DIGITALISERINGSSTYRELSEN

NemLog-in

Integrationstest ved tilslutning til NemLog-in

Version 3.0.3

Indholdsfortegnelse

1 Dokumenthistorik

Dato	Version	Ændringsbeskrivelse	Initialer
14.01.2008	0.61	Første udkast offentliggjort på modernisering.dk	TG
28.02.2008	0.62	• Diverse referencer er opdateret med links. • Fejl omkring niveau af autenticitetssikring af OCES digital signatur login er ændret (fra 4 til 3).	TG
12.09.2008	1.0	Referencer opdaterede; versionsnummer sat til 1.0. Nyt løsningsnavn (NemLog-in) indført.	TG
12.01.2008	1.1	Gennemrevideret med konkrete henvisninger til NemLog-in's integrationstestmiljø. Test casen IT-CERT-1 er fjernet, da den i praksis var særdeles vanskelig for tjenesteudbydere at udføre.	TG
15.11.2012	1.2	Opdateret med beskrivelse af integrationstestmiljø for den nye NemLog-in løsning. Common Domain Cookie understøttelse er blevet valgfri i OIOSAML, og derfor er den tilhørende test case ikke længere obligatorisk.	TG
14.03.2013	1.3	Dokument opdateret med test cases for med privilegier i SAML Assertion (udstedt via FBRS), og signeringstjenesten.	TG
19.04.2013	1.4	Tilføjet obligatorisk test case som verificerer, at tjenesteudbydere håndterer korrekt logoutrequest fra IdP på lokal session, der er timet ud.	TG
24.10.2013	1.5	Fejl i IT-SLO-3 er rettet.	TG
03.03.2014	1.6	Det er præciseret, at test cases med privilegier både omfatter almindelige privilegier og fuldmagtsprivilegier. Præcisering omkring returkode i SLO-3.	TG
21.03.2014	1.7	Test cases med fuldmagtsprivilegier præciseret, så man både tester at borgere og medarbejdere kan være fuldmagtshaver. Henvisninger til diverse materiale og hjemmesider opdateret.	TG
23.02.2021	1.8	Tilføjelse vedr. logud-anbefaling til IT-SLO-1 og IT-SLO-2. Levetid for assertion opdateret i IT-TIM-1. Links til referencer opdateret.	ANNJU
15.03.2021	1.9	• Opdateret til NemLog-in3 go-live med både offentlige og private tjenesteudbydere og brug af OIOSAML 3.0. • Common domain cookie understøttelse er fjernet fra løsningen og indgår derfor ikke længere i beskrivelser. • Beskrivelser af sikringsniveauer peger nu på NSIS. Diverse links opdateret.	TG
01.09.2021	3.0	• Opdateret og tydeligt beskrivelser på baggrund af feedback, herunder markering af krav for apps. • Tilføjelse af testcase for brokeres videresendelse af navn på bagvedliggende tjeneste.	TG

Dato	Version	Ændringsbeskrivelse	Initialer
07.10.2021	3.0.1	• Opdateret beskrivelse af IT-TIM-1 ved nye skærmbilleder og instruktioner i brug af tamper data plug-in. • Opdateret IT-LOA-1 og IT-SSO-1 med beskrivelser af, hvornår test cases ikke er relevante.	TG
09.12.2021	3.0.2	• Links til testtjenester opdateret	LEASA
28.06.2022	3.0.3	• Tydeliggjort, hvornår test cases er relevante. • Tilrettet sprog, referencer og links.	TG

2 Introduktion

Dette dokument henvender sig til udbydere af it-systemer (både offentlige myndigheder og private tjenester), der skal tilsluttes NemLog-in3 løsningen og dermed indgå i den fællesoffentlige føderation. Dokumentet beskriver obligatoriske integrationstest, der skal udføres, før udbyderens it-system kan kobles på NemLog-in's produktionsmiljø. Endvidere beskrives en række valgfrie test, der dækker funktionalitet, som ikke anvendes af alle tjenesteudbydere. Disse kan udføres i det omfang, de skønnes relevante.

Beskrivelsen tager udgangspunkt i integrationstestmiljøet for den nye NemLog-in3 løsning, der gik i drift 22. september 2021. Test cases i dokumentet fokuserer på test ved tilslutning til den nye OIOSAML 3.0 IdP. For de tjenester, der helt undtagelsesvis tilslutter sig den gamle OIOSAML 2.1.0 IdP efter september 2021, kan dokumentet dog stadig anvendes med mindre tilpasninger - eksempelvis skal der så ses bort fra test som involverer NSIS sikringsniveauer.

Når test cases er gennemført udfyldes en testrapport, som uploades via NemLog-in's tilslutningssystem. Efter godkendelse fra NemLog-in-forvaltningen, kan systemet herefter kalde NemLog-in's produktionsmiljø.

3 Introduktion og formål

Dette dokument henvender sig til udbydere af it-systemer, der skal tilsluttes den fællesoffentlige log-in-løsning kaldet NemLog-in3. Formålet er at beskrive de tekniske integrationstest, en tjenesteudbyder[1] skal udføre for at verificere, at tilslutningen mod NemLog-in[2] er udført funktionelt korrekt.

Målgruppen for dette dokument er teknisk personale hos tjenesteudbydere (eller disses leverandører), som skal planlægge og udføre integrationstesten.

Beskrivelsen omfatter en række obligatoriske test, der verificerer funktionalitet, som alle tjenesteudbydere skal implementere. Derudover beskrives en række valgfrie test, som dækker funktionalitet ikke alle tjenesteudbydere forventes at anvende.

Integrationstesten er et af de sidste trin i tilslutningsprocessen. For en gennemgang af de øvrige aktiviteter i tilslutningsforløbet NemLog-in's tjenesteudbydersite[3]. Før en tjeneste kan gå i drift kan der derudover være en række aktiviteter som f.eks. test af applikationsspecifik funktionalitet og evt. integration med offentlige

[1] Begreberne it-systemudbyder og tjenesteudbyder anvendes synonymt om den organisation, som udbyder det it-system, der tilsluttes NemLog-in.
[2] I det følgende benyttes termerne NemLog-in, Identity Provider (IdP) og fællesoffentlig loginløsning synonymt.
[3] https://tu.nemlog-in.dk

portaler. Disse aktiviteter ligger udenfor rammerne af dette dokument. En succesfuld integrationstest er med andre ord en nødvendig men ikke tilstrækkelig betingelse for at gå i drift.

4 Offentlige og private tjenester

I NemLog-in3 kan både offentlige og private tjenester blive tilsluttet. Typen af tjenesten er som udgangspunkt fastlagt ud fra tjenesteudbyderens CVR-nummer, og der er funktionalitet i NemLog-in, som kun kan anvendes af offentlige tjenester, herunder:

- Single Sign-on (SSO)
- Brug af rettigheder og fuldmagter i NemLog-in
- Modtagelse af CPR-nummer i SAML Assertions.

Private tjenester skal derfor ikke udføre de test, der er relateret til ovenstående områder. Bemærk at private tjenesteudbydere af tekniske årsager skal implementere Single Logout protokollen, så single logout kan aktiveres fra andre tjenesteudbydere, selvom private tjenester ikke deltager i SSO. Man behøver derimod ikke kunne *initiere* single logout fra en privat tjenesteudbyder.

5 Teststrategi

Formålet med integrationstesten er som tidligere nævnt at verificere, at integrationen mod NemLog-in løsningen er udført *funktionelt og teknisk* korrekt. Der er således en række ikke-funktionelle aspekter, som en tjenesteudbyder selv må teste i forhold til den ønskede servicekvalitet som f.eks.:

- tilgængelighed
- svartider
- kapacitet
- skalérbarhed
- sikkerhed
- brugervenlighed (herunder sprog og understøttelse af browsere)

Da NemLog-in tilbyder en række sikkerhedsfunktioner, vil en række af de beskrevne integrationstest verificere sikkerhedsrelateret funktionalitet - primært i samspillet mellem tjenesteudbyder og NemLog-in. Disse har til formål at verificere, at tjenesteudbyderen anvender føderationens protokoller (OIOSAML) korrekt.

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

En tjenesteudbyder vil derfor have behov for at sikkerhedsteste systemer og infrastruktur udover, hvad der er beskrevet i dette dokument[4]. Dette arbejde bør tilrettelægges i overensstemmelse med den risikovurdering, der indledningsvis er foretaget, samt organisationens sikkerhedspolitik og -arbejde i øvrigt.

[4] Dette kan eksempelvis være forskellige former for penetrationstest.

En anden vigtig afgrænsning for den her beskrevne integrationstest er, at det alene er samspillet med NemLog-in, der beskrives. Test af applikationsspecifik funktionalitet og test af integrationsformer mod portaler behandles derfor ikke.

6 Forudsætninger hos tjenesteudbyder

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

- Tilsluttet sin organisation til NemLog-in som it-systemudbyder (se tjenesteudbydersite for detaljer).
- Oprettet it-system i NemLog-in og udpeget en teknisk administrator for systemet.
- Konfigureret og installeret et SAML produkt (fx en af OIOSAML 3 referenceimplementeringerne[5])
- Bestilt, modtaget og installeret test certifikater
- Etableret infrastruktur og forbindelser (firewalls etc.)
- Udvekslet metadata med NemLog-in's Identity Provider
    - Dette foregår via NemLog-in's tilslutningssystem på https://administration.nemlog-in.dk
- Konfigureret tidsservice, logning etc.

For en nærmere beskrivelse af de indledende aktiviteter henvises til NemLog-in supportsiden på Digitaliser.dk.

7 Oversigt over Test Cases

I nedenstående tabel gives et overblik over de test cases, der indgår i integrationstesten. I efterfølgende kapitler findes en detaljeret gennemgang af hver test case inklusive de enkelte trin, testen består af, start- og slutbetingelser, nødvendige testdata, samt hvorledes resultatet af testen observeres.

De udvalgte test cases 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 NemLog-in fungerer korrekt.

Som tidligere nævn er ikke alle testcases er relevante for private tjenesteudbydere, idet disse kun har adgang til et begrænset sæt af services i NemLog-in. Dette er markeret i tredje kolonne i skemaet.

Endvidere er de fleste test cases skrevet med web-applikationer for øje. Hvis NemLog-in anvendes til eksempelvis indrullering af en 'native app'[6], er der en række test cases, som ikke er relevante, idet NemLog-in's sessionsstyring eksempelvis ikke udstrækker sig til 'native apps'. Relevansen af en test case for apps er angivet i fjerde kolonne. For apps må beskrivelsen af test cases fortolkes lidt mere 'frit', så den giver mening i denne kontekst.

[5] https://github.com/digst/OIOSAML.Net
https://github.com/digst/OIOSAML.Java

[6] Som det eksempelvis kendes fra OAuth og OpenID Connect standarderne.

Test Case ID	Obligatorisk	Relevant for privat TU	Relevant for Apps	Beskrivelse
IT-LOGON-1	Ja	Ja	Ja	Brugeren tilgår en beskyttet web-side hos tjenesteudbyder uden forudgående session. Der re-directes til NemLog-in's Identity Provider (IdP), hvor brugeren foretager log-in med NemID eller MitID, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen.
IT-SSO-1	Ja	Nej	Nej	Brugeren tilgår en beskyttet side hos tjenesteudbyder og har allerede en session med NemLog-in's Identity Provider. Der foretages single sign-on via NemLog-in, hvorefter brugeren får adgang til siden hos tjenesteudbyderen uden at autentificere sig.
IT-SPSES-1	Ja	Ja	Nej	Brugeren tilgår en beskyttet side hos tjenesteudbyder og har allerede en session med denne. Brugeren får adgang til siden uden at blive sendt til IdP'en.
IT-SLO-1	Ja	Nej	Nej	Brugeren vælger single logout fra den aktuelle tjenesteudbyder og bliver logget ud af alle sessioner i føderationen (dvs. alle it-systemer som der aktuelt er logget på via NemLog-in). Dette tester, at tjenesteudbyderen kan initiere single logout. Varianter: SOAP eller HTTP redirect binding
IT-SLO-2	Ja	Ja	Nej	Brugeren vælger single logout fra en *anden* tjenesteudbyder og bliver logget ud af sessionen hos den aktuelle tjenesteudbyder. Dette tester, at tjenesteudbyderen kan indgå i single logout uden at være den initierende part.
IT-SLO-3	Ja	Ja	Nej	Brugeren vælger single logout fra en *anden* tjenesteudbyder, men den lokale SP-session er timet ud på grund af inaktivitet. Dette tester, at tjenesteudbyderen håndterer logoutrequests som ikke kan matches til den lokale session på en korrekt måde.
IT-LOA-1	Ja	Ja	Ja	Brugeren tilgår en beskyttet ressource hos tjenesteudbyderen med et for lavt NSIS sikringsniveau. Adgang afvises. Varianter: med og uden eksisterende session.
IT-TIM-1	Ja	Ja	Ja	Brugeren søger at få adgang med en assertion, der er udløbet. Adgangen gives ikke.
IT-TIM-2	Ja	Nej	Nej	Bruger tilgår en beskyttet ressource hos tjenesteudbyderen efter hans session er timet ud. Derimod er hans IdP session stadig aktiv.
IT-LOG-1	Ja	Ja	Ja	Tester udvalgte aspekter af logningspolitik, herunder at nødvendige data logges.
IT-USER-1	Nej	Ja	Ja	Bruger ikke kendt lokalt og adgang afvises.
IT-ATTQ-1	Nej	Ja	Nej	Tester attributforespørgsler hos IdP.
IT-FORCE-1	Nej	Ja	Ja	Tester brug af tvungen autentifikation hos IdP (ForeAuthn attributten er sat fra SP). Brugeren tvinges til at foretage logon hos IdP'en, selvom vedkommende har en gyldig IdP session.

Test Case ID	Obligatorisk	Relevant for privat TU	Relevant for Apps	Beskrivelse
IT-REPL-1	Nej	Ja	Ja	Der prøves replay af assertion.
IT-PRIV-1	Nej	Nej	Ja	Bruger logger på side hos tjenesteudbyder, som kræver privilegier i SAML Assertion. Adgang opnås på baggrund af tildelte privilegier. Obligatorisk hvis privilegier anvendes i løsningen.
IT-PRIV-2	Nej	Nej	Ja	Bruger logger på side hos tjenesteudbyder, som kræver privilegier i SAML Assertion. Adgang afvises på grund af manglede privilegier. Obligatorisk hvis privilegier anvendes i løsningen.
IT-PRIV-3	Nej	Nej	Ja	Bruger logger på side hos tjenesteudbyder, som kræver privilegie. Adgang opnås gennem en delegering af privilegiet fra en anden organisation.
IT-SIGN-1	Nej	Ja	Nej	Bruger anvender signeringstjenesten. Obligatorisk hvis signeringstjenesten anvendes.

OBS: Hvis en tjenesteudbyder alene anvender signeringsløsningen i NemLog-in (men ikke log-in), er det kun testcasen IT-SIGN-1, som er relevant.

8 Testmiljø hos tjenesteudbyder

I det følgende beskrives en række testdata, der skal anvendes i de enkelte test cases, i form af testsider, brugere og opsætninger.

De beskrevne testdata skal konfigureres i tjenesteudbyderens systemer forud for gennemførelsen af integrationstesten. Da disse systemer vil variere i praksis, gives nedenfor kun generelle anvisninger, som vil skulle realiseres i kontekst af de konkret anvendte systemer. De abstrakte testdata skal med andre ord oversættes (mappes) til fysiske web sider, testbrugere etc.

Det forudsættes, at flg. generiske systemer / funktionalitet er til rådighed i testmiljøet hos tjenesteudbyderen:

- En web server, hvor der kan oprettes web / html sider.
- Et adgangskontrolsystem, hvor beskyttelse kan sættes på web-sider og adgangspolitik kan konfigureres for brugere (herunder krævet NSIS sikringsniveau). Det er muligt at inspicere systemet og se hvilke sessioner, der er oprettet, herunder om en given bruger har en aktiv session, og hvornår denne udløber.
- Et brugerkatalog / brugerdatabase hvor brugere kan administreres. Dette kan være en integreret del af adgangskontrolsystemet eller separat herfra.
- Et SAML produkt der kan fungere sammen med brugerkataloget og adgangskontrolsystemet, herunder oversætte (mappe) fra en assertion til interne testbrugerne / konti.

Alle testdata nedenfor er markeret med 'SP' prefix for at adskille dem fra testdata, som Identity Provideren leverer.

8.1 Testdata

SP-åben-side-1
Dette er en statisk html side, hvorpå der ikke er sat adgangsbegrænsninger.

SP-beskyttet-side-1
Dette er en statisk html side, hvor kun SP-testbruger-1 (se nedenfor) kan få adgang. Det krævede NSIS sikringsniveau er sat til Betydelig.
Siden rummer et link eller en knap til at initiere single logout fra tjenesteudbyderen (for offentlige tjenesteudbydere).

SP-beskyttet-side-3
Dette er en statisk html side, hvor det krævede NSIS sikringsniveau er sat til Høj, som er over det niveau, der opnås ved autentifikation med fx NemID eller almindeligt MitID. Denne side anvendes til at teste, at forsøg på adgang med for lavt opnået sikringsniveau afvises hos tjenesteudbyderen.
Siden rummer et link eller en knap til at initiere single logout fra tjenesteudbyderen (for offentlige tjenesteudbydere).

SP-beskyttet-side-4
Dette er en statisk html side, som er konfigureret til at kræve et eller flere privilegier i brugerens SAML Assertion, før der opnås adgang.

OBS: Denne side er kun relevant for offentlige tjenester, som benytter rettighedsstyring via NemLog-in.

SP-hent-attributter-side-1 (valgfri - anvendes til test af attributforespørgsler)
Dette er en web-side med et link eller en knap, som igangsætter en attributforespørgsel (SAML Attribute Query) hos NemLog-in's Identity Provider. Forespørgslen går på udvalgte attributter og resultatet vises i browservinduet.

SP-force-authn-side-1 (valgfri)
Dette er en web-side med et link eller en knap, som aktiverer en forespørgsel til NemLog-in's Identity Provider om at re-autentificere brugeren (et SAML <AuthnRequest> med ForceAuthn attributten sat).

SP-testbruger-1
Dette er en testbruger, der er udstyret med en test NemID eller MitID. Brugerens identitet udveksles mellem IdP og tjenesteudbyder via attributterne i den udstedte SAML Assertion. Brugeren er oprettet i adgangskontrolsystemet og tildelt adgang til SP-beskyttet-side-1. SAML produktet er konfigureret til at oversætte fra brugerens SAML assertion til den interne brugerkonto. Dette kan ske ved at tage udgangspunkt i Subject (UUID), PID, RID eller evt. CPR-attributten.

9 NemLog-in's Integrationstestmiljø

Nedenfor beskrives en række testsider, der stilles til rådighed i NemLog-in's integrationstestmiljø. Siderne har til formål at lade tjenesteudbydere teste og fejlsøge deres løsninger, og de refereres fra test cases beskrevet i næste kapitel. Overordnet består testmiljøet af en Identity Providere og to tjenesteudbyderinstanser, hvorimellem der er udvekslet metadata. Alle testsider nedenfor er markeret med 'IdP' prefix for at adskille dem fra testdata, som tjenesteudbyderen selv skal etablere.

En uddybende dokumentation af integrationstestmiljøets funktionalitet findes på dette link: https://tu.nemlog-in.dk/testportal/

IdP-Login-start-side
Link: https://tu.nemlog-in.dk/testportal/

Dette er "forsiden" til de øvrige testsider i integrationstestmiljøet, som rummer links til et antal tjenesteudbydere i testmiljøet, og et link til metadatavalidatoren.

— Testtjenester

Integrationstestmiljøet udstiller et antal testtjenester, som kan anvendes i forskellige testscenarier.

Test-tjeneste	OIOSAML-version	NameIDFormat	Privat/offentlig
TU0	2.0.9*	X509Subject	Offentlig
TU1	2.1.0	X509Subject	Offentlig
TU2	2.1.0	Persistent Pseudonym	Offentlig
TU3	3.0.2	Persistent	Offentlig
TU4	3.0.2	Transient	Offentlig
TU5	3.0.2	Persistent	Privat
TU6	3.0.2	Transient	Privat

Figur 1: Test-tjenester i integrationstestmiljøet, som kan anvendes til integrationstesten.

IdP-SP-side-1
Link**:** https://sp1.test-nemlog-in.dk

Dette er forsiden på test service provider 1 i testmiljøet, som er konfigureret mod OIOSAML 2.1.0 IdP'en. Siden kan være i to tilstande afhængigt af, om brugeren har logget ind eller ej.

Hvis brugeren ikke er logget ind, rummer siden en knap til at initiere login mod Identity Provideren ("Login"). Siden kan anvendes til at simulere, at brugeren har sessioner med flere tjenesteudbydere på én gang, hvilket er relevant for test af single sign-on samt single logout.

Hvis brugeren er logget ind, viser siden et udsnit af attributterne fra den modtagne SAML assertion fra IdP'en. Denne tjenesteudbyder er hos IdP'erne konfigureret til at anvende OCES attributprofilen, hvilket er afspejlet i de viste attributter, der tager udgangspunkt i OCES certifikatets indhold. For detaljer om attributprofilerne henvises til [OIOSAML].

Siden rummer desuden en række knapper:

- "Force" sender et nyt login request mod IdP'en (et SAML <AuthnRequest>), hvor attributten ForceAuthn, så brugerne tvinges til at gennemføre log-in.
- Knappen "Login" sender et nyt login request mod IdP'en (et SAML <AuthnRequest>) uden at attributten ForceAuthn er sat.
- Knappen "Logout" igangsætter logout mod IdP'en hvorefter alle tjenesteudbydere, brugeren aktuelt har en session med, vil blive kaldt af IdP'en med en SAML logout besked.

IdP-SP-side-2
Link: https://sp2.test-nemlog-in.dk

Denne side er ækvivalent til den første tjenesteudbyder (IdP-SP-side-1) bortset fra, at tjenesteudbyderen er konfigureret til at anvende persistente pseudonymer. Dette betyder, at det modtagne sæt af attributter i SAML Assertion er et andet. For detaljer om attributprofilerne henvises til [OIOSAML].

IdP-SP-side-3
Link: https://sp3.test-nemlog-in.dk

Denne side er ækvivalent til den første tjenesteudbyder (IdP-SP-side-1) bortset fra, at tjenesteudbyderen er konfigureret til anvende OIOSAML 3.0 snitfladen med persistent NameID konfigureret.

Identity Provider i testmiljøet
Testmiljøet rummer en test Identity Provider med flg. entity IDs: https://saml.test-nemlog-in.dk

Det er således denne, en tjenesteudbyder skal udveksle SAML metadata med.

Identity Provideren i testmiljøet rummer en række interne web sider (f.eks. login sider, fejlsider mv.), som vil fremkomme under testen. Disse sider skal dog ikke refereres direkte af testeren, og der er derfor ikke angivet links til disse.

Det skal endvidere bemærkes, at loginsiderne hørende til Identity Provideren er konfigureret, så man kun kan logge på med testbrugere.

Oprettelse af testbrugere og tildeling af privilegier
For de løsninger, som anvender Nemlog-in's brugeradministrationsmodul (FBRS), er der behov for at kunne teste log-in til løsningen, hvor brugeren er tildelt de privilegier, som løsningen anvender. Tjenesteudbydere kan her anvende NemLog-in's administrationsportal til at selv at oprette nogle testbrugere og tildele dem de privilegier, som løsningen anvender. Herefter vil de pågældende brugere ved log-in få indlejret de tildelte privilegier i den udstedte SAML Assertion.

10 Andre testværktøjer

Tamper Data Plug-in i Firefox

En del af de beskrevne test cases nedenfor går på fejlsituationer, hvor tjenesteudbyderen skal reagere korrekt på fejlbehæftede svar fra NemLog-in's Identity Provider. Dette kan være fejl i beskeder herunder signaturer og certifikater, svar som er forsinkede (timeout), eller genafspilninger af tidligere svar (replays).

For at kunne fremprovokere disse specielle situationer kan de tilhørende test cases eksempelvis afvikles i Mozilla Firefox browseren med plug-in'et "Tamper Data" aktiveret. Dette plug-in kan downloades gratis fra hjemmesiden https://addons.mozilla.org/da/firefox/addon/tamper-data-for-ff-quantum/

Beskrivelsen af test cases vil rumme instruktioner i, hvorledes dette plug-in anvendes.

Alternativt kan man vælge at anvende mere avancerede proxy servere, der tillader manipulering af beskeder, som f.eks. Fiddler (https://www.telerik.com/fiddler), Burp suite eller WebScarab. I givet fald må man selv finde ud af, hvordan beskeder kan manipuleres som beskrevet i test cases.

11 Test Cases

Nedenfor beskrives de test cases, integrationstesten består af. For hver test case opstilles startbetingelser, der skal være opfyldte inden testen kan udføres, hvilke trin, en bruger/administrator skal udføre, og hvilke slutbetingelser, der gælder efter testcasen er gennemført.

Som en fælles startbetingelse for alle test cases gælder, at de i forrige kapitel beskrevne test data er oprettet.

Bemærk at slutbetingelser i nogle test cases kan være startbetingelser i andre test cases. Dette betyder, at en hensigtsmæssigt valgt rækkefølge kan reducere testarbejdet.

Det anbefales at udføre testene i flg. rækkefølge:

- IT-LOGON-1, IT-SSO-1, IT-SPSES-1, IT-LOG-1, IT-ATTQ-1, IT-FORCE-1, IT-REPL-1, IT-SLO-1, IT-USER-1
- (*session etableres*) IT-SLO-2, IT-TIM-1, IT-LOA-1
- IT-TIM-2

Navn	**IT-LOGON-1**
Beskrivelse	Brugeren tilgår en beskyttet web side hos tjenesteudbyder uden forudgående session. Der re-directes til NemLog-in's Identity Provider, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen.
Startbetingelser	• Ingen IdP session • Ingen SP session Startbetingelser kan etableres ved at slette alle cookies i browseren og genstarte denne.
Trin	1. Indtast URL på SP-beskyttet-side-1 i browseren. 2. Kontrollér at IdP'ens loginside fremkommer. 3. Foretag login med NemID eller MitID svarende til en bruger, der er tildelt adgang til SP-beskyttet-side-1. 4. Kontrollér at SP-beskyttet-side-1 fremvises. 5. Kontrollér at session er oprettet hos tjenesteudbyder.

Navn	IT-LOGON-1
Slutbetingelser	• SP-beskyttet-side-1 er vist • Session oprettet hos IdP • Session oprettet hos tjenesteudbyder
Varianter	Evt. med og uden CPR

Navn	IT-SSO-1
Beskrivelse	Brugeren tilgår en beskyttet side hos tjenesteudbyder og har allerede en session med IdP'en. Brugeren får adgang til siden hos tjenesteudbyderen uden at autentificere sig. *Bemærk: denne test case er ikke relevant for tjenesteudbydere, som konsekvent gennemtvinger aktivt brugerlog-in i NemLog-in ved at sætte SAML-parameteren ForceAuthn=true i deres request mod NemLog-in.*
Startbetingelser	Ingen (etableres i test casen).
Trin	1. Genstart browseren. 2. Log på IdP'en via af en af test tjenesteudbyderne (IdP-SP-side-1 eller IdP-SP-side-2). Der skal anvendes NemID eller MitID hørende til en bruger, der er tildelt adgang til SP-beskyttet-side-1. 3. Indtast URL på SP-beskyttet-side-1 i browseren. 4. Kontrollér at SP-beskyttet-side-1 fremvises uden brugeren er blevet bedt om at logge ind (igen) – dvs. der er foretaget single sign-on. 5. Kontrollér at session er oprettet hos egen tjenesteudbyder.
Slutbetingelser	• SP-beskyttet-side-1 er vist • Session oprettet hos egen tjenesteudbyder
Varianter	

Navn	IT-SPSES-1
Beskrivelse	Brugeren tilgår en beskyttet side hos tjenesteudbyder og har allerede en session med denne. Brugeren får adgang til siden uden at blive sendt til IdP'en.
Startbetingelser	• SP-session er oprettet. Kan etableres ved at udføre IT-LOGON-1
Trin	1. Indtast URL på SP-beskyttet-side-1 i browseren. 2. Kontrollér at SP-beskyttet-side-1 fremvises uden redirects har fundet sted til IdP ("browser flicker"). Hvis der anvendes en proxy server, kan man kontrollere, at der ikke har været requests til IdP'en.
Slutbetingelser	• SP-beskyttet-side-1 er vist • Browseren har ikke været forbi IdP'en.
Varianter	

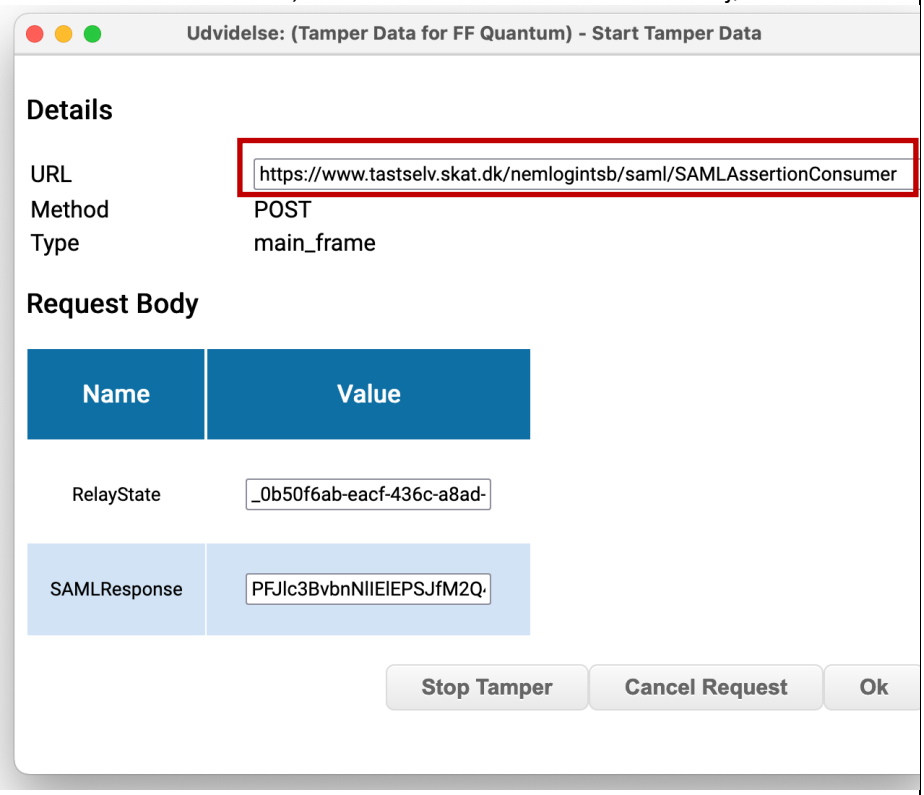
Navn	IT-SLO-1 (kun offentlige tjenester)
Beskrivelse	Brugeren vælger single logout fra den aktuelle tjenesteudbyder og bliver logget ud af alle sessioner etableret via NemLog-in. Dette tester, at tjenesteudbyderen kan initiere single logout. OBS: Testcasen kan fraviges, hvis tjenesteudbyderen ikke opretter en lokal session i sin applikation.
Startbetingelser	• IdP session er oprettet. • SP session er oprettet mod test service provider 1. Kan etableres ved at udføre IT-LOGON-1
Trin	1. Indtast URL på SP-beskyttet-side-1 i browseren. 2. Kontrollér at SP-beskyttet-side-1 fremvises uden at brugeren er blevet bedt om at logge på. 3. Tryk på sidens link / knap til initiering af single logout. 4. Kontrollér at bekræftelsesside for single logout vises (evt. skal det bekræftes i en dialog, at man ønsker SLO). Bekræftelsessiden skal indeholde en vejledende tekst til brugeren om at denne skal huske at lukke browservinduet for at sikre korrekt logud. 5. Indtast URL på SP-beskyttet-side-1 i browseren. 6. Kontrollér at siden ikke vises, men at IdP'ens loginside i stedet fremkommer (dette betyder at såvel SP som IdP sessionerne er nedlagte). 7. Indtast URL på IdP-SP-side-1 i browseren. 8. Kontrollér at siden ikke vises, men at IdP'ens loginside i stedet fremkommer. Dette tester, at den anden (test) tjenesteudbyders session også er nedlagt.
Slutbetingelser	• SP sessioner nedlagt • IdP session nedlagt
Varianter	Tjenesteudbyderen kan konfigurere sit system til at anvende SOAP binding (foretrukken), HTTP POST eller HTTP Redirect binding i kommunikationen med IdP'en. Alle disse varianter kan evt. testes.

Navn	IT-SLO-2
Beskrivelse	Brugeren vælger single logout fra en *anden* tjenesteudbyder og bliver logget ud af sessionen hos den aktuelle tjenesteudbyder. Dette tester, at tjenesteudbyderen kan indgå i single logout (uden at være den initierende part). OBS: Testcasen kan fraviges, hvis tjenesteudbyderen ikke opretter en lokal session i sin applikation.
Startbetingelser	• IdP session er oprettet. • SP session er oprettet. Kan etableres ved at udføre IT-LOGON-1
Trin	1. Indtast URL på IdP-SP-side-1 i browseren (en af test SP'erne i testmiljøet). 2. Kontrollér at siden fremvises uden re-directs har fundet sted ("browser flicker"). 3. Tryk på sidens link / knap til single logout. 4. Kontrollér at bekræftelsesside for single logout vises (evt. skal det bekræftes i en dialog, at man ønsker SLO). Bekræftelsessiden skal indeholde en vejledende tekst til brugeren om at denne skal huske at lukke browservinduet for at sikre korrekt logud. 5. Indtast URL på SP-beskyttet-side-1 i browseren. 6. Kontrollér at siden ikke vises, men at IdP'ens loginside i stedet fremkommer. Dette betyder, at såvel SP'ens som IdP'ens sessioner er nedlagte.
Slutbetingelser	• SP session nedlagt • IdP session nedlagt
Varianter	

Navn	IT-SLO-3
Beskrivelse	Brugeren vælger single logout fra en *anden* tjenesteudbyder, mens sessionen hos den lokale SP er timet ud. Dette tester, at tjenesteudbyderen kan håndtere logoutrequests fra IdP'en på en lokal session, som er timet ud. OBS: Testcasen kan fraviges, hvis tjenesteudbyderen ikke opretter en lokal session i sin applikation. Trin 6 i testcasen kan overspringes, hvis tjenesteudbyderen anvender SOAP logout mekanismen (SAML SOAP Binding), idet der så ikke kommunikeres logout-beskeder via brugerens browser men i stedet direkte system-til-system.
Startbetingelser	

Navn	IT-SLO-3
Trin	1. Log på den lokale SP ved at indtaste URL på SP-beskyttet-side-1 i browseren og foretag log-in via IdP. 2. Vent 15 minutter og log på en af de andre SP-sider i testmiljøet f.eks. ved indtaste URL'en på IdP-SP-side-1 i browseren. 3. Vent yderligere 20 minutter så sessionen hos den første / lokale SP-side er timet ud (SP-beskyttet-side-1), hvilket skal ske efter 30 minutters samlet inaktivitet (nu skulle der være gået mindst 15 + 20 minutter). 4. Start et program som optager browserens HTTP trafik som eksempelvis Fiddler, Firefox Tamperdata eller en HTTP proxy. 5. Klik på single logout på den anden SP-side (IdP-SP-side-1) og kontroller, at der hverken kommer fejlmeddelelser på skærmen eller i loggen. 6. Tjek HTTP trace og kontrollér, at der svares med et SAML <LogoutResponse> fra den lokale SP (SP-beskyttet-side-1) til IdP'en.
Slutbetingelser	• Session hos lokal SP er timet ud. • Session hos fremmed SP er logget ud. • IdP session nedlagt
Varianter	Værdien for lokal timeout af session kan nedsættes til en kortere periode inden afvikling af test cases, så man ikke skal vente så lang tid.

Navn	IT-LOA-1
Beskrivelse	Brugeren tilgår en beskyttet ressource hos tjenesteudbyderen og er autentificeret med et for lavt NSIS sikringsniveau. Adgang afvises hos tjenesten. Varianter: med og uden eksisterende session. Bemærk: denne test case er ikke relevant for tjenesteudbydere, som accepterer alle NSIS sikringsniveauer inkl. sikringsniveau Lav. Bemærk at det med MitID er muligt at logge ind med sikringsniveau Lav.
Startbetingelser	• Ingen IdP session er oprettet. • Ingen SP session er oprettet.
Trin	1. Indtast URL på SP-beskyttet-side-3 i browseren, som kræver NSIS sikringsniveau Høj. 2. Log ind hos IdP'en med et identifikationsmiddel, som er på NSIS Lav eller Betydelig. 3. Kontrollér at SP'en viser fejlside om for lavt sikringsniveau og evt. re-direct'er til ny IdP login.
Slutbetingelser	• Der er oprettet en IdP session for brugeren med sikringsniveau Lav eller Betydelig. • Adgang til den beskyttede side er ikke givet, og der er vist en fejlmeddelelse med for lavt sikringsniveau.
Varianter	

Navn	IT-TIM-1
Beskrivelse	Brugeren søger at få adgang med en assertion, der er udløbet. Adgangen gives ikke.
Startbetingelser	• Ingen SP session • Ingen IdP session
Trin	1. Indtast URL på SP-beskyttet-side-1 i browseren. 2. Når login klienten fremkommer, aktiveres tamper data plug-in i Firefox (se beskrivelse af dette plugin i forrige kapitel). Tamper data plug-in vil nu prompte hver gang, der sendes et http request fra browseren til serveren. 3. Log-in med med den valgte bruger. 4. Tryk "Ok" i tamper data indtil det tidspunkt, hvor IdP'en vil sende den udstedte SAML assertion tilbage til SP'en. Dette kan detekteres ved, at URL peger på tjenestens domæne (i eksemplet nedenfor skat.dk) og at der optræder en SAMLResponse parameter. Herefter ventes 61 minutter med at trykke "submit", idet levetid på en assertion er 60 minutter. Nedenfor vises et eksempel på, hvordan skærmbilledet kunne se ud, når SP'en er en af test SP'erne i testmiljøet:  5. Kontrollér at SP'en giver en passende fejlmeddelelse om udløbet assertion, og at adgang til den beskyttede side ikke gives.
Slutbetingelser	• Adgang er afvist, og der er givet en passende fejlmeddelelse.
Varianter	

Navn	IT-TIM-2 (kun offentlige tjenester)
Beskrivelse	Brugeren tilgår en beskyttet ressource hos tjenesteudbyderen efter hans session er timet ud. Derimod er hans IdP session stadig aktiv.
Startbetingelser	• IdP session aktiv
Trin	1. Konfigurér SP'ens IT til 2 minutter. 2. Indtast URL på SP-beskyttet-side-1 i browseren. 3. Kontrollér at SP-beskyttet-side-1 vises i browseren 4. Vent 3 minutter og indtast på ny URL på SP-beskyttet-side-1 i browseren. 5. Kontrollér at siden atter vises uden at brugeren er blevet bedt om at logge på (dvs. SP sessionen er fornyet).
Slutbetingelser	• Brugeren har fået adgang til den beskyttede side uden at logge ind. • SP sessionen er fornyet via en ny assertion fra IdP'en.
Varianter	

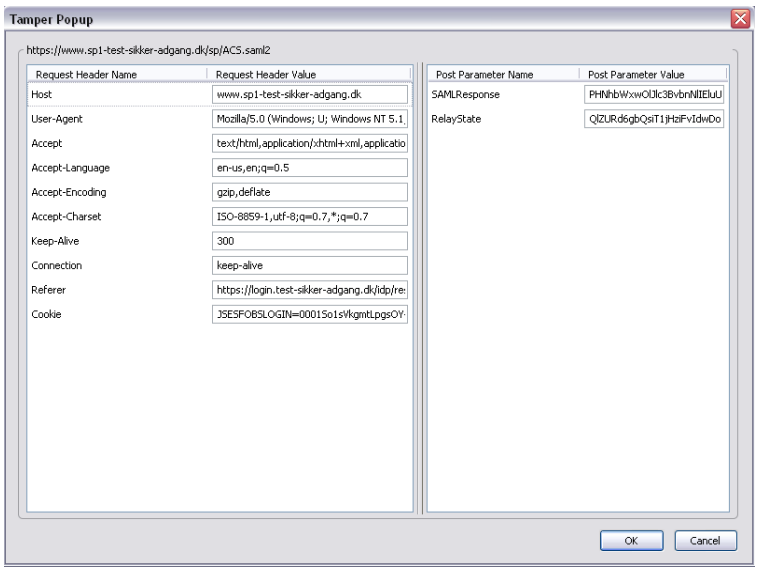
Navn	IT-LOG-1
Beskrivelse	Tester udvalgte aspekter af logningspolitik hos tjenesteudbyder. Nedenstående er en stikprøvekontrol, som ikke garanterer, at alle aspekter af NemLog-in's logningspolitik overholdes. For detaljer om logningspolitikken henvises til [LOGPOL].
Startbetingelser	• Brugeren er logget på og har fået adgang til en beskyttet ressource. Kan etableres ved at udføre IT-LOGON-1.
Trin	Inspicér logfilerne i tjenesteudbyderens systemer og kontrollér at flg. data er til stede, og at logningerne er forsynet med korrekt tidsangivelse: 1. ID på SAML <AuthnResponse> fra NemLog-in 2. Sikringsniveau angivet i Assertion 3. ID på request der svares på (fra InResponseTo) 4. Resultat af validering af <Response> meddelelse og <Assertion> (herunder signaturvalidering) 5. Bruger ID fra assertion (dvs. Subject NameID fra assertion) 6. Evt. identifikation af den interne brugerkonto (hvis nogen) som relateres til SAML assertionen. 7. Rettigheder og/eller fuldmagtsprivilegier indeholdt i Assertion. Unikt ID på lokal session, som dannes på baggrund af autentifikationssvaret.
Slutbetingelser	• Ovenstående data er logget
Varianter	

Navn	IT-USER-1
Beskrivelse	Brugeren er ikke kendt hos tjenesteudbyderen. OBS: Bemærk at test casen kan overspringes tjenesteudbydere, som accepterer alle borgere, som oversætter eksterne brugere til en generisk, intern brugerkonto, eller som starter et brugeroprettelsesforløb, hvis brugeren er ukendt.
Startbetingelser	• Ingen session med tjenesteudbyder eller IdP (kan etableres ved at genstarte browseren).
Trin	1. Indtast URL på SP-beskyttet-side-1 i browseren. 2. På IdP'ens loginside logges på med NemID eller MitID hørende til en testbruger, der ikke har adgang til SP-beskyttet-side-1 i tjenesteudbyderens miljø. 3. Kontroller at tjenesteudbyderen giver en sigende fejlmeddelelse, og at brugeren ikke får adgang til den beskyttede side – alternativt at der startes et brugeroprettelsesforløb for nye brugere. 4. Kontrollér at fejlen er logget i tjenesteudbyderens systemer.
Slutbetingelser	• Brugeren har ikke fået adgang til den beskyttede side. • Der er vist en sigende fejlmeddelelse til brugeren.
Varianter	Testen kan varieres med forskellige typer af ukendte brugere, herunder borgere og medarbejdere.

Navn	IT-ATTQ-1
Beskrivelse	Tester attributforespørgsler hos IdP (SAML AttributeQuery). OBS: Test casen er kun relevant for tjenesteudbydere, der anvender AttributeQuery funktionaliteten i NemLog-in.
Startbetingelser	• Brugeren har en session med tjenesteudbyder og Identity Provider. Kan etableres ved at udføre IT-LOGON-1
Trin	1. Indtast URL på SP-hent-attributter-side-1. 2. Aktivér knap eller link som igangsætter attributforespørgsel. 3. Observér at attributter vises korrekt i browservinduet.
Slutbetingelser	• Der er afsendt en attributforespørgsel mod Identity Provideren. • Brugerens attributter er vist i browservinduet.
Varianter	Forskellige varianter af attributforespørgsler kan konstrueres herunder hentning af navngivne attributter, alle attributter (tom query string) eller forsøg på adgang til attributter, som den pågældende tjenesteudbyder ikke er autoriseret til.

Navn	IT-FORCE-1
Beskrivelse	Tester tvungen brug af autentifikation hos IdP (ForceAuthn attribut er sat). OBS: Test casen er kun relevant for tjenesteudbydere, der anvender ForceAuthn funktionaliteten på login-anmodninger til NemLog-in.
Startbetingelser	• Brugeren har en session med tjenesteudbyder og Identity Provider. Kan etableres ved at udføre IT-LOGON-1
Trin	1. Indtast URL på siden SP-force-authn-side-1. 2. Klik på knappen / linket som aktiverer gen-autentifikationen. 3. Observér at IdP'ens loginside fremkommer.
Slutbetingelser	• Brugeren er blevet genautentificeret.
Varianter	Kan evt. testes med gen-autentifikation, hvor NSIS sikringsniveau'et skiftes i forhold til den eksisterende session.

Navn	IT-REPL-1
Beskrivelse	Der forsøges replay af svar fra IdP'en. OBS: Test case er skrevet med udgangspunkt i, af Tamper Data plug-in anvendes. Hvis der anvendes et andet værktøj, skal testhandlingerne tilpasses dette.
Startbetingelser	Ingen (etableres under testen).
Trin	1. Indtast URL på SP-beskyttet-side-1. 2. Når login applet'en fremkommer aktiveres "tamper data" plug-in i firefox (se beskrivelse i forrige kapitel). 3. Indtast password til identifikationsmiddel og tryk ok. 4. Tamper data plug-in vil nu prompte hver gang, der sendes et http request fra browseren til serveren. 5. Tryk på "submit" i tamper data indtil det punkt, hvor svaret sendes tilbage til SP'en (det er ca. 5 gange). Dette kan identificeres ved at se på den URL, som IdP'en vil poste til. 6. Tryk på "tamper" for det request, der skal til at sendes til SP'en. Dette skulle gerne resultere i et skærmbillede som følger:

Navn	IT-REPL-1
	 7. I det fremkomne vindue kopieres værdien af ”SAMLResponse” parameteren til en editor. Tryk ”ok” for at sende sende svaret til SP’en. 8. Luk browseren og gentag trin 1-6. 9. Kopier værdien af den gamle SAMLResponse parameter over i den nye værdi af parameteren og tryk på ”ok” knappen for at sende det til SP’en. 10. Observér at svaret afvises hos tjenesteudbyder med en sigende fejlmeddelelse.
Slutbetingelser	• Svaret fra IdP’en er afvist af tjenesteudbyder som et ”replay”, og der er vist en sigende fejlmeddelelse.
Varianter	I stedet for at gensende hele svaret kan man vælge at modificere det nye svar, så kun assertion byttes ud (er dog valgfrit for tjenesteudbyderne). Dette vil teste, at SP-implementationen ikke blot detekterer et replay ud fra ID felter i protokollen (f.eks. InReponseTo), men at selve assertion også kun kan bruges én gang: • Først skal SAMLResponse parameteren URL dekodes. Dette kan eksempelvis gøres via værktøjet http://meyerweb.com/eric/tools/dencoder/ • Dernæst skal den resulterende værdi base 64 dekodes. Dette kan gøres via værktøjet: http://www.motobit.com/util/base64-decoder-encoder.asp • Nu fremkommer SAML response meddelelsen i klar tekst. Her udskiftes indholdet af elementet <saml:EncryptedAssertion> i det nye svar med samme element fra det gamle svar. • Herefter skal det modificerede svar base64 indkodes og dernæst URL indkodes (igen via de ovennævnte værktøjer). • Den resulterende værdi indsættes nu via tamper data i SAMLResponse parameteren og sendes tilbage til SP’en ved at trykke på ”ok” knappen. • Herefter bør svaret afvises af SP’en idet assertion er modtaget tidligere.

I nedenstående test cases beskrives test med privilegier. Dette kan være almindelige privilegier, som kan tildeles medarbejdere på vegne af en virksomhed, eller fuldmagtsprivilegier, der udtrykker borgerfuldmagter. Der bør testes individuelt med alle privilegier, som løsningen understøtter (dog kun relevant for offentlige

tjenester). I test case beskrivelserne nedenfor skal termen ”privilegie” opfattes som en samlebetegnelse for både almindelige privilegier og fuldmagtsprivilegier.

Navn	IT-PRIV-1 (kun offentlige tjenester)
Beskrivelse	Brugeren tilgår en beskyttet web-side hos tjenesteudbyder, der kræver et eller flere privilegier for adgang. Browseren re-directes til NemLog-in's Identity Provider, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen. OBS: Test casen er kun relevant for tjenesteudbydere, der anvender privilegier i NemLog-in.
Startbetingelser	• Ingen IdP session • Ingen SP session • Brugeren er tildelt det eller de privilegier, som kræves for adgang til løsningen. Sessioner kan nulstilles ved at slette alle cookies i browseren og genstarte denne.
Trin	1. Indtast URL på SP-beskyttet-side-4 i browseren. 2. Kontrollér at IdP'ens loginside fremkommer. 3. Foretag log-in med den testbruger, der er tildelt de privilegier, der giver adgang til SP-beskyttet-side-4. 4. Kontrollér at SP-beskyttet-side-4 fremvises. 5. Kontrollér at session er oprettet hos tjenesteudbyder.
Slutbetingelser	• SP-beskyttet-side-4 er vist • Session oprettet hos IdP • Session oprettet hos tjenesteudbyder
Varianter	• Ved test af fuldmagtsprivilegier bør man afprøve log-in med både borger- og medarbejdercertifikater (i egenskaben fuldmagtshaver). Dette skyldes, at fuldmagter altid kan gives både til borgere og medarbejdere, og derfor skal tjenesteudbydernes løsning kunne håndtere, at begge typer forsøger at anvende en fuldmagt.

Navn	IT-PRIV-2 (kun offentlige tjenester)
Beskrivelse	Brugeren tilgår en beskyttet web-side hos tjenesteudbyder, der kræver et eller flere privilegier for adgang. Browseren re-directes til NemLog-in's Identity Provider, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og bliver afvist adgang på grund af manglende privilegier. OBS: Test casen er kun relevant for tjenesteudbydere, der anvender privilegier i NemLog-in.
Startbetingelser	• Ingen IdP session • Ingen SP session • Brugeren er IKKE tildelt de privilegier, som kræves for adgang til løsningen. Sessioner kan nulstilles ved at slette alle cookies i browseren og genstarte denne.
Trin	1. Indtast URL på SP-beskyttet-side-4 i browseren. 2. Kontrollér at IdP'ens log-in-side fremkommer. 3. Foretag log-in med en testbruger, der IKKE er tildelt de privilegier, der giver adgang til SP-beskyttet-side-4. 4. Kontrollér at adgang til SP-beskyttet-side-4 ikke opnås, og at der gives en passende fejlmeddelelse.
Slutbetingelser	• Adgang til SP-beskyttet-side-4 er ikke opnået • Session oprettet hos IdP • Session oprettet hos tjenesteudbyder
Varianter	

Navn	IT-PRIV-3 (kun offentlige tjenester)
Beskrivelse	Brugeren tilgår en beskyttet web-side hos tjenesteudbyder, der kræver et eller flere privilegier for adgang. Browseren re-directes til NemLog-in's Identity Provider, hvor brugeren foretager log-in, hvorefter brugeren sendes tilbage og får adgang til den ønskede side hos tjenesteudbyderen. OBS: Test casen er kun relevant for tjenesteudbydere, der anvender privilegier i NemLog-in.
Startbetingelser	• Ingen IdP session • Ingen SP session • Brugeren er tildelt det eller de privilegier, som kræves for adgang til løsningen. ***Privilegierne er tildelt ved en delegering fra en anden organisation (f.eks. med scope af et andet CVR-nummer end den organisation, brugeren selv hører til).*** • Sessioner kan nulstilles ved at slette alle cookies i browseren og genstarte denne.
Trin	1. Indtast URL på SP-beskyttet-side-4 i browseren. 2. Kontrollér at IdP'ens loginside fremkommer. 3. Foretag log-in med den testbruger, der er tildelt de privilegier, der giver adgang til SP-beskyttet-side-4. 4. Kontrollér at SP-beskyttet-side-4 fremvises. 5. Kontrollér at session er oprettet hos tjenesteudbyder.
Slutbetingelser	• SP-beskyttet-side-4 er vist • Session oprettet hos IdP • Session oprettet hos tjenesteudbyder
Varianter	

Navn	IT-SIGN-1
Beskrivelse	Brugeren anvender en funktion hos tjenesteudbyderen, der benytter signeringstjenesten (f.eks. en indberetning). Browseren re-dirigeres til signeringstjenesten, hvor brugeren underskriver med sit NemID eller MitID. Herefter re-dirigeres browseren tilbage til tjenesteudbyderen, hvor arbejdsgangen fortsætter. Bemærk: test case er kun relevant for tjenesteudbydere, der anvender signering.
Startbetingelser	• Bruger er logget på tjenesteudbyder (f.eks. ved at gennemføre test case IT-LOGON-1)**.**
Trin	1. Tilgå side/funktion hos tjenesteudbyder, som kræver underskrift. 2. Kontrollér at browseren re-dirigeres til signeringstjenesten. 3. Afgiv signatur med NemID eller MitID. 4. Kontrollér at browseren re-dirigeres tilbage til tjenesteudbyderen, og at arbejdsgangen, som krævede underskrift, kan fortsættes. 5. Kontrollér at tjenesteudbyderens applikation har logget signeringssvaret fra signeringstjenesten i overensstemmelse med logningspolitikken. Dette trin kræver opslag i log-filer fra en systemadministrator eller anden person med adgang til loggen.

Navn	IT-SIGN-1
Slutbetingelser	• Brugeren har underskrevet dokument og kan fortsætte arbejdsgangen, der krævede underskrift. • Tjenesteudbyder har logget signaturbeviset modtaget fra signeringstjenesten.
Varianter	

12 Referencer

[OIO-SAML] ”OIOSAML Web SSO Profile V3.0.3”, Digitaliseringsstyrelsen.

https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

[MAN] ”Brugermanual til NemLog-in Administration”, Digitaliseringsstyrelsen.
https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/brugermanual-til-nemlog-in-administration/

[LOGPOL] ”Logningspolitik for tjenesteudbydere tilsluttet NemLog-in”

https://www.nemlog-in.dk/tu/krav/logningspolitik

13 Øvrige relevante dokumenter og links

NemLog-in driftsgruppen på digitaliser.dk

http://digitaliser.dk/group/2354775

NemLog-in supportgruppen på digitaliser.dk

http://digitaliser.dk/group/25501855

OISOSAML gruppen på digitaliser.dk

https://www.digitaliser.dk/group/42063

Digitaliseringsstyrelsens web-side om NemLog-in:

https://digst.dk/it-loesninger/nemlog-in/