisa diunduh sebanyak satu kali.

Endpoint

Method	URL
GET	<code>/api/sign/download/{idDokumen}</code>

Parameter

Type	Params	Values
URL_PARAM	<code>idDokumen</code>	<code>string</code>

Berdasarkan daftar parameter di atas, berikut adalah penjelasan masing-masing parameter yang digunakan.

1. IdDokumen

IdDokumen merupakan parameter yang diisi dengan dokumen yang akan diunduh. Dokumen ini merupakan dokumen yang sudah pernah di TTE oleh sistem dan hanya bisa diunduh sebanyak satu kali. Dokumen akan didapatkan dalam bentuk PDF.

Berikut adalah beberapa respon yang mungkin akan didapatkan pengguna setelah melakukan unduh dokumen.

5.4. VERIFY PDF

Endpoint ini berfungsi untuk melakukan verifikasi dokumen yang sudah ditandatangani. Respon yang diberikan berbentuk JSON.

Endpoint

Method	URL
POST	/api/sign/verify

Parameter

Type	Params	Values
POST	signed_file	file (.pdf)

Berdasarkan daftar parameter di atas, berikut adalah penjelasan masing-masing parameter yang digunakan.

1. Signed_file

Signed_file merupakan parameter untuk dokumen yang akan diperiksa keasliannya. parameter ini diisi dengan file PDF yang sudah memiliki tanda tangan elektronik.

Response

Status	Response
200	<pre>{ "nama_dokumen" : {{nama_dokumen}}, "jumlah_signature" : 2, "notes" : {{notes}}, "details" : [{ "info_tsa": { "name": "Timestamp Authority...", "tsa_cert_validity": null }, "signature_field": "sig_1697437714025", "info_signer": { "issuer_dn": "C=ID,O=Lembaga Sandi Negara...", "signer_name": "Hantek BSR E", "signer_cert_validity": "2023-10-06 12:56:15.00 to...", "signer_dn": "Hantek BSR E", "cert_user_certified": true }, "signature_document": { "signed_using_tsa": true, "reason": "Dokumen telah disetujui...", "document_integrity": true, "signature_value": null, } }] }</pre>

```
    "signed_in": "2023-10-16 13:28:34.00",  
    "location": null,  
    "hash_value": null  
  }  
},  
],  
"summary" : "{{summary}}"  
}
```

6. API SERVICE VERSION 2

API versi 2 ini merupakan pengembangan Esign Client terbaru (versi 2.2.2) dari BSR.E. Dengan menambahkan fitur terbaru antara lain Segel Elektronik, Bulk Signing, Two Factor Auth, Password PDF Signing, dan Certificate Expired Check.

Pengguna kini dapat memilih untuk melakukan tanda tangan menggunakan passphrase atau dengan One Time Password (OTP).

6.1. AUTHORIZATION

Sebelum mengakses endpoint, pengguna harus mengisi terlebih dahulu otorisasi yang berfungsi sebagai pemberian hak akses penggunaan. Tipe otorisasi yang digunakan adalah Basic Auth yang diisi dengan username dan password aplikasi. Kedua kredensial ini bisa didapatkan dari halaman admin Esign Client Service.

Header

Tipe	Content
Basic Auth	base64(username:password)

6.2. API SIGN

Pada API versi 2 ini tersedia empat metode untuk melakukan tanda tangan, yaitu dengan menggunakan OTP dan passphrase. Sedangkan untuk data yang dikirimkan dapat menggunakan NIK atau Email yang terdaftar di BSR.E.

Endpoint

Method	Endpoint
POST	/api/v2/sign/pdf

Request Body

Tipe	JSON
POST	<pre>{ "nik": "", "email": "", "passphrase": "", "totp": "", "signatureProperties": ["tampilan": "", "imageBase64": "" "page": 0, "originX": 0.0, "originY": 0.0, "width": 0.0, "height": 0.0, "location": "", "reason": "", "pdfPassword": ""], "file": [""]</pre>

Berdasarkan parameter yang terdapat pada tabel di atas, berikut merupakan penjelasan masing-masing kegunaannya.

1. NIK & Email

NIK dan email merupakan parameter yang digunakan sebagai ID penandatanganan. Pada penggunaannya, cukup memilih salah satu dari NIK atau Email sebagai ID penandatanganan.

2. Passphrase dan TOTP

Passphrase dan TOTP merupakan parameter yang digunakan sebagai *credential* untuk melakukan tanda tangan. Pada penggunaannya, cukup memilih salah satu dari passphrase atau TOTP sebagai *credential* penandatanganan.

3. SignatureProperties

Parameter ini mengatur properti tanda tangan elektronik pada dokumen yang akan ditandatangani. Parameter dapat diisi dengan array dengan ketentuan jumlah, yaitu satu atau sebanyak dokumen yang akan ditandatangani.

4. Tampilan

Parameter ini mengatur tampilan spesimen tanda tangan. Ada dua tipe pada parameter ini, yaitu `VISIBLE` dan `INVISIBLE`. `INVISIBLE` digunakan jika pengguna tidak ingin menampilkan visualisasi tanda tangan elektronik. Sedangkan `VISIBLE` digunakan jika pengguna ingin menampilkan visualisasi tanda tangan elektronik, dan properti lain yang terkait yaitu `imageBase64`, `page`, `originX`, `originY`, `width`, `height`, `tag`.

5. ImageBase64

Parameter ini mengatur spesimen visualisasi tanda tangan. Dapat diisi dengan String Base64 dari file tipe gambar (`.jpg`, `.jpeg`, dan `.png`).

6. Page

Parameter ini menentukan halaman letak spesimen visualisasi. Parameter ini diisi dengan nomor halaman.

7. OriginX

Parameter ini mengatur koordinat sumbu X letak spesimen visualisasi terhadap halaman dokumen.

8. OriginY

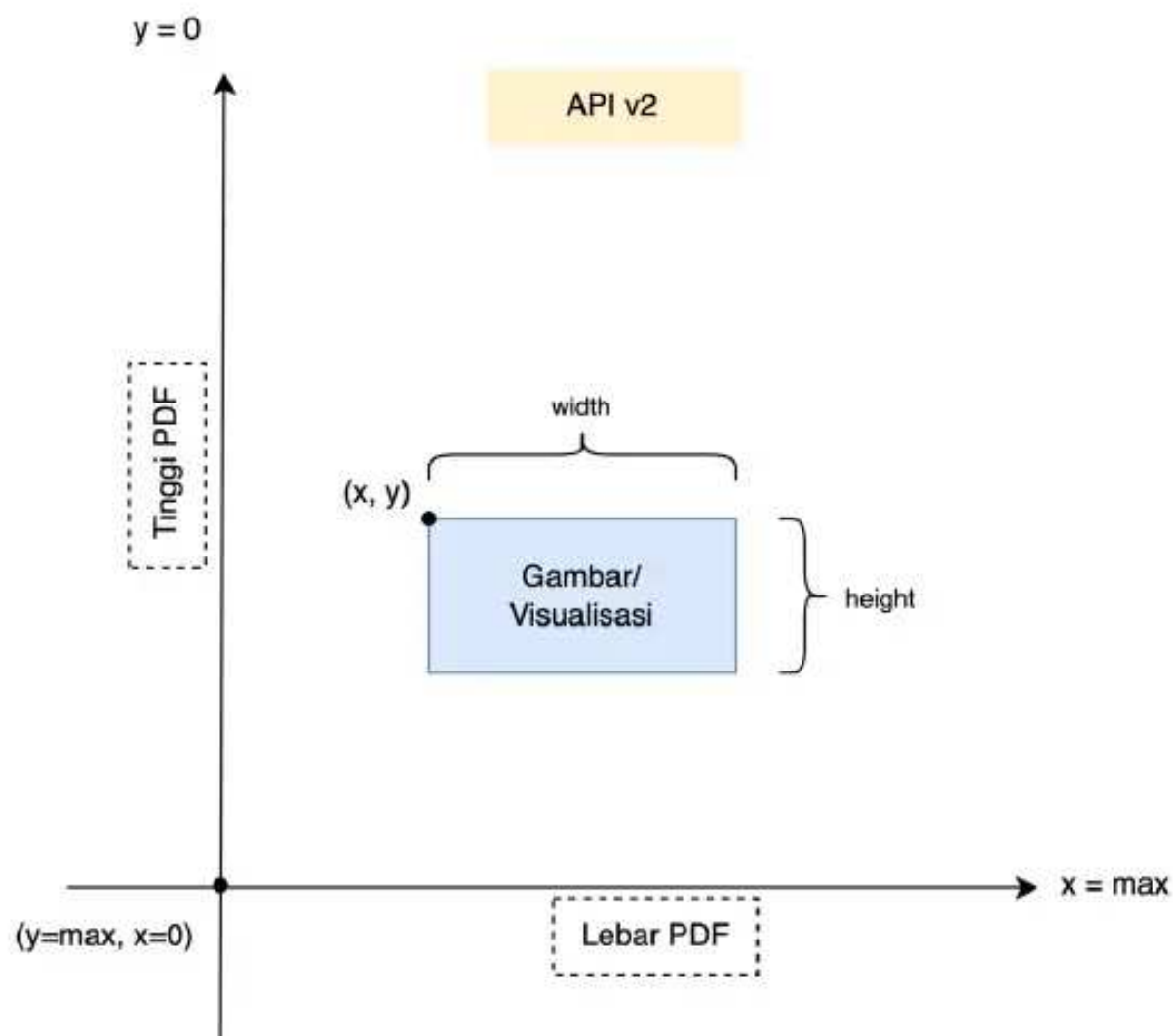
Pada versi 1, parameter ini bernama `yAxis`. Parameter origin ini berfungsi sama seperti `yAxis`, yaitu untuk meletakkan titik koordinat secara vertikal. Parameter ini dapat digunakan jika tipe visualisasi yang dikirimkan melalui parameter Tampilan adalah `visible`.

9. Width

Parameter ini digunakan untuk menentukan lebar spesimen visualisasi yang akan ditampilkan di dalam dokumen. Parameter ini diisi dalam bentuk angka dengan satuan pixel, dan wajib diisi untuk tipe visualisasi `visible`.

10. Height

Parameter ini digunakan untuk menentukan tinggi spesimen visualisasi yang akan ditampilkan dalam dokumen. Parameter ini diisi dalam bentuk angka dengan satuan pixel, dan wajib diisi untuk tipe visualisasi `visible`. Sebagai gambaran bagaimana parameter ini terkait untuk menentukan koordinat visualisasi dapat dilihat pada ilustrasi di bawah ini.



11. Location

Parameter ini dapat diisi dengan lokasi tempat di mana tanda tangan dibubuhkan (misal: Jakarta, Jayapura, dll). Penggunaan parameter ini juga bersifat opsional.

12. Reason

Parameter ini digunakan jika pengguna ingin memasukkan catatan saat melakukan tanda tangan. Catatan ini akan muncul sebagai properti yang melekat pada tanda tangan. Penggunaan parameter ini bersifat opsional.

13. File

Parameter ini berfungsi untuk mengirimkan dokumen yang akan ditandatangani. Berbeda dengan versi 1, file yang diterima di parameter ini adalah tipe base64 string. Jadi, jika pengguna ingin melampirkan dokumen yang akan diproses, pengguna harus mengubah tipe dokumen terlebih dahulu.

14. IdSubscriber

Parameter ini adalah parameter baru untuk memproses Segel Elektronik. Saat pengguna mendaftarkan instansi untuk membuat Segel Elektronik, pengguna akan mendapatkan idSubscriber yang akan menjadi parameter utama untuk pembubuhan Segel.

15. Totp

Selain idSubscriber, totp merupakan parameter baru yang hadir pada Esign Client Service versi 2. Totp berfungsi untuk menampung OTP yang diterima pengguna melalui email. Totp diperlukan setiap akan melakukan pembubuhan tanda tangan elektronik dan sertifikasi elektronik.

16. Password

Parameter ini digunakan apabila pengguna ingin melakukan pembubuhan tanda tangan elektronik atau segel elektronik pada dokumen yang dikunci dengan password.

Contoh

Berikut adalah contoh penggunaan API SIGN Service 2.

a. Visualisasi Invisible

Tipe	JSON
POST	<pre>{ "email": "{{email}}", "passphrase": "{{passphrase}}", "signatureProperties": [{ "tampilan": "INVISIBLE" }] }</pre>

Tipe	JSON
	<pre> }], "file": [{{fileBase64}}] } </pre>

b. Visualisasi Visible Koordinat

Tipe	JSON
POST	<pre> { "nik": "{{nik}}", "passphrase": "{{passphrase}}", "signatureProperties": [{ "tampilan": "VISIBLE", "imageBase64": "{{imageBase64}}", "page": 1, "originX": 10, "originY": 10, "width": 200, "height": 100, }], "file": [{{fileBase64}}] } </pre>

c. Visualisasi Visible Tag Koordinat

Tipe	JSON
POST	<pre> { "nik": "{{nik}}", "otp": "{{otp}}", "signatureProperties": [{ "tampilan": "VISIBLE", "tag_koordinat": "\$", "imageBase64": "{{imageBase64}}", "width": 200, "height": 100, }], "file": [{{fileBase64}}] } </pre>

d. Visualisasi Banyak Jenis

Tipe	JSON
POST	<pre> { "email": "{{email}}", "otp": "{{otp}}", "signatureProperties": [{ "tampilan": "VISIBLE", "imageBase64": "{{imageBase64}}" "page": 1, "originX": 10, "originY": 10, "width": 200, "height": 100, "location": "Jakarta" , "reason": "Tanda tangan elektronik" },{ "tampilan": "INVISIBLE", "location": null, "reason": "Tanda tangan elektronik" },{ "tampilan": "VISIBLE", "tag_koordinat": "\$" "imageBase64": "{{imageBase64}}" "width":120, "height": 40, "location": "Jakarta" , "reason": null }] "file": [{{fileBase64_1}}, {{fileBase64_2}}, {{fileBase64_3}},] } </pre>

6.3. API REQUEST SIGN TOTP

Endpoint Request OTP digunakan untuk mendapatkan OTP yang akan menjadi kredensial saat melakukan tanda tangan elektronik berdasarkan NIK atau email milik pengguna. Respon OTP akan dikirimkan melalui email yang terdaftar.

Endpoint

Method	URL
POST	/api/v2/sign/get/totp

Request Body

Tipe	JSON
POST	<pre>{ "nik": "3216785087543986", "email": "email_pengguna@instansi.go.id", "data": 0, }</pre>

Response

Status	Response
200	<pre>{ "time": 1000, "file": [{{base64_sealedFile_1}}, {{base64_sealedFile_2}} , {{base64_sealedFile_3}}, ... , {{base64_sealedFile_N}}] }</pre>

1. NIK & Email

NIK dan email merupakan parameter yang digunakan sebagai ID penandatanganan. Pada penggunaannya, cukup memilih salah satu dari NIK atau Email sebagai ID penandatanganan.

2. Data

Jumlah atau banyaknya file yang akan ditandatangani pada endpoint API Sign. Jika jumlah file yang akan ditandatangani sebanyak dua file, maka data dapat diisi 2 (dengan angka).

6.4. API REQUEST SEAL ACTIVATION TOTP

Jika instansi pertama kali menggunakan Segel Elektronik, maka pengguna harus mengaktifkan terlebih dahulu akses TOTP. Untuk mengaktifkannya, pengguna dapat menggunakan endpoint Request Seal Activation TOTP.

Request

Method	URL
POST	/api/v2/seal/get/activation

Request Body

Tipe	JSON
POST	<pre>{ "idSubscriber": "{{idSubscriber}}", }</pre>

Response

Status	Response
200	<pre>{ "success": true, "message": "TOTP Aktivasi berhasil dikirim", "data": null, }</pre>

Jika pengguna ingin memperpanjang masa berlaku token, maka bisa kembali melakukan **Refresh Seal Activation OTP**.

Endpoint

Method	URL
POST	/api/v2/seal/get/activation

Request Body

Tipe	JSON
POST	<pre>{ "idSubscriber": "{{idSubscriber}}", "totp": "{{totp}}", }</pre>

Response

Status	Response
200	<pre>{ "success": true, "message": null, "data": { "message": "TOTP Aktivasi masih berlaku", "totp": "{{totp}}", "expires": "2023-08-07T04:24:40.927+0000", "result": true, } }</pre>

Sedangkan jika ingin mencabut OTP yang sudah diaktivasi, pengguna dapat menggunakan endpoint **Revoke Seal Activation**.

Request

Method	URL
POST	/api/v2/seal/revoke/activation

Request Body

Tipe	JSON
POST	<pre>{ "idSubscriber": "{{idSubscriber}}", "totp": "{{totp}}", }</pre>

Berdasarkan parameter yang tertulis pada tabel di atas, berikut merupakan penjelasan masing-masing parameter yang dapat digunakan di endpoint ini.

1. IdSubscriber

Parameter ini digunakan untuk mencantumkan idSubscriber yang dimiliki pengguna.

2. Totp

Parameter ini merupakan isian yang didapatkan dari endpoint API Request Seal Activation TOTP. Parameter ini digunakan untuk melakukan perpanjangan masa berlaku token (Refresh Seal Activation OTP) dan pencabutan token (Revoke Seal Activation).

6.5. API REQUEST SEAL OTP

Setelah mengaktifkan akses ke OTP, pengguna dapat meminta kode OTP jika ingin melakukan pembubuhan Segel Elektronik.

Endpoint

Method	URL
POST	/api/v2/seal/get/totp

Request Body

Tipe	JSON
POST	<pre>{ "idSubscriber": "{{idSubscriber}}", "data": "2", "totp": "{{totp}}", }</pre>

Berdasarkan parameter yang terdapat pada tabel di atas, berikut penjelasan kegunaan masing-masing parameter tersebut.

1. IdSubscriber

Parameter ini digunakan untuk mencantumkan idSubscriber yang dimiliki pengguna.

2. Data

Parameter ini diisi dengan jumlah atau banyaknya file yang akan disegel pada endpoint API Seal PDF. Jika jumlah file yang akan disegel sebanyak dua file, maka data dapat diisi 2 (dengan angka).

3. Totp

Parameter ini diisi dengan TOTP yang didapatkan pengguna dari endpoint Request Seal Activation.

Setelah melakukan transaksi dengan endpoint di atas, berikut adalah beberapa respon yang mungkin akan didapatkan pengguna.

Response

Status	Response
200	<pre>{ "message": "TOTP berhasil dibuat", "totp": "{{totp}}", "expires": "2023-08-07T04:24:40.927+0000", "result": true, }</pre>

6.6. API SEAL PDF

Endpoint ini dapat digunakan jika pengguna sudah menerima kode OTP di email. Endpoint ini akan membubuhkan Segel Elektronik pada dokumen.

Request

Method	URL
POST	/api/v2/seal/pdf

Request Body

Tipe	JSON
POST	<pre> { "idSubscriber": "{{id_subscriber}}", "totp": "629109", "signatureProperties": [{ "tampilan": "INVISIBLE", "location": null, "reason": null, }], "file": ["{{file in base64}}"] } </pre>

Berdasarkan parameter yang tercantum pada tabel di atas, berikut merupakan penjelasan masing-masing penggunaan parameter pada endpoint ini.

1. IdSubscriber

Parameter ini digunakan untuk mencantumkan idSubscriber yang dimiliki pengguna.

2. Totp

Parameter ini diisi dengan TOTP yang didapatkan pengguna dari endpoint Request Seal Activation.

3. SignatureProperties

Parameter ini mengatur properti tanda tangan elektronik pada dokumen yang akan disegel. Parameter dapat diisi dengan array dengan ketentuan jumlah, yaitu satu atau sebanyak dokumen yang akan disegel.

4. Tampilan

Parameter ini digunakan untuk mengatur visualisasi segel yang akan diterapkan pada dokumen. Ada dua jenis tampilan yang dapat digunakan, yaitu VISIBLE untuk menampilkan visualisasi dan INVISIBLE untuk menyembunyikan visualisasi.

5. Location (Opsional)

Parameter location digunakan untuk mencantumkan lokasi di mana dokumen tersebut disegel. Jika posisi pengguna segel berada di Jakarta, maka lokasi akan secara otomatis terdaftar di Jakarta.

6. Reason (Opsional)

Parameter ini digunakan jika pengguna ingin memasukkan catatan saat melakukan segel. Catatan ini akan muncul sebagai properti yang melekat pada segel. Penggunaan parameter ini bersifat opsional.

7. File

Parameter ini berfungsi untuk mengirimkan dokumen yang akan disegel. Berbeda dengan versi 1, file yang diterima di parameter ini adalah tipe base64 string. Jadi, jika pengguna ingin melampirkan dokumen yang akan diproses, pengguna harus mengubah tipe dokumen terlebih dahulu.

Setelah melakukan hit endpoint ini, pengguna akan mendapatkan beberapa jenis respon seperti yang tercantum pada tabel di bawah ini.

Response

Status	Response
200	File yang sudah disegel

6.7. CHECK STATUS USER

Endpoint ini berfungsi untuk memeriksa status pengguna yang akan melakukan Tanda Tangan Elektronik. Secara umum, terdapat beberapa status pengguna tertulis pada tabel di bawah ini.

No	Status	Keterangan
1.	ISSUE	Pengguna memiliki Sertifikat Elektronik aktif dan bisa melakukan tanda tangan elektronik
2.	EXPIRED	Masa berlaku Sertifikat Elektronik pengguna telah berakhir
3.	RENEW	Sertifikat Elektronik milik pengguna sedang dalam proses pembaruan
4.	WAITING_FOR_VERIFICATION	Sertifikat Elektronik milik pengguna sedang dalam verifikasi
5.	NEW	Pengguna memiliki Sertifikat Elektronik namun belum melakukan aktivasi
6.	NO_CERTIFICATE	Pengguna sudah terdaftar namun belum memiliki Sertifikat Elektronik
7.	NOT_REGISTERED	Pengguna belum terdaftar dan belum memiliki Sertifikat Elektronik
8.	SUSPEND	Pengguna terdaftar namun dalam kondisi <i>suspend</i>
9.	REVOKE	Sertifikat Elektronik milik pengguna sudah dicabut

Hanya pengguna dengan status ISSUE saja yang dapat melakukan Tanda Tangan Elektronik. Pada endpoint ini terdapat dua cara untuk memeriksa status user, yaitu dengan menggunakan parameter NIK dan Email.

Request

Method	URL
POST	/api/v2/user/check/status

Request Body (NIK)

Tipe	JSON
POST	{ "nik": "3216785087543986", }

Request Body (Email)

Tipe	JSON
POST	<pre>{ "email": "email_pengguna@instansi.go.id", }</pre>

Dari parameter yang tercantum pada tabel di atas, berikut merupakan penjelasan masing-masing kegunaan dari parameter tersebut.

1. NIK/Email

NIK dan email merupakan parameter yang digunakan sebagai ID untuk memeriksa status user. Pada penggunaannya, cukup memilih salah satu dari NIK atau Email sebagai ID.

6.8. REGISTRASI USER

Endpoint ini berfungsi untuk mendaftarkan pengguna yang belum memiliki akun BSR.E.

Request

Method	URL
POST	<code>/api/v2/user/registration</code>

Request Body

Tipe	JSON
POST	<pre>{ "nama": "nama user", "email": "nama@email.go.id", }</pre>

Berdasarkan tabel parameter di atas, berikut penjelasan kegunaan masing-masing.

1. Nama

Parameter ini berisi nama pengguna yang akan didaftarkan.

2. Email

Parameter ini diisi dengan email pengguna yang akan didaftarkan.

6.9. VERIFY PDF

Endpoint ini berfungsi untuk melakukan verifikasi dokumen yang telah ditandatangani. Pengguna cukup mengirimkan base64 string dari dokumen yang akan diverifikasi.

Request

Method	URL
POST	/api/v2/verify/pdf

Request Body (Dokumen Tanpa Password)

Tipe	JSON
POST	<pre>{ "file": "{{file in base64}}", }</pre>

Jika dokumen yang akan diverifikasi adalah dokumen yang dikunci dengan kata sandi, maka pengguna dapat menambahkan satu parameter yaitu password. Parameter ini diisi dengan kata sandi dokumen yang dikunci.

Request Body (Dokumen dengan Password)

Tipe	JSON
POST	<pre>{ "file": "{{file in base64}}", "password": "{{password}}", }</pre>

Berikut merupakan penjelasan parameter yang digunakan pada endpoint ini.

1. File

Parameter ini berfungsi untuk mengirimkan dokumen yang akan diverifikasi. Berbeda dengan versi 1, file yang diterima di parameter ini adalah tipe base64 string. Jadi, jika pengguna ingin melampirkan dokumen yang akan diproses, pengguna harus mengubah tipe dokumen terlebih dahulu.

2. Password

Parameter ini digunakan jika dokumen yang akan diverifikasi dikunci dengan password. Parameter ini diisi dengan password atau kata sandi dokumen.

Berikut merupakan beberapa respon yang akan didapatkan pengguna jika melakukan hit endpoint verify PDF ini.



Response

Status	Response
200	<pre>{ "conclusion": "NO_SIGNATURE", "description": "Dokumen tidak memiliki tandatangan elektronik", "signatureInformations": [{ "id": "S-95753E0AA2976206696F9A4052E13AB6DFE057...", "signatureFormat": "PKCS7-T", "signerName": "User Development", "signatureDate": "2023-07-11T02:41:23.000+00:00", "fieldName": "sig_1689043283248", "reason": "Dokumen ini telah ditandatangani...", "location": "Indonesia", "certLevelCode": 0, "signatureAlgorithm": null, "digestAlgorithm": null, "timestampInfomation": { "id": "T-73049E0B76BC9223590E4DB041EB6DE13F14...", "signerName": "Timestamp Authority...", "timestampDate": "2023-07-11T02:46:28.000+00:00" }, }, "certificateDetails": [{ "id": "C-84C1AD5F3227F9404B570DC237D39112...", "commonName": "User Development", "issuerName": "C=ID,0=Badan Siber dan Sandi Negara...", "serialNumber": "4614630145441590286786176...", "notAfterDate": "2023-12-22T07:47:10.000+00:00", "notBeforeDate": "2022-12-22T07:47:11.000+00:00", "signatureAlgoritm": "RSA with SHA256", }] } }</pre>

Status	Response
	<pre> "keyUsages": ["digitalSignature", "nonRepudiation"], { "id": "C-755C3FC16A810C6D7C5ABC57AE361E...", "commonName": "OSD DEMO", "issuerName": "C=ID,O=Badan Siber dan Sandi Negara...", "serialNumber": "1077311342475385395", "notAfterDate": "2028-04-07T17:23:28.000+00:00", "notBeforeDate": "2018-04-08T17:23:28.000+00:00", "signatureAlgorithm": "RSA with SHA256", "keyUsages": ["digitalSignature", "keyCertSign", "crlSign"] }, "integrityValid": true, "certificateTrusted": false, "lastSignature": false }, "signatureCount": 0 } </pre>

Jika terjadi kendala silahkan menghubungi kami di:

BALAI SERTIFIKASI ELEKTRONIK

	JL. Harsono RM, No.70, Ragunan, Jakarta Selatan.
	183

	https://t.me/infobsre
	info.bsre@bssn.go.id