Nets Denmark A/S
Lautrupbjerg 10
P.O. 500
DK-2750 Ballerup

T +45 44 68 44 68
F +45 44 86 09 30
www.nets.eu

CVR-nr. 20016175

NemID JS Developer site Guidelines

Table of Contents

History

2019-02-18	Version 1.4	RMELG
2019-01-17	Version 1.3	RMELG
2018-11-08	Version 1.2	PKAJB
2017-10-24	Version 1.1	EJAKO
2017-10-11	Version 1.0	EJAKO
2017-09-25	Version 0.9	RPLAU
2017-03-30	Version 0.8	RSNIE
2016-06-08	Version 0.7	PKAJB
2016-04-21	Version 0.6	ABHAN
2014-09-24	Version 0.5	KSANO
2014-06-02	Version 0.4	PHJER
2014-05-12	Version 0.3	OYVMO
2014-01-31	Version 0.2	OYVMO
2013-11-15	Version 0.1	KSANO

1. Documents purpose and target group

This document is a part of the NemID Service Provider Package.

Nets-DanID has created a web site where service providers can create test users for NemID. The purpose of this document is to provide guidance on the use of the website.

The document is aimed at testers and developers who have to integrate with NemID.

2. NemID JS Developer Support Site

Nets-DanID has developed a support website to assist service providers implementing NemID JavaScript. The site allows for creation of NemID test users and shows a sample implementation of NemID JavaScript.

2.1 Purpose of the tool

In the tool it is possible to create test users and view their data, such as OTP cards and a transcript of the latest IVR call received. The tool provides functionality to create test users of various types and options to bring them in various states. The tool also includes functionality to start examples of NemID login flows and signing flows. The flows can be completed with the created test users.

The purpose of the tool is to assist a service provider in testing how their own NemID implementation handles the different response codes NemID will return.

2.2 Access to the tool

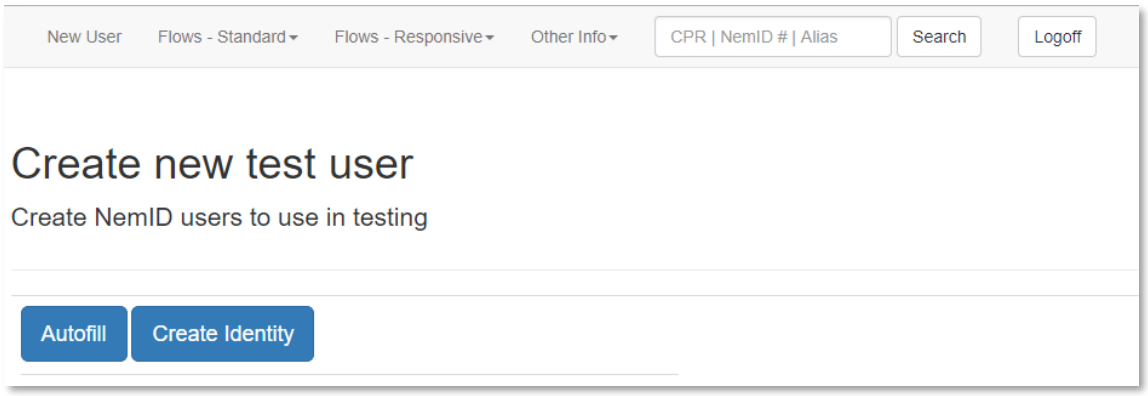
The tool is accessible from this address:

https://appletk.danid.dk/developers

Access to this page is blocked by an IP filter.

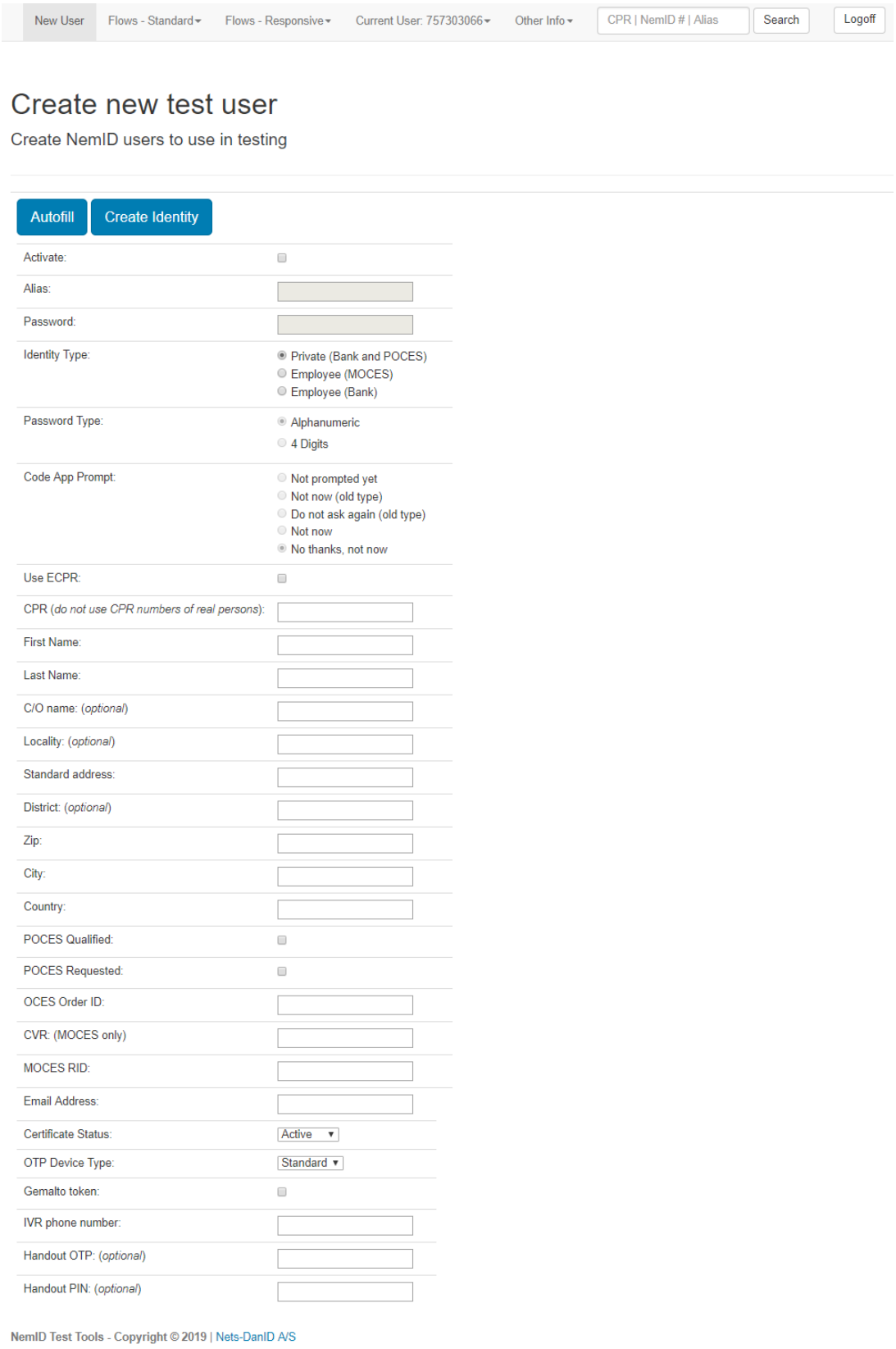
2.3 Start page

From the start page you can either search for an existing identity (test user), create a new identity. The top menu provides access to initiate a flow from the menu options *Flows – Standard* and *Flows – Responsive*. In the menu option *Other Info* a list of error codes is available, as well as a list of parameters that the client can be called with.



2.4 Create new identity

Activate the menu item *New User,* fill out the form and press *Create Identity*. Alternatively, press *Autofill* followed by *Create Identity* and the form will be


New User
Flows - Standard
Flows - Responsive
Current User: 757303066
Other Info
CPR | NemID # | Alias
Search
Logoff
Create new test user
Create NemID users to use in testing
Autofill
Create Identity
Activate:
Alias:
Password:
Identity Type:
Private (Bank and POCES)
Employee (MOCES)
Employee (Bank)
Password Type:
Alphanumeric
4 Digits
Code App Prompt:
Not prompted yet
Not now (old type)
Do not ask again (old type)
Not now
No thanks, not now
Use ECPR:
CPR (do not use CPR numbers of real persons):
First Name:
Last Name:
C/O name: (optional)
Locality: (optional)
Standard address:
District: (optional)
Zip:
City:
Country:
POCES Qualified:
POCES Requested:
OCES Order ID:
CVR: (MOCES only)
MOCES RID:
Email Address:
Certificate Status:
Active
OTP Device Type:
Standard
Gemalto token:
IVR phone number:
Handout OTP: (optional)
Handout PIN: (optional)
NemID Test Tools - Copyright © 2019 | Nets-DanID A/S

populated with random personal data and an active private user is created with an OTP card, a bank agreement and a public certificate.

If *Activate* is checked, the system will auto generate a user alias and a password. When selecting *Activate* the system will automatically create a user that is ready for login. This is the fastest way to generate a standard user.

If the form is filled in manually, do the following:

Fill in a random, fictitious address.

Also, fill in a random, fictitious CPR number (i.e. a personal identification number). If the CPR number is already in use, an error message is shown.

Please note, that the CPR number must comply with the general rules for CPR numbers (please refer to http://en.wikipedia.org/wiki/Personal_identification_number_(Denmark)), however, mod11 is not relevant here.

Handout OTP and I is selected if you have a physical code card and an activation password, which is to be linked to the specific test user. This is however not possible for service providers to do.

The *POCES Qualified* and *POCES Requested* flags determine whether the user gets an OCES digital signature and can use his NemID for logging on to non-banks. By default, both parameters are checked.

The *POCES Qualified* checkbox indicates whether the user can get an OCES digital signature or not. If not checked, the user can only logon to online banks and to self-service on nemid.nu using the NemID for bank login screen. You can create a "bank only" user for testing the error messages OCES002 and OCES004.

If the user is *POCES Qualified* and logs on to an OCES Service Provider, i.e. a non-bank Service Provider, the user will be prompted for extending his NemID with OCES digital signature. (This use case is relevant for users, who initially ordered NemID from a bank.).

By checking the *POCES Requested* flag, an OCES digital signature will be ordered for the user and issued at the first logon to an OCES Service Provider.

You can choose between an alphanumeric and a 4 digit password in *Password Type*. If you select *Alphanumeric*, then you can choose whether the system will ask the user if he wants to change his password to a 4 digit password. Furthermore it is possible to configure a future date to re-ask the user if he selects to be prompted again later.

The Code App Prompt setting applies to the code app download notification and five options are available. The setting only applies for active private users.

- *Not prompted yet*
  Will create a user that hasn't been asked before. E.g. the next time a 2-factor login is started the notification screen will be shown. Assuming that the user doesn't have a code app already.

- *Not now (old type)*
  Will create a user that in a previous version of the code app notification screen has answered "Not now". The new version of the notification screen will be shown when current date is after Next Code App Prompt value (see the user's View Identity page).

- *Do not ask again (old type)*
  Will create a user that in a previous version of the code app notification screen has answered "Do not show again". The user will never see the notification screen again.

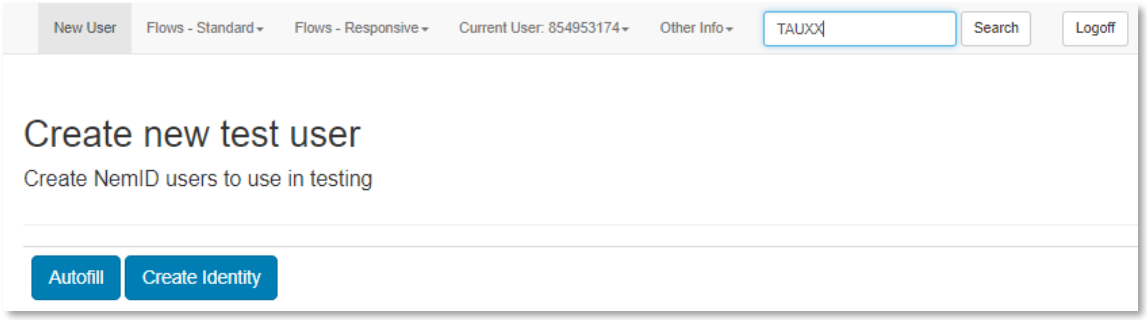
- *Not now*
  Will create a user that has just answered "Not now" when previously shown the notification screen. The notification screen will be shown when current date is after 'Code app Prompt – Next Prompt' (see the user's View Identity page).

- *No thanks, not now*
  Will create a user that has answered "No thanks, not now" when previously shown the notification screen. The user will for now not see the notification screen again. This is also the default setting.

When all information is provided, press *Create Identity*. The system will now redirect you to the *View Identity* page.

2.5 Search for existing user

Enter the CPR-number, NemID-number or the alias (chosen user ID) in the search field. Press <Enter>, or click the button *Search* to view the test user.



2.6 View existing user

This menu option is only displayed in the top menu if a user has been selected. When a new user is created it is automatically selected and this screen is displayed. To display the page for an existing user, search for the user as described in section 2.5.

This is the main page for viewing and managing the active users information.

From here you have access to the following information and links to additional functionality:

- NemID number (found under *OTP Devices* - must be used at the user's first login/activation)
- Alias, if chosen
- Password Status, Preferred Device and a number of authentication attempt counters
- Password Type: STANDARD(Alphanumeric)/FOURDIGITS(4-digit)
- Device action links (issuing/revoking devices and pins, setting preferred device etc.)
- Code card (link with the code card number is found under *OTP Cards*)
- Any TOTP Gemalto tokens (if any have been issued for the user), including the current (as of the latest page-refresh) key-value
- Any code apps (if any have been enrolled for the user)

- PIN codes used for activation (if *Activate* was not checked during user creation), password unlock and device unrevoke procedures. All PIN codes are found under *Pin Data* in the *PIN Codes* section

- Content of the certificate (under *Private Keys* – provided the certificate has been issued, which will happen the first time the test user logs on using an OCES flow)

- Code App Prompt values (prefixed 'Code App Prompt – '), only shown for private users

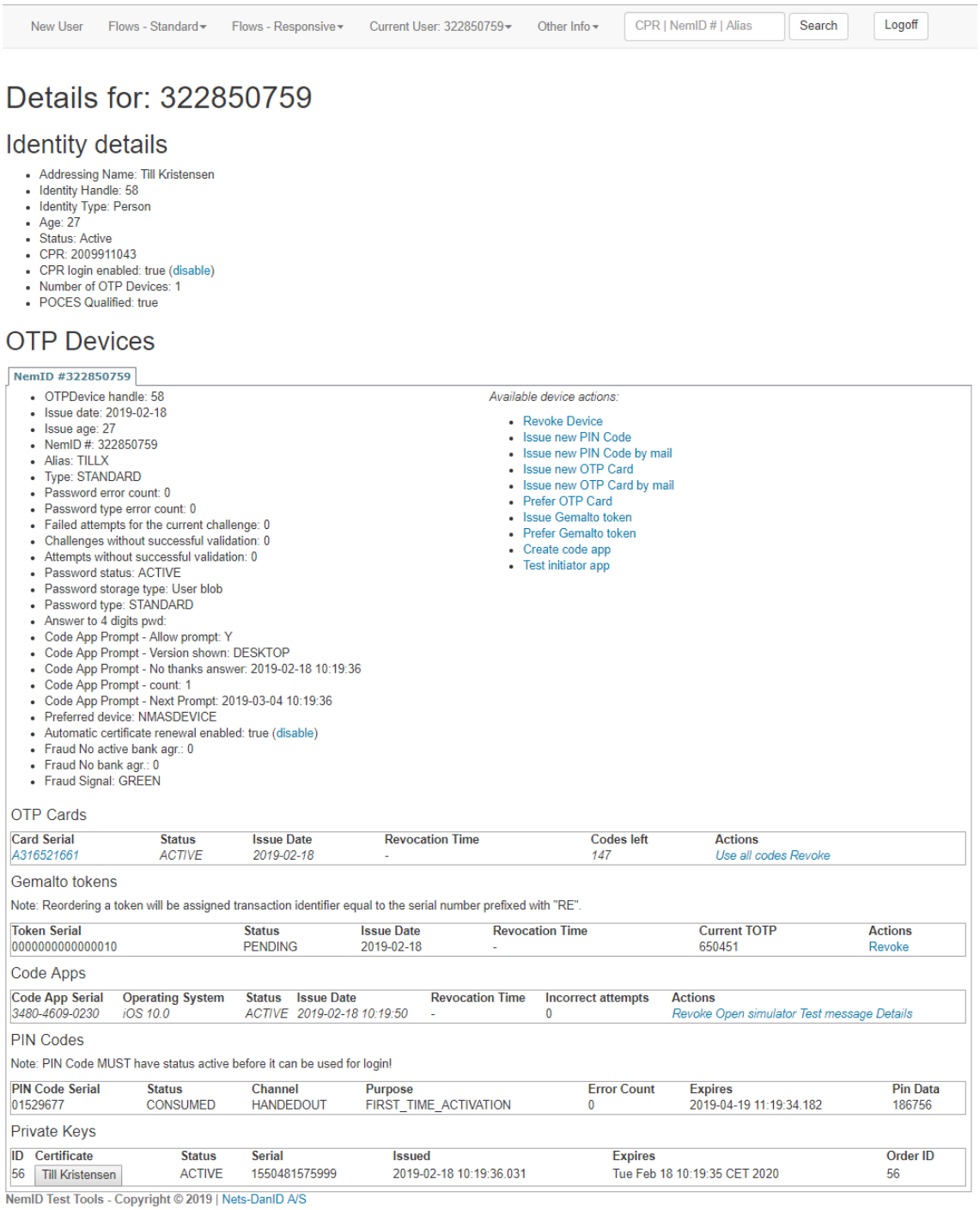
    - Allow prompt: Can have values: Y or N.

    - Version shown (if shown): Can have the values: Desktop or Mobile.

    - No thanks answer: Time when use chose 'No thanks, not now' in the Code App information screen.

    - count: Number of times the notification has been shown. Field is only shown if user has been prompted at least once.

    - Next Prompt: Shows the next time for showing the notification screen. The field is only shown if such a date exists, i.e. if the user has opted to show the prompt again later.


New User
Flows - Standard
Flows - Responsive
Current User: 322850759
Other Info
CPR | NemID # | Alias
Search
Logoff
Details for: 322850759
Identity details
Addressing Name: Till Kristensen
Identity Handle: 58
Identity Type: Person
Age: 27
Status: Active
CPR: 2009911043
CPR login enabled: true (disable)
Number of OTP Devices: 1
POCES Qualified: true
OTP Devices
NemID #322850759
OTPDevice handle: 58
Issue date: 2019-02-18
Issue age: 27
NemID #: 322850759
Alias: TILLX
Type: STANDARD
Password error count: 0
Password type error count: 0
Failed attempts for the current challenge: 0
Challenges without successful validation: 0
Attempts without successful validation: 0
Password status: ACTIVE
Password storage type: User blob
Password type: STANDARD
Answer to 4 digits pwd:
Code App Prompt - Allow prompt: Y
Code App Prompt - Version shown: DESKTOP
Code App Prompt - No thanks answer: 2019-02-18 10:19:36
Code App Prompt - count: 1
Code App Prompt - Next Prompt: 2019-03-04 10:19:36
Preferred device: NMASDEVICE
Automatic certificate renewal enabled: true (disable)
Fraud No active bank agr.: 0
Fraud No bank agr.: 0
Fraud Signal: GREEN
Available device actions:
Revoke Device
Issue new PIN Code
Issue new PIN Code by mail
Issue new OTP Card
Issue new OTP Card by mail
Prefer OTP Card
Issue Gemalto token
Prefer Gemalto token
Create code app
Test initiator app
OTP Cards
Card Serial
Status
Issue Date
Revocation Time
Codes left
Actions
A316521661
ACTIVE
2019-02-18
-
147
Use all codes Revoke
Gemalto tokens
Note: Reordering a token will be assigned transaction identifier equal to the serial number prefixed with "RE".
Token Serial
Status
Issue Date
Revocation Time
Current TOTP
Actions
0000000000000010
PENDING
2019-02-18
-
650451
Revoke
Code Apps
Code App Serial
Operating System
Status
Issue Date
Revocation Time
Incorrect attempts
Actions
3480-4609-0230
iOS 10.0
ACTIVE
2019-02-18 10:19:50
-
0
Revoke Open simulator Test message Details
PIN Codes
Note: PIN Code MUST have status active before it can be used for login!
PIN Code Serial
Status
Channel
Purpose
Error Count
Expires
Pin Data
01529677
CONSUMED
HANDEDOUT
FIRST_TIME_ACTIVATION
0
2019-04-19 11:19:34.182
186756
Private Keys
ID
Certificate
Status
Serial
Issued
Expires
Order ID
56
Till Kristensen
ACTIVE
1550481575999
2019-02-18 10:19:36.031
Tue Feb 18 10:19:35 CET 2020
56
NemID Test Tools - Copyright © 2019 | Nets-DanID A/S

2.6.1 Code card

Under *OTP cards*, links to the test user's code cards can be found.

New User Flows - Standard Flows - Responsive Current User: 322850759 Other Info

NemID Nøglekort A316521661

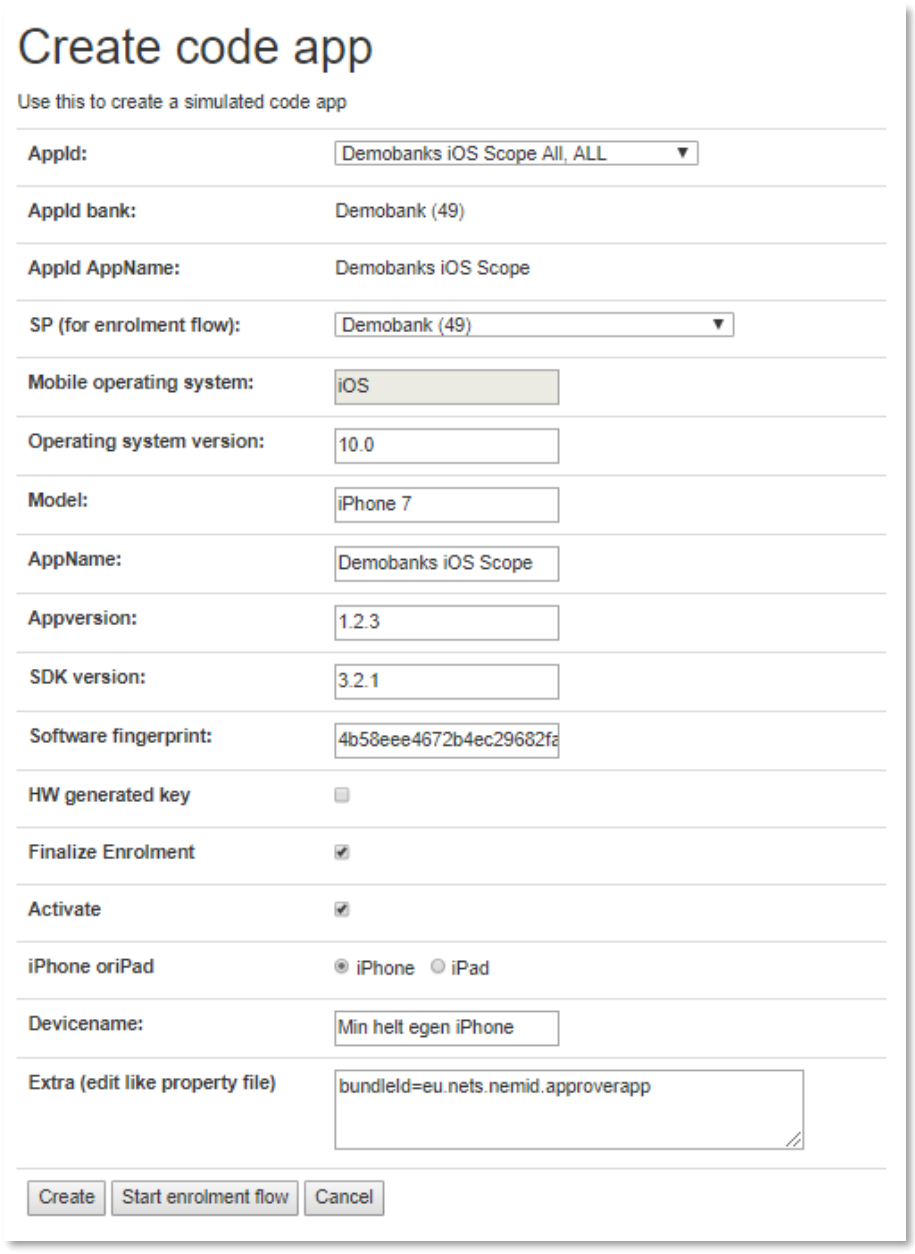
Nøglekortnummer: A316521661

Nøgle nr.	Nøgle	Nøgle nr.	Nøgle	Nøgle nr.	Nøgle	Nøgle nr.	Nøgle
0190	370361	3126	793368	5206	362441	7641	172652
0259	040158	3162	147667	5207	164169	7650	048242
0436	095412	3222	024739	5218	243984	7668	902460
0451	541487	3236	760091	5272	081790	7711	009209
0536	831120	3329	004863	5314	026613	7980	576504
0603	184549	3370	054309	5330	933841	7981	064077
0658	810233	3385	656103	5333	098397	8012	744277
0673	134865	3414	415971	5419	759746	8061	980417
0694	174827	3475	643340	5451	441003	8063	809852
0736	017822	3519	176442	5497	147160	8148	962312
0750	850652	3671	256088	5555	726692	8184	650610
0753	387723	3746	847814	5664	450749	8212	670830
0837	598421	3771	546569	5775	169851	8267	642818
0891	801448	3804	496118	5786	899845	8638	866421
0904	787444	3806	673731	5895	954964	8664	960413
1063	621903	3929	648238	5960	539465	8814	816262
1116	908485	3951	264325	5975	315887	8828	936303
1147	511122	3985	166770	5991	966749	8875	327534
1179	328299	4077	067650	6160	000155	8903	266364
1259	055168	4090	211617	6192	499897	8926	256680
1279	043332	4276	174956	6206	312037	8941	711879
1303	916508	4433	676394	6250	743564	9112	094635
1380	435213	4521	886702	6289	956211	9163	549740
1485	044260	4749	801911	6311	728248	9167	793302
1518	837890	4784	733518	6445	951582	9260	198107
1702	020298	4840	467217	6480	748603	9514	353224
1840	825011	4862	975814	6652	563420	9619	950661
1850	596766	4935	219591	6670	645619	9652	384442
1980	915437	4943	793497	6700	008983	9710	141203
2030	592802	4964	141424	6813	883691	9798	766920
2153	766636	4979	938656	6950	399176	9822	185956
2249	463776	5006	842980	7050	056254	9825	089153
2531	890334	5020	943971	7159	867714	9827	889639
2708	090515	5066	455493	7255	746220	9844	021980
2784	193751	5087	440793	7277	341195	9869	682829
2937	787296	5126	936934	7495	644736	9963	777716
2975	793190	5132	091232	7584	358193	9996	083046

2.6.2 Code apps

A list of the user's code apps can be found under *Code Apps*. The list contains both simulated and real code apps. Simulated code apps can be used to test the code app functionality without having to enrol a real code app on a mobile device first.

You can create a simulated code app by clicking the link *Create code app* under *Available Device Actions*. This opens a new window, where various metrics about the simulated code app can be specified:



The simulated code app can be created using the normal enrolment flow for code apps by clicking the button *Start enrolment flow*. Alternatively, the simulated code app can be created directly as a shortcut without using the enrolment flow by clicking *Create*. Real code apps are always created using the enrolment flow.

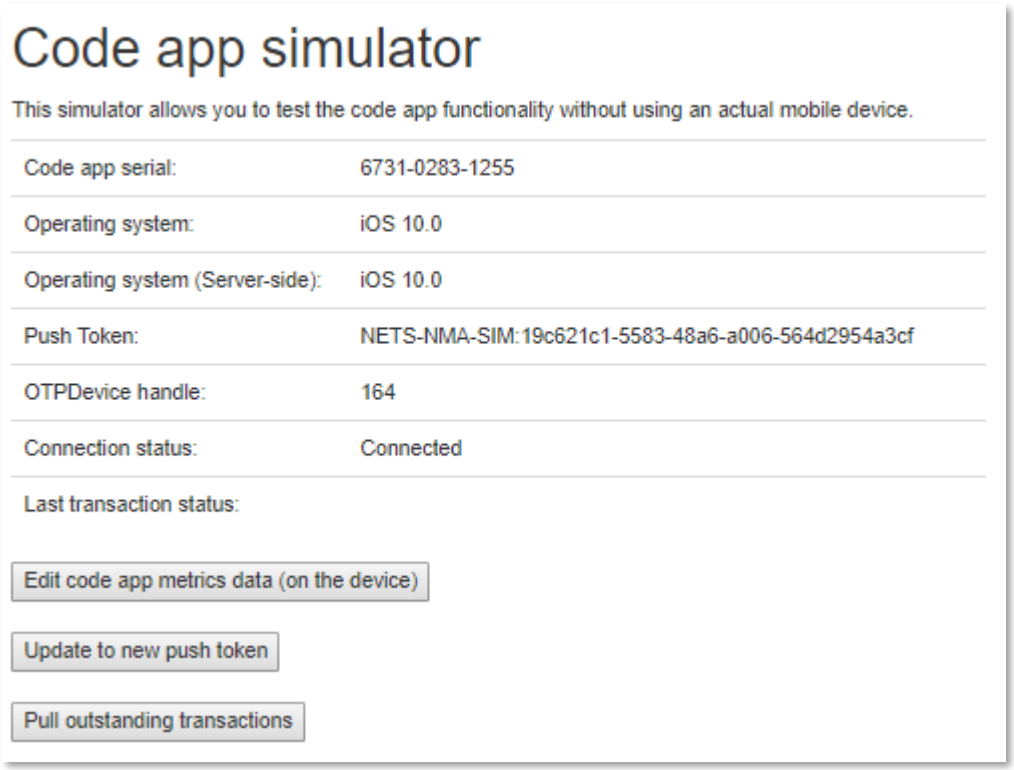
When a code app has been created, the following test functionality is available via links to the right in the code app list:

Revoke
Only shown for code apps in status VALIDATION_MISSING or ACTIVE. Revokes the code app, so it no longer can be used.

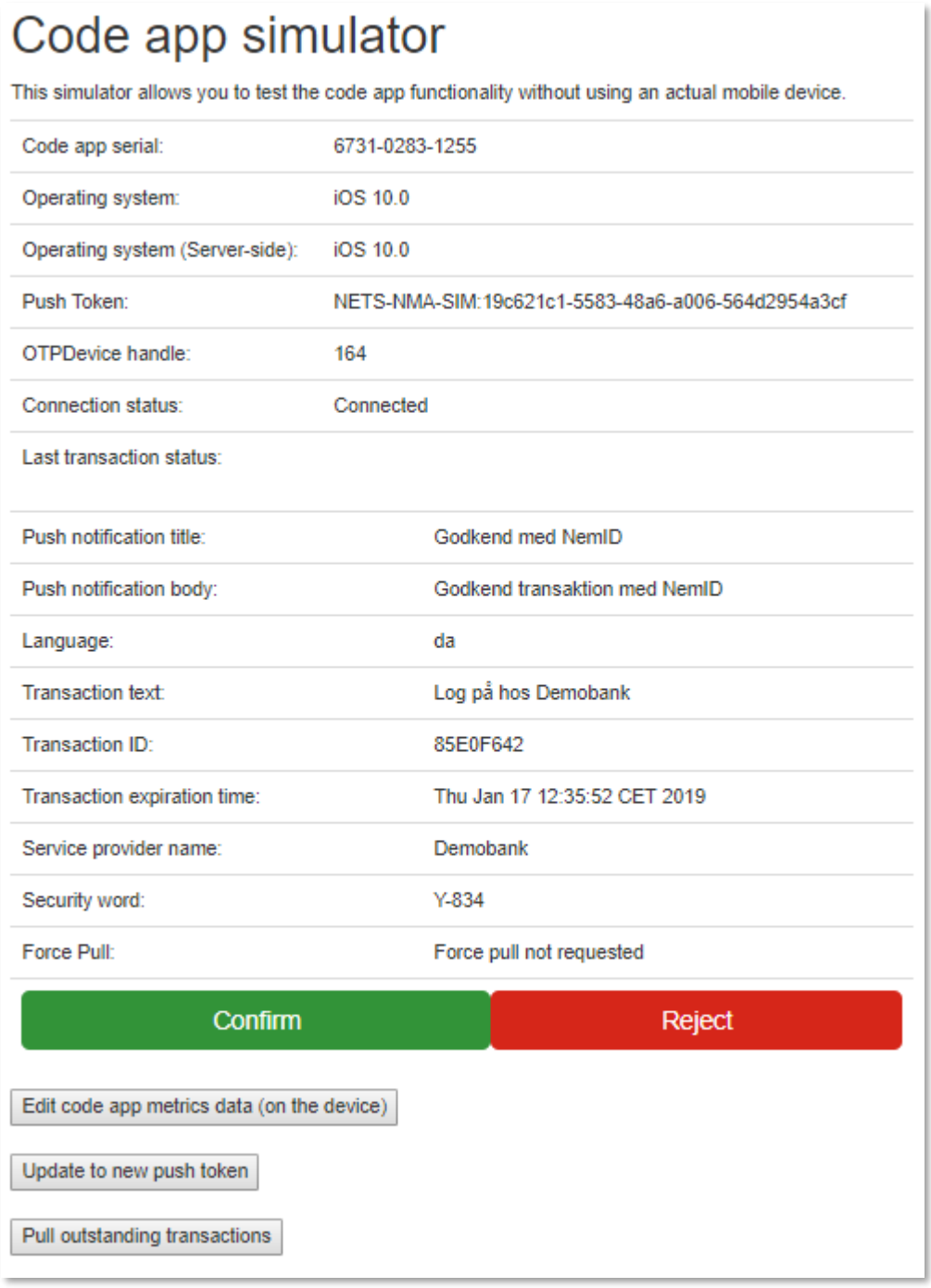
Activate
Only shown for code apps in status VALIDATION_MISSING. Changes the code app's status to ACTIVE. Notice that code apps in status VALIDATION_MISSING cannot be used for confirming requests.

Finalize Enrolment
Only shown for code apps in status ENROLMENT. Changes the code app's status to VALIDATION_MISSING. Notice that code apps in status ENROLMENT cannot be used for confirming requests.

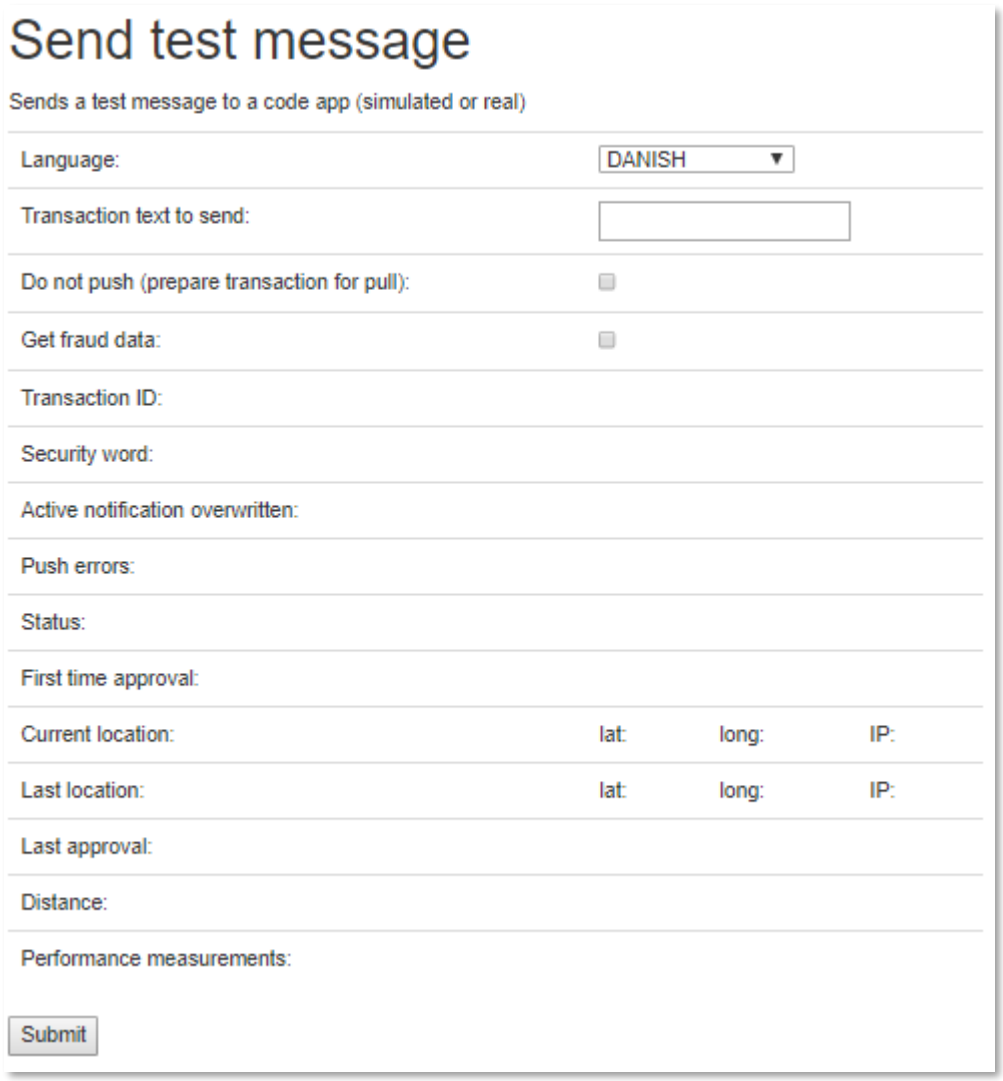
Open simulator
Only shown for simulated code apps in status VALIDATION_MISSING or ACTIVE. Opens a window where requests sent from the NemID client or using the link "Test push" can be confirmed or rejected. Data for the simulated code app can also be edited here. This can be used to test of OS updates, etc. Notice that editing the code app data only changes them in the simulator, not in the NemID backend.
Initially the window looks like this:



When a request from the NemID client or a test push is received, the window is updated to show information about the push and buttons are shown, that can be used to confirm or reject the request:


Code app simulator
This simulator allows you to test the code app functionality without using an actual mobile device.
Code app serial: 6731-0283-1255
Operating system: iOS 10.0
Operating system (Server-side): iOS 10.0
Push Token: NETS-NMA-SIM:19c621c1-5583-48a6-a006-564d2954a3cf
OTPDevice handle: 164
Connection status: Connected
Last transaction status:
Push notification title: Godkend med NemID
Push notification body: Godkend transaktion med NemID
Language: da
Transaction text: Log på hos Demobank
Transaction ID: 85E0F642
Transaction expiration time: Thu Jan 17 12:35:52 CET 2019
Service provider name: Demobank
Security word: Y-834
Force Pull: Force pull not requested
Confirm
Reject
Edit code app metrics data (on the device)
Update to new push token
Pull outstanding transactions

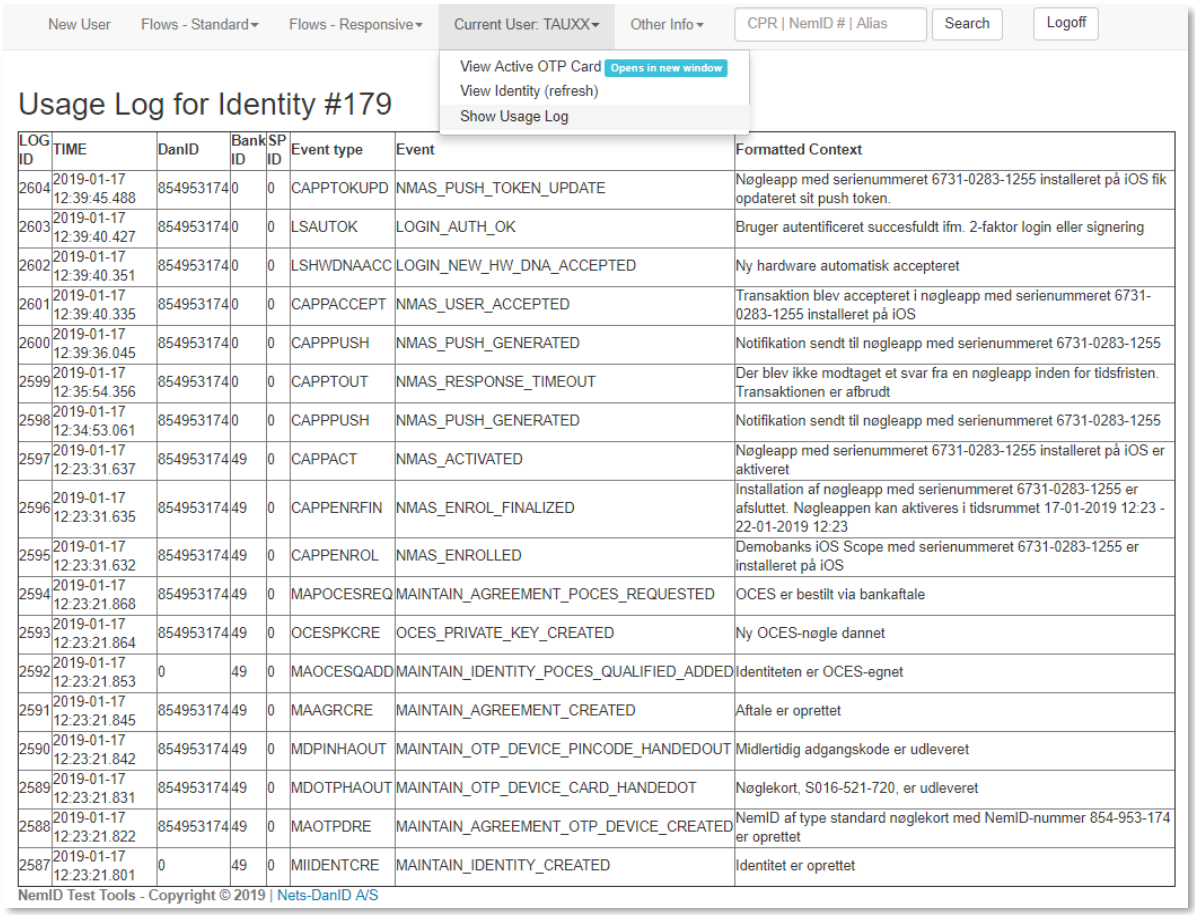
Test message
Only shown for code apps in status ACTIVE. Opens a window where a push request for confirmation can be sent to the code app without using the NemID client:



Details
Opens a window showing the code app data that is stored in the NemID backend.

2.6.3 Usage log

The usage log shows the most important events concerning the test user. The log is accessible from the menu under *Current User > Show Usage Log*. Note that the menu item *Current user* is only visible, if a user is logged in or if you have searched for and selected a user.



Usage Log for Identity #179

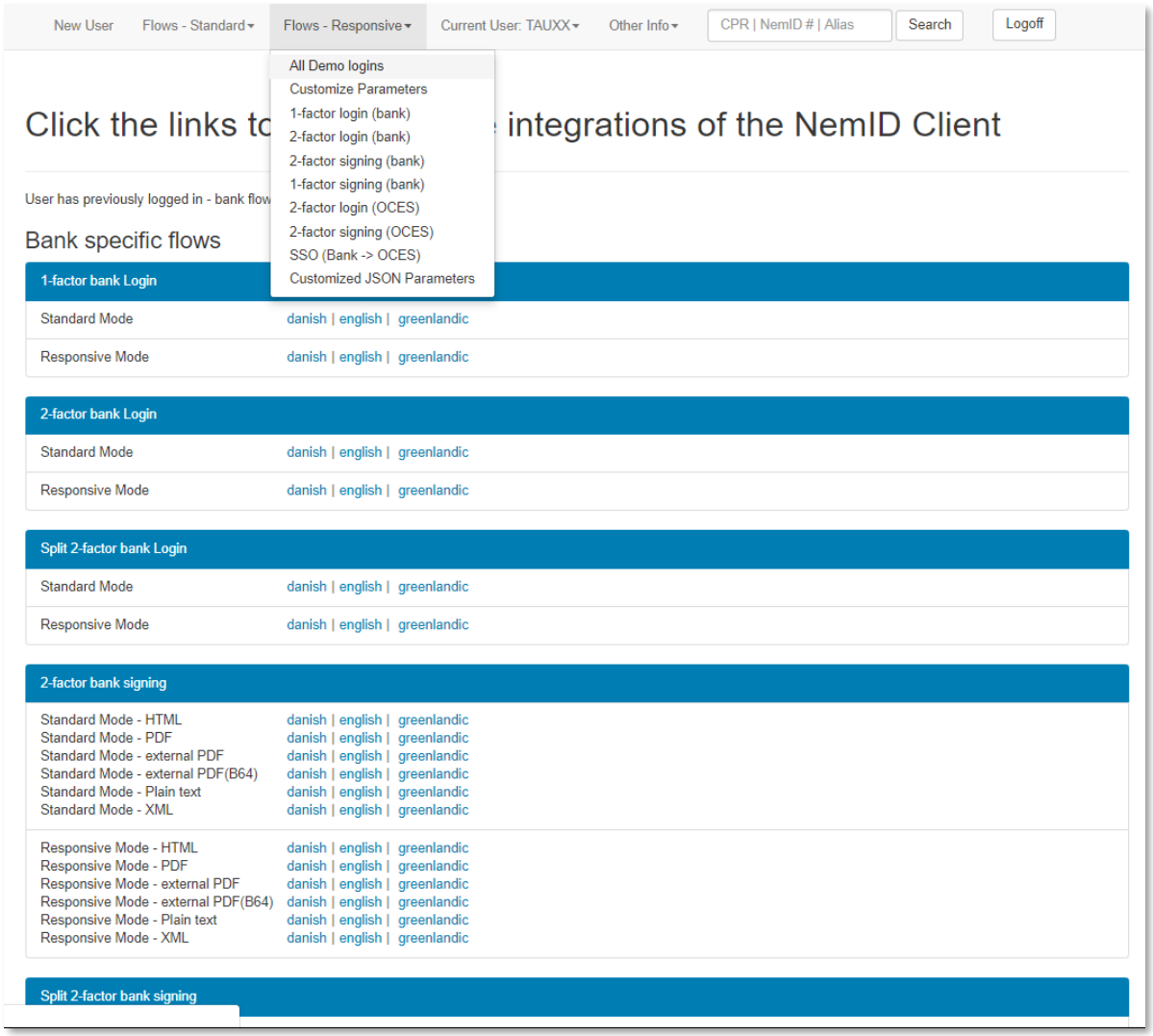
LOG ID	TIME	DanID	Bank ID	SP ID	Event type	Event	Formatted Context
2604	2019-01-17 12:39:45.488	854953174	0	0	CAPPTOKUPD	NMAS_PUSH_TOKEN_UPDATE	Nøgleapp med serienummeret 6731-0283-1255 installeret på iOS fik opdateret sit push token.
2603	2019-01-17 12:39:40.427	854953174	0	0	LSAUTOK	LOGIN_AUTH_OK	Bruger autentificeret succesfuldt ifm. 2-faktor login eller signering
2602	2019-01-17 12:39:40.351	854953174	0	0	LSHWDNAACC	LOGIN_NEW_HW_DNA_ACCEPTED	Ny hardware automatisk accepteret
2601	2019-01-17 12:39:40.335	854953174	0	0	CAPPACCEPT	NMAS_USER_ACCEPTED	Transaktion blev accepteret i nøgleapp med serienummeret 6731-0283-1255 installeret på iOS
2600	2019-01-17 12:39:36.045	854953174	0	0	CAPPPUSH	NMAS_PUSH_GENERATED	Notifikation sendt til nøgleapp med serienummeret 6731-0283-1255
2599	2019-01-17 12:35:54.356	854953174	0	0	CAPPTOUT	NMAS_RESPONSE_TIMEOUT	Der blev ikke modtaget et svar fra en nøgleapp inden for tidsfristen. Transaktionen er afbrudt
2598	2019-01-17 12:34:53.061	854953174	0	0	CAPPPUSH	NMAS_PUSH_GENERATED	Notifikation sendt til nøgleapp med serienummeret 6731-0283-1255
2597	2019-01-17 12:23:31.637	854953174	49	0	CAPPACT	NMAS_ACTIVATED	Nøgleapp med serienummeret 6731-0283-1255 installeret på iOS er aktiveret
2596	2019-01-17 12:23:31.635	854953174	49	0	CAPPENRFIN	NMAS_ENROL_FINALIZED	Installation af nøgleapp med serienummeret 6731-0283-1255 er afsluttet. Nøgleappen kan aktiveres i tidsrummet 17-01-2019 12:23 - 22-01-2019 12:23
2595	2019-01-17 12:23:31.632	854953174	49	0	CAPPENROL	NMAS_ENROLLED	Demobanks iOS Scope med serienummeret 6731-0283-1255 er installeret på iOS
2594	2019-01-17 12:23:21.868	854953174	49	0	MAPOCESREQ	MAINTAIN_AGREEMENT_POCES_REQUESTED	OCES er bestilt via bankaftale
2593	2019-01-17 12:23:21.864	854953174	49	0	OCESPKCRE	OCES_PRIVATE_KEY_CREATED	Ny OCES-nøgle dannet
2592	2019-01-17 12:23:21.853	0	49	0	MAOCESQADD	MAINTAIN_IDENTITY_POCES_QUALIFIED_ADDED	Identiteten er OCES-egnet
2591	2019-01-17 12:23:21.845	854953174	49	0	MAAGRCRE	MAINTAIN_AGREEMENT_CREATED	Aftale er oprettet
2590	2019-01-17 12:23:21.842	854953174	49	0	MDPINHAOUT	MAINTAIN_OTP_DEVICE_PINCODE_HANDEDOUT	Midlertidig adgangskode er udleveret
2589	2019-01-17 12:23:21.831	854953174	49	0	MDOTPHAOUT	MAINTAIN_OTP_DEVICE_CARD_HANDEDOT	Nøglekort, S016-521-720, er udleveret
2588	2019-01-17 12:23:21.822	854953174	49	0	MAOTPDRE	MAINTAIN_AGREEMENT_OTP_DEVICE_CREATED	NemID af type standard nøglekort med NemID-nummer 854-953-174 er oprettet
2587	2019-01-17 12:23:21.801	0	49	0	MIIDENTCRE	MAINTAIN_IDENTITY_CREATED	Identitet er oprettet

2.7 Flows

From the top menu, it is possible to start the flows using the standard or responsive JSClient using the respective menu item. In each menu you can select between initiating some of the most common flows directly, you can select to display a list of standard flows (All Demo logins), or to access a page for specifying parameters for any type of flow.

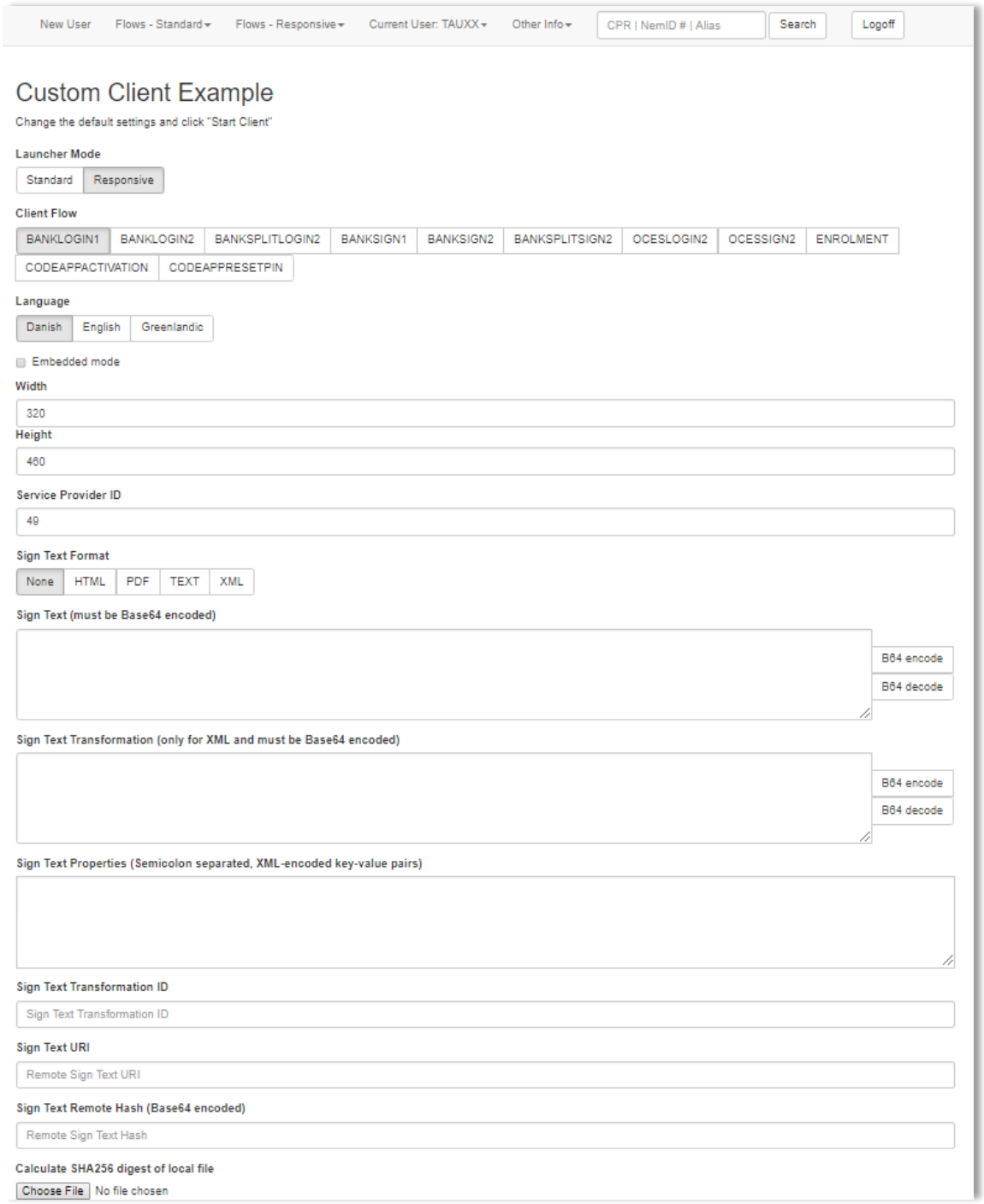
Selecting *All Demo logins* brings up a list of links that allow the user to initiate flows with the most common combination of modes and parameters. The flows are initiated either as DemoBank (ID 49) or as www.nemid.nu as the OCES service provider (ID 1). Each flow can be

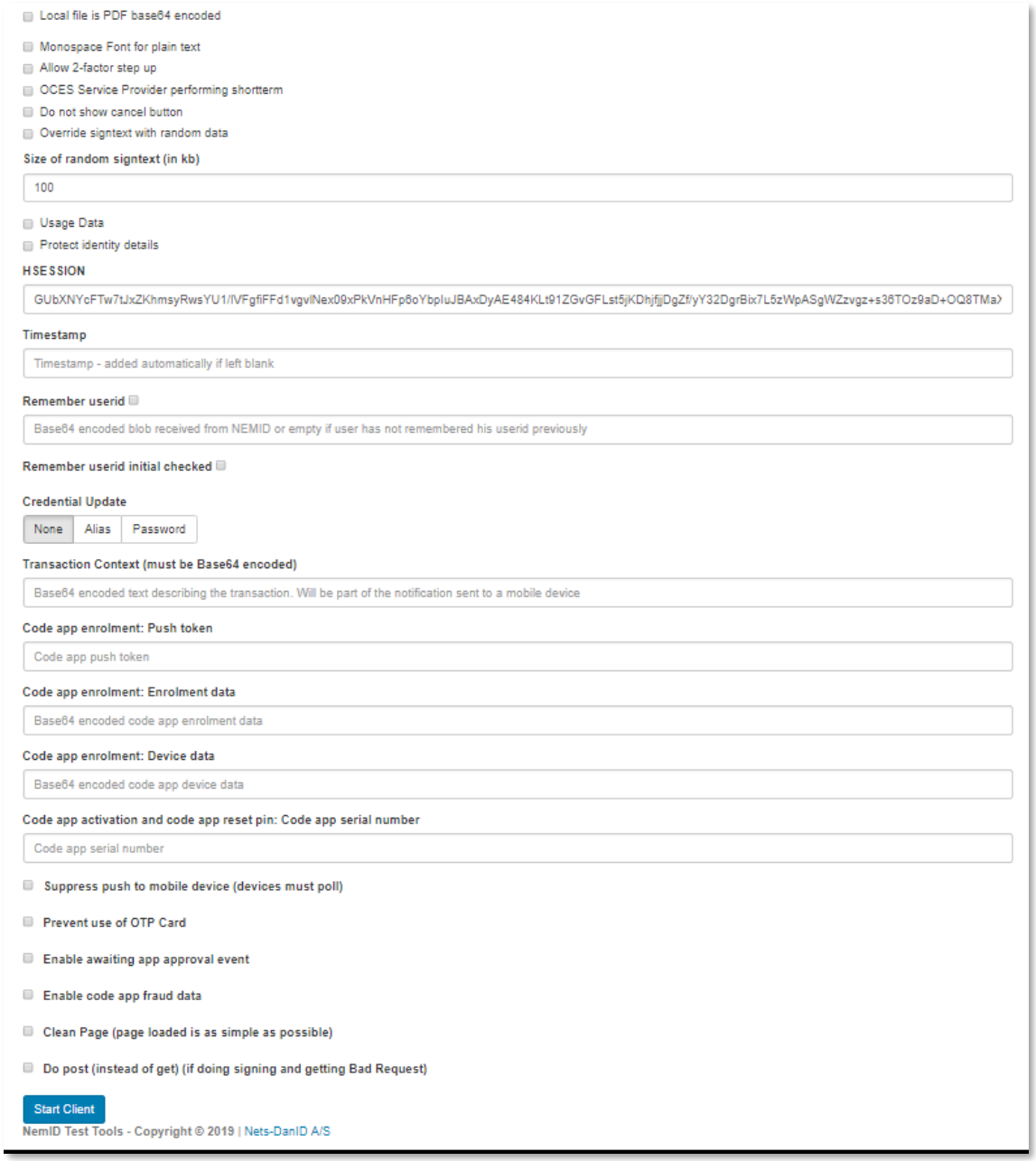
started in either Standard or Responsive mode. For both modes, options are available to start the flow in Danish, English and Greenlandic. For signing flows options are available to start the flows with sample signing texts in the formats HTML, PDF, plain text and XML.



2.7.1 Customize parameters

The direct links to start a flow will use typical or default values for the relevant parameters. When other parameter values are required, the customize parameters site allows you finer grained control of the parameters and values that will be sent to the NemID Client.


New User
Flows - Standard
Flows - Responsive
Current User: TAUXX
Other Info
CPR | NemID # | Alias
Search
Logoff
Custom Client Example
Change the default settings and click "Start Client"
Launcher Mode
Standard
Responsive
Client Flow
BANKLOGIN1
BANKLOGIN2
BANKSPLITLOGIN2
BANKSIGN1
BANKSIGN2
BANKSPLITSIGN2
OCESLOGIN2
OCESSIGN2
ENROLMENT
CODEAPPACTIVATION
CODEAPPRESETPIN
Language
Danish
English
Greenlandic
Embedded mode
Width
320
Height
460
Service Provider ID
49
Sign Text Format
None
HTML
PDF
TEXT
XML
Sign Text (must be Base64 encoded)
B64 encode
B64 decode
Sign Text Transformation (only for XML and must be Base64 encoded)
B64 encode
B64 decode
Sign Text Properties (Semicolon separated, XML-encoded key-value pairs)
Sign Text Transformation ID
Sign Text Transformation ID
Sign Text URI
Remote Sign Text URI
Sign Text Remote Hash (Base64 encoded)
Remote Sign Text Hash
Calculate SHA256 digest of local file
Choose File
No file chosen



The values specified for *Width* and *Height* define the dimensions of the iframe in which the NemID client will be displayed.

Note that the buttons on the side of the *Sign Text* and *Sign Text Transformation* text areas can be used to encode or decode any text that has already been placed in the respective text areas.

Note that the *Sign Text Remote Hash* must be supplied for an external PDF file, and that a tool is provided to easily produce a digest from a locally stored file.

Note that the *Sign Text Format* must be explicitly set for signing flows (the type is never inferred from the SignText itelf, nor from any file used to calculate a SHA256 digest).

Checking the *Monospace Font for Plain text* checkbox will add "SIGNTEXT_MONOSPACEFONT": "true" as a parameter. This only has an effect for signing flows with signtext format TEXT.

Checking the *Allow 2-factor step up* checkbox will add "ALLOW_STEPUP": "true" as a parameter. This will allow switching to 2-factor authentication if an existing short-term session cannot be used.

Checking the *OCES Service Provider performing shortterm* checkbox will add "OCES_SERVICEPROVIDER": "true" as a parameter. This is only relevant for initiating a short term flow as an OCES service provider.

Checking the *Do not show cancel button* checkbox will add "DO_NOT_SHOW_CANCEL": "true" as a parameter This will prevent the cancel button from displaying in the username and password screen.

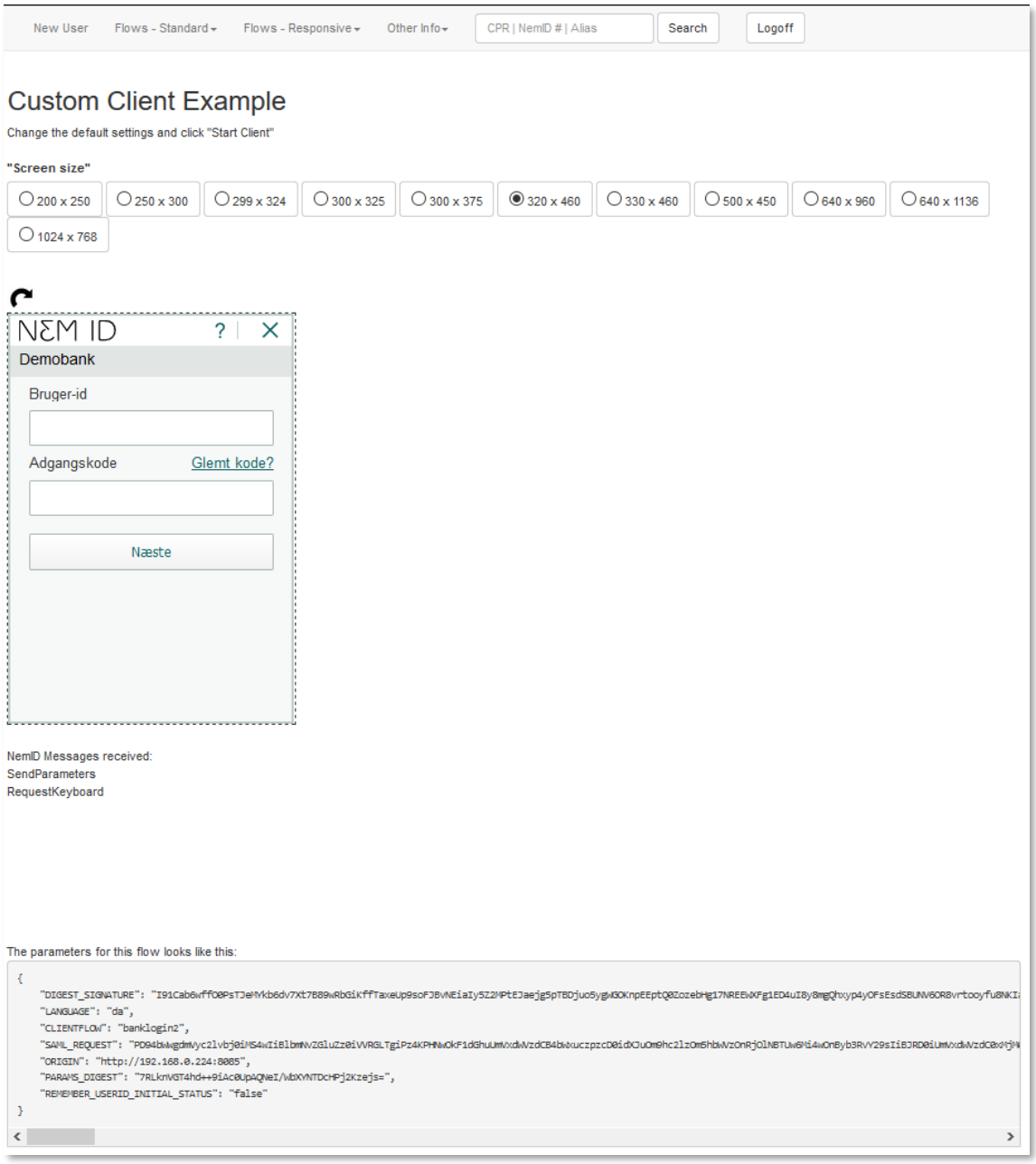
Checking the *Usage Data* checkbox will include "USAGEDATA": "true" as a parameter, which will enable the inclusion of BehavioSec data as part of the Encrypted Assertion of the SAML response (short term only).

Checking the *Remember userid* checkbox will enable the user to let the system remember his user ID. If the user choses to let the system remember the user ID, then the system will show the 4-digit component if the user has a 4 digit password. Otherwise the system will show the alphanumeric insertion field.

Checking the *Enable awaiting app approval event* will enable that the event is sent when the JS client is awaiting approval from the app(s). When the event is send out by the JS client a pop-up will appear stating that an awaiting app approval event was received.

Checking the *Do post* can be used for signing flows where the base64 encoded sign text become too large. If the browser returns an error like "server is busy" or "server unexpectedly dropped the connection" during a custom sign flow then it could be an indication that the sign text is too large. Try to use the "Do post" checkbox in this case.

When the Start Client button is pressed the same page is shown but with the JS client included at the top of the page:



New sections on the page are:

Screen size: Here the size of the JS client can be changed.

The iFrame containing the JS client: If in responsive mode there is an arrow above the client which when pressed will rotate the JS client window.

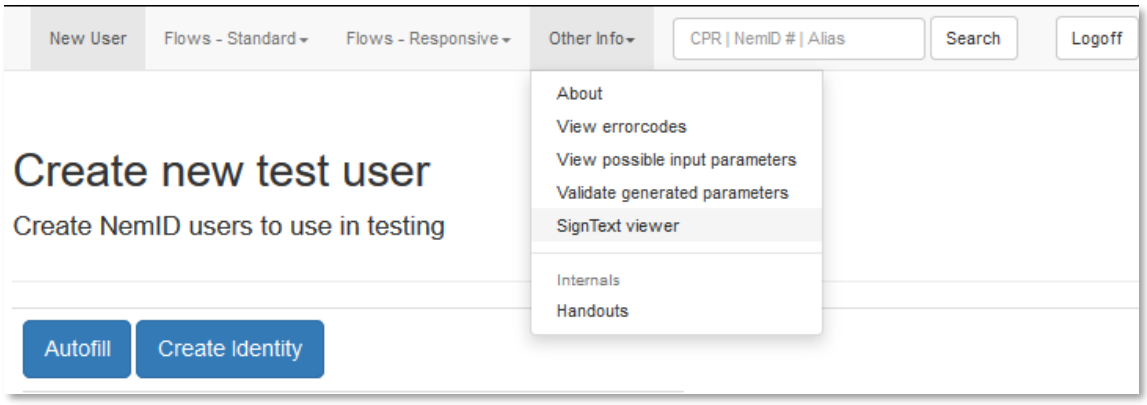
NemID Messages received: here is listed the NemID messages/javascript events sent out by the JS client for use by javascript code.

The parameters for this flow looks like this: Show the parameters passed to the JS client started above.

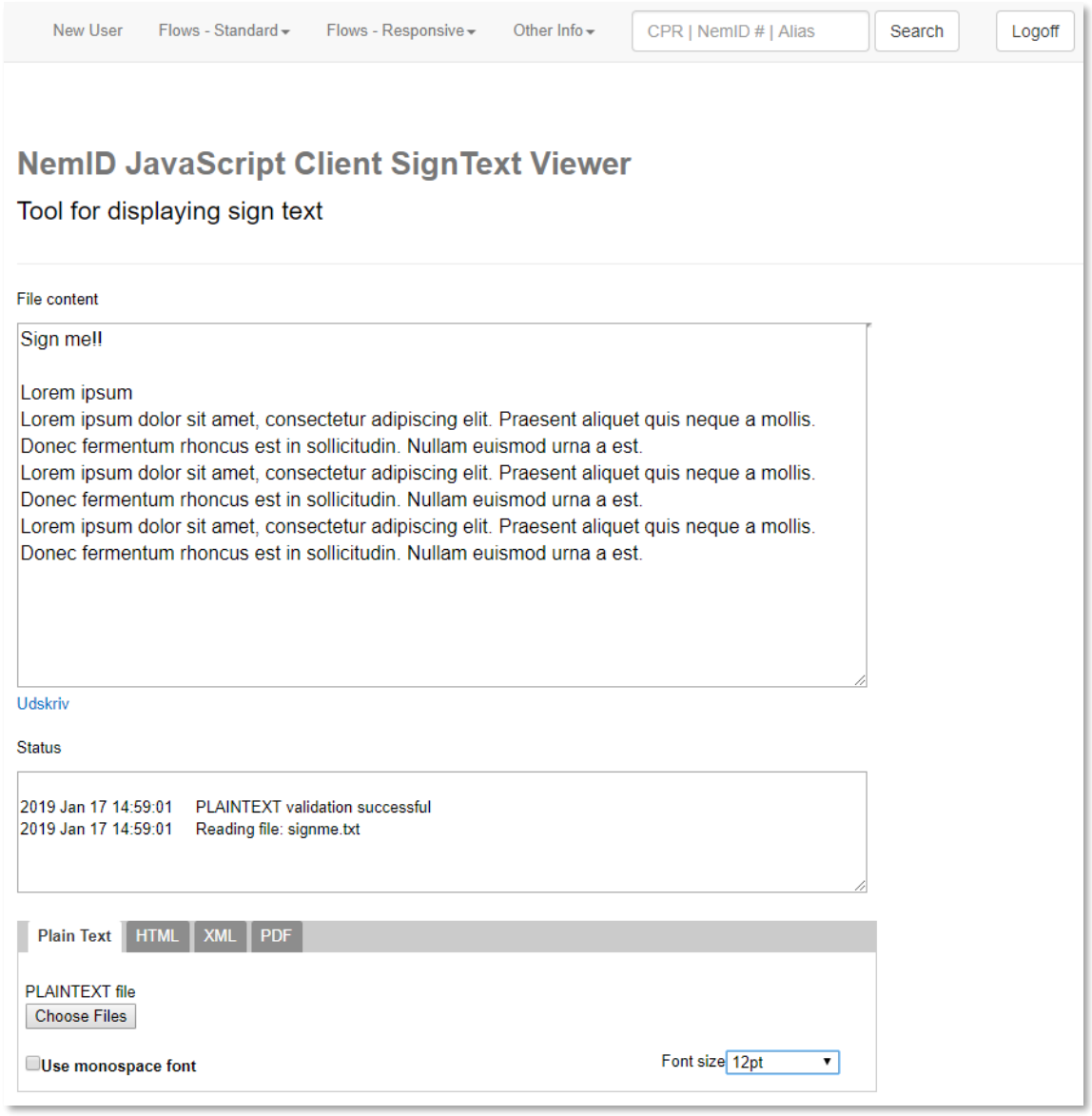
2.8 SignText Viewer

The SignText Viewer application is available through the menu option *Other Info* in the top menu. The application enables previewing of sign text in plain text, html, xml and pdf formats. The interface will be displayed in the same way as the end user will see it, so a service provider can use it for viewing and validating the visual layout of the sign text prior to integrating signing in their own applications.

2.8.1 Overview



2.8.2 Plain text tab

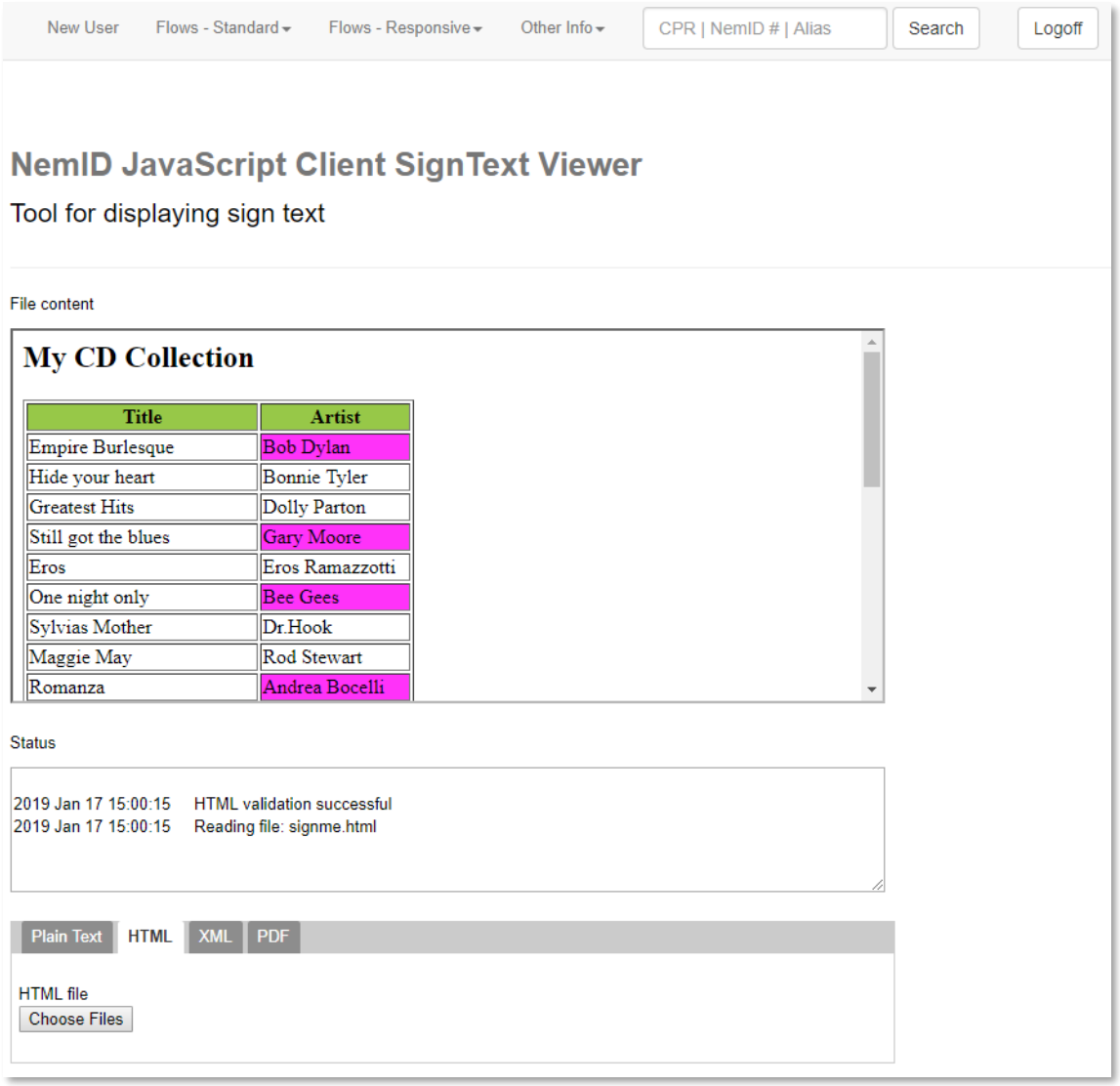


At the plain text tab, the sign text is rendered by the plain text viewer and is displayed in the *File content section*.

When the sign text file is chosen, it is possible to alter the font size and use monospace font.

As stated in the *Status section*, no validation rules are applied for the plain text.

2.8.3 HTML tab

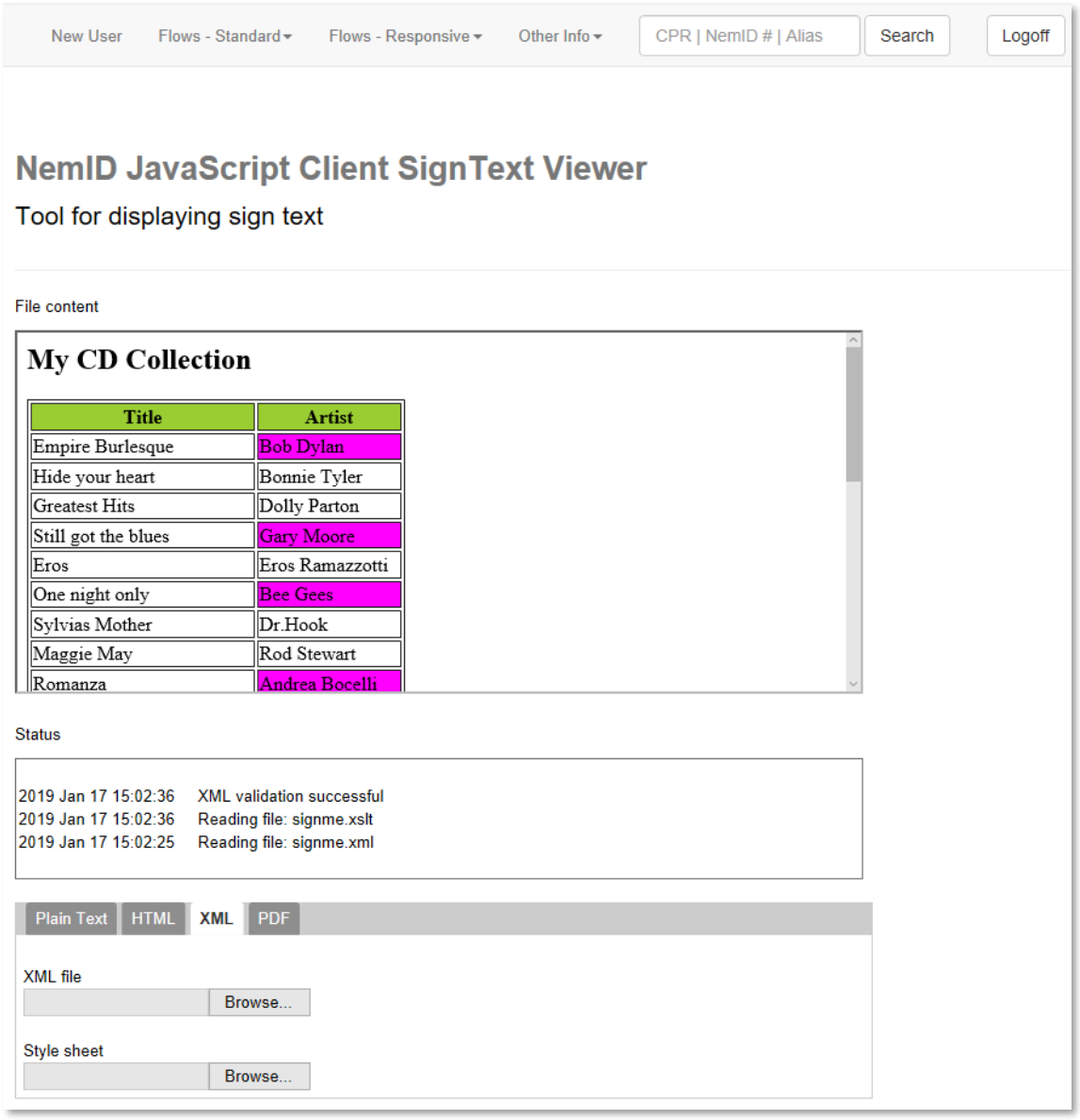


At the HTML tab, sign text in HTML format is rendered by the HTML viewer.

Upon choosing a sign text file in HTML format, the file content is validated. If the HTML validation is successful the sign text is rendered in the *File content section*, otherwise the reason for validation failure is displayed in the *Status section*. If there are any comments in the source html, the validation fails without further information. Otherwise, an exhaustive list of non-valid HTML tags is displayed the *Status section*.

Please refer to the NemID Integration document for a list of whitelisted tags.

2.8.4 XML tab



At the XML tab sign text in XML format is rendered by the HTML viewer.

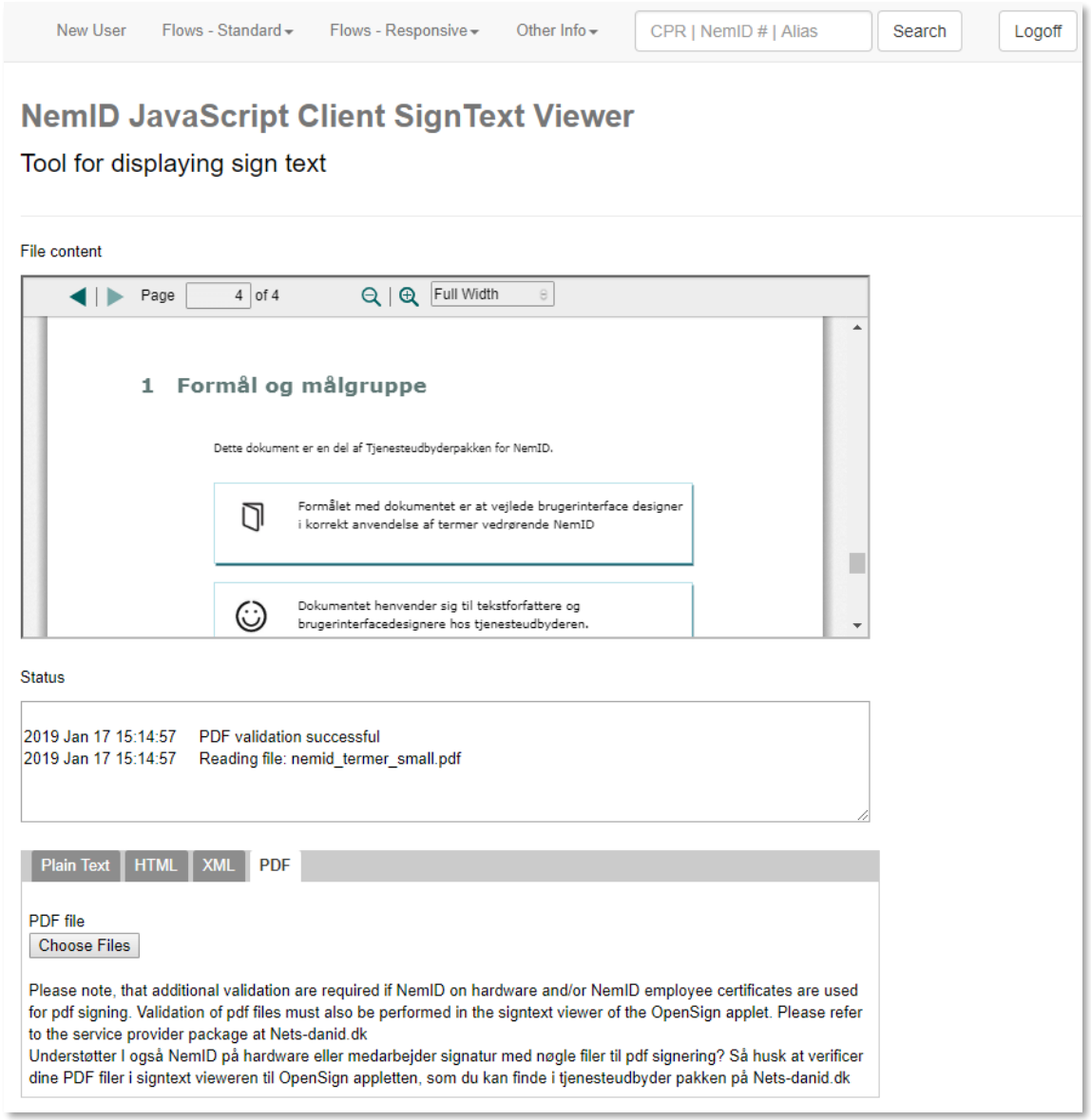
Please provide both an XML file and a corresponding XSLT style sheet.

Viewing the sign text in XML format is a two-step process:

1. The XML is transformed to HTML by applying the chosen XSLT style sheet. Please note that the transformation is done by the browser's XSLT engine. Small differences in the XSLT support and output may occur between different browsers, so it is highly recommended that service providers test the document transformation thoroughly across browsers.

2. The HTML validation rules are applied to the generated HTML. If the HTML validation is successful the generated sign text in HTML format is rendered in the *File content section*, otherwise an exhaustive list of non-valid HTML tags is rendered in the *Status section*. Comments are not allowed in the resulting html, and their existence will cause an error to be displayed and block any further errors from being listed.

2.8.5 PDF tab



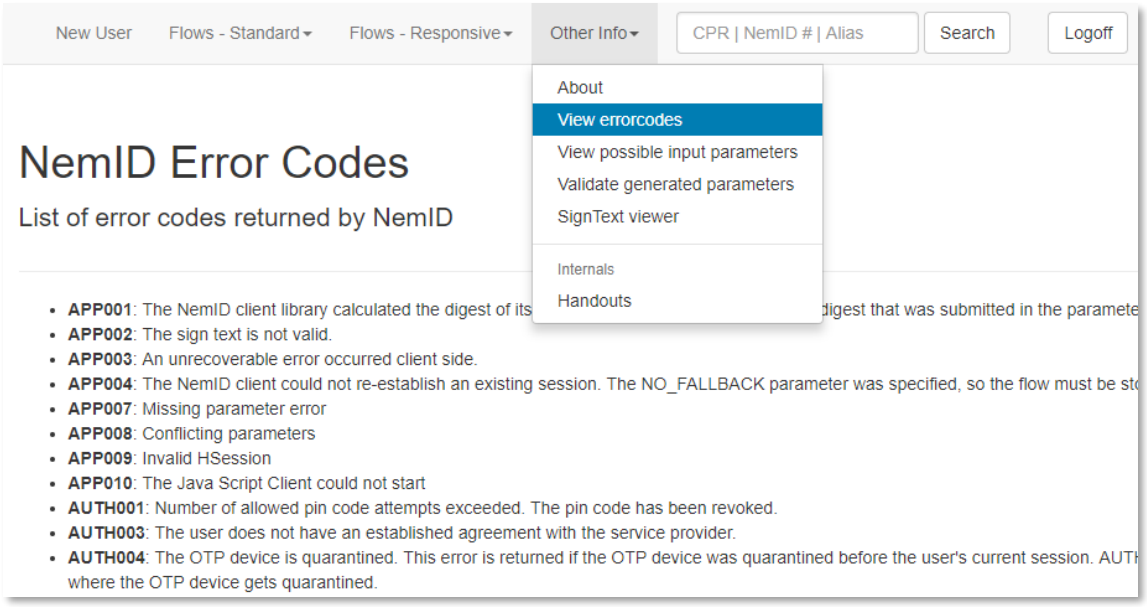
On the PDF tab, the NemID PDF viewer renders sign text in PDF format. If the PDF validation is successful the sign text is rendered in the *File content section*, otherwise an exhaustive list of parse or validation errors are displayed in the *Status section*.

The user interface for PDF sign text enables the user to scroll through the document, zoom in or out, and also to view the document in full screen mode.

Note, that the NemID PDF viewer uses certain HTML5 features not supported by Internet Explorer 8, and thus end-users using IE 8 cannot sign PDF documents. The NemID user interface will display an error message to the user, if the user's browser does not support the required HTML5 features.

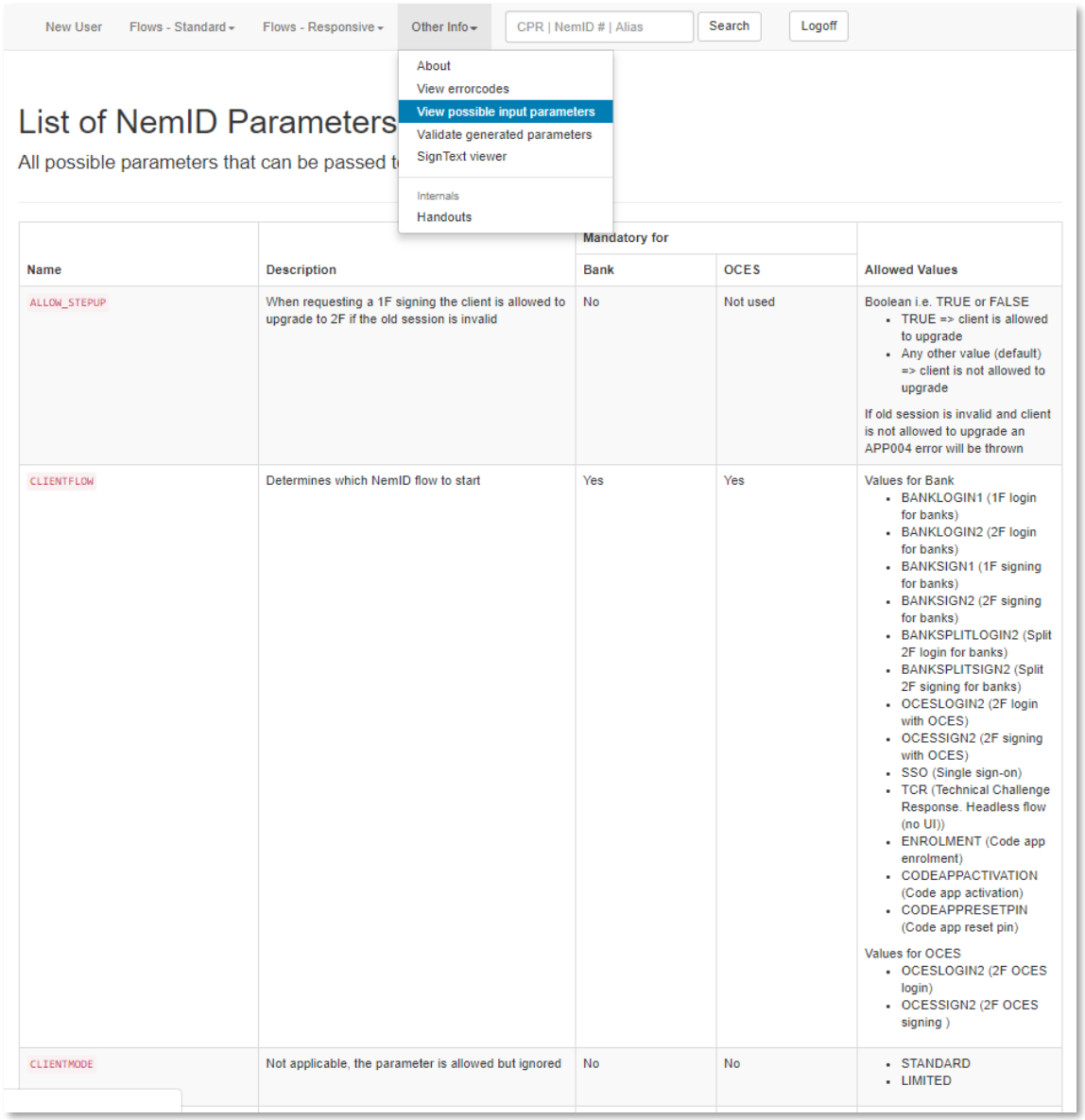
2.9 Error codes

From the menu *Other Info* you can choose to see an exhaustive list of client error codes that the NemID client can return:



2.10 NemID parameters

From the menu *Other Info* you can choose to see an exhaustive list of parameters that can be sent to the NemID client:



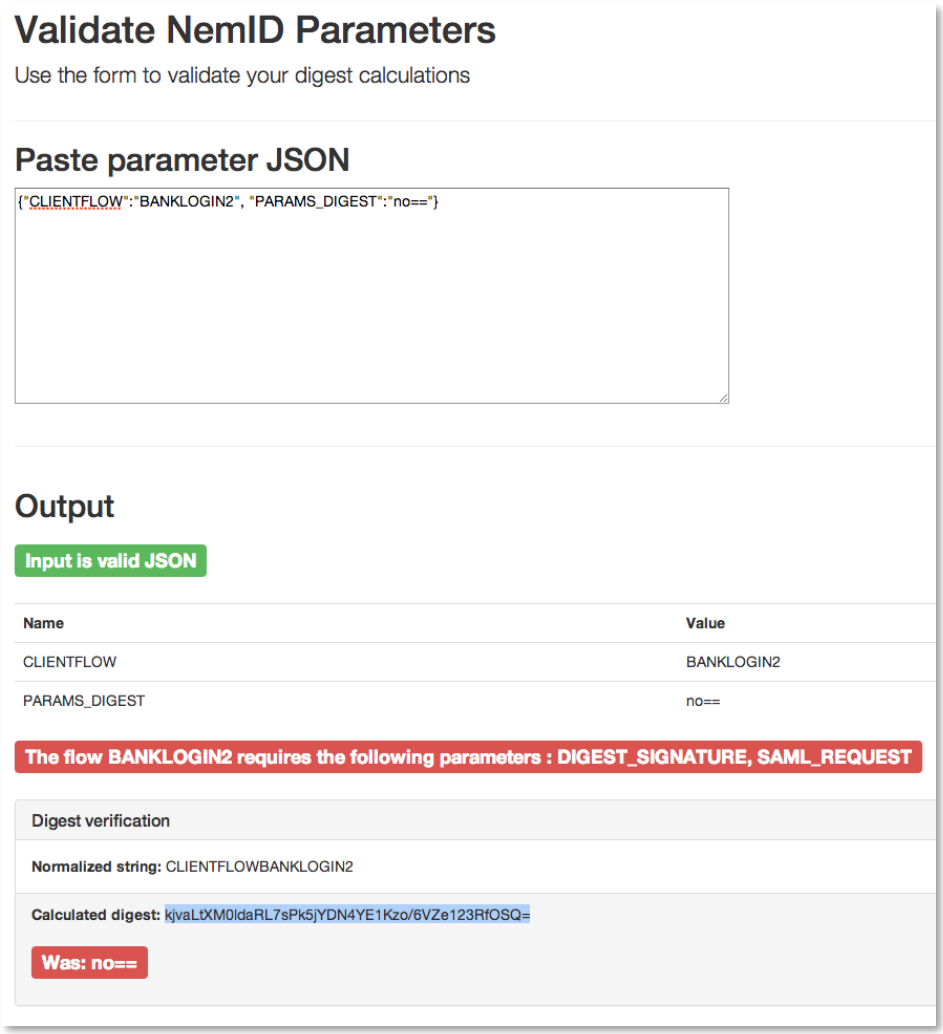
Name	Description	Mandatory for Bank	Mandatory for OCES	Allowed Values
ALLOW_STEPUP	When requesting a 1F signing the client is allowed to upgrade to 2F if the old session is invalid	No	Not used	Boolean i.e. TRUE or FALSE • TRUE => client is allowed to upgrade • Any other value (default) => client is not allowed to upgrade If old session is invalid and client is not allowed to upgrade an APP004 error will be thrown
CLIENTFLOW	Determines which NemID flow to start	Yes	Yes	Values for Bank • BANKLOGIN1 (1F login for banks) • BANKLOGIN2 (2F login for banks) • BANKSIGN1 (1F signing for banks) • BANKSIGN2 (2F signing for banks) • BANKSPLITLOGIN2 (Split 2F login for banks) • BANKSPLITSIGN2 (Split 2F signing for banks) • OCESLOGIN2 (2F login with OCES) • OCESSIGN2 (2F signing with OCES) • SSO (Single sign-on) • TCR (Technical Challenge Response. Headless flow (no UI)) • ENROLMENT (Code app enrolment) • CODEAPPACTIVATION (Code app activation) • CODEAPPRESETPIN (Code app reset pin) Values for OCES • OCESLOGIN2 (2F OCES login) • OCESSIGN2 (2F OCES signing)
CLIENTMODE	Not applicable, the parameter is allowed but ignored	No	No	• STANDARD • LIMITED

2.11 NemID parameter validation

When selecting *Validate generated parameters* from the menu *Other Info*, you can validate your parameters and the parameters digest in JSON and validate your parameter digest:

The single textarea accepts JSON-formatted text and immediately responds by:

- Stating whether the text is valid JSON.
- Displaying a table containing all of the parameters found in the JSON text.
- Displaying parameter integrity errors (erroneous parameters are marked with a red background in the table of parameters).
    - Checks for the presence of required parameters.
    - Checks for the validity of the parameter values.
    - Checks whether values that must be BASE64 encoded appear to actually have been encoded.
- Displaying the normalized string of parameters.
- Calculating and displaying the parameter digest
    - Displays an error if the calculated parameter digest does not match the value of the compulsory "PARAMS_DIGEST" parameter.



2.12 Logoff

To clear an existing session, press the button *Logoff* in the right side of the top menu.