Reykjavík 13.11.2025

Signet Login

Website and services

TABLE OF CONTENTS

1 INTRODUCTION

Signet Login is a part of Signet Mandate which handles authentication (and mandates) for other websites. The solution support SAML and JWT tokens and has been adapated to handle legacy SAML like innskaning.island.is delivers.

2 TECH

The solution is composed of a website for authentication and giving mandates as well as a REST API for validating tokens, fetching mandates and saving mandates. Authentication for the website and webservice is by way of digital certificates.

3 URLS

Signet Login has a preproduction and production environment with the following urls.

3.1 PREPRODUCTION

- Web for handling mandates
  - https://prufa.signet.is/login
- Web to use as an authentication portal
  - https://prufa.signet.is/login/Login/?id=<reqid>&path=<path>&authid=<authid>
- Get current certificate used for signing tokens
  - https://prufa.signet.is/login/login/cert
- Filling out forms with certificate authentication
  - https://prufa.signet.is/login/home/form/<Form ID>
- Filling out forms with token authentication
  - https://prufa.signet.is/login/home/tokenform/<Form ID>
- Web API
  - https://prufa.signet.is/loginservice

3.2 PRODUCTION

- Web for handling mandates
  - https://login.signet.is/
- Web to use as an authentication portal
  - https://login.signet.is/Login/?id=<reqid>&path=<path>&authid=<authid>
- Get current certificate used for signing tokens
  - https://login.signet.is/login/cert
- Filling out forms with certificate authentication
  - https://login.signet.is/home/form/<Form ID>
- Filling out forms with token authentication
  - https://login.signet.is//home/tokenform/<Form ID>
- Web API
  - https://login.signet.is/service

4 WEBSITE

To use Signet Login for authentication you redirect your user to the appropritate URL (see chapter 3 above) with your alloted id and some optional parameters.

4.1 ATTRIBUTES

The login website supports these query parameters.

- id
  - The id you have been allotted by the Signet Team
- path
  - An optional parameter in the form of an URL path which will be appended to the end of the registered return URL.
- authid
  - An optional parameter in the form of GUID or number which will be included in the token returned after authentication. Helpful in linking to a website session.
- onbehalf
  - An optional parameter which will require the user to use a valid mandate for authentication. If the user has no mandate it will not be redirected to the return URL after authentication.
  - onbehalf = 0 means the user **can't** select/use any mandates
  - onbehalf = 1 means the user **must** select a mandate
- returnUrl
  - An optional parameter for a different url that you user will be sent to after authentication.
  - The URL must be registered in the list of supported URLs for the account. Can be done by contacting the Signet Team or on the management portal.
  - The path parameter will be ignored when returnUrl is provided.

4.2 RETURNED TOKEN

After authentication the uset is returned (via POST) to a registered return url with an issued token contaning information on the user who authenticated. The token is returned via the post parameter „token" unless requested otherwise and can be JWT or SAML.

Websites which have been using innskraning.island.is for authentication can easily connect to Signet Login as service providers can request getting SAML tokens in the same form as Innskraning.island.is provides (same attributes). All that is needed is to trust the token issuer (referred, certificate etc)

Signet Login will normally supply the users name, national registry number and the authentication certificate.

Signet Login can provide various extra attributes in the token such as address, maritial status, gender, used certitife etc.

Example tokens are supplied in the appendix of this document.

4.3 AUTHENTICATION ATTRIBUTE

If the account has been registered to get the Authentication attribute that attribute will be returned in the token and can contain the following values:

- SimCert
  - User authenticated using his mobile certificate
- CardCert
  - User authenticated using his Audkenni card
- AppCert
  - User authenticated using his Audkenni app
- Evrotrust
  - User authenticated using his Evrotrust app

4.4 EVROTRUST USERS

In the case that the user was authenticated using Evrotrust app there a subtle differences in the returned token.

- If service provider has requested the „Authentication“ attribute it will contain the value „Evrotrust“.
- If the user is Icelandic and authenticated using the certificate containing his personal ID number the UserSSN token attribute will contain his Icelandic Id number (kennitala)
- If the user is foreign and authenticated using the certificate containing his personal ID number the UserSSN token attribute will contain a value of the form PNOXX-Y… where XX is the country language code and the Y.. will be the users personal ID number from that country.
- If the user authenticated using the certificate NOT containing his personal ID number the UserSSN token attribute will contain a value of the form A[0-9}{12} which is an unique number for that user and certificate at Evrotrust.

4.5 INNSKRANING.ISLAND.IS COMPATABLE

When a service provider which is using innskraning.island.is wants to migrate to Signet Login very few adjustments will have to be made and will be listed below.

4.5.1 TRUSTING THE SIGNET SAML SIGNING CERTIFICATE

The SAML signing certificate which Signet Login uses is issued by **Fullgilt audkenni 2021** and issued to **Signet Advania** compared to **Fullgilt audkenni** and **Innskraning Island.is**.

Signet login certificate issuer:

SERIALNUMBER = 5210002790
CN = Fullgilt audkenni 2021
2.5.4.97 = NTRIS-5210002790
O = Audkenni ehf.
C = IS

Signet login signing certificate:

SERIALNUMBER = 5902697199
CN = Signet Advania
2.5.4.97 = NTRIS-5902697199
O = Advania Ísland ehf.
C = IS

Innskraning.island.is certificate issuer:

CN = Fullgilt audkenni
OU = Utgefandi fullgildra skilrikja
O = Audkenni hf.
SERIALNUMBER = 5210002790
C = IS

Innskraning.island.is signing certificate:

CN = Innskraning Island.is
SERIALNUMBER = 6503760649
OU = Auðkenning og undirritun
OU = Bunadarskilriki
C = IS
O = Þjóðskrá Íslands
OU = 20220516123320

A common certificate validation had lines like

```
cert.Issuer.StartsWith("CN=Fullgilt audkenni“) &&
       cert.Subject.Contains("SERIALNUMBER=6503760649“)
```

Which will have to be changed to

```
cert.Issuer.Contains("CN=Fullgilt audkenni 2021“) &&
       cert.Subject.Contains("SERIALNUMBER=5902697199“)
```

4.5.2 LOGIN URL

The login url(link) will have to be changed from https://innskraning.island.is/login.aspx?id=<reqid> to https://login.signet.is/login?id=<reqid>. Signet login also supports the **path** and **authid** parameters like innskraning.island.is.

4.5.3 TOKEN VALIDATION

Please make sure to validate the token which is returned from Signet Login. Validations that need to be performed are but not limited to:

- Correct destination in token
- Correct signer certificate
- Correct issuer of certificate
- Token signature is valid (token has not been modified after signature)
- Token validity is valid (valid at current time)
- Fetch authenticated attributes from inside signed part of token

5 WEB API

The webservice has as controller for handling token info and validation as well as a controller for mandates. There is also a swagger interface (/swagger) on the service to help with integration.

5.1 TOKEN WEBSERVICE CLASSES

The API uses the following classes for requests and responses.

5.1.1 MANDATETOKENREQUEST

When requesting signed mandate after authentication or a list of users mandate a MandateRequest is used.

- Token
  - The returned token after authentication

5.1.2 VALIDATETOKENREQUEST

When validating a returned token a ValidateTokenRequest is used

- Token
  - The returned token after authentication
- Audience
  - The audience/destination of token

5.1.3 MANDATEDATA

When getting mandate information the response is a MandateData.

- ID
  - GUID
  - ID of mandate
- HolderSSN
  - String[]
  - National registry numbers of mandate holders
- OnBehalfSSN
  - string
  - National registry number of identity giving mandate
- GiverSSN
  - string
  - National registry number of person giving mandate
- Document
  - Byte[]
  - The signed PDF mandated
- Data
  - KeyValuePair<string, string>[]
  - Array of KVP with mandate values
- Added
  - date
  - Time when mandate was saved
- Signed
  - date
  - Time when mandate was signed
- ValidFrom
  - date
  - Time when mandate gets valid
- ValidTo
  - date
  - Time mandate is valid to
- State
  - AuthorizationState

- State of mandate (Issuance = 0, Revocation = 1)

5.1.4 VALIDATETOKENRESPONSE

When validating a returned token with ValidateTokenDetailed a ValidateTokenResponse object is returned.

- FoundInDB
  - bool
  - Was the token found in Signet database
- BelongsToAccount
  - bool
  - Does the token belong to account
- SignatureOK
  - bool
  - The the token signature OK
- ValidityOK
  - bool
  - Is the token validity ok (valid at current time)
- AudienceOK
  - bool
  - Does the token destination match the audience
- AllOK
  - bool
  - Are all the checks OK

5.2 MANDATE WEBSERVICE CLASSES

The API uses the following classes for requests and responses on the mandate controller.

5.2.1 PINGREQUEST

When testing the connection and authentication info a PingRequest is used:

- UserName
  - string
  - The account username, identity in addition to the digital certificate
- Password
  - string
  - The account password, identity in addition to the digital certificate
- Message
  - string
  - A message that will be returned if succesful

5.2.2 MANDATEREQUEST

When searching mandates we use MandateRequest.

- MandateID
  - string
  - ID of mandate, required when getting a single mandate (GetMandate)
- GiverSSN
  - string

    - National registry number of person giving the mandate, used when searching for mandates (plural)
- HolderSSN
    - string
    - National registry number of person holding the mandate, used when searching for mandates (plural)
- OnBehalfSSN
    - string
    - National registry number of identity giving mandate, used when searching for mandates (plural)
- FromTime
    - date
    - Time to search for (mandate given after time)
- ToTime
    - date
    - Time to search for (mandate given befor time)
- UserName
    - string
    - The account username, identity in addition to the digital certificate
- Password
    - string
    - The account password, identity in addition to the digital certificate

5.2.3 TOKENREQUEST

When requesting token for submitting mandates we use a TokenRequest.

- SSN
    - string
    - National registry number of user giving mandate
- Mobile
    - string
    - Mobile phone number (holding digital signatures) of the person who is giving/signing the mandate. Phone numbers should start with +354, ie. „+354-8765432“.
- MandateForm
    - integer
    - ID of mandate form
- ReturnURL
    - string
    - Where to redirect person after signing
- UserName
    - string
    - The account username, identity in addition to the digital certificate
- Password
    - string
    - The account password, identity in addition to the digital certificate

5.2.4 FORMREQUEST

When searching for mandate forms we user FormRequest.

- FormID

    - integer
    - ID of form. Required when getting a single form (GetForm)
- FromTime
    - date
    - Time to search for (form created after time)
- ToTime
    - date
    - Time to search for (form created before time)
- OnlyEnabled
    - boolean
    - Only get enabled forms
- UserName
    - string
    - The account username, identity in addition to the digital certificate
- Password
    - string
    - The account password, identity in addition to the digital certificate

5.2.5 SAVEMANDATEREQUEST

When pre-saving mandate we user SaveMandateRequest;

- MandateID
    - string
    - ID the mandate being used (GUID).
- FormID
    - integer
    - ID of the mandate form.
- GiverSSN
    - string[]
    - Array of national registry numbers of users giving mandate
- ExtraAttribute
    - string
    - Mandates extra value (ie amount)
- Onebehalfs
    - string[]
    - Array of mandate behalfs (national registy numbers)
- Receivers
    - string[]
    - Array of receivers of mandate (national registy numbers)
- UserName
    - string
    - The account username, identity in addition to the digital certificate
- Password
    - string
    - The account password, identity in addition to the digital certificate

5.2.6 SUBMITMANDATEREQUEST

When submitting (filling) mandate we user SubmitMandateRequest;

- MandateID

    - string
    - ID the mandate being used (GUID).
- ValidTo
    - DateTime
    - Validity of mandate, max 2 years from now.
- AuthToken
    - string
    - The authentication received from authenticating user via Signet Login
- ReturnUrl
    - string
    - If mandate needs signature a token for sending user to Signet is returned and the user will be returned to ReturnUrl after signature.
- UserName
    - string
    - The account username, identity in addition to the digital certificate
- Password
    - string
    - The account password, identity in addition to the digital certificate

5.2.7 MANDATEDATA

When getting mandate information the response is a MandateData.

- ID
    - GUID
    - ID of mandate
- HolderSSN
    - String[]
    - National registry numbers of mandate holders
- OnBehalfSSN
    - string
    - National registry number of identity giving mandate
- GiverSSN
    - string
    - National registry number of person giving mandate
- Document
    - Byte[]
    - The signed PDF mandated
- Data
    - KeyValuePair<string, string>[]
    - Array of KVP with mandate values
- Added
    - date
    - Time when mandate was saved
- Signed
    - date
    - Time when mandate was signed
- ValidFrom
    - date
    - Time when mandate gets valid

- ValidTo
  - date
  - Time mandate is valid to
- State
  - AuthorizationState
  - State of mandate (Issuance = 0, Revocation = 1)

5.2.8 MANDATEFORMINFO

When getting information about mandate form the response is a MandateFormInfo.

- FormID
  - integer
  - ID of form
- FormString
  - string
  - HTML form for mandate. Only returned in GetForm
- Attributes
  - string[]
  - Array of form attributes
- ExtraAttrName
  - string
  - Name for mandate extraattribute
- ExtraAttrID
  - string
  - Unique id for mandate extraattribute
- ExtraAttrPlaceholder
  - string
  - Placeholder gildir fyrir aukagildi (s.s. Sláðu inn skráningarnúmer)
- Added
  - date
  - Time when form was created
- Edited
  - date
  - Time when form was last edited
- Enabled
  - boolean
  - True if form is enabled
- Visible
  - boolean
  - True if form is visible in list of forms (/home/forms).

5.3 TOKEN METHODS

The following methods are available in the token webservice (<service url>/api/token)

5.3.1 GETMANDATE

To get the mandate referenced in an issued token you can call the GetMandate method. The method acceps a MandateTokenRequest and responds with MandateData if the mandate is found from the token.

5.3.2 GETMANDATES

To get a list of valid users mandates you can call the GetMandates method. The method acceps a MandateTokenRequest and responds with an array of MandateData if there are any valid mandates found for the user.

5.3.3 VALIDATETOKEN

To validate an issued token you can call the ValidateToken method. The method accepts a ValidateTokenRequest and responds with true or false if the token is valid.

5.3.4 VALIDATETOKENDETAILED

To validate an issued token you can call the ValidateToken method. The method accepts a ValidateTokenRequest and responds with ValidateTokenResponse with detailed validation information.

5.3.5 GETAUTHENTICATIONDATA

To get the users authentication data (issued authentication from identiy provider i.e. Auðkenni) you can call the GetAuthenticationData method. The method accepts a MandateTokenRequest and responds with the authentication data (base64 encoded string) if the token and its authentication data is found.

5.4 MANDATE METHODS

The following methods are available in the mandate webservice (<service url>/api/mandate) for handling mandates issued with Signet Login/Mandate.

5.4.1 PING

The method accepts a PingRequest to test connection and authentication information. Will return a string containing that message as well as the username.

5.4.2 GETMANDATE

The methods acceps MandateRequest and repsonds with MandateData if the mandate is found and belongs to account.

5.4.3 GETMANDATES

The method accepts MandateRequest and responds with an array of MandateData if mandates are found.

5.4.4 DELETEMANDATE

The method accepts a MandateRequest and responds with true or false if mandate was successfully deleted.

5.4.5 GETTOKEN

The method acceps a TokenRequest and responds with a base64 coded token which can be used for filling out mandate.

5.4.6 GETFORM

The method accepts a FormRequest and responds with a MandataFormInfo if a form is found.

5.4.7 GETFORMS

The method accepts a FormRequest and responds with an array of MandataFormInfo if forms are found.

5.4.8 SAVEMANDATE

The method accepts a SaveMandateRequest and responds with a ID string for the mandate if successful. This ID will be used with GetToken to get an authentication token to finish filling out a new mandate or used in SubmitMandate to fill mandate via API.

5.4.9 SUBMITMANDATE

The method accepts a SubmitMandateRequest and responds with an empty OK response if successful and doesn‘t need users signatures. If the mandate needs a signature the Signet document ID (GUID) is returned (for sending the user to <SignetUrl>/login/<ID>) or a token for direct access to the document (for sending the user to <SignetUrl>/token/sign) if AuthToken was supplied.

5.5 LOGIN METHODS

The following methods are available in the login controller (<service url>/api/login) for authenticating an user through webservice requests instead of using the Signet Login website. The controller uses basic authentication scheme using the supplied username and password.

The process for different certificates are the same:

First call the appropriate method for the method the user will use for authentication and get back a login ID.

- Auðkenni SIM - SimLogin
- Auðkenni APP - AppLogin
- Evrotrust APP - EvrotrustLogin

Poll using the login ID on PollLogin (please keep poll period above 2seconds) and when the user has authenticated you will receive an authentication token with users information.

See table in Appendix for error codes.

5.5.1 PING

A simple method to test authentication and connection. Accepts a message parameter which will returned back if succesful.

5.5.2 SIMLOGIN

To start authenticating an user with Auðkenni SIM certificates you perform a GET request on /SimLogin with the parameters

- phonenumber
  - string
  - Users mobile number

    - format 354[1-9]{1}[0-9]{6}
- message
    - string
    - Message to display to user on its mobile phone
    - Maximum length 100 characters

If successful a login ID is returned which is used to poll for users authentication on PollLogin. If not successful a 400 (BadRequest) is returned with a ReturnStatus object with the error.

5.5.3 APPLOGIN

To start authenticating an user with Auðkenni App you perform a GET request on /AppLogin with the parameters

- ssn
    - string
    - Users national registry number
    - format [0-9] {10}
- message
    - string
    - Message to display to user on its mobile phone
    - Maximum length 100 characters

If successful a login ID is returned which is used to poll for users authentication on PollLogin. If not successful a 400 (BadRequest) is returned with a ReturnStatus object with the error.

5.5.4 EVROTRUSTLOGIN

To start authenticating an user with Evrotrust certificates you perform a GET request on /EvrotrustLogin with the parameters

- phonenumber
    - string
    - Users mobile number
    - format [+]([0-9]{5,15})
- message
    - string
    - Message to display to user on its mobile phone
    - Maximum length 100 characters

If successful a login ID is returned which is used to poll for users authentication on PollLogin. If not successful a 400 (BadRequest) is returned with a ReturnStatus object with the error.

5.5.4.1 POLLLOGIN

To poll for the users authentication you perform a GET request on /PollLogin using the login id from the previous step. The login id is in a UUID form.

If the user is still performing the authentication an empty 204 response is returned.

If the authentication failed for some reason a 400 response with ResultStatus object describing the reason is returned.

If successful a token (JWT or SAML) is returned with appropriate data depending on how the account was set up.

This token can then be used on the /token interface to get users mandate or the authentication data from the appropriate certificate issuer (Auðkenni or Evrotrust).

6 APPENDIX

Below are some example tokens issued by Signet Login and process for saving mandates as well as a list of test users.

6.1 TEST USERS

This chapter has a list of test users available in the test environment.

6.1.1 AUÐKENNI TEST USERS

Mock users with Audkenni SIM and APP

Name	SSN	Mobile
Test Notandi	1234567890	+3541111111
Test Notandi 2	1234567899	+3541111112
Test Notandi 3	1234567891	+3541111113
Test Notandi 4	1234567892	+3541111114
Test Notandi 5	1234567893	+3541111115
Test Notandi Cancel	0987654321	+3542222222
Test Notandi Problem	0202021234	+3544444444
Test Notandi Timeout	0101011234	+3543333333

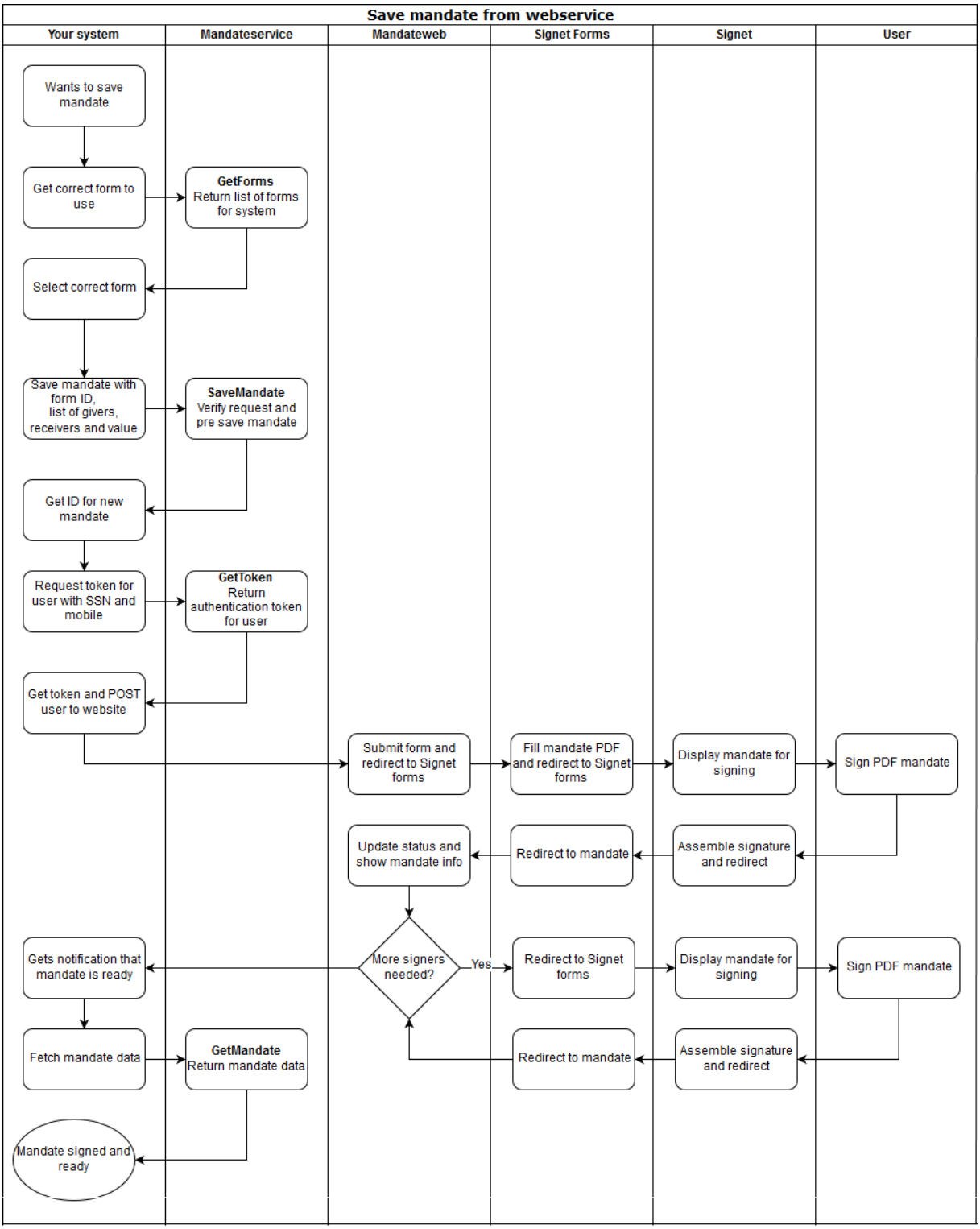
6.1.2 EVROTRUST USERS

Mock users with Evrotrust app

Name	SSN	Mobile
BULGARIAN TEST,	A000002291179	+35908882445123
ANDERS AND	PNODK-1206717661	+4533227997
JOAKIM VON AND	PNODK-0101467661	+4533151001

6.2 PRE SAVING MANDATE WITH WEBSERVICE

Below is a process diagram for pre saving a mandate with webservice.



6.3 NORMAL JWT TOKEN

eyJhbGciOiJSUzI1NiIsImtpZCI6IjU4Njk4MEYwQUIwODBERDRDMkQzQjM1REM5MDI5QkFFODR
FMDRFNzciLCJ0eXAiOiJKV1QifQ.eyJqdGkiOiIxZDc0MTFhNi04YTM3LTQ5YTktYmVlYS1jMTl
lYzZiOGQyYmYiLCJuYW1laWQiOiIxMjM0NTY3ODkwIiwiU1NOIjoiMTIzNDU2Nzg5MCIsIk5hbW
UiOiJUZXN0IE5vdGFuZGkiLCJNb2JpbGUiOiIxMTExMTExIiwibmJmIjoxNjk5NDUzOTI0LCJle
HAiOjE2OTk0NTgxMjQsImlhdCI6MTY5OTQ1NzUyNCwiaXNzIjoicHJ1ZmEuc2lnbmV0LmlzIiwi
YXVkIjoiaHR0cHM6Ly9wcnVmYS5zaWduZXQuaXMvIn0.fC8cDZB3PI3pVFFZos46odhpRhuTiAa

a9UpS7psKwfnhekDnqG1gLN0drj4sKO3x7OzRyUpnZ8MjLG2tw-SV_7eDjim29ZZRIQ5c-
bB2GZz57fUqo6bkt6vhDbAz40b4oLqkjQ-
TQq_DPe_u0aQvVi4pqC_joDwLvHBYhsG30RWb5AeZDGCsnzgbjmkHUs8kK2LEA8CQqfaBEsQHMR
DWezZuB5SEOTTN_GcmoZZWm2PlsXb82k-
C4HrgtyQxz49ocsoH3hqIoi8lWMg_7LBShk716zMUa-
QHXnNFBpi_m8fttmZqfJkkyxh6aTDxyFP8kvhq3Pz67RLPXPn8-RRPqA

6.4 NORMAL SAML TOKEN

<?xml version="1.0" encoding="UTF-8"?><Response
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_5f7aa1d7-4f40-
4fed-9652-9855f52c913f" Version="2.0" IssueInstant="2023-11-
08T15:34:50.8516772Z" Destination="https://prufa.signet.is/"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol"><Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">Signet
Mandate</Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMet
hod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" /><Reference URI="#_5f7aa1d7-4f40-4fed-9652-
9855f52c913f"><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/><DigestValue>Iyzbodwmv/+v559FnTXOjsg30yxnKjDvSSfx5ZxiEMQ=</DigestValue></
Reference></SignedInfo><SignatureValue>SW93RiQs9Dc9vb6q7oDGXx0GSEEPUvIBU++u
VFVQq3ItkWDy8nkQ+y6kZiTzkCXcMUK90kWuf/a9eqdMA+xb/Qcp9aqYA9pELOMxwyvAbl1IWgd
a/pjsXCyJf3tvULUMMWBqwilFwcB7gbNC/auaLYZLeqqK3pbHe3qWW9MM2rcFwyL8jSWaRwiVXK
jO4XT9UTS8xgzjM59msAwNpptDXwGFO7n/fIxPxyap1hi8ESgtmI9/ARWVDSLYbK4vUb8vlookN
tgtkbnhIxWKfqlaFTmjv+8SkWis1skXb7qm+6evRbsPw+8ourewo3l7Hpeyjo65xVS1/GuZjOO/
k6Ky3A==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF2zCCBMOgAw
IBAgIDJFaqMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTAklTMRMwEQYDVQQFEwo1MjEwMDAyN
zkwMRUwEwYDVQQKEwxBdWRrZW5uaSBoZi4xJzAlBgNVBAsTHlV0Z2VmYW5kaSBmdWxsZ2lsZHJh
IHNraWxyaWtqYTEaMBgGA1UEAxMRRnVsbGdpbHQgYXVka2VubmkwHhcNMjIwMjAxMDkxNDA3Whc
NMjQwMjAxMDkxNDA3WjCBsTEXMBUGA1UECxMOMjAyMjAxMzEwOTQwMDAxHTAbBgNVBAoMFEFkdm
FuaWEgw41zbGFuZCBlaGYuMQswCQYDVQQGEwJJUzEYMBYGA1UECxMPQnVuYWRhcnNraWxyaWtpM
SIwIAYDVQQLDBlBdcOwa2VubmluZyBvZyB1bmRpcnJpdHVuMRMwEQYDVQQFEwo1OTAyNjk3MTk5
MRcwFQYDVQQDEw5TaWduZXQgQWR2YW5pYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BAL4PgInUEqo+9EUpbhkvEfwsCReEo13B8jyZPr7DbFljNkoYJOR5tbOFm4k3jHbCbTp8c4/6gB
yPoJCnoDT50FkserP0zv9VADC1sqro5dHYgRI9yFwqh+6KN2C+MXl7waqC8d+XT1oj/t05bdupT
Q3f/pMVDSrNzQprMMZ4rfi8IUWXUMlofhrS/Gsoo+YrdfrlBDYDI7QoCSydveB0p1+PU/Y88iyd
5wFlxsceZEwq97oJcVsNoCFAzhiwRb1hBRLQ/Blfuw2bwssODwaDi33zFSfP3838yqfmZ2v0FXM
oPs7UnG3l24vMRsbeUv8Vd4PjJowF5JpXbMrnTsRykYUCAwEAAaOCAiwwggIoMAwGA1UdEwEB/w
QCMAAwggELBgNVHSAEggECMIH/MIH8BglggmABAgEBAQIwge4wgcQGCCsGAQUFBwICMIG3GoG0V
GhpcyBjZXJ0aWZpY2F0ZSBpcyBpbnRlbmRlZCBmb3IgZGlnaXRhbCBzaWduYXR1cmVzIGFuZCBh
dXRoZW50aWNhdGlvbi4gVGhpcyBjZXJ0aWZpY2F0ZSBmdWxmaWxzIHRoZSByZXF1aXJlbWVudHM
gb2Ygbm9ybWFsaXplZCBjZXJ0aWZpY2F0ZSBwb2xpY3kgKE5DUCkgZGVmaW5lZCBpbiBFVFNJIF
RTIDEwMiAwNDIuMCUGCCsGAQUFBwIBFhlodHRwczovL3JlcG8uYXVka2VubmkuaXMvMHcGCCsGA
QUFBwEBBGswaTAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuYXVka2VubmkuaXMwQgYIKwYBBQUH
MAKGNmh0dHA6Ly9jZHAuaXNsYW5kc3JvdC5pcy9za2lscmlraS9mdWxsZ2lsdGF1ZGtlbm5pLnA
3YjALBgNVHQ8EBAMCBeAwHwYDVR0jBBgwFoAUwik+hv+GxNo1H2mmpP8BgzxKM6kwQwYDVR0fBD
wwOjA4oDagNIYyaHR0cDovL2NybC5hdWRrZW5uaS5pcy9mdWxsZ2lsdGF1ZGtlbm5pL2xhdGVzd

C5jcmwwHQYDVR0OBBYEFL+65R/0Sev5/7Q3/y2wl/6UhpHaMA0GCSqGSIb3DQEBCwUAA4IBAQAH
mlbwk6w1WhX0CikuMBu40ET9/kY4RuH4lG0ioNd6sXTcRq193PgLRZhxpbeBvLqNEcil3+AAy6l
uaYWgkpMoVUuvvbApkm/8+EziDOMEMaXFiYDtzNvxpXUHh6N4lR8o0Wfhs2KgtfYDMRkDaWfaho
FBQOzaEjS3xv17hushmfG40/E1GhKmUOH6f5OJZDmksi4BoC5MToOxpXwdyKQvwBCfIaONGXmtk
BnC+X7/H+SzY2NUf/hE/huw/os10mgXO67tRGtDoSd386HoEXjH/qF/4j1Qg+vIszpzAxNHPnZk
SZNP5+J+TeI6I8IfIn2l2jj0EJZ6zu4PGtqBM67S</X509Certificate></X509Data></KeyI
nfo></Signature><Status><StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></Status><Assertion
Version="2.0" ID="_2fb084db-36b8-47c1-be19-970524287206"
IssueInstant="2023-11-08T15:34:50.8516772Z"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><Issuer>Signet
Mandate</Issuer><Subject><NameID NameQualifier="signet.is">Signet
Mandate</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
Address="127.0.0.1" NotOnOrAfter="2023-11-08T15:44:50.8516772Z"
Recipient="https://prufa.signet.is/"
/></SubjectConfirmation></Subject><Conditions NotBefore="2023-11-
08T15:33:50.8516772Z" NotOnOrAfter="2023-11-
08T15:44:50.8516772Z"><AudienceRestriction><Audience>prufa.signet.is</Audie
nce></AudienceRestriction></Conditions><AuthnStatement AuthnInstant="2023-
11-08T15:34:50.8516772Z"><SubjectLocality Address="172.16.193.82"
/><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classe
s:X509</AuthnContextClassRef></AuthnContext></AuthnStatement><AttributeStat
ement><Attribute Name="UserSSN"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue
xsi:type="xsd:string">1234567890</AttributeValue></Attribute><Attribute
Name="Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">Test
Notandi</AttributeValue></Attribute><Attribute Name="Certificate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue
xsi:type="xsd:string">MIIFUTCCBDmgAwIBAgIIGn8qoiTKK+cwDQYJKoZIhvcNAQELBQAwg
ZcxCzAJBgNVBAYTAklTMRUwEwYDVQQKDAxBZHZhbmlhIGVoZi4xIzAhBgNVBAsMGlV0Z2VmYW5k
aSBidW5hZGFyc2tpbHJpa2phMRYwFAYDVQQLDA1NaWxsaXNraWxyaWtpMRMwEQYDVQQFEwo1OTA
yNjk3MTk5MR8wHQYDVQQDDBZCdW5hZGFyc2tpbHJpa2kgUHJvZnVuMB4XDTIzMDIyNzEzMTAxN1
oXDTI1MDIyNjEzMTAxN1owgYUxCzAJBgNVBAYTAklTMQ0wCwYDVQQKDARUZXN0MQ0wCwYDVQQLD
AQxMDQyMRYwFAYDVQQLDA1laW5rYXNraWxyaWtpMRQwEgYDVQQLDAtBdcOwa2VubmluZzETMBEG
A1UEBRMKMTIzNDU2Nzg5MDEVMBMGA1UEAwwMVGVzdCBOb3RhbmRpMIIBIjANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIBCgKCAQEAzGnyW5nAD5mJaokYs47tNVgT7f5cBTO0G8LE6sZd1ftQsOaOC5Itjb
wIpE0cik31s5tbtCeztR17BwHb7ggDbqp73qwxjDWe4UXtlMKQxTt+MP8+jCbO9j2mOt7AMiY+I
U8rGa8JQoOPM/wAKsryog5OT/qYgURJydZHmorUSXbArYilECZwal+JFkbrQmBt+SbOYOJFP/zj
RHMcUGw4I7mKylW64dWx5IrI3DLaQw01g8BLIaVW4aui9cBDZGD6UImF8agQMVIWaz26z/x7pal
IX6PuJtm03Q4SUQuQ+VVVE7nKlcnkC0XLfMIjtL7W/ahJxuqzW343r/joWI49QQIDAQABo4IBrz
CCAaswUAYIKwYBBQUHAQEERDBCMEAGCCsGAQUFBzABhjRodHRwczovL2NlcnRzLmFkdmFuaWEua
XMvZWpiY2EvcHVibGljd2ViL3N0YXR1cy9vY3NwMB0GA1UdDgQWBBSYjH/oBL3Mgumcun7PxujD
iC194zAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFIMPw0bdmwExR+imDBA99d2JjiTIMIHPBgN
VHR8EgccwgcQwgcGggb6ggbuGgbhodHRwOi8vY2VydHMuYWR2YW5pYS5pcy9lamJjYS9wdWJsaW
N3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9Y3JsJmlzc3Vlcj1DTj1CdW5hZGFyc2tpbHJpa2klM
jBQcm9mdW4sU049NTkwMjY5NzE5OSxPVT1NaWxsaXNraWxyaWtpLE9VPVV0Z2VmYW5kaSUyMGJ1
bmFkYXJza2lscmlramEsTz1BZHZhbmlhJTIwZWhmLixDPUlTMA4GA1UdDwEB/wQEAwIF4DAnBgN
VHSUEIDAeBggrBgEFBQcDAgYIKwYBBQUHAwQGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQ
AMFfLcCrbMlvD8FeeDJQhfBVzZLFTiy5VpfQKnWRnJKorBcLo6xeymJmR3bdZBHl+Jgdo7LfW4K
ke6WzdjFRwbSVA9aGYX7WlAZxS3tnd/U0Z8gQsSsWQHcTR+KZFsMyz/Aj3YtP1VXgCLUsQLARtq

f+64VdcbHLaC7OKSBG8uTPFo3GxmbMBj1jhCXQfD2yfWsQZOl7i6aS+yMLtdgAMcqAnT3by+XA4
ZmRwPL/HZ+MIZB4RSfHJA3uxAJPELHKWiMSxM2RX4IKcqgTfGOm7dxqBWCPwPCBnC1K7bRVCG8t
9bc3PRt0Q4IQ1Njw7ep2gDuJy/knMHpemgzkgG3BWT</AttributeValue></Attribute><Att
ribute Name="Mobile" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">+354-
1111111</AttributeValue></Attribute></AttributeStatement></Assertion></Resp
onse>

6.5 INNSKRANING.ISLAND.IS COMPATABLE SAML

<?xml version="1.0" encoding="UTF-8"?><Response
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_8bdb8cae-4705-
4888-b9eb-164d00f6fae9" Version="2.0" IssueInstant="2023-11-
08T15:39:10.3423716Z" Destination="https://prufa.signet.is/"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol"><Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">Signet
Mandate</Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMet
hod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" /><Reference URI="#_8bdb8cae-4705-4888-b9eb-
164d00f6fae9"><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/><DigestValue>+5W7yyKCzON4747v8TSkHBiM036GQ9Fa8HIunUzmu0k=</DigestValue></
Reference></SignedInfo><SignatureValue>Cn51P3LJCLza12jkfpuNNqv0CvB4rM4pne/i
LmMGZGWzBUDypPs3Sl3ERm6YLFh7zDz8Rwd7gG949wPfRVGknOxWx+r+hqzKkc2jdeKPIsEFvQF
/pr4PWCsy3FrsrKM7fsFh+exrhO5jFY27GX1pbOfa52aDCclDPbrphiWPqewLIBvIy8UDSnN/u3
ODugfMw4mamJJlFW17E96RW6SrbiYoVzK+Xr0Dcu0ttNwVt1T87VKU1Br2uf/jBijdtggMJUJE9
SlPG3E2vpFCuB1UPx9AiJpLCHsrOihA1rzG4t3OYPxWqZH3o/2BXxXeALi0l0SYdG2aJzUIG3R5
sgD2wg==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF2zCCBMOgAw
IBAgIDJFaqMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTAklTMRMwEQYDVQQFEwo1MjEwMDAyN
zkwMRUwEwYDVQQKEwxBdWRrZW5uaSBoZi4xJzAlBgNVBAsTHlV0Z2VmYW5kaSBmdWxsZ2lsZHJh
IHNraWxyaWtqYTEaMBgGA1UEAxMRRnVsbGdpbHQgYXVka2VubmkwHhcNMjIwMjAxMDkxNDA3Whc
NMjQwMjAxMDkxNDA3WjCBsTEXMBUGA1UECxMOMjAyMjAxMzEwOTQwMDAxHTAbBgNVBAoMFEFkdm
FuaWEgw41zbGFuZCBlaGYuMQswCQYDVQQGEwJJUzEYMBYGA1UECxMPQnVuYWRhcnNraWxyaWtpM
SIwIAYDVQQLDBlBdcOwa2VubmluZyBvZyB1bmRpcnJpdHVuMRMwEQYDVQQFEwo1OTAyNjk3MTk5
MRcwFQYDVQQDEw5TaWduZXQgQWR2YW5pYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BAL4PgInUEqo+9EUpbhkvEfwsCReEo13B8jyZPr7DbFljNkoYJOR5tbOFm4k3jHbCbTp8c4/6gB
yPoJCnoDT50FkserP0zv9VADC1sqro5dHYgRI9yFwqh+6KN2C+MXl7waqC8d+XT1oj/t05bdupT
Q3f/pMVDSrNzQprMMZ4rfi8IUWXUMlofhrS/Gsoo+YrdfrlBDYDI7QoCSydveB0p1+PU/Y88iyd
5wFlxsceZEwq97oJcVsNoCFAzhiwRb1hBRLQ/Blfuw2bwssODwaDi33zFSfP3838yqfmZ2v0FXM
oPs7UnG3l24vMRsbeUv8Vd4PjJowF5JpXbMrnTsRykYUCAwEAAaOCAiwwggIoMAwGA1UdEwEB/w
QCMAAwggELBgNVHSAEggECMIH/MIH8BglggmABAgEBAQIwge4wgcQGCCsGAQUFBwICMIG3GoG0V
GhpcyBjZXJ0aWZpY2F0ZSBpcyBpbnRlbmRlZCBmb3IgZGlnaXRhbCBzaWduYXR1cmVzIGFuZCBh
dXRoZW50aWNhdGlvbi4gVGhpcyBjZXJ0aWZpY2F0ZSBmdWxmaWxzIHRoZSByZXF1aXJlbWVudHM
gb2Ygbm9ybWFsaXplZCBjZXJ0aWZpY2F0ZSBwb2xpY3kgKE5DUCkgZGVmaW5lZCBpbiBFVFNJIF
RTIDEwMiAwNDIuMCUGCCsGAQUFBwIBFhlodHRwczovL3JlcG8uYXVka2VubmkuaXMvMHcGCCsGA
QUFBwEBBGswaTAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuYXVka2VubmkuaXMwQgYIKwYBBQUH
MAKGNmh0dHA6Ly9jZHAuaXNsYW5kc3JvdC5pcy9za2lscmlraS9mdWxsZ2lsdGF1ZGtlbm5pLnA
3YjALBgNVHQ8EBAMCBeAwHwYDVR0jBBgwFoAUwik+hv+GxNo1H2mmpP8BgzxKM6kwQwYDVR0fBD

wwOjA4oDagNIYyaHR0cDovL2NybC5hdWRrZW5uaS5pcy9mdWxsZ2lsdGF1ZGtlbm5pL2xhdGVzd
C5jcmwwHQYDVR0OBBYEFL+65R/0Sev5/7Q3/y2wl/6UhpHaMA0GCSqGSIb3DQEBCwUAA4IBAQAH
mlbwk6w1WhX0CikuMBu40ET9/kY4RuH4lG0ioNd6sXTcRq193PgLRZhxpbeBvLqNEcil3+AAy6l
uaYWgkpMoVUuvvbApkm/8+EziDOMEMaXFiYDtzNvxpXUHh6N4lR8o0Wfhs2KgtfYDMRkDaWfaho
FBQOzaEjS3xv17hushmfG40/E1GhKmUOH6f5OJZDmksi4BoC5MToOxpXwdyKQvwBCfIaONGXmtk
BnC+X7/H+SzY2NUf/hE/huw/os10mgXO67tRGtDoSd386HoEXjH/qF/4j1Qg+vIszpzAxNHPnZk
SZNP5+J+TeI6I8IfIn2l2jj0EJZ6zu4PGtqBM67S</X509Certificate></X509Data></KeyI
nfo></Signature><Status><StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></Status><Assertion
Version="2.0" ID="_1a466050-88de-413f-958c-a17f4f126d15"
IssueInstant="2023-11-08T15:39:10.3423716Z"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><Issuer>Signet
Mandate</Issuer><Subject><NameID NameQualifier="signet.is">Signet
Mandate</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
Address="127.0.0.1" NotOnOrAfter="2023-11-08T15:49:10.3423716Z"
Recipient="https://prufa.signet.is/"
/></SubjectConfirmation></Subject><Conditions NotBefore="2023-11-
08T15:38:10.3423716Z" NotOnOrAfter="2023-11-
08T15:49:10.3423716Z"><AudienceRestriction><Audience>prufa.signet.is</Audie
nce></AudienceRestriction></Conditions><AuthnStatement AuthnInstant="2023-
11-08T15:39:10.3423716Z"><SubjectLocality Address="172.16.193.82"
/><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classe
s:TLSClient</AuthnContextClassRef></AuthnContext></AuthnStatement><Attribut
eStatement><Attribute Name="UserSSN"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue
xsi:type="xsd:string">1234567890</AttributeValue></Attribute><Attribute
Name="Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">Test
Notandi</AttributeValue></Attribute><Attribute Name="DestinationSSN"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue
xsi:type="xsd:string">5902697199</AttributeValue></Attribute><Attribute
Name="Authentication" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">Rafræn
símaskilríki</AttributeValue></Attribute><Attribute Name="UserAgent"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/119.0</AttributeValue></Attribute><Attribute Name="IPAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue
xsi:type="xsd:string">127.0.0.1</AttributeValue></Attribute><Attribute
Name="Mobile" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><AttributeValue xsi:type="xsd:string">+354-
1111111</AttributeValue></Attribute></AttributeStatement></Assertion></Resp
onse>

6.6 LOGIN ERROR CODES

The following table list error codes encountered when authenticating users using the Login controller

Code	Auðkenni code	Icelandic explanation	English expanation
20.401	akreg_401	Notandi má ekki framleiða skilríki með núverandi skilríki	User is not allowed to create certificate
20.400	audkenni_400	Notandi er ekki með símanúmer	User does not have a mobile phone number
20.404	audkenni_404	Notandi finnst ekki	User not found
20.403	audkenni_403	Þjónustuveitandi ekki þekktur	AP unknown
20.100	mssp_100		Got accepted state when checking the status. This should not happen
20.101	mssp_101	Beiðni ekki rétt	Wrong parameter
20.102	mssp_102	Vantar breytu	Missing parameter
20.103	mssp_103	Svæði í beiðni of stórt	Wrong data length
20.104	mssp_104	Þjónustuveitandi ekki þekktur	AP unknown
20.105	mssp_105	Notandi finnst ekki.	User not found
20.107	mssp_107	Ekki hægt að vinna úr beiðni	Unable to handle given data
20.108	mssp_108	Misræmi í útgáfum	Incompatible interface version.
20.109	mssp_109	Óþekktur prófíll	Unsupported profile
20.208	mssp_208	Rann út á tíma	Timeout - Ekkert svar frá síma
20.209	mssp_209	Rann út á tíma	Timeout - Næst ekki í síma
20.401	mssp_401	Notandi hætti við	User cancel
20.402	mssp_402	PIN læst	PIN blocked
20.403	mssp_403	Kort læst	Card blocked
20.404	mssp_404	Skilríki finnast ekki	No key found
20.422	mssp_422	Skilríki finnast ekki	No certificate found
20.425	mssp_425	Villa við sannreyningu	Error in certificate validation
20.501	mssp_501	Skilríki er afturkallað	Certificate is revoked
20.503	mssp_503	Villa við sannreyningu	Error in signature verfication
20.504	mssp_504	Beiðni í vinnslu	Request in progress
20.900	mssp_900	Villa í innri kerfum	Error
20.467	SmartID_467	Notandi hætti við	User cancel
20.468	SmartID_468	Rann út á tíma	Timeout
20.469	SmartID_469	Villa í samskiptum	Communication error
2.470	SmartID_470	Rangur staðfestingarkóði valinn	Wrong verification code selected
20.471	SmartID_471	Notandi finnst ekki	User not found
20.472	SmartID_472	Villa - athugið Auðkennis APP	Error - Check Audkennis APP
20.480	SmartID_480	Misræmi í útgáfum	Incompatible interface version.
20.580	SmartID_580	Viðhaldsvinna í gangi, reynið aftur síðar	System is under maintenance, retry later
20.900	SmartID_900	Villa í innri kerfum	Error
20.1	1	Notandi hætti við	User cancel
20.404	404	Notandi finnst ekki	User not found
20.408	408	Rann út á tíma	Timeout

20.501	501		Invalid certificate
20.429		Hægðu á þér. Of stutt frá síðustu fyrirspurn	Slow down. The polling interval has not elapsed since the last request.