Digitaliseringsstyrelsen

Vejledning i tilslutning til eID-gateway integrationstestmiljø

Gennemgang af integrationstest og integrationstestmiljøet

Version: 1.5
ID: 53443
2022-03-23

Indhold

1 Introduktion

Nærværende dokument beskriver leverandørens integrationstestmiljø, som stilles til rådighed for tjenesteudbydere i forbindelse med integrationstest af tjenester mod eID-gateway.

Denne vejledning er struktureret således:

- Afsnittet "Komponenter i eID-gateway" beskriver, hvorledes integrationstestmiljøet er opbygget.
- Afsnittet "Anbefalinger til UX/UI" beskriver de anbefalinger, der gives til eIDAS.
- Afsnittet "Loginforløb i integrationstestmiljøet" beskriver, hvordan brugere navigerer i integrationstestmiljøet.
- Afsnittet "Tilslutningsproces" beskriver, hvordan tjenesteudbydere opnår adgang til integrationstestmiljøet.
- Afsnittet "Krav til tjenesteudbyder metadata" beskriver, hvordan tjenesteudbydere skal strukturere og validere metadata for tjenesteudbyderens tjeneste.
- Afsnittet "Integrationstest" beskriver, hvordan tjenesteudbydere skal teste deres tjeneste mod integrationstestmiljøet.
- Afsnittet "Referencer" indeholder en liste af referencer, som anvendes gennem dokumentet ved angivelse af referencenr. i firkantet parentes. F.eks. henviser [1] til National eID-snitfladespecifikation for tjenester.

Begreber og forkortelser

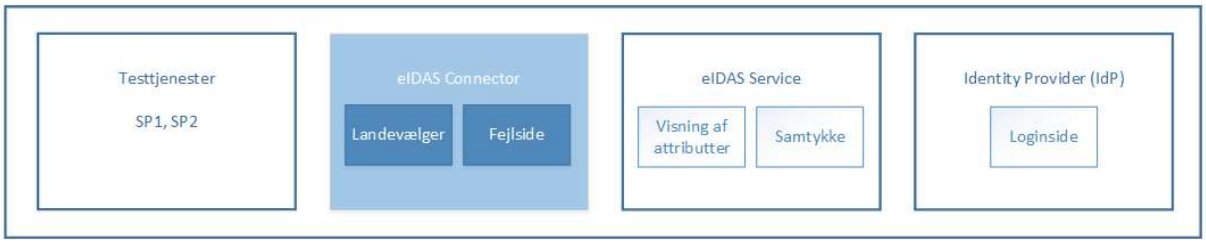
I dokumentet anvendes de følgende vigtige begreber og forkortelser:

Begreb	Reference
DIGST	Digitaliseringsstyrelsen
DK	Danmark / dansk
eID	Electronic identification scheme (eID)
eIDAS	eIDAS Interoperability Architecture v1.00 [4]
eIDAS Connector	En eIDAS komponent, som på vegne af tjenester sender forespørgsler om autentificering af brugere til andre EU/EØS MS. Hver EU/EØS MS har en eller flere nationale eIDAS Connector(s), som stilles til rådighed for deres respektive tjenester. eID-gateway, og dermed integrationstestmiljøet, udstiller én eIDAS DK Connector, som danske tjenester sender forespørgsler om autentificering af brugere til.
eIDAS Service	En eIDAS komponent, som modtager forespørgsler om autentificering af brugere fra andre EU/EØS MS via disse MS respektive eIDAS Connector(s). Hver EU/EØS MS udstiller én eIDAS Service. En eIDAS Service udsteder assertions om brugere med afsæt i MS respektive eID løsninger for autentifikation af brugere.
IdP	En Identity Provider autentificerer brugere
INTTEST	Integrationstestmiljøet for den danske eID-gateway
LoA	eIDAS Level of Assurance (sikringsniveau)[1]
MS	Member State (MS) / land
OIOSAML	OIOSAML profile 2.0.9 [3]
PROD	Produktionsmiljøet for den danske eID-gateway
SAML	OASIS SAML Core v2 standard [2]
SP	Service Provider / DK tjenesteudbyder
Tjeneste	En DK tjeneste, som i eID-gateway (DK Connector) regi tilgås af brugere fra andre EU/EØS MS
URL	Uniform Resource Locator (Web-adresse)

[1] Note: Ved grænseoverskridende autentifikation: Bemærk at der af og til også anvendes begrebet ”koblingsstyrke” om sikringsniveau. Vi har valgt at bruge begrebet ”sikringsniveau”, da det er det mest anvendte begreb i eID-gateway regi.

2 Komponenter i eID-gateway integrationstestmiljøet

Dette afsnit indeholder en beskrivelse af eID-gateways komponenter med afsæt i integrationstestmiljøet. Integrationsmiljøet tilsigtes at være en "spejling" af produktionsmiljøet. Det følgende afsnit har især fokus på eIDAS Connector komponenten som illustreret i Figur 1. Denne vejledning kommer også kort ind på testtjenester og IdP.



Figur 1 - Logisk oversigt over komponenterne i integrationstestmiljøet

De følgende afsnit 2.1 - 2.4 beskriver komponenterne i integrationstestmiljøet.

2.1 Testtjenester

I integrationsmiljøet (INTTEST) stilles to testtjenester til rådighed, som kan benyttes til at opleve komponenterne i integrationstestmiljøet samt til at afprøve et loginforløb. Testtjenesterne udstilles på de følgende websider (hver af disse åbnes blot i en browser):

URL 1 (LoA = 'substantial'): https://sp1.test.eid.digst.dk/demo/login.ashx

URL 2 (LoA = 'low'): https://sp2.test.eid.digst.dk/demo/login.ashx

Bemærk: Der findes i det hele taget ikke udstillet lignende testtjenester i produktionsmiljøet (PROD).

2.2 eIDAS Connector

eIDAS Connector er komponenten, som på vegne af tjenester, sender forespørgsler om autentificering af brugere videre til andre EU lande.

Al SAML kommunikation mellem eID-gateway og tjenester sker via eIDAS Connector, hvorfor tjenester skal udveksle metadata med denne. Tjenesteudbydere (TU) kan downloade metadata til integrationstestmiljøets eIDAS Connector på følgende URL: https://eidasconnector.test.eid.digst.dk/idp

Generelle informationer omkring forespørgsler mod eIDAS Connector findes i [1], og forståelse af indholdet i [1] er således en forudsætning for at opnå succesfuld integration mod eIDAS Connector. Oplysningerne refereret til i [1] indeholder blandt andet:

1) Krav til tjenesters request (afsnit 2.1)
2) Oversigt over svar (afsnit 2.2)
3) Oversigt over SAML fejl (afsnit 2.2.2)

2.2.1 Landevælger

På eIDAS Connector præsenteres en landevælger for brugeren, hvor denne skal vælge sit oprindelsesland. Efter valg af et givet land viderestilles brugeren til den respektive EU/EØS MS eIDAS Service.

Det er kun muligt at vælge lande, som integrationstestmiljøet har etableret forbindelse med. Er et land ikke aktivt (eller midlertidigt deaktiveret), vil der fremgå en forklaring herom ved at holde musen over udråbstegnet. Der arbejdes løbende på at etablere forbindelse til eIDAS proxy Services i andre landes respektive integrationstestmiljøer.

Integrationstestmiljøets egen demo eIDAS Service stilles til rådighed under flaget 'EU'. Denne "EU eIDAS proxy Service" kan være nyttig i udarbejdelsen af metadata.

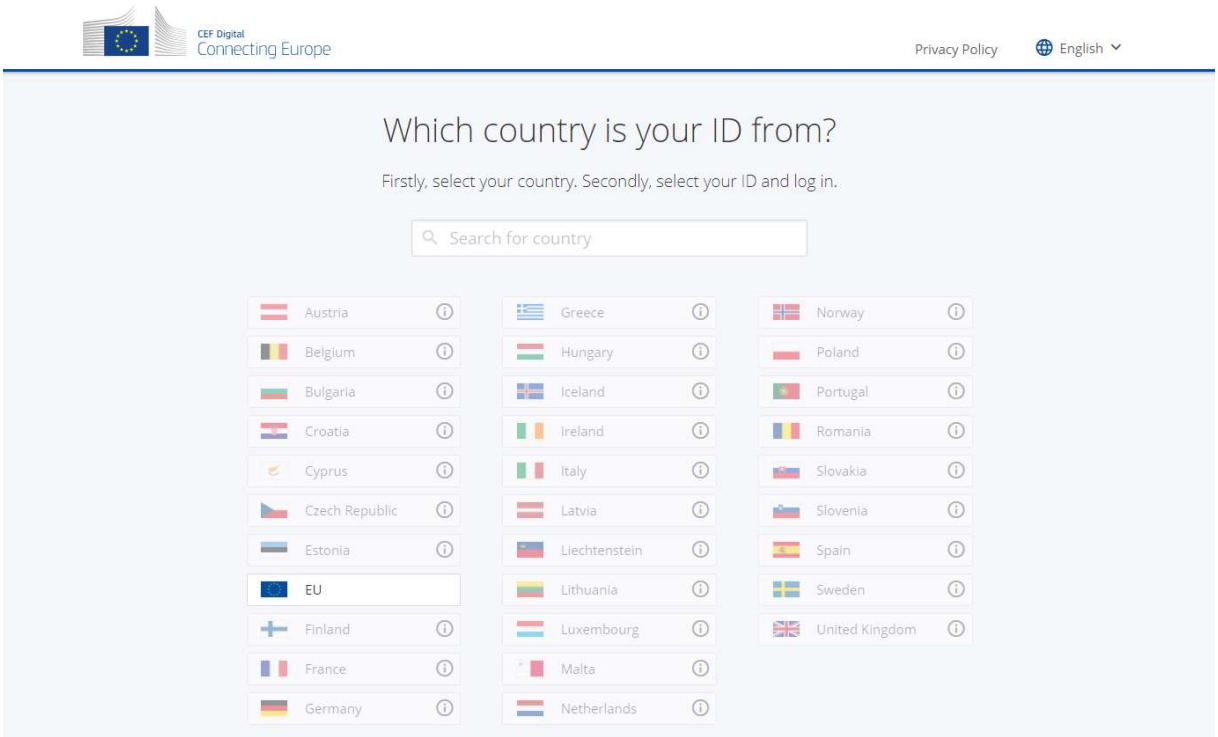
Bemærk at landevælgeren i DK Connector ikke er fuldt funktionelt udviklet i den nuværende anvendte version af EU referenceimplementeringen (pt. version 2.5), der stilles til rådighed i integrationstestmiljøet. Det betyder bl.a. at:

- At det kun er engelsk som understøttes som sprog.
- At det ikke kan forventes, at layoutet er *responsive* på mobile enheder, etc.
- At oplysninger om privatlivspolitikker (*privacy*) ikke er tilgængelige.

Hvad angår produktionsmiljøet: Bemærk at landevælgeren i DK Connector *er* fuldt funktionel i den version, der stilles til rådighed i produktionsmiljøet, hvad angår:

- Oplysninger om privatlivspolitikker ("privacy policy") er tilgængelige.

Et skærmbillede af *Landvælgeren* i integrationstestmiljøet vises i Figur 2.



Figur 2 - Landevælgeren i DK Connector

2.2.2 Fejlside

Hvis der opstår fejl under loginforløb, vil DK eIDAS Connector - afhængig af fejltypen - enten sende brugeren til fejlsiden på eID-gateway eller sende et SAML svar med "styret" fejl tilbage til tjenesten.

Tjenester skal kunne håndtere SAML svar med "styret" fejl fra eIDAS Connector, og skal i den forbindelse sikre, at brugeren oplyses om afbrudt loginforløb[2].

I tilfælde hvor brugeren sendes til fejlsiden på eID-gateway, oplyses brugeren følgende:

- Et 'transactionId' (et unikt ID for en oplevet fejl)
- En fejlmeddelelse (som kan være af generel karakter afhængig af fejltypen)

Dette 'transactionId' kan med fordel benyttes ved senere henvendelse til DIGST på fejl.

[2] Note: Se snitfladespecifikation for tjenester [1] afsnit 2.2.2, findes der en oversigt over forventede SAML fejl.

2.2.3 Behov for Webside der anerkender login uanset egenskaber

Udover at en dansk tjeneste kræver et bestemt sikringsniveau (LoA), så er der yderligere det forhold, at en dansk tjeneste kan have brug for et CPR-nummer. Hvis en tjeneste kræver for eksempel CPR-nummer, og dette CPR-nummer ikke er registreret på det pågældende eID, så vil EU/EØS borgeren blive viderestillet til tjenesten som et succesfuldt login.

Det er således ikke tilladt for eID-gateway at afvise et succesfuldt login, selvom det mangler påkrævede landespecifikke attributter. Den enkelte tjeneste kan dog vælge ikke at lukke brugeren ind i fagsystemet, hvis krav til sikringsniveau (LoA) eller krav til attributter ikke er imødekommet.

Danske tjenester skal derfor have en webside, som kan informere EU/EØS borgeren om, at deres login har været succesfuldt, og at tjenesten anerkender deres login, *men,* at der ikke kan tillades adgang til tjenesten hvad enten det er pga. manglende attributter eller pga. utilstrækkeligt sikringsniveau (LoA).

2.3 EU Referenceimplementeringen i integrationstestmiljøet

Figur 3 og 4 viser den i integrationstestmiljøet installerede og tilgængelige EU Referenceimplementeringen, som simulerer en integration med en eIDAS Service for et andet vilkårligt EU/EØS land. For tjenesteudbydere er det *denne* komponent, som muliggør test af login i egne tjenester.

EU referenceimplementeringen præsenterer følgende skærmbilleder i et loginforløb:

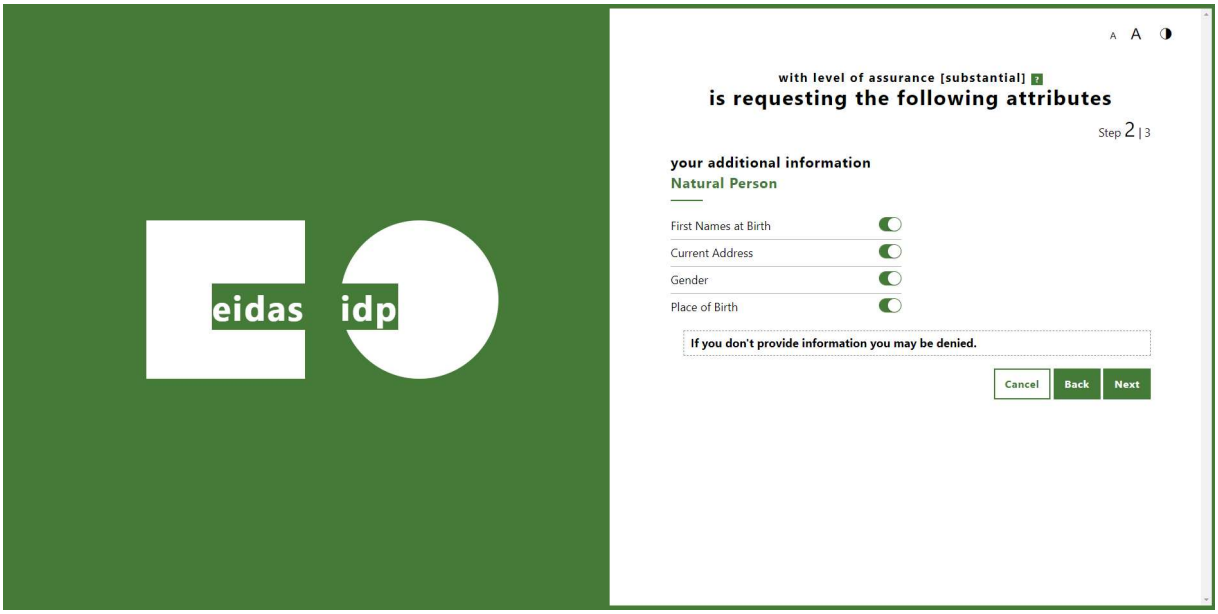
- Visning af attributter i forespørgsel fra en tjeneste – denne præsenteres for brugeren efter viderestilling fra DK eIDAS Connector.
- Samtykkeskærm - som præsenteres for brugeren efter login i Identity Provider.

2.3.1 Visning af attributter i forespørgsel fra tjeneste

Figur 3 viser et skærmbillede for referenceimplementeringen, der viser hvilke valgfrie attributter eIDAS Servicen har modtaget i en forespørgsel (”request”) fra en tjeneste.

Bemærk at skærmbillede i Figur 4 kun fremkommer, såfremt en tjeneste har valgfrie attributter inkluderet i forespørgslen (dvs. ”request”).

Figur 3 - Obligatoriske attributter



Figur 4 - Valgfrie attributter

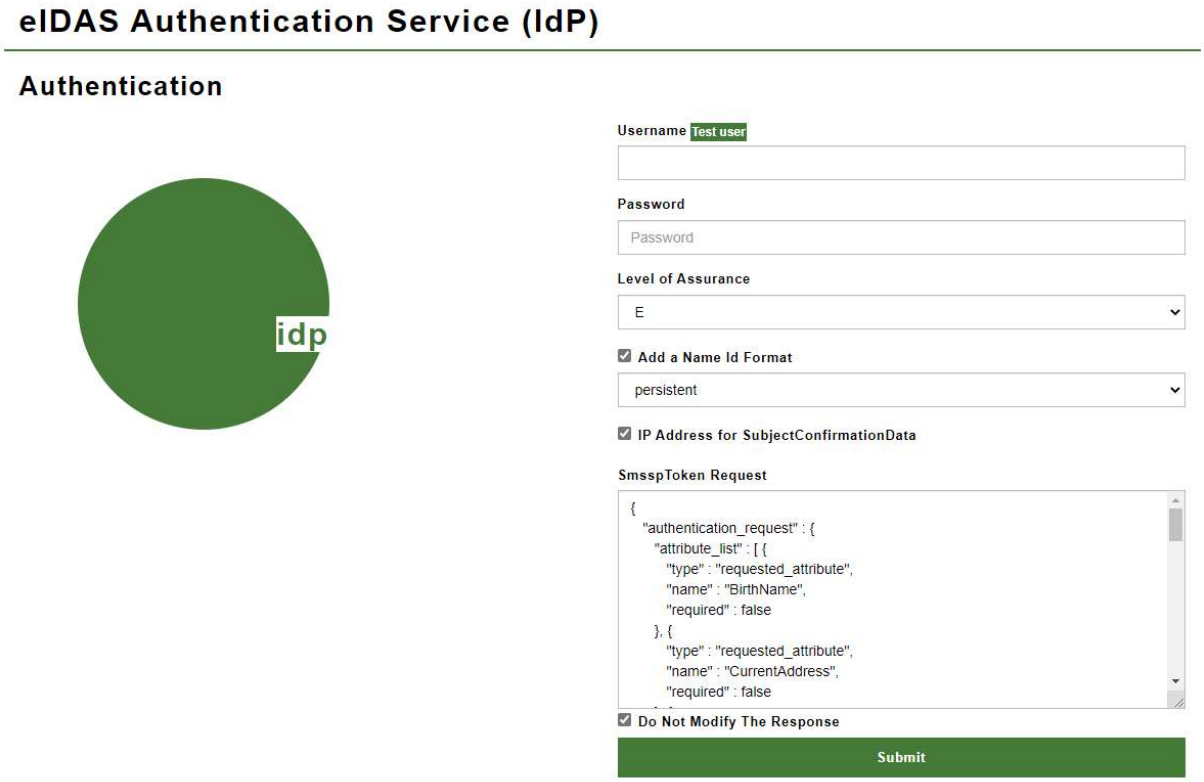
Bemærk at ovenstående skærmbillede i Figur 4 kun fremkommer, såfremt en tjeneste har valgfrie attributter inkluderet i forespørgslen (dvs. requestet).

2.4 Identity Provider

Identity Provider (IdP) er en installation af EU Referenceimplementeringens demo Identity Provider, som simulerer en loginløsning i et vilkårligt EU/EØS land.

Der skal anvendes en testbruger, som er oprettet på demo IdP for at teste integrationen. I Bilag B – Liste over testbruger, findes en liste over hvilke testbrugere, som er tilgængelige for tjenesteudbydere til at teste deres tjenester med.

Figur 5 viser et skærmbilledet af brugergrænsefladen for demo IdP.



Figur 5 - Demo Identity Provider login

Ved tryk på den grønne "Test user" knap[3] vises en oversigt (i et modalvindue) af oprettede testbrugere, deres passwords samt en kort beskrivelse af brugeregenskaberne.

Vigtige valg i formularen før "Submit":

- Der skal vælges "Level of Assurance" svarende til tjenestens ønskede niveau. I integrationstestmiljøet er dette altid lig 'High' og angives ved at vælge "E".

[3] Note: Knappen findes til højre for "Username" feltet øverst i Websiden.

- Herudover sættes der kryds i "Add a Name Id Format", og følgende værdi angives i træk-ned (pull-down) menuen: ”Persistent”.

Der findes som nævnt tidligere to aktive test service providers, som begge er i integrationstestmiljøet. Netop disse test service providers kan frit anvendes af tjenesteudbyderne til at prøve eID-gateway/DK eIDAS Connector forbindelsesflow til en vilkårlig EU eIDAS proxy Service. De to *test service providers* åbnes via følgende links:

URL 1 (LoA = ’substantial’): https://sp1.test.eid.digst.dk/demo/login.ashx

URL 2 (LoA = ’low’): https://sp2.test.eid.digst.dk/demo/login.ashx

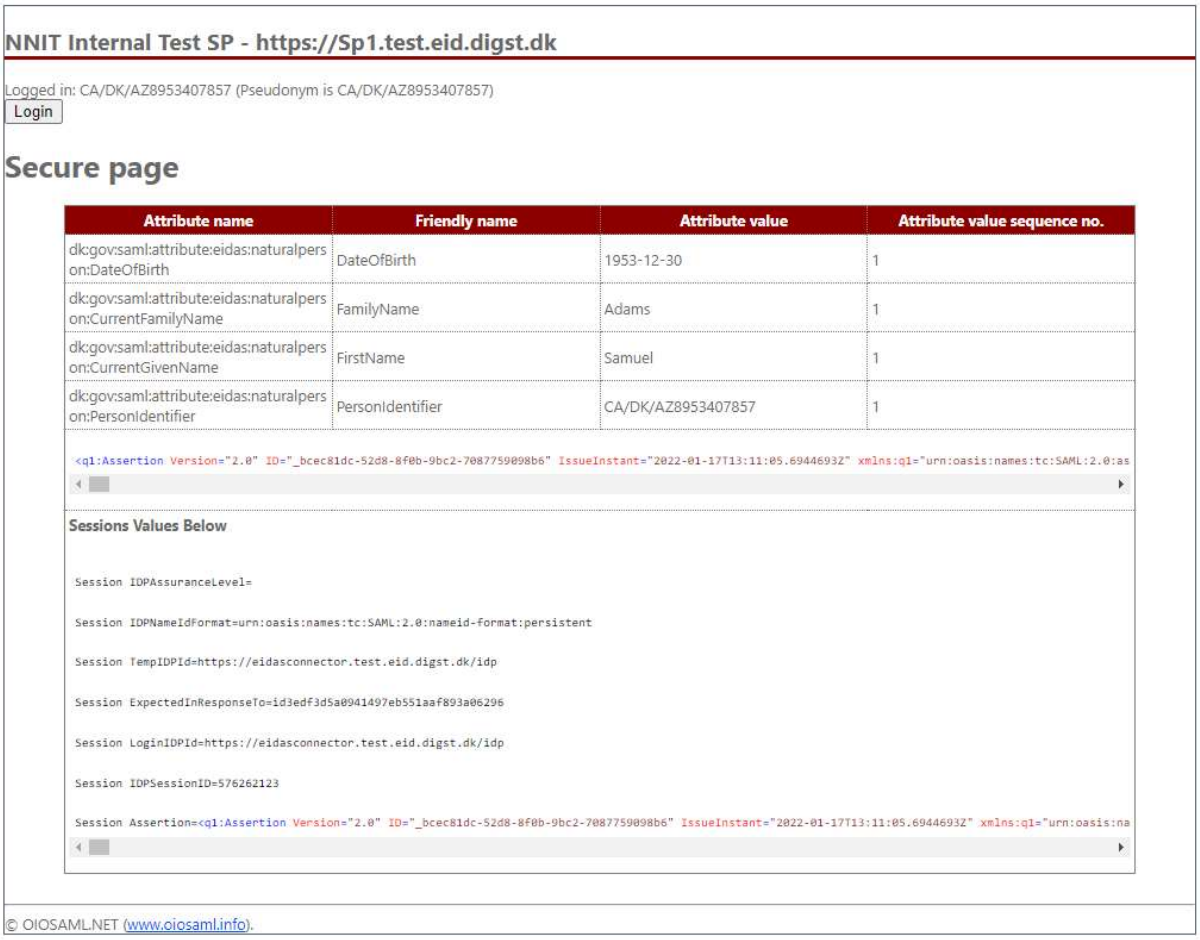
Herudover kan disse to test service providers af og til anvendes af andre medlemslande (MS) til at teste med (pendenter til den danske eID-gateway), jf. Figur 6.

Figur 6 - Test service provider ”SP1” åbnet i en browser.

Ved at logge ind med de specificerede testbrugere, kan brugernes attributter aflæses for hver given testbruger. Dermed kan også de forventede resultater fremfindes og aflæses.

Guide til anvendelse af test service providers (SP1, SP2):

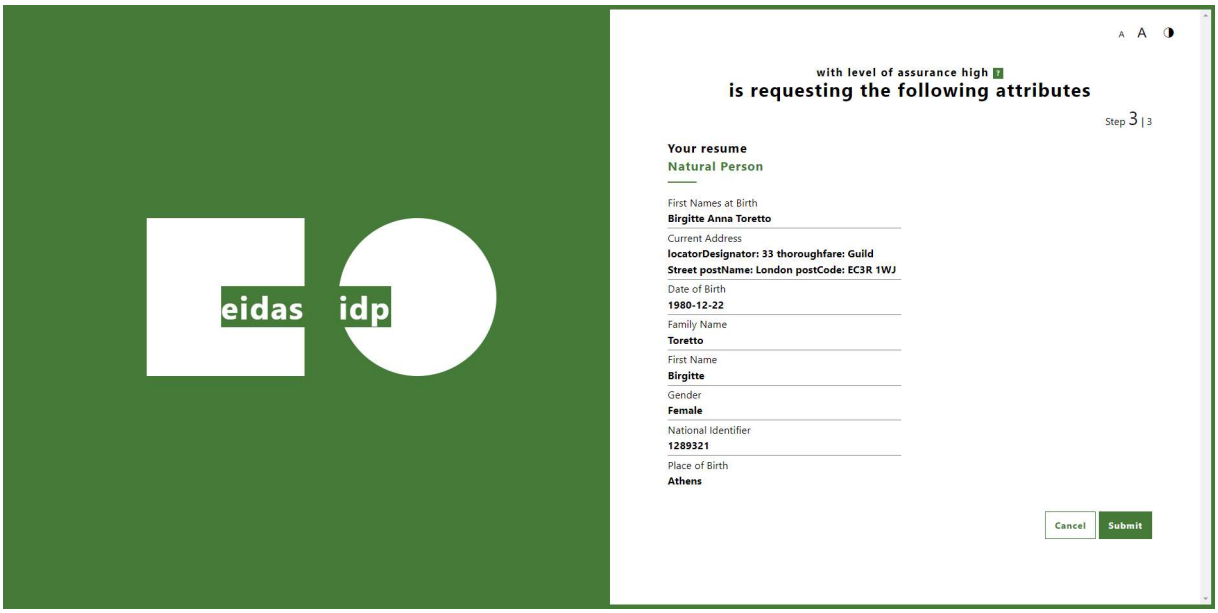
1. Åben én af de førnævnte test service providers (f.eks. SP1).
2. Når der klikkes på linket på siden, vil der foretages et login (jf. Figur 7).
3. Efter et succesfuldt login vil der vises en ”Secure page” webside, som indeholder sessionsværdier samt de anvendte attributter, attributværdier, osv. (jf. Figur 8):



Figur 7 - "Secure page" viser attributter, attributværdier, session values.

2.4.1 Samtykkeskærm(e)

Figur 8 viser et skærmbillede, der eksemplificerer de obligatoriske attributter og værdier, som eIDAS Servicen har modtaget om brugeren efter login i demo IdP.



Figur 8 - Samtykkeskærm med attributter og værdier

Bemærk: Såfremt valgfrie attributter er valgt præsenteres en ny samtykkeskærm med brugerens tilknyttede værdier til disse valgfrie attributter (hvis der er værdier angivet).

3 Anbefalinger til UX/UI

3.1 Loginknap

Tjenesten som Tjenesteudbyderen ønsker at stille til rådighed til grænseoverskridende anvendelse, skal synliggøre for brugeren på brugergrænsefladen, at der er mulighed for login med et eID fra EU/EØS. Login-knappen vil lede brugeren til "Landevælgeren", jf. afsnit 2.2.1.

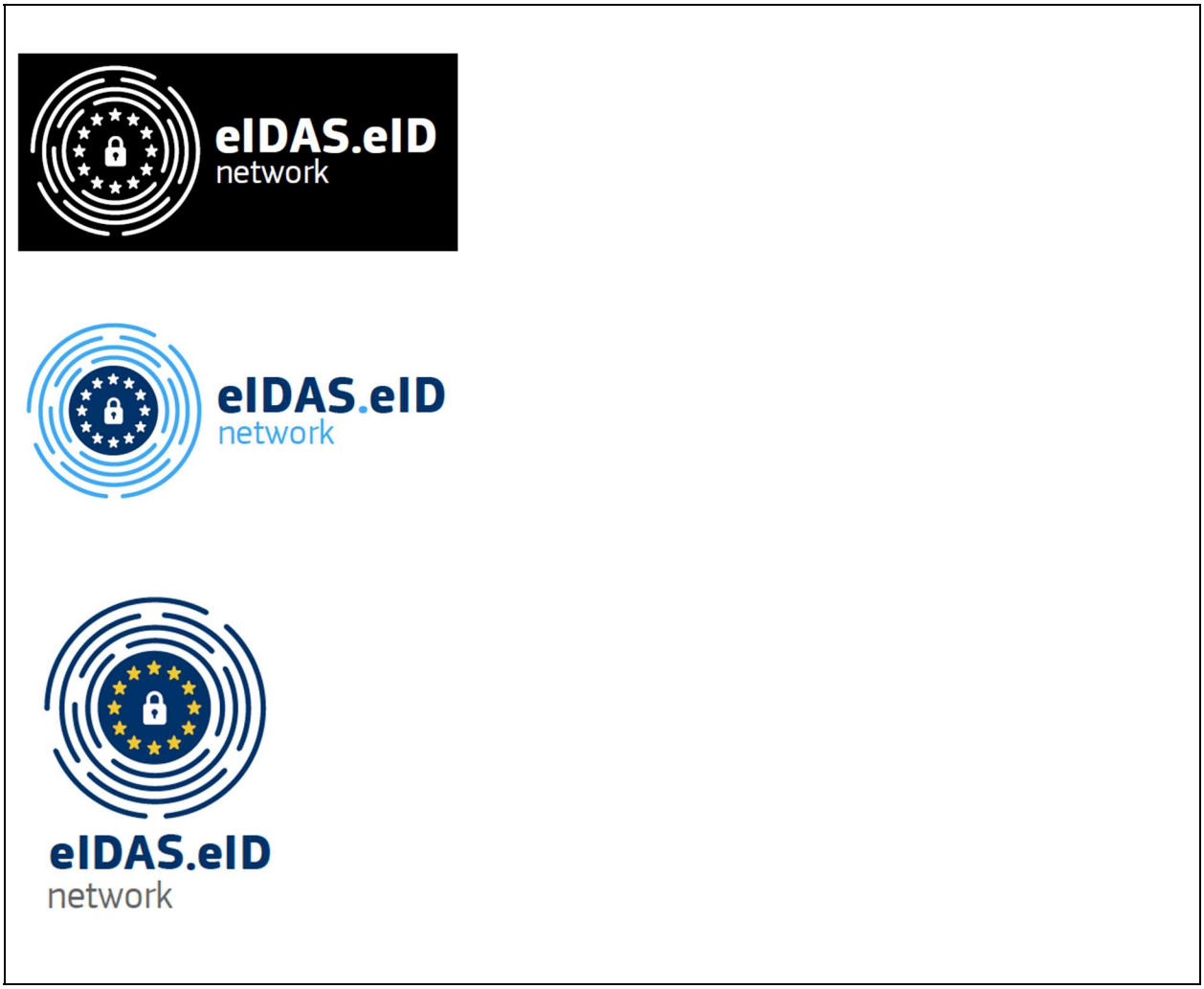
EU-Kommissionen har udarbejdet specifikke terminologiske og visuelle retningslinjer, der skal være med til at understøtte synligheden af eIDAS på tværs af tjenester og EU medlemslande.

En oversat version af retningslinjerne til brug af visuel repræsentation og terminologi på brugergrænseflade fremgår af følgende skema:

Anvend en beskrivende tekst, til at understøtte eIDAS log-in funktionen	Ved brug af det officielt godkendte logo til at repræsentere eIDAS log-in muligheden, skal der anvendes en understøttende tekst (f.eks. *"Sign in with a digital identity from another European country" eller "Foreign eID*"). Denne løsning vil også være til fordel for brugere med synsbesvær og vil være kompatibel med evt. maskine-oversættelse.
Anvend en terminologi der er forståelig	Generelt bør brugen af termer som "eIDAS" og "eID" undgås, hvis *ikke* der gives en tilstrækkelig og dækkende forklaring. Specielt når konteksten har at gøre med brugere (EU/EØS borgere), hvor et forudgående kendskab til termerne *ikke* kan antages at være kendt af brugeren på forhånd.
Referer konsekvent til "digital identitet" / "Foreign eID"	På tværs af EU/EØS medlemsstaterne og tjenesteudbydere bør der være en fælles konsensus om, hvordan der refereres til "digitale identiteter". For hvert sprog hvor en service er tilgængelig, bør der findes et passende og dækkende ord for disse termer.
Brug EU-logoet til visuelt at understøtte eIDAS log-in funktionen, hvis nødvendigt, men aldrig uden brug af beskrivende tekst	Hvis brug af et visuelt element ikke kan undværes, ved præsentation af eIDAS log-in mulighed, skal eIDAS-logoet anvendes. Logoet bør ikke anvendes uden brug af en understøttende tekst.

Filer til implementering af "eIDAS Network"-logo varierer i udtryk og findes yderligere i en vertikal og horisontal udgave i hhv. PNG eller JPG filformat. Materialepakken med filer til implementering af "eIDAS Network"-logo kan rekvireres via: eidas@digst.dk.

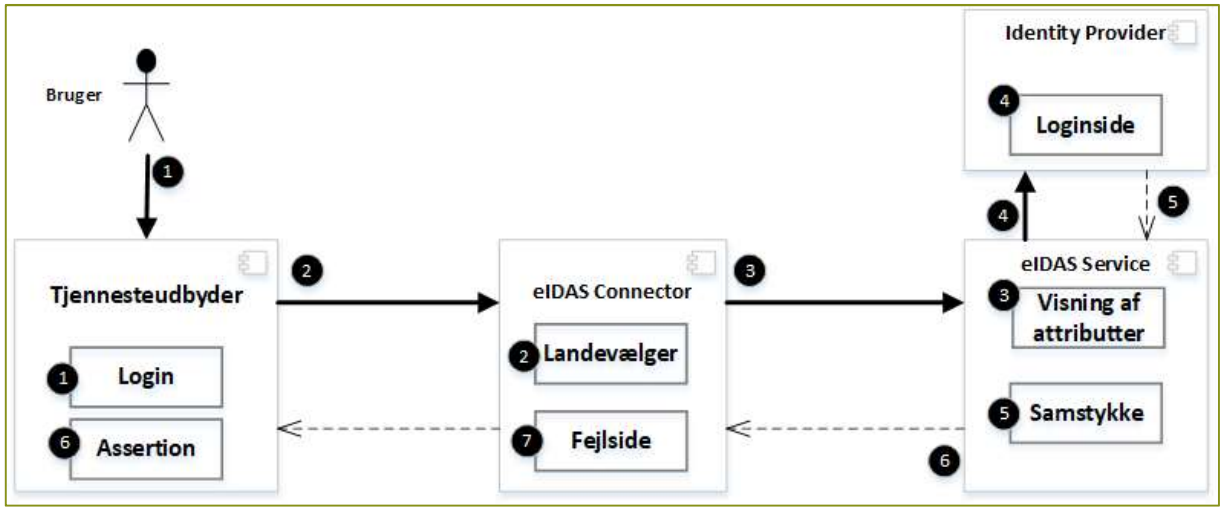
Et udpluk af logo-materialet fremgår nedenfor af Figur 9.



Figur 9 - EU eIDAS logo materiale-udpluk

4 Loginforløb i integrationstestmiljøet

Dette afsnit indeholder en beskrivelse af loginforløbet igennem integrationstestmiljøets komponenter, som illustreres i Figur 10 nedenfor:



Figur 10 - Loginforløb i eID-gateway integrationstestmiljøet

Loginforløbet beskrives med afsæt i en af de udstillede testtjenester, som findes beskrevet i afsnit 2.1:

1. Brugeren påbegynder et loginforløb med tryk på ”Login” knappen på tjenesteudbyder webside (trin 1).
2. Brugeren viderestilles til landevælgeren på DK eIDAS Connector (trin 2).
3. Brugeren vælger landet med ’EU’ flaget i landevælgeren og viderestilles til Referenceimplementeringens eIDAS proxy Service skærmbilledet, som viser hvilke obligatoriske og evt. valgfrie attributter (trin 3), som tjenesten forespørger om (trin 4).
4. Brugeren trykker på ”Next” knappen og viderestilles til demo Identity Provider loginside, hvor brugeren angiver en testbruger og password (trin 5).
5. Brugeren trykker på ”Submit” knappen og viderestilles til samtykkeskærmen på Referenceimplementeringens eIDAS proxy Service (trin 6).
6. Brugeren trykker på ”Submit” knappen. Der viderestilles til tjenesteudbyderens side for visning af attributter og assertion.
7. Hvis der opstår fejl under loginforløb, vil eIDAS Connector, afhængig af fejltype, enten sende brugeren til fejlsiden på eID-gatewayen, eller sende et SAML svar med ”styret” fejl tilbage til tjenesten (trin 7).

5 Tilslutningsproces til integrationstestmiljø

Nedenstående proces skal følges for at opnå adgang til testmiljøet:

1. Tjenesteudbyder udfylder metadata iht. krav beskrevet i afsnit 7 (Krav til tjenesteudbyder metadata).
2. Tjenesteudbyder udfylder Bilag I jf. vejledning. Tjenesteudbyder fremsender herefter Bilag I sammen med metadata til DIGST via e-mail: eidas@digst.dk.
3. DIGST indlæser metadata og bekræfter til tjenesteudbyder. Ved problemer med indlæsning af metadata vil tjenesteudbyder blive kontaktet af DIGST.
4. Tjenesteudbyder indlæser metadata for integrationstestmiljøets DK eIDAS Connector fra URL angivet i afsnit 2.2.
5. Tjenesteudbyder tilgår integrationstestmiljøet ud fra beskrivelsen i afsnit 2 og tester tilslutning, som beskrevet i afsnit 8 (obligatoriske testscenarier i afsnit 8.6).
6. Når de obligatoriske testscenarier er gennemført, anbefaler DIGST tjenesteudbyder at referere til de ikke-obligatoriske testcases og at eksekvere disse, jf. afsnit 8.7. Tjenesteudbyder opfordres herudover til at teste selvstændigt.
7. Tjenesteudbyder udarbejder en integrationstest testrapport og sender denne til eidas@digst.dk med en gennemgang af de gennemførte testscenarier, obligatoriske såvel som ikke-obligatoriske.

5.1 Særligt at bemærke vedr. sikringsniveau

Level of Assurance (LoA) - også kaldet sikringsniveau - angiver, hvilket krav den pågældende tjeneste stiller til EU/EØS IdP. For IdP'en bruges følgende LoA niveauer:

- Low
- Substantial
- High

Disse deklareres ikke i metadata. Tjenesteudbyder oplyser LoA-niveau til DIGST i formularen i Bilag I – Skabelon til fremsendelse af metadata (INTTEST) ved fremsendelse af metadatafiler ifbm. integration til integrationstestmiljøet.

Bemærk: Det er et lovkrav i eIDAS-forordningen, at de danske myndigheder skal anerkende EU/EØS eID'er, hvor LoA minimum er på samme niveau, som det nationalt anerkendte niveau (i Danmark) [4]. Da LoA for NemID er anmeldt på niveau 'Substantial', betyder dette, at en dansk myndighed altid skal stille et login-forløb til rådighed for de borgere, som har et eID med LoA 'Substantial' eller højere. Danske tjenester er derfor ikke påtvunget at anerkende eID'er, hvor LoA er på niveau 'Low'.

[4] Note: Når MitID er færdiganmeldt i 2022, vil disse forhold forventeligt kunne ændre sig. Derfor forventer vi, at dette afsnit vil blive revideret efter gennemført anmeldelse af MitID.

6 Tilslutningsproces til produktionsmiljø

Ved overgang til produktion skal nedenstående proces overholdes. Processen herefter forudsætter, at metadata er indlæst for den pågældende tjeneste i eID-gateway:

1. Når de obligatoriske testscenarier og ikke-obligatoriske testcases er gennemført i integrationstestmiljøet, jf. afsnit 5, og testrapporten er modtaget via e-mail: eidas@digst.dk, gennemgår DIGST testrapporten og vender tilbage herefter.
2. Tjenesteudbyder underskriver tilslutningsaftale med DIGST, når testrapporten er godkendt.
3. Tjenesteudbyder udarbejder metadata til produktion og signerer metadata med et FOCES produktionscertifikat.
4. DIGST indlæser metadata og bekræfter til tjenesteudbyder. Ved problemer med indlæsning af metadata vil tjenesteudbyder blive kontaktet af DIGST.
5. Tjenesteudbyder indlæser metadata for produktionsmiljøets DK eIDAS Connector fra URL angivet i afsnit 2.2.

Bemærk: DIGST anbefaler, at tjenesteudbyder gennemfører test i produktionsmiljøet, så vidt muligt for at tjenesteudbyder kan være på forkant med potentielle problematikker i produktionsmiljøet / eventuelle forskelle i forbindelsesflowet.

6.1 Revideringer af metadata som er konfigureret tidligere

Såfremt der på et senere tidspunkt ønskes konfigureret ny metadata i eID-gateway, er processen som udgangspunkt, at der først fremsendes ny metadata til INTTEST miljøet, hvorefter DIGST konfigurerer denne metadata i INTTEST miljøet.

Herefter udfærdiger og fremsender tjenesteudbyder en revideret testrapport (INTTEST).

Dette foretages for bedre tidligere at afdække og afklare eventuelle mangler i metadata og for samtidigt at sikre, at integrationen løbende testes af tjenesteudbyderen. Dette er igen for at undgå, at der først opdages mangler eller problematikker, når metadata er konfigureret i produktionsmiljøet (i værste fald når man er gået i drift/produktion)

Ved regulære ændringer som fx certifikatskift – hvor det er tydeligt, at der *kun* er tale om ændring af certifikater, kan metadata fremsendes for INTTEST, hvorefter der foretages et kvalitets-tjek af tjenesteudbyderen på tjenesten. Herefter kan metadata for PROD færdiggøres og fremsendes, hvorefter PROD metadata konfigureres af DIGST.

7 Krav til tjenesteudbyder metadata

Metadata leveres til DIGST i form af en XML fil. Dette er en forudsætning for at få tilsluttet en tjeneste i eID-gateway.

Metadata skal bl.a. oplyse om tjenestens identifikation, certifikater og kontaktpersoner. Metadata skal dertil indeholde specifikation af de attributter, som tjenesten ønsker medsendt fra brugerne.

Dette afsnit beskriver de regler, som nævnte metadata skal efterleve. Tjenesteudbydere skal sikre, at metadata lever op til disse regler, før en metadatafil sendes til DIGST.

Se afsnit 4 for krav til udfyldelse af skabelon ved fremsendelse af metadata.

7.1 ”SKAL/KAN”-valideringer:

Element/attribut	Beskrivelse
`q1:EntityDescriptor entityID="https://sp.myndighed.dk" xmlns:q1="urn:oasis:names:tc:SAML:2.0:metadata">`	Metadata SKAL deklarere en `EntityDescriptor` med et unikt `entityID`.
`q1:EntityDescriptor ID= ”id03db376464ca49a8a21929166d61c833” entityID="https://sp.myndighed.dk" xmlns:q1="urn:oasis:names:tc:SAML:2.0:metadata">`	`EntityDescriptor` KAN deklarere et `ID`.
`<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://sp.myndighed.dk" validUntil="2020-01-27T16:32:46.316Z">`	`EntityDescriptor` KAN deklarere `validUntil`.
`<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"> ... </Signature>`	Metadata KAN signeres. Hvis signeret, SKAL certifikatet angivet for ”signing” nedenfor være i stand til at verificere signaturen. Hvis signeret, SKAL sha256 anvendes som digest og signatur algoritmer.

`<q1:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" AuthnRequestsSigned="true" WantAssertionsSigned="true">`	Metadata SKAL deklarere en `SPSSODescriptor`. `SPSSODescriptor` SKAL deklarere `AuthnRequestsSigned="true"`. `SPSSODescriptor` SKAL deklarere `WantAssertionsSigned="true"`.

`<q1:KeyDescriptor use="signing">`
`  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">`
`  <X509Data>`
`  <X509Certificate>`
`  <!–Here goes certificate -->`
`  </X509Certificate>`
`  </X509Data>`
`  </KeyInfo>`
`</q1:KeyDescriptor>`
	Metadata SKAL deklarere en `KeyDescriptor` for et certifikat til signering.
	
	`X509Certificate` SKAL indeholde et base64 *encodet* certifikat.
	
	Certifikatet til signering SKAL være et validt VOCES- eller FOCES- certifikat.

`<q1:KeyDescriptor use="encryption">`
`  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">`
`  <X509Data>`
`  <X509Certificate>`
`  <!–Here goes certificate -->`
`  </X509Certificate>`
`  </X509Data>`
`  </KeyInfo>`
`</q1:KeyDescriptor>`
	Metadata SKAL deklarere en `KeyDescriptor` for et krypteringscertifikat.
	
	`X509Certificate` SKAL indeholde et base64 *encoded* certifikat.
	
	Krypteringscertifikatet SKAL være et validt VOCES eller FOCES certifikat.

`<q1:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://sp.myndighed.dk/logout" ResponseLocation="https://sp.myndighed.dk/logout" />`	Metadata KAN deklarere en `SingleLogoutService`. Single logout er **ikke** supporteret af eID og vil blive ignoreret af eID. `SingleLogoutService` er tilladt i metadata for bagudkompatibilitet for OIOSAML.Net/Java.

`<q1:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</q1:NameIDFormat>`	Metadata KAN have **en** `NameIDFormat` deklaration. Hvis deklareret SKAL `NameIDFormat` bruge "`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`". `NameIDFormat` ignoreres af eID. eID vælger automatisk "`persistent`" for tjenester. `NameIDFormat` er tilladt i metadata for bagudkompatibilitet for OIOSAML.Net/Java.
`<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sp.myndighed.dk/response" isDefault="true"/>`	Metadata SKAL deklarere en `AssertionConsumerService` med **POST** binding'en. Default location (`isDefault="true"`) SKAL angives i metadata for **POST** binding'en. Dette er også tilfældet, hvis der kun er angivet en "AssertionConsumerService".
`<q1:AttributeConsumingService index="0" isDefault="true">` `  <q1:ServiceName xml:lang="da">MyndighedSP </q1:ServiceName>`	Metadata KAN deklarere et `ServiceName` med visningsnavnet for tjeneste.

`<q1:AttributeConsumingService index="0" isDefault="true">`
`<q1:RequestedAttribute FriendlyName="PersonIdentifier" Name="urn:oid:1.2.752.201.3.7" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>`
`  <q1:RequestedAttribute FriendlyName="FamilyName" Name="urn:oid:2.5.4.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>`
	Metadata SKAL deklarere en `RequestedAttribute` for hver af attributterne, som DKSP forespørger og ønsker at modtage.
	
	eID definerer fire datasæt:
	• Et datasæt med attributter for "natural person"
	• Et datasæt med attributter for "natural person representative"
	• Et datasæt med attributter for "legal person"
	• Et datasæt med attributter for "legal person representative".
	
	Metadata SKAL deklarere attributter for enten "natural person" eller "legal person" eller begge datasæt.

	Metadata KAN deklarere attributter for ”natural person representative”. Metadata KAN deklarere attributter for ”legal person representative”. Metadata SKAL deklarere alle obligatoriske attributter inden for valgte datasæt. F.eks. hvis der deklareres attributter for ”natural person”, så skal alle obligatoriske ”natural person” attributter deklareres. Metadata KAN deklarere valgfrie attributter for et datasæt. Attributter SKAL være deklareret med korrekt `Name`. Attributter SKAL deklareres med korrekt `NameFormat`. Obligatoriske attributter SKAL deklareres med `isRequired="true"`. Valgfrie attributter MÅ IKKE deklareres med `isRequired="true"`.

`<md:Organization>`
`  <md:OrganizationName xml:lang="en">Myndighed name</md:OrganizationName>`
`  <md:OrganizationDisplayName xml:lang="en">Myndighed name</md:OrganizationDisplayName>`
`  <md:OrganizationURL xml:lang="en">https://www.nnit.com</md:OrganizationURL>`
`  </md:Organization>`
	Metadata KAN deklarere en `Organization`.
	
	Hvis deklareret SKAL `Organization` indeholde:
	
	`OrganizationName,`
	`OrganizationDisplayName,`
	`OrganizationURL.`

`<q1:ContactPerson contactType="administrative">`
`  <q1:Company>Myndighed name</q1:Company>`
`  <q1:GivenName>Administrator first name</q1:GivenName>`
`  <q1:SurName>Administrator lastname</q1:SurName>`
	Metadata SKAL deklarere en `ContactPerson` med `contactType=”administrative”`.
	
	`ContactPerson` SKAL indeholde:
	
	`Company,`
	`GivenName,`
	`SurName,`

<q1:EmailAddress>email@domain</q1:EmailAddress> <q1:TelephoneNumber>+00 0000000</q1:TelephoneNumber> </q1:ContactPerson>	EmailAddress, TelephoneNumber.
<md:ContactPerson contactType=”technical”> <md:Company>Technician company</md:Company> <md:GivenName>Technician first name</md:GivenName> <md:SurName>Technician last name</md:SurName> <md:EmailAddress>email@domain</md:EmailAddress> <md:TelephoneNumber>+00 0000000</md:TelephoneNumber> </md:ContactPerson>	Metadata KAN deklarere en ContactPerson med contactType=”technical”. Hvis deklareret SKAL ContactPerson indeholde: Company, GivenName, SurName, EmailAddress, TelephoneNumber
<md:ContactPerson contactType=”support”> <md:Company>Support company</md:Company> <md:GivenName>Supporter first name</md:GivenName> <md:SurName>Supporter last name</md:SurName> <md:EmailAddress>email@domain</md:EmailAddress> <md:TelephoneNumber>+00 0000000</md:TelephoneNumber> </md:ContactPerson>	Metadata KAN deklarere en ContactPerson med contactType=”support”. Hvis deklareret, SKAL ContactPerson indeholde: Company, GivenName, SurName, EmailAddress, TelephoneNumber

7.2 ”MÅ IKKE”-valideringer

Element/attribut	Beskrivelse
<q1:Extensions>	Metadata MÅ IKKE deklarere Extensions.

7.3 Attributter

eID-gateway Snitfladespecifikation [1] beskriver de tilgængelige attributter, som tjenester kan forespørge i metadata. Disse tilgængelige attributter kan samtidig også findes i Bilag A – Tjenesteudbyder metadata eksempel.

7.3.1 Særlige forhold i deklarering af attributter

Tjenesteudbyder skal være opmærksomme på, at der er en direkte sammenhæng mellem de deklarerede attributter i metadata og mulighederne i eID-gateway for at honorere login.

For deklarerede "natural person" og "legal person" attributter i metadata gælder:

- I henhold til eIDAS skal ønskede "natural person" og "legal person" attributter inkluderes i forespørgsler til eIDAS Services.
- En eIDAS Service må kun returnere succesfuldt svar, såfremt at denne, som minimum kan honorere de obligatoriske attributter med værdier.

Vær opmærksom på, at DK eIDAS Connector forespørger eIDAS Services med alle "natural person" og/eller "legal person" attributter, som findes deklareret i tjenesteudbyder metadata;

- Hvis tjenesteudbyder deklarerer attributter for både "natural person" og "legal person", må det anses som overvejende sandsynligt, at mange logins ikke vil kunne gennemføres.

For "representative" attributter vil det på sigt gælde[5]:

- I henhold til eIDAS må "representative" attributter ikke inkluderes i forespørgsler til eIDAS Services.
- En EU/EØS eIDAS Service kan returnere "representative" attributter i svar, såfremt en bruger er givet fuldmagt og repræsenterer en anden person.

Vær opmærksom på, at DK eIDAS Connector i disse tilfælde kun returnerer svar til tjenesten, såfremt denne har deklareret tilsvarende "representative" attributter i metadata.

For danske tjenester der understøtter begge attribut-profiler, kan derfor vælges at opdele metadata i hhv. en natural person og en legal person.

7.3.2 Særlige forhold vedr. CPR-nummer

Det vil fremover være muligt for tjenester at forespørge på registrerede CPR-numre som er koblet til et EU/EØS eID. Sikringsniveauet er altid angivet til niveauet 'Substantial'.

[5] Note: DIGST gør opmærksom på, at eIDAS på nuværende tidspunkt ikke understøtter login med fuldmagt.

Tjenesteudbydere som har behov for CPR-nummer skal i metadata deklarere sikringsniveauet 'Substantial'.

Alle offentlige myndigheder som fastlagt i dansk lovgivning har hjemmel til anvendelse af CPR-numre til identifikation af borgere og til journalnummer, jf. CPR-Loven §52 og §53.

Det er således et krav, at videregivelse af CPR-numre fremgår af lov eller af bestemmelser fastsat i henhold til lov. Er dette ikke tilfældet, kan Digitaliseringsstyrelsen ikke lovligt videregive denne personoplysning.

7.4 Eksempel på tjenesteudbyder metadata

Eksempel på tjenesteudbyder metadatafil for tilslutning til integrationstestmiljøet kan ses i kassen herunder. Eksemplet repræsenterer en standard opsætning for en tjenesteudbyder, som kun har behov for de obligatoriske oplysninger + CPR-nummeret.

I Bilag A – Tjenesteudbyder metadataeksempel findes der flere metadata eksempler.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     entityID="INDSÆT UNIKT ENTITYID">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate> INDSÆT X509 CERTIFIKAT TIL SIGNERING </X509Certificate>
</X509Data>
</KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate> INDSÆT X509 CERTIFIKAT TIL KRYPTERING </X509Certificate>
</X509Data>
</KeyInfo>
<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
```

```
</md:KeyDescriptor>

<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</md:NameIDFormat>

    <md:AssertionConsumerService Location="INDSÆT URL"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true"
index="0"/>


          <md:AttributeConsumingService isDefault="true" index="0">

      <md:ServiceName xml:lang="da">SP</md:ServiceName>

      <md:RequestedAttribute
Name="dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier"

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"
/>

      <md:RequestedAttribute
Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"
/>

      <md:RequestedAttribute
Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"
/>

      <md:RequestedAttribute
Name="dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"
/>

    </md:AttributeConsumingService>

</md:SPSSODescriptor>

<md:Organization>

<md:OrganizationName xml:lang="en">INDSÆT TJENESTEUDBYDER
NAVN</md:OrganizationName>

<md:OrganizationDisplayName xml:lang="en">INDSÆT
TJENESTEUDBYDERNAVN</md:OrganizationDisplayName>

    <md:OrganizationURL xml:lang="en">INDSÆT ORGANISATIONS
HJEMMESIDE</md:OrganizationURL>

</md:Organization>

  <md:ContactPerson contactType="administrative">

    <md:Company>INDSÆT FIRMANAVN</md:Company>

    <md:GivenName>INDSÆT FORNAVN PÅ KONTAKTPERSON</md:GivenName>

    <md:SurName> INDSÆT EFTERNAVN PÅ KONTAKTPERSON </md:SurName>
```

```
    <md:EmailAddress>INDSÆT EMAIL ADRESSE</md:EmailAddress>
    <md:TelephoneNumber>INDSÆT TELEFONNUMMER</md:TelephoneNumber>
  </md:ContactPerson>
  <md:ContactPerson contactType="other">
  <md:ContactPerson contactType="administrative">
    <md:Company>INDSÆT FIRMANAVN</md:Company>
    <md:GivenName>INDSÆT FORNAVN PÅ KONTAKTPERSON</md:GivenName>
    <md:SurName> INDSÆT EFTERNAVN PÅ KONTAKTPERSON </md:SurName>
    <md:EmailAddress>INDSÆT EMAIL ADRESSE</md:EmailAddress>
    <md:TelephoneNumber>INDSÆT TELEFONNUMMER</md:TelephoneNumber>
  </md:ContactPerson>
</md:EntityDescriptor>
```

7.5 Metadata-valideringsværktøj

Der stilles et valideringsværktøj til rådighed for tjenesteudbydere (og leverandører). Værktøjet anvendes ved hjælp af en browser, hvor det følgende URL åbnes op:

URL: https://metadata.eid.digst.dk/

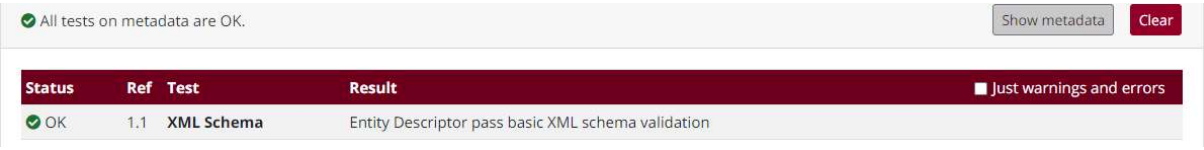
Valideringsværktøjet kan anvende som et yderligere input og støtte til udarbejdelse af metadata samt til sikring af at metadata er struktureret som nødvendigt forud for fremsendelse til Digitaliseringsstyrelsen. Værktøjet kan anvendes både til validering af metadata til integrationstestmiljøet såvel som til metadata til produktionsmiljøet.

Vigtige bemærkninger om metadata-valideringsværktøjet:

- Der kan i værktøjet forekomme falske negativer (dvs. fejl *kan* vises, selvom metadata vil virke ved opsætning i integrationstestmiljøet).
- Der kan i værktøjet forekomme falske positiver (hvor fejl *ikke* vises, dvs. der kan forekomme fejl, som først opdages ved upload/validering af konfiguration).

Værktøjet er tænkt som et yderligere input/en støtte til arbejdet med strukturering af metadata ved tjenesteudbyder/tjenesteudbyder leverandør men er fortsat udvikling og tilpasning. Værktøjet kan derfor kun ses som et supplement til tjenesteudbyders arbejde.

Figur 11 - Validering i metadata-valideringsværktøjet i browser. viser et eksempel på en de mulige valideringer i metadata-valideringsværktøjet.



Figur 11 - Validering i metadata-valideringsværktøjet i browser.

8 Integrationstest

Afsnittet beskriver den obligatoriske integrationstest, der skal udføres i integrationstestmiljøet (INTTEST), før tjenesteudbyderens tjeneste kan kobles på eID-gateway produktionsmiljø. Nedenfor findes en række obligatoriske testscenarier.

Endvidere beskrives en række ikke-obligatoriske testcases, som DIGST anbefaler tjenesteudbyderen at udføre, når de obligatoriske testscenarier er gennemført. Disse testcases kan udføres i det omfang, som det skønnes relevant.

Herefter udarbejder tjenesteudbyderen en overordnet testrapport, som fremsendes til DIGST via e-mail: eidas@digst.dk. Ved spørgsmål til integrationstesten så kontakt gerne DIGST i god tid, da det kan tage tid at få alle nødvendige afklaringer og tilpasninger gennemført.

Herudover indeholder nærværende afsnit nu informationer om, hvad der er uden for rammerne af integrationstesten, teststrategi, forudsætninger, detaljer om testmiljøer, testdata til eksekvering af testcases, samt de førnævnte nye (ikke-obligatoriske) testcases[6].

8.1 Aktiviteter ud over integrationstesten

Integrationstesten er et af de sidste trin i tilslutningsprocessen. Før en tjeneste kan gå i produktion (drift), kan der derudover være en række andre testaktiviteter, som fx test af applikationsspecifik funktionalitet og evt. integration med offentlige portaler. Disse aktiviteter ligger uden for rammerne af dette dokument. En succesfuld integrationstest er med andre ord en nødvendig, men ikke en tilstrækkelig betingelse for at gå i drift.

8.2 Teststrategi

Formålet med integrationstesten er som tidligere nævnt at verificere, at integrationen mod eID-gateway løsningen er udført funktionelt og teknisk korrekt.

Der er således en række ikke-funktionelle aspekter, som en tjenesteudbyder selv må teste og vurdere selvstændigt i forhold til den ønskede servicekvalitet som f.eks.:

- Tilgængelighed
- Svartider
- Kapacitet
- Skalérbarhed
- Sikkerhed

[6] Note: Tilføjelser er fra "Integrationstest ved tilslutning til NemLog-in", jf. reference [5].

- Brugervenlighed (herunder sprog og understøttelse af browsere)

Det skal imidlertid kraftigt understreges, at tjenesteudbyderen selv har ansvaret for sikkerheden af de systemer, der tilsluttes eID-gateway!

Tjenesteudbyder vil derfor selv skulle sørge for at sikkerhedsteste systemer og infrastruktur udover, hvad der er beskrevet i dette dokument[7].

En anden vigtig afgrænsning for den her beskrevne integrationstest er, at det alene er samspillet med eID-gateway, der beskrives.

Test af applikationsspecifik funktionalitet og test af integrationsformer mod portaler, behandles derfor ikke i materialet og foretages af den enkelte tjenesteudbyder. Der henvises til vilkårene for tilslutning af tjenester til eID-gateway på digitalisér.dk, hvortil der beskrives rammer for beredskabspolitik, logningspolitik, certifikatpolitik mv.

Læs vilkårene for tilslutning af tjeneste til eID-gateway på digitalisér.dk.

8.3 Miljøer

- INTTEST: Integrationstestmiljøet. Dette miljø vil for tjenesteudbyderen ofte være det, som svarer til PREPROD. Det er her, hvor tjenesteudbyderen vil udvikle og teste, og hvor følgende findes:
  - EU Referenceimplementeringen af en eIDAS proxy Service (EU flaget)
  - eIDAS demo Identity Provider (også refereret til som 'demo IdP').
- PROD: Produktionsmiljøet. Dette miljø, er det miljø, som EU/EØS borgere vil tilgå.

8.4 Generelle forudsætninger hos tjenesteudbyder

I de følgende beskrivelser forudsættes, at tjenesteudbyderen har etableret et miljø til integrationstest. Dette indebærer bl.a., at tjenesteudbyderen har foretaget følgende:

- Etableret infrastruktur og forbindelser (firewalls etc.)
- Oprettet IT-systemer
- Tilsluttet IT-systemer foranlediget af andre nødvendige integrationer
- Udvekslet INTTEST metadata med Digitaliseringsstyrelsen (metadata sendes via e-mail: eidas@digst.dk)
- Konfigureret tidsservice, logning etc.

[7] Note: Dette kan eksempelvis være forskellige former for penetrationstest.

8.5 Forudsætninger for afvikling af testscenarierne

Tjenesteudbyderens metadata er oprettet på integrationstestmiljøet med metadata for en eller begge af de nedestående personer:

#	Meta-dataset for	Attributspecifikation i metadatafil
1a	**Natural Person**	<!-- Natural person dataset attributes --> <q1:RequestedAttribute FriendlyName="PersonIdentifier" Name="dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="FamilyName" Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="FirstName" Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="DateOfBirth" Name="dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="BirthName" Name="dk:gov:saml:attribute:eidas:naturalperson:BirthName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="PlaceOfBirth" Name="dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="CurrentAddress" Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="Gender" Name="dk:gov:saml:attribute:eidas:naturalperson:Gender" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="CprNummer" Name="dk:gov:saml:attribute:CprNumberIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="CprNummerContext" Name="dk:gov:saml:attribute:CprNumberIdentifier:context" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <q1:AttributeValue q1:type="xs:string"> https://data.gov.dk/attributes/coupling/loa/Substantial </q1:AttributeValue> </q1:RequestedAttribute>
1b	**Legal Person**	<!-- Legal person dataset attributes -->

		<q1:RequestedAttribute FriendlyName="LegalPersonIdentifier" Name="dk:gov:saml:attribute:eidas:legalperson:LegalPersonIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="LegalName" Name="dk:gov:saml:attribute:eidas:legalperson:LegalName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/> <q1:RequestedAttribute FriendlyName="LegalAddress" Name="dk:gov:saml:attribute:eidas:legalperson:LegalPersonAddress" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="VATRegistration" Name="dk:gov:saml:attribute:eidas:legalperson:VATRegistrationNumber" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="TaxReference" Name="dk:gov:saml:attribute:eidas:legalperson:TaxReference" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="D-2012-17-EUIdentifier" Name="dk:gov:saml:attribute:eidas:legalperson:D-2012-17-EUIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="LEI" Name="dk:gov:saml:attribute:eidas:legalperson:LEI" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="EORI" Name="dk:gov:saml:attribute:eidas:legalperson:EORI" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="SEED" Name="dk:gov:saml:attribute:eidas:legalperson:SEED" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/> <q1:RequestedAttribute FriendlyName="SIC" Name="dk:gov:saml:attribute:eidas:legalperson:SIC" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>

8.6 Testscenarierne – et overblik

I nedenstående Tabel 1 findes et overordnet overblik over de testscenarier, som indgår i integrationstesten. Selve testscenarierne findes i Bilag E – Obligatoriske testscenarier, inklusiv de handlinger, som testscenarierne består af, samt hvad det forventede resultat vil være af eksekvering af hvert testscenarie.

Tjenesteudbyderen kan vælge at lave sine egne testscenarier som et supplement hertil. De følgende testscenarier Tabel 1 forventes gennemgået i testrapporten.

Herudover anbefales tjenesteudbyderen at referere til og lade sig inspirere af de ikke-obligatoriske testcases, som nævnes i kommende afsnit og generelt teste selvstændigt.

Tabel 1 - Oversigt over testscenarierne (obligatoriske)

Testscenarie ID	Overskrift	Formål
IT-EIDG-TS01-POSITIV	Positiv testscenarie (Succesfuld login)	Formålet med testen er at verificerer et succesfuldt loginforløb.
IT-EIDG-TS02-NEGATIV	Negativ testscenarie (Invalide brugeroplysninger)	Formålet med testen er at verificerer et loginforløb som fejler.
IT-EIDG-TS03-BYPASSING	Sessionssikkerhed testscenarie 1	Test af 'Bypassing Session Management Schema'
IT-EIDG-TS04-EXPOSED	Sessionssikkerhed testscenarie 2	Test af 'Exposed Session Variables'

Formålet med at inkludere de sidste to testscenarier[8] er at komme med konkrete forslag til, hvordan tjenesteudbyder kan sikre sig, at den grundlæggende sikkerhed er på plads før en endelig tilslutning i integrationstestmiljøet (og efterfølgende produktionslægning).

Der henvises i denne forbindelse til OWASP Testing Guide, jf. reference [7], for detaljer omhandlende, hvordan de enkelte testcases udføres.

8.7 Ikke-obligatoriske testcases – overblik

Tabel 2 gives et overblik over en række mere granulerede ikke-obligatoriske testcases, der kan indgå i testen udover de obligatoriske testscenarier i integrationstesten. Testcases findes i Bilag F – Ikke-obligatoriske testcases. Bilaget beskriver mere udførligt disse testcases.

For hver testcase opstilles startbetingelser, der skal være opfyldte, inden testen kan påbegyndes og udføres. Herudover gennemgås: Hvilke trin en bruger/administrator skal udføre samt hvilke slutbetingelser, der forventes at gælde efter testcasen er gennemført. Som en fælles startbetingelse for alle de inkluderede testcases gælder, at de i forrige kapitel beskrevne testdata er oprettet.

De udvalgte ikke-obligatoriske testcases giver *ikke* en fuldstændig gennemtestning af al funktionalitet, fejlsituationer og kombinationer, da dette ville blive særdeles omfattende. I stedet er tilstræbt en hensigtsmæssig balance mellem omfang af test kontra graden af sikkerhed for, at integrationen mellem tjenesteudbyder og eID-gateway fungerer korrekt.

[8] Note: Tanken bag disse to testscenarier er at få gennemført som minimum en basal test af sikkerheden i tjenesteudbyderens løsning (ikke at følge dem dogmatisk, hvis det ikke giver mening for den løsning der skal testes).

Som udgangspunkt er disse testcases tiltænkt web-applikationer og ikke fx 'native apps'. For apps må beskrivelsen af testcases fortolkes mere 'frit', så testcase vil give mening i en 'native app' kontekst. Tjenesteudbyderen opfordres derfor til at tilpasse testcases.

Bemærk at slutbetingelser i nogle testcases kan være startbetingelser i andre testcases. Dette betyder, at en hensigtsmæssigt valgt rækkefølge kan reducere testarbejdet. Ud fra dette anbefales pt at udføre de ikke-obligatoriske testcases i den følgende rækkefølge:

- IT-EIDG-TC01-LOGN-01
- IT-EIDG-TC02-SPSN-01
- IT-EIDG-TC03-LOGG-01
- IT-EIDG-TC04-LOA-01
- IT-EIDG-TC05-LOA-02
- IT-EIDG-TC06-LOA-03

Tabel 2 - Oversigt over ikke-obligatoriske testcases

Testscenarie ID	Testcase beskrivelse
IT-EIDG-TC01-LOGN-01	Brugeren tilgår en beskyttet webside hos tjenesteudbyder uden forudgående session. Der re-directes efter "Landevælger"-siden til eIDAS demo IdP, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen.
IT-EIDG-TC02-SPSN-01	Brugeren tilgår en beskyttet side hos tjenesteudbyder og har allerede en session med denne. Brugeren får adgang til siden uden at blive sendt til eIDAS demo IdP.
IT-EIDG-TC03-LOGG-01	Tester udvalgte aspekter af eID-gateway logningspolitik hos tjenesteudbyder (SP).
IT-EIDG-TC04-LOA-01	Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'Substantial'). Brugeren er autentificeret med LoA niveau 'Low'. Adgang afvises hos tjenesten.
IT-EIDG-TC05-LOA-02	Brugeren tilgår en beskyttet ressource hos tjenesteudbydere (som kræver LoA niveau 'Substantial'). Brugeren er autentificeret med LoA niveau 'Substantial' og adgang tillades hos tjenesten.
IT-EIDG-TC06-LOA-03	Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'Low'). Brugeren er autentificeret med LoA niveau 'Substantial' og adgang tillades hos tjenesten.

Følgende testcases er et udkast til hvordan det foreløbigt forventes i grove træk, at man vil kunne teste LoA = 'High', når det på et senere tidspunkt bliver aktuelt at gøre dette.

IT-EIDG-TC07-LOA-04	Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'High'). Brugeren er autentificeret med LoA niveau 'High'. Adgangen tillades hos tjenesten.
IT-EIDG-TC08-LOA-06	Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'High'). Brugeren er autentificeret med LoA niveau 'Substantial'. Adgang afvises hos tjenesten.

8.8 Generelle testdata - testbrugere

Dette afsnit beskriver et eksempel på en testbruger 'testSP', som stilles til rådighed for danske tjenesteudbydere i integrationstestmiljøet. Brugeren er en generisk defineret testbruger, der skal benyttes af tjenesteudbyder til de obligatoriske testscenarier i afsnit 8.6 samt til alle ikke-obligatoriske testcases i afsnit 8.7.

Testbrugeren har attributværdier som beskrevet nedenfor.

Testbruger beskrivelse	Brugernavn & password	Testbrugerens attributværdier		
Natural Person med alle obligatoriske og valgfri attributter	***Brugernavn:*** testSP ***Password:*** Test1234	dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier	PersonIdentifier	CA/DK/1289321
		dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName	FamilyName	Toretto
		dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName	FirstName	Birgitte
		dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth	DateOfBirth	22-12-1980
		dk:gov:saml:attribute:eidas:naturalperson:BirthName	BirthName	Birgitte Anna Toretto
		dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth	PlaceOfBirth	Athens
		dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress	CurrentAddress	LocatorDesignator=33;Thoroughfare=Guild%20Street;PostName=London;PostCode=EC3R%201WJ
		dk:gov:saml:attribute:eidas:naturalperson:Gender	Gender	Female

Testbruger beskrivelse	Brugernavn & password	Testbrugerens attributværdier		
Legal Person med alle obligatoriske og valgfri attributter	***Brugernavn:*** testSP [9]	dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier	PersonIdentifier	
		dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName	FamilyName	

[9] Note: Bemærk at testbrugeren 'testSP' har "Legal attribute" værdier tilknyttet, som dog ikke kan modtages i eID-gateway og derfor vil værdier heller ikke blive vist pt.

Testbruger beskrivelse	Brugernavn & password	Testbrugerens attributværdier		
	Password: Test1234	dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName	FirstName	
		dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth	DateOfBirth	
		dk:gov:saml:attribute:eidas:naturalperson:BirthName	BirthName	
		dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth	PlaceOfBirth	
		dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress	CurrentAddress	
		dk:gov:saml:attribute:eidas:naturalperson:Gender	Gender	
		dk:gov:saml:attribute:eidas:legalperson:LegalPersonIdentifier	LegalPersonIdentifier	
		dk:gov:saml:attribute:eidas:legalperson:LegalName	LegalName	
		dk:gov:saml:attribute:eidas:legalperson:LegalPersonAddress	LegalAddress	
		dk:gov:saml:attribute:eidas:legalperson:VATRegistrationNumber	VATRegistration	
		dk:gov:saml:attribute:eidas:legalperson:TaxReference	TaxReference	
		dk:gov:saml:attribute:eidas:legalperson:D-2012-17-EUIdentifier	D-2012-17-EUIdentifier	
		dk:gov:saml:attribute:eidas:legalperson:LEI	LEI	
		dk:gov:saml:attribute:eidas:legalperson:EORI	EORI	
		dk:gov:saml:attribute:eidas:legalperson:SEED	SEED	
		dk:gov:saml:attribute:eidas:legalperson:SIC	SIC	

Det er muligt at anvende andre testebrugere i integrationstestmiljøet, jf. Bilag B, og derfor vil det forventede resultatet af testen afhænge af, hvilken testbruger og dermed hvilket sæt attributter tjenesteudbyderen vælger at anvende og forespørge på.

Ved anvendelse af andre end ovennævnte testbruger til testen, vil testen have en række begrænsninger på grund af kendte fejl i EU referenceimplementeringen. De kendte fejl er dokumenteret jf. **Bilag C – Kendte fejl i EU referenceimplementeringen**. Herudover kendes der til fejl med andre testbrugere. Der henvises til **Bilag D – Kendte fejl ved testbrugere** for en liste over testbrugere, som pt. ikke forventes anvendelige.

8.9 Testdata til de ikke-obligatoriske testcases

Om de følgende tjenesteudbydersider *SP-beskyttet-side-A, SP-beskyttet-side-B, SP-beskyttet-side-C* gælder der for disse tre testdata, at de hver især antages at inkludere:

- Et link eller en knap til at initiere single log-on (SSO) til tjenesteudbyderens service (gælder for offentlige tjenesteudbydere).

SP-åben-side-1
Dette er en statisk HTML side, hvorpå der ikke er sat adgangsbegrænsninger.
- Siden anvende til at sammenligne med følgende sider, hvor der *er* begrænsning.

SP-beskyttet-side-A
Dette er en statisk HTML side, hvor det krævede LoA sikringsniveau er sat til 'Substantial'.
- Denne side anvendes til at teste, at forsøg på adgang med samme opnået sikringsniveau (her 'Substantial') accepteres. Herudover kan siden anvendes til at teste, at forsøg på adgang med et lavere LoA ('Low') *ikke* accepteres.

SP-beskyttet-side-B
Dette er en statisk HTML side, hvor det krævede LoA sikringsniveau er sat til 'Low'.
- Denne side anvendes til at teste, at forsøg på adgang med for højere opnået sikringsniveau (her 'Substantial') accepteres. Herudover kan siden anvendes til at teste, at forsøg på adgang med et lavere LoA ('Low') accepteres.

SP-beskyttet-side-C
Dette er en statisk HTML side, hvor det krævede LoA sikringsniveau er sat til 'High'.
- Denne side anvendes til at teste, at forsøg på adgang med samme opnået sikringsniveau (her 'High') accepteres. Herudover kan siden anvendes til at teste, at forsøg på adgang med et lavere LoA ('Substantial', 'Low') *ikke* accepteres.

IdP-testbruger-1
En testbruger der har en række attributter, som tjenesteudbyder kan finde jf. afsnit 8.8. Den definerede testbruger er her 'testSP'. Brugerens identitet udveksles mellem eIDAS demo IdP og tjenesteudbyder (SP) via attributterne i den udstedte SAML Assertion.

IdP-testbruger-2
Dette er en anden testbruger, som har en række andre attributter, som tjenesteudbyder selv kan vælge, jf. Bilag B. Brugerens identitet udveksles mellem eIDAS demo IdP og tjenesteudbyder (SP) via attributterne i den udstedte SAML Assertion.

9 Referencer

[1]	National eID-gateway Snitfladespecifikation for tjenester: https://www.digitaliser.dk/resource/3909626
[2]	OASIS SAML Core v2 standard: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[3]	OIOSAML profile 2.0.9: https://www.digitaliser.dk/resource/2377872
[4]	eIDAS Interoperability architecture v1.00: https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf
[5]	Integrationstest ved tilslutning til NemLog-in version 3.0.1: https://www.nemlog-in.dk/media/qb5dpmrv/integrationstest-v3-0-1-oiosaml-3.pdf
[6]	National eID-gateway politikker for tilslutning til eID-gateway for tjenesteudbydere: https://www.digitaliser.dk/resource/4210242
[7]	OWASP Testing Guide: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

10 Ændringslog

Date	Version	Beskrivelse af ændring	Initialer
2018-02-28	0.1	Oprettet	LEAO
2018-03-16	0.2	Opdatering efter DIGST review og andre rettelser	LEAO, SLTK, MWL
2018-04-18	1	Bilag D med konfiguration af OIOSAML.net tilføjet efter aftalen med DIGST DIGST mailadresse opdateret til eidas@digst.dk	SLTK, MWL
2018-06-22	1.2	Tilføjelse af testcases under punkt 6	KES
2018-17-10	1.2.3	Afsnit om tests gjort skarpere	THOKM
2019-02-12	1.3	Opdatering af testbrugere, afsnit om CPR-attribut & Opdatering af tilslutningsproces	THOKM, JUBJJ
2020-02-10	1.3.3	Brug af SHA1 er erstattet af SHA256	IDAWI
2021-29-01	1.4	Test af autentifikation er opdateret med ny LoA Bilag F er opdateret ift. stillingtagen til nødvendige attributter Enkelte figurer er opdateret så de afspejler vores test IdP	IDAWI
2022-03-23	1.5	Større sæt ændringer herunder et nyt afsnit om: integrationstest (testcases, forudsætninger, afgrænsninger, ny oversigt over testbrugere), liste over testbrugere med kendte fejl, metadataeksempel erstattet, metadata validatorværktøj, samt generelle rettelser og korrektioner.	JACVEE, IDAWI, THOKM

11 Bilag A – Tjenesteudbyder metadataeksempel

Dette bilag indeholder en metadatafil med alle potentielle attributter angivet. Eksemplet indeholder en vejledning til felter, som skal erstattes med tjenesteudbyders egne værdier, samt forespørgsel (”request”) på alle attributter for en ”natural person”, en ”legal person” og en ”representative” for begge disse (”natural person”, ”legal person”).

Tjenesteudbyder skal tilrette dette til kun at forespørge på de nødvendige attributter.

Eksemplet i afsnit 7.4 repræsenterer en standard opsætning for en tjenesteudbyder, som kun har behov for de obligatoriske oplysninger + CPR-nummer.

Tjenesteudbydere skal desuden være opmærksom på, at de i afsnit 7 beskrevne krav til metadata bliver overholdt i den (af tjenesteudbyderen) tilrettede metadatafil.

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Replace with your own ID, entityID and validUntil (ID and validUntil may be
omitted) -->
<q1:EntityDescriptor ID="_2a1341c9-ba37-4e6a-a3b0-47167ddf212b"
entityID="https://sp.myndighed.dk" validUntil="2020-02-26T15:24:59.0696275Z"
xmlns:q1="urn:oasis:names:tc:SAML:2.0:metadata">
  <!-- Signature may be omitted -->
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
      <Reference URI="#id3c22e5debc5d497bbe90e0c81086eb81">
        <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>s8w+HK/...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      SE7NZn5kfnJW...
    </SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>
          <!-- Replace with your metadata signing certificate (metadata must be
signed with the signing certificate declared below) -->
```

```
          MIIGGzCCBQO...
        </X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>

  <q1:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
AuthnRequestsSigned="true" WantAssertionsSigned="true">
    <q1:KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>
           <!-- Replace with your signing certificate -->
           MIIGGzCCBQO...
          </X509Certificate>
       </X509Data>
     </KeyInfo>
  </q1:KeyDescriptor>
  <q1:KeyDescriptor use="encryption">
     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
       <X509Data>
          <X509Certificate>
           <!-- Replace with your encryption certificate -->
           MIIGGzCCBQO...
          </X509Certificate>
       </X509Data>
     </KeyInfo>
  </q1:KeyDescriptor>
  <!-- SingleLogoutService is not supported by eID and is ignored (is allowed in
metadata for OIOSAML.Net/Java backwards compatibility) -->
    <q1:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://sp.myndighed.dk/logout"
ResponseLocation="https://sp.myndighed.dk/logout" />
    <!-- If present, NameIDFormat must be "urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent".
        Otherwise NameIDFormat may be omitted as eID will always default to
persistent for Danish SP's -->
          <q1:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</q1:NameIDFormat>
    <!-- Replace with your Location -->
          <q1:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://sp.myndighed.dk/response" index="0" isDefault="true"/>
          <q1:AttributeConsumingService index="0" isDefault="true">
      <!-- Replace with your ServiceName -->
      <q1:ServiceName xml:lang="da">Myndighed SP</q1:ServiceName>

      <!-- You should only declare attributes required by your SP -->
      <!-- Natural person dataset attributes -->
      <q1:RequestedAttribute FriendlyName="PersonIdentifier"
Name="dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="FamilyName"
Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
```

```
      <q1:RequestedAttribute FriendlyName="FirstName"
Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="DateOfBirth"
Name="dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="BirthName"
Name="dk:gov:saml:attribute:eidas:naturalperson:BirthName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="PlaceOfBirth"
Name="dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="CurrentAddress"
Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="Gender"
Name="dk:gov:saml:attribute:eidas:naturalperson:Gender"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="CprNummer"
Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="CprNummerContext"
Name="dk:gov:saml:attribute:CprNumberIdentifier:context"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <q1:AttributeValue q1:type="xs:string">
     https://data.gov.dk/attributes/coupling/loa/Substantial
  </q1:AttributeValue>
</q1:RequestedAttribute>


      <!-- Natural person representative dataset attributes -->
      <q1:RequestedAttribute FriendlyName="RepresentativePersonIdentifier"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeFamilyName"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeFirstName"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeDateOfBirth"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeBirthName"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:BirthName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativePlaceOfBirth"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeCurrentAddress"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:CurrentAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeGender"
Name="dk:gov:saml:attribute:eidas:naturalperson:representative:Gender"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
```

```
      <q1:RequestedAttribute FriendlyName="RepresentativeCprNummer"
Name="dk:gov:saml:attribute:representative:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeCprNummerContext"
Name="dk:gov:saml:attribute:representative:CprNumberIdentifier:context"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <q1:AttributeValue q1:type="xs:string">
   https://data.gov.dk/attributes/coupling/loa/Substantial
  </q1:AttributeValue>
</q1:RequestedAttribute>


      <!-- Legal person dataset attributes -->
      <q1:RequestedAttribute FriendlyName="LegalPersonIdentifier"
Name="dk:gov:saml:attribute:eidas:legalperson:LegalPersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="LegalName"
Name="dk:gov:saml:attribute:eidas:legalperson:LegalName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="LegalAddress"
Name="dk:gov:saml:attribute:eidas:legalperson:LegalPersonAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="VATRegistration"
Name="dk:gov:saml:attribute:eidas:legalperson:VATRegistrationNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="TaxReference"
Name="dk:gov:saml:attribute:eidas:legalperson:TaxReference"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="D-2012-17-EUIdentifier"
Name="dk:gov:saml:attribute:eidas:legalperson:D-2012-17-EUIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="LEI"
Name="dk:gov:saml:attribute:eidas:legalperson:LEI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="EORI"
Name="dk:gov:saml:attribute:eidas:legalperson:EORI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="SEED"
Name="dk:gov:saml:attribute:eidas:legalperson:SEED"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="SIC"
Name="dk:gov:saml:attribute:eidas:legalperson:SIC"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>

      <!-- Legal person representative dataset attributes -->
      <q1:RequestedAttribute FriendlyName="RepresentativeLegalPersonIdentifier"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:LegalPersonIdentifier
" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeLegalName"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:LegalName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeLegalAddress"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:LegalPersonAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
```

```
      <q1:RequestedAttribute FriendlyName="Representative"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:VATRegistrationNumber
" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeTaxReference"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:TaxReference"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeD-2012-17-EUIdentifier"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:D-2012-17-
EUIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeLEI"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:LEI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="Representative"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:EORI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeSEED"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:SEED"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
      <q1:RequestedAttribute FriendlyName="RepresentativeSIC"
Name="dk:gov:saml:attribute:eidas:legalperson:representative:SIC"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>

    </q1:AttributeConsumingService>
  </q1:SPSSODescriptor>
  <!-- Replace according to your organization (Organization may be omitted) -->
  <q1:Organization>
    <q1:OrganizationName xml:lang="en">Myndighed name</q1:OrganizationName>
    <q1:OrganizationDisplayName xml:lang="en">Myndighed display
name</q1:OrganizationDisplayName>
    <q1:OrganizationURL
xml:lang="en">https://sp.myndighed.dk/info</q1:OrganizationURL>
  </q1:Organization>
  <!-- Replace according to your 'administrative' contact person-->
  <!-- It is possible to add ‘technical’ and ‘support’ contact persons-->
  <q1:ContactPerson contactType="administrative">
          <q1:Company>Myndighed name</q1:Company>
          <q1:GivenName>Administrator first name</q1:GivenName>
          <q1:SurName>Administrator lastname</q1:SurName>
          <q1:EmailAddress>email@domain</q1:EmailAddress>
          <q1:TelephoneNumber>000000000000</q1:TelephoneNumber>
  </q1:ContactPerson>
</q1:EntityDescriptor>
```

12 Bilag B – Liste over testbrugere

Værdier for en testbruger kan kontrolleres ved at anvende SP1/SP2, jf. afsnit 2.1.

Testbruger	Password	Beskrivelse af testbrugerens egenskaber
dktestuser25	Test1234	A Natural Person Test User with all mandatory attributes only that can be linked to dktestuser1
dktestuser24	Test1234	A Natural Person Test User with all mandatory attributes only that can be linked to dktestuser1
dktestuser23	Test1234	A Natural Person Test User with all mandatory attributes only that can be linked to dktestuser1
dktestuser22	Test1234	A Natural Person Test User with all mandatory attributes only (ATP Test user)
dktestuser21	Test1234	A Natural Person Test User with all mandatory attributes only (ATP Test user)
dktestuser20	Test1234	A Natural Person Test User with all mandatory attributes only (ATP Test user)
dim	dim	Natural Person Test User.
testSP	Test1234	A Natural and Legal Person Test user with mandatory and all optional attributes
dktestuser14	Test1234	Legal Person Test user with missing values on the optional attributes
dktestuser13	Test1234	Legal Person Test user with missing values on the mandatory attributes
dktestuser12	Test1234	Natural Person Test user with missing values on the optional attributes
dktestuser11	Test1234	Natural Person Test user with missing values on the Mandatory attributes
dktestuser10	Test1234	Legal Person Test User with special character value on the attributes
dktestuser2	Test1234	A Natural Person Test User with all mandatory and optional attributes
dktestuser3	Test1234	Legal Person Test User with all mandatory attributes only
idmtest8	Test1234	All Attributes Match
dktestuser1	Test1234	A Natural Person Test User with all mandatory attributes only
dktestuser19	Test1234	A Natural and Legal Person Test User with all mandatory and optional attributes with both Natural and Legal Representatives - With different markup value for representative address
dktestuser18	Test1234	
idmtest5	Test1234	All Attributes Match
dktestuser17	Test1234	
idmtest4	Test1234	All Attributes Match
dktestuser16	Test1234	Legal Person Test user with invalid characters on mandatory attributes
idmtest7	Test1234	All Attributes Match - Norwegian nationality
dktestuser15	Test1234	Natural Person Test user with invalid characters on the mandatory attributes
idmtest6	Test1234	All Attributes Match - Nepal Address and Country
idmtest1	Test1234	All Attributes Match
idmtest3	Test1234	All Attributes Match
dktestuser9	Test1234	Natural Person Test user with special character value on the attributes
idmtest2	Test1234	All Attributes Match
dktestuser6	Test1234	Representative Natural Person Test user with all mandatory and optional attributes
dktestuser7	Test1234	Representative Legal Person Test user with all mandatory attributes
dktestuser5	Test1234	Representative Natural Person Test user with all mandatory attributes

13 Bilag C – Kendte fejl i anvendte EU referenceimplementering

#	Fejlbeskrivelse	Testbruger
1	EU eIDAS Service oversætter ikke 'CurrentAddress' og returnerer ikke de 2 sets af værdier til DK eIDAS Connector	**dktestuser9** **dktestuser10**
2	EU eIDAS Service returnere 2 sets af 'PlaceofBirth' værdier, men specificere ikke, hvilket er latin-script. DK eIDAS Connector kan ikke identificere den rigtige værdi og returnere en tilfældig værdi af de to.	**dktestuser9**
3	EU eIDAS Service kan ikke sende usigneret response	**negative test på alle testbrugere**

Bemærkninger til ovenstående kendte fejl i anvendte EU referenceimplementering:

- Ovenstående fejl resulterer ikke nødvendigvis i en hård fejl med 'transactionID' og fejlbesked.
- Det vil sige, at man ikke nødvendigvis ser en fejlbesked med det samme.

Den nuværende installerede version af EU Referenceimplementeringen er version 2.5.

14 Bilag D – Kendte fejl ved testbrugere

#	Fejlbeskrivelse	Testbruger	Egenskaber
1	Denne testbruger har pt. problemer og bør derfor ikke anvendes foreløbigt. **Fejl: ”***The DK eID Gateway received an expected response from the eIDAS Service, but the eIDAS Service reported an error***”**	**dktestuser 4**	Legal Person Test User with all mandatory and optional attributes
2	Denne testbruger har pt. problemer og bør derfor ikke anvendes foreløbigt. **Fejl:** *"The DK eID Gateway received an expected response from the eIDAS Service, but the eIDAS Service reported an error"*	**dktestuser 8**	Representative Legal Person Test user with all mandatory and optional attributes
3	Denne testbruger har pt. problemer og bør derfor ikke anvendes foreløbigt. **Fejl:** *"The DK eID Gateway received an expected response from the eIDAS Service, but the returned subject (user identifier) is not formatted correctly or is expired"*	**xavi**	Test User (Natural and Legal person).

Bemærk at der er en sandsynlighed for, at der også eksisterer andre testbrugere, som vil kunne opleves at have problemer. Der foregår pt. en afklaring heraf med leverandøren.

15 Bilag E – Obligatoriske testscenarier

15.1 Positiv testscenarie (succesfuld login)

Formålet med testen er at verificerer et succesfuldt loginforløb.

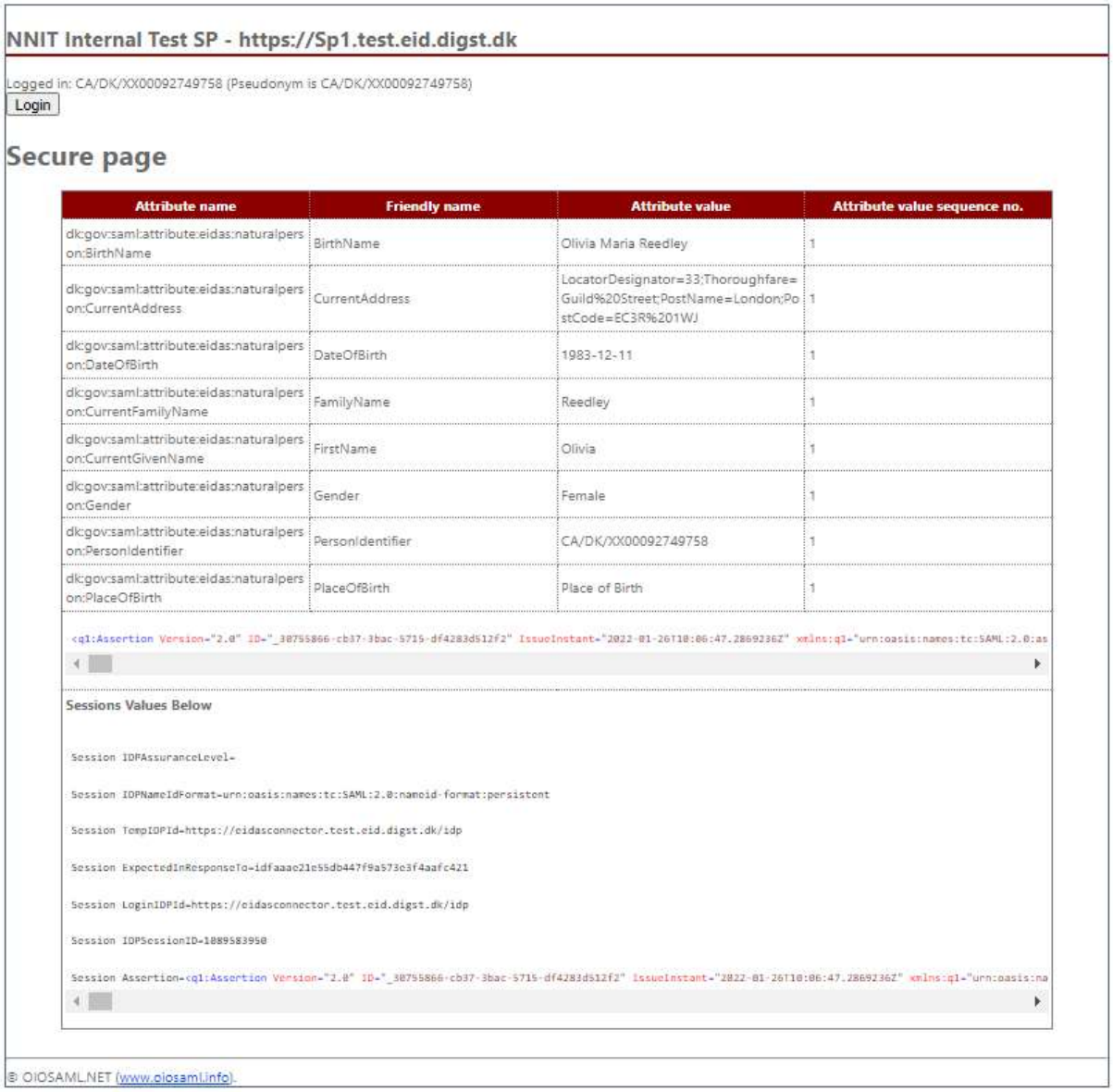
15.1.1 Testscenarie steps

Testscenarie - Eksempel på testforløb		
#	**Handling**	**Forventet resultat**
1	Tilgå integrationstestmiljøet gennem tjenesteudbyder webside	Tjenesteudbyder webside vises
2	Klik ”Login” knappen på tjenesteudbyder webside	Brugeren viderestilles til landevælgeren
3	Vælg land med ”EU” flaget på landevælgeren og bekræft valget	Brugeren viderestilles til skærmbilledet, som viser hvilke obligatoriske attributter tjenesten forespørger om
4	Tryk ”Next”	Brugeren viderestilles til skærmbilledet, som viser hvilke valgfri attributter kan vælges
5	Tilvælg samtlige valgfri attributter og bekræft handlingen ved tryk ”Next”	Brugeren viderestilles til Identity Provider login
6	Indtast brugeroplysningerne på login siden: Brugernavn: **dktestuser1** (1 til 23) Password: **Test1234** Vælg ”Level of Assurance”: **HIGH** (svarende til 'E') Vælg "Name Identifiers": **Persistent**	Brugeren viderestilles til samtykkeskærmen, der viser samtlige attributtværdier, som returneres til tjenesteudbyder
7	Tryk ”Submit”	Brugeren returneres til tjenesteudbyder websider, hvor indholdet af assertion vises
8	Verificer indholdet af attributterne i assertion i henhold til det forventede resultat	Attributterne i assertion matcher testbruger persondata afhængig af de forespurgte attributter.

15.1.2 Forventet resultat

Et eksempel på et forventet resultat for dette testscenarie er vist i nedenstående skærmbillede, jf. Figur 12. De valgfrie attributter returneres kun i tilfælde af, at de er udspecificeret i tjenesteudbyderens metadatafil.

Vigtig note: Vær opmærksom på at ikke alle testpersoner har alle eller de samme attributter. Derfor kan det forventede resultat godt være, at en fejl fremkommer – på grund af testpersonen.



Figur 12 - Loginforløb i integrationstestmiljøet

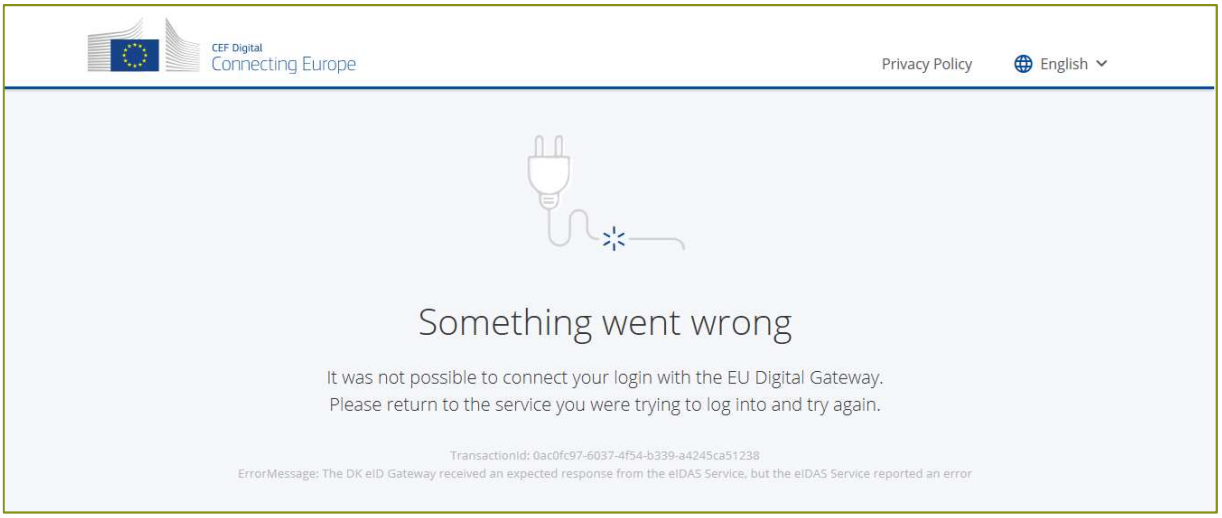
15.2 Negativ testscenarie (Invalide brugeroplysninger)

Formålet med testen er at verificerer et loginforløb som fejler, jf. Figur 13 – ”Something went wrong” fejlbesked

15.2.1 Testscenarie steps

Testscenarie - Eksempel på testforløb		
#	**Handling**	**Forventet resultat**
1	Tilgå integrationstestmiljøet gennem tjenesteudbyder webside	Tjenesteudbyder webside vises.
2	Klik ”Login” knappen på tjenesteudbyder webside	Brugeren viderestilles til landevælgeren.
3	Vælg land med ”EU” flaget på landevælgeren og bekræft valget	Brugeren viderestilles til skærmbilledet, som viser hvilke obligatoriske attributter, som tjenesten forespørger om.
4	Tryk ”Next”	Brugeren viderestilles til skærmbilledet, som viser hvilke valgfri attributter, der kan vælges .
5	Tilvælg samtlige valgfri attributter og bekræft handlingen ved tryk ”Next”	Brugeren viderestilles til Identity Provider login.
6	Indtast brugeroplysningerne på login siden Brugernavn: **dktestuser4** (9 til 15) Password: **Test1234** Vælg ”Level of Assurance”: **HIGH** (svarende til 'E') Vælg "Name Identifiers": **Persistent**	Testbrugeren returneres til fejlsiden.
7	Verificer at login ikke var succesfuldt og at brugeren viderestilles til fejlsiden	Den samme fejlside vises uafhængig af de af tjenesteudbyder forespurgte metadata.

15.2.2 Forventet resultat



Figur 13 – "Something went wrong" fejlbesked

15.3 Sikkerhedstestscenarie 1: Bypassing Session Management Schema

Følgende testscenarie beskriver overordnet en test af "Bypassing Session Management Schema" (SessionID analysis prediction, unencrypted cookie transport, brute-force).

Det undersøges her, om det er muligt at ændre brugers privilegier og/eller ID i forhold til det der er tildelt ved login.

Testscenarie - Eksempel på testforløb		
#	**Handling**	**Forventet resultat**
1	Udfør "Log-in"	-
2	Forsøg at manipuler Session Management	Forsøget fejler.
3	Evaluer at forsøget er registreret	Verificer at forsøget er blevet registreret og logget af jeres system.

15.4 Sikkerhedstestscenarie 2: Exposed Session Variables

Følgende testscenarie beskriver (overordnet) en test af "Exposed Session Variables" (Evaluate encryption & reuse of session Tokens vulnerabilities).

Testscenarie - Eksempel på testforløb		
#	**Handling**	**Forventet resultat**
1	Udfør "Log-in"	Verificer at al trafik er krypteret.
2	Kopier session Tokens	Gem denne information til senere brug.
3	Luk og åben browseren igen	-
4	Forsøg at genbrug session Tokens i en ny session	Fejl. Det er ikke mulig at tilgå den "gamle" session.
5	Evaluer at forsøget er registreret	Verificer at forsøget er blevet registreret og logget af jeres system.

16 Bilag F – Ikke-obligatoriske testcases

Bemærk at slutbetingelser i nogle testcases kan være startbetingelser i andre testcases.

Dette betyder, at en hensigtsmæssigt valgt rækkefølge kan reducere testarbejdet. Ud fra dette anbefales at udføre de ikke-obligatoriske testcases i følgende rækkefølge for at spare tid:

- IT-EIDG-TC01-LOGN-01
- IT-EIDG-TC02-SPSN-01
- IT-EIDG-TC03-LOGG-01
- IT-EIDG-TC04-LOA-01
- IT-EIDG-TC05-LOA-02
- IT-EIDG-TC06-LOA-03

Navn	**IT-EIDG-TC01-LOGN-01**
Beskrivelse	- Brugeren tilgår en beskyttet web side hos tjenesteudbyder (SP) uden forudgående session. - Der redirectes efter "Landevælger" siden til eIDAS demo IdP, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen.
Startbetingelser	- Ingen eIDAS demo IdP session aktiv. - Ingen SP session aktiv. - Startbetingelser kan etableres ved at slette alle cookies i browseren og genstarte browseren.
Trin	1. Indtast URL på *SP-beskyttet-side-A* i browseren. Indlæs siden på URL. 2. Kontroller at eIDAS demo IdP loginside fremkommer. 3. Foretag login med *IdP-testbruger-1* svarende til en bruger, der bør kunne tilgå *SP-beskyttet-side-A.* 4. Kontrollér at *SP-beskyttet-side-A* fremvise (efter login er gennemført). 5. Kontrollér at session er oprettet hos tjenesteudbyderen (SP).
Slutbetingelser	- *SP-beskyttet-side-A* er vist. - Session oprettet hos eIDAS demo IdP. - Session oprettet hos tjenesteudbyder.
Varianter	- Natural person (med/uden CPR)[10] - Foretag login med *IdP-testbruger-2.*

[10] Note: 'Legal' person samt 'Representative' person forventes på sigt (*ikke relevant pt*).

Navn	IT-EIDG-TC02-SPSN-01
Beskrivelse	- Brugeren tilgår en beskyttet side hos tjenesteudbyder (SP) og har allerede en session med denne. - Det forventes i så fald, at brugeren får adgang til siden uden at blive sendt til eIDAS demo IdP.
Startbetingelser	- SP-session er oprettet. - Kan etableres ved at udføre IT-EIDG-TC01-LOGON-01.
Trin	1. Indtast URL på *SP-beskyttet-side-A* i browseren. 2. Kontrollér at *SP-beskyttet-side-A* fremvises uden re-direct har fundet sted til eIDAS demo IdP. 3. Hvis der anvendes en proxy server, kan man kontrollere, at der ikke har været requests til eIDAS demo IdP.
Slutbetingelser	- *SP-beskyttet-side-A* er vist. - Browseren har ikke været forbi eIDAS demo IdP.
Varianter	- Foretag login med *IdP-testbruger-2* svarende til en bruger, der bør kunne tilgå *SP-beskyttet-side-A.*

Navn	IT-EIDG-TC03-LOGG-01
Beskrivelse	- Tester udvalgte aspekter af eID-gateway logningspolitik hos tjenesteudbyder (SP). - Nedenstående er en stikprøvekontrol, som ikke garanterer, at alle aspekter af eID-gateway logningspolitik overholdes.[11]
Startbetingelser	- Brugeren er logget på og har fået adgang til en beskyttet ressource, e.g. *SP-beskyttet-side-A* - Kan etableres ved at udføre IT-EIDG-TC01-LOGON-01.
Trin	1. Inspicér logfilerne i tjenesteudbyderens systemer og kontrollér, at logningerne er forsynet med korrekt tidsangivelse, og at de følgende data er til stede i logningen, dvs.: - ID på SAML <AuthnResponse> fra eIDAS demo IdP - Sikringsniveau angivet i Assertion - ID på request der svares på (fra 'InResponseTo') - Resultat af validering af <Response> meddelelse - Resultat af validering af <Assertion> - Bruger ID fra assertion (dvs. 'Subject NameID' fra assertion) - Unikt ID på lokal session, som dannes på baggrund af autentifikationssvaret.
Slutbetingelser	- Ovenstående data er logget.
Varianter	- (Ingen varianter for nuværende).

[11] Note: For detaljer om logningspolitikken henvises til reference [6].

Navn	IT-EIDG-TC04-LOA-01
Beskrivelse	- Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'Substantial') - Brugeren er autentificeret med LoA niveau 'Low'. - Adgang afvises hos tjenesten.
Startbetingelser	- Ingen eIDAS demo IdP session - Ingen SP session.
Trin	1. Indtast URL på *SP-beskyttet-side-A* i browseren, som kræver sikringsniveau sat til 'Substantial'. 2. Log ind hos eIDAS demo IdP med et eID identifikationsmiddel, som er på sikringsniveau 'Low', jf. testbrugere liste i Bilag B. 3. Kontrollér at SP'en viser fejlside om for lavt sikringsniveau og evt. re-direct'er til ny eIDAS demo IdP login.
Slutbetingelser	- Der er *ikke* oprettet en eIDAS demo IdP session for brugeren med sikringsniveau sat til 'Low' - Adgangen til den beskyttede side er *ikke* givet. - **N.B.** der forventes samtidig vist en fejlmeddelelse om, at sikringsniveauet er fundet for lavt.
Varianter	- Med/uden en eksisterende session
Bemærkninger	- **N.B.** denne testcase er ikke relevant for tjenesteudbydere, som accepterer sikringsniveau 'Low'.

Navn	IT-EIDG-TC05-LOA-02
Beskrivelse	- Brugeren tilgår en beskyttet ressource hos tjenesteudbydere (som kræver LoA niveau 'Substantial') - Brugeren er autentificeret med LoA niveau 'Substantial' og adgang tillades hos tjenesten.
Startbetingelser	- Ingen eIDAS demo IdP session - Ingen SP session.
Trin	1. Indtast URL på *SP-beskyttet-side-A* i browseren, som kræver sikringsniveauet sat til 'Substantial'. 2. Log ind hos eIDAS demo IdP med et identifikationsmiddel, som er på sikringsniveau 'Substantial', jf. testbrugere liste i Bilag B. 3. Kontrollér at SP'en viser fejlside om for lavt sikringsniveau og evt. re-direct'er til ny eIDAS demo IdP login.
Slutbetingelser	- Der er oprettet en eIDAS demo IdP session for brugeren med sikringsniveau 'Substantial'. - Adgang til den beskyttede side *er* givet. - **N.B.** *ingen* fejlbeskeder om sikringsniveauet forventes vist.
Varianter	- Med/uden en eksisterende session

Navn	IT-EIDG-TC05-LOA-02
Bemærkninger	- **N.B**. denne testcase er ikke relevant for et tjeneste, som accepterer sikringsniveau 'Low'.

Navn	IT-EIDG-TC06-LOA-03
Beskrivelse	- Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'Low'). - Brugeren er autentificeret med LoA niveau 'Substantial' og adgang tillades hos tjenesten.
Startbetingelser	- Ingen eIDAS demo IdP session - Ingen SP session.
Trin	1. Indtast URL på *SP-beskyttet-side-B* i browseren, som kræver sikringsniveauet sat til 'Low'. 2. Log ind hos eIDAS demo IdP med et identifikationsmiddel, som er på sikringsniveau 'Substantial', jf. testbrugere liste i Bilag B. 3. Kontrollér at SP'en *ikke* viser fejlside om utilstrækkeligt sikringsniveau og re-direct'er til ny eIDAS demo IdP login.
Slutbetingelser	- Der er oprettet en eIDAS demo IdP session for brugeren med sikringsniveau 'Substantial'. - Adgang til den beskyttede side *er* givet. - **N.B.** *ingen* fejlbeskeder om sikringsniveauet forventes vist.
Varianter	- Med/uden en eksisterende session
Bemærkninger	- **N.B**. denne testcase *er* relevant for et tjeneste, som accepterer sikringsniveau 'Low'.

Testcases (foreløbige):

Følgende testcases TC07 og TC08 er et udkast til hvordan det foreløbigt forventes, at man på et senere tidspunkt vil kunne teste LoA = 'High', når dette på sigt bliver aktuelt.

Tidspunktet for dette forventes at afhænge af, hvornår selvbetjeningsløsninger som kræver LoA niveau 'High' fineds og udstilles offentligt. Herudover forudsættes, at der anvendes et dansk eID, som tillader autentificering på LoA niveau 'High'. Sidst men ikke mindst vil test af et LoA niveau 'High' kræve en testtjeneste på et LoA niveau 'High' [12].

[12] Note: Der er i dag kun udstillet to test service providers: SP1 ('Substantial'), SP2 ('Low').

Navn	IT-EIDG-TC07-LOA-04 (udkast)
Beskrivelse	- Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'High'). - Brugeren er autentificeret med LoA niveau 'High' - Adgangen tillades hos tjenesten.
Startbetingelser	- Ingen eIDAS demo IdP session - Ingen SP session.
Trin	4. Indtast URL på *SP-beskyttet-side-C* i browseren, som kræver sikringsniveauet sat til 'Low'. 5. Log ind hos eIDAS demo IdP med et identifikationsmiddel, som er på sikringsniveau 'Substantial', jf. testbrugere liste i Bilag B. 6. Kontrollér at SP'en *ikke* viser fejlside om utilstrækkeligt sikringsniveau og re-direct'er til ny eIDAS demo IdP login.
Slutbetingelser	- Der er oprettet en eIDAS demo IdP session for brugeren med sikringsniveau 'High'. - Adgang til den beskyttede side *gives*. - **N.B.** *ingen* fejlbeskeder om sikringsniveauet forventes vist.
Varianter	- Med/uden en eksisterende session
Bemærkninger	- **N.B**. denne testcase *er* relevant for et tjeneste, som accepterer sikringsniveau 'High'.

Navn	IT-EIDG-TC08-LOA-05 (udkast)
Beskrivelse	- Brugeren tilgår en beskyttet ressource hos tjenesteudbyder (som kræver LoA niveau 'High'). - Brugeren er autentificeret med LoA niveau 'Substantial'. - Adgang afvises hos tjenesten.
Startbetingelser	- Ingen eIDAS demo IdP session - Ingen SP session.
Trin	7. Indtast URL på *SP-beskyttet-side-C* i browseren, som kræver sikringsniveauet sat til 'High'. 8. Log ind hos eIDAS demo IdP med et identifikationsmiddel, som er på sikringsniveau 'Substantial', jf. testbrugere liste i Bilag B. 9. Kontrollér at SP'en viser fejlside om utilstrækkeligt sikringsniveau.
Slutbetingelser	- Der er ikke oprettet en eIDAS demo IdP session for brugeren med sikringsniveau 'Substantial'. - Adgang til den beskyttede side er *ikke* givet. - **N.B.** fejlbeskeder om sikringsniveauet forventes vist.
Varianter	- Med/uden en eksisterende session
Bemærkninger	- **N.B**. denne testcase *er* relevant for et tjeneste, som accepterer sikringsniveau 'High'.

17 Bilag G – Konfiguration af OIOSAML.NET

Dette bilag er rettet mod tjenesteudbydere, som benytter OIOSAML.NET referenceimplementeringen i deres tjeneste til at kommunikere med eID-gateway.

NNIT har testet en installation af version 2.0.1 af OIOSAML.NET's kompilerede distribution (*binary distribution*). Dette bilag beskriver de nødvendige generelle tilretninger for at kommunikere med eID-gateway. Version 3.0.0 og nyere af OIOSAML.NET vil ikke fungere uden markante tilpasninger til bl.a. håndtering af 'AssuranceLevel'. Nedenstående ændringer dækker ikke over de nødvendige ændringer.

For tjenesteudbydere kan der være behov for individuelle tilretninger rettet mod deres respektive tjenester.

Konfigurationsændringer
Dette afsnit beskriver generelle tilretninger i web.config.

NameIDFormats
eID-gateway understøtter kun NameIDFormat værdien 'persistent' mod tjenester. I web.config skal elementet <NameIDFormats> derfor som minimum tillade dette format.

Web.config kan tilrettes til kun at tillade 'persistent', som vist i eksemplet nedenfor:

```
<NameIdFormats all="false">
  <add nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
</NameIdFormats>
```

Alternativt kan web.config tilrettes til at tillade alle NameIdFormats, som vist i eksemplet nedenfor:

```
<NameIdFormats all="true">
</NameIdFormats>
```

RequestedAttributes
I web.config skal <RequestedAttributes> elementet tilrettes så det erklærer danske versioner af eIDAS attributter.

I eksemplet nedenfor er erklæret attributter for fysisk person datasættet:

```
<RequestedAttributes>
  <att name="dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier"
isRequired="true" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName"
isRequired="true" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName"
isRequired="true" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth"
isRequired="true" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:BirthName" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress" />
  <att name="dk:gov:saml:attribute:eidas:naturalperson:Gender" />
</RequestedAttributes>
```

Der henvises i øvrigt til afsnit 5 for nærmere beskrivelse af krav til tjenesteudbyderes metadata samt til bilag A, som indeholder et eksempel på metadata med alle tilgængelige attributter oplistet.

.NET version
eID-gateway benytter SHA-256 i assertion signatur (i svar fra eID-gateway).

Tjenesteudbydere skal i den forbindelse være opmærksomme på, at der kræves **minimum** .NET Framework 4.6.2[13] for understøttelse af signaturalgoritmer indenfor SHA-2 familien. Det er derfor nødvendigt, at opgradere .NET Framework, hvis man benytter en tidligere version end denne. Hvis man alligevel skal opgradere, bør man overveje at opgradere til seneste version af .NET[14].

N.B. det er tidligere blevet bekræftet, at SHA-256 fungerer sammen med OIOSAML.NET 2.0.1 og .NET 4.7.1 på følgende Windows versioner:

- Windows Server 2012R
- Windows Server 2016

Andre konfigurationer er ikke blevet testet af vores leverandør, og kan derfor ikke bekræftes af vores leverandør / DIGST.

[13] Note: Der henvises til Microsofts .NET blog for information om SHA-2 understøttelse fra .NET 4.6.2: https://blogs.msdn.microsoft.com/dotnet/2016/03/30/announcing-the-net-framework-4-6-2-preview/

[14] Note: På skrivende tidspunkt er den seneste version af .NET version 4.8.

18 Bilag H – Konfiguration af OIOSAML.java

Dette bilag er rettet mod tjenesteudbydere, som benytter OIOSAML.java referenceimplementeringen i deres tjeneste til at kommunikere med eID-gateway.

Den ældste version af OIOSAML.java, der er kompatibel med eID-gateway er version 2.0.3. Tjenesteudbydere, der anvender en ældre version end denne, skal opdatere OIOSAML.java, før de kan kommunikere med eID-gateway.

Version 3.0.0 og nyere af OIOSAML.java vil ikke fungere uden markante tilpasninger til bl.a. håndtering af 'AssuranceLevel'. Nedenstående ændringer dækker ikke over de nødvendige ændringer.

Konfiguration af OIOSAML til at være kompatibel med eID-gateway

I konfigurationsfilen 'oiosaml-sp.properties' skal følgende setting være sat til "true":

oiosaml-sp.eid.compatible=true

Denne indstilling ændrer den måde OIOSAML genererer *AuthnRequests*, så de accepteres af eID-gateway.

Generering og tilpasning af SAML-metadata

Hvis man har metadata, der er genereret af en tidligere udgave af OIOSAML, vil disse ikke være kompatible med eID-gateway. Man kan enten vælge at gennemføre konfigurationen af OIOSAML forfra, eller man kan rette de allerede genererede metadata.

Hvis man vælger at tilpasse eksisterende metadata, er det nemmeste at gennemføre konfiguration af OIOSAML på en lokal maskine, så der dannes nye metadata. Herefter kopieres *RequestedAttribute*, *NameIDFormat* og *ContactPerson* sektionerne fra de nye metadata over i de eksisterende.

Hvis man vælger at gennemføre konfigurationen forfra, skal man sætte flueben i " *Enable EID compatibility*", samt flueben i mindst én af "*Enable EID Natural Person attribute set*" eller "*Enable EID Legal Person attribute set*".

Dette vil sikre, at 'NameIDFormat' sættes til en værdi som understøttes af eID-gatewayen, samt at mindst én af de understøttede attributsæt tilføjes til 'requested attributes'-sektionen.

Samtidig udfyldes de relevante sektioner om administrative kontaktpersoner, som er krævet af eID-gateway.

19 Bilag I – Skabelon til fremsendelse af metadata (INTTEST)

Punkter til udfyldelse	Forklaring
Myndighed	<Navnet på den myndighed som er systemejer>
Navn	<I bedes her angive det 'navn' som i ønsker vist til brugeren ved afgivelse af samtykke>
Beskrivelse	<Her kan det være relevant at skrive lidt om løsningen>
Leverandør	<I bedes her angive hvem leverandøren er/har været>
Titel på selvbetjeningsløsning	<Her skriver I titlen på den selvbetjeningsløsning. Hvis integrationen laves til flere løsninger skal alle løsninger specificeres her>
CVR-nummer	<CVR-nummer for myndigheden>
Level of Assurance	<Ønsket sikringsniveau for autentifikationen af borgeren som enten kan være 'Low', 'Substantial' eller 'High'>[15]
Nødvendige attributter	<Her bedes I angive og tage stilling til, hvilke attributter, som I ønsker medsendt om brugeren fra EU/EØS landets IdP>

[15] Note: Digitaliseringsstyrelsen anbefaler som minimum et LoA niveau på 'Substantial'.

20 Bilag J – Relevante dokumenter og links

eID-gateway driftsgruppen på digitaliser.dk:

https://www.digitaliser.dk/group/3003373

Digitaliseringsstyrelsens webside om eID-gateway:

https://digst.dk/it-loesninger/eid-og-selvbetjeningsloesninger-i-eueoes/

Funktionspostkasse:

eidas@digst.dk