

# Elektronisk paraksta izveidošana server

## Elektronisk paraksta izveidošana server

### Description

Creates a digital signature (PKCS #1) of data using a signing identity on server. As input, the hash of the data or a byte string to be signed raw can be received.

The signature is created with the signing identity on server specified in the request. This identity must belong to the end-user on behalf of whom the operation is performed.

### Request

```
POST /trustedx-resources/esigp/v1/signatures/server/raw
```

### Content-Type Header

```
Content-Type: application/json
```

### Body

```
{
  "digest_value" : {string},
  "signature_algorithm" : {string},
  "sign_identity_id" : {string}
}
```

Property	Description
digest_value	Hash of the data to be signed encoded in base64.
signature_algorithm	Algorithm that must be used to generate the digital signature ("rsa-sha1", "rsa-sha256", "rsa-sha384" and "rsa-sha512")
sign_identity_id	Identifier of the signing identity that must be used for generating the signature (it must be a server signing identity that belongs to the end-user on behalf of whom the signature is performed).

### Example

```
POST /trustedx-resources/esigp/v1/signatures/server/raw
Host: eidas.eparaksts.lv
Content-Type: application/json
Authorization: Bearer abc...6daf
Content-Length: 213
{
  "digest_value" : "n4bQgYhMfWWaL+qgxVrQFaO/TxsrC4Is0V1sFbDwCgg",
  "signature_algorithm" : "rsa-sha256",
  "sign_identity_id" : "nio...omq"
}
```

### Response

Response contains the binary value of the PKCS #1 signature.



If you are using Sign API service, PKCS#1 shall be base64 encoded (`hexToBase64`)