DIGITALISERINGSSTYRELSEN

NemLog-in

Vejledning til NemLog-ins Security Token Service

Indholdsfortegnelse

Ændringslog

Dato	Version	Ændringsbeskrivelse	Initialer
23.11.2021	1.0	Formatering af guide samt teksttilpasninger	TG/LEASA

1 Om denne guide

Denne guide indeholder en kort beskrivelse af, hvordan en offentlig tjenesteudbyder eller dennes it-leverandør kan benytte NemLog-in's Security Token Service (STS) komponent. Guiden er henvendt til it-arkitekter, udviklere og andre, der skal planlægge, hvorledes komponenten kan bruges i en digital selvbetjeningsløsning. Det forudsættes, at læseren har kendskab til NemLog-in løsningen.

Der henvises til NemLog-in supportsite www.tu.nemlog-in.dk for øvrige vejledninger og dokumentation.

2 Baggrund

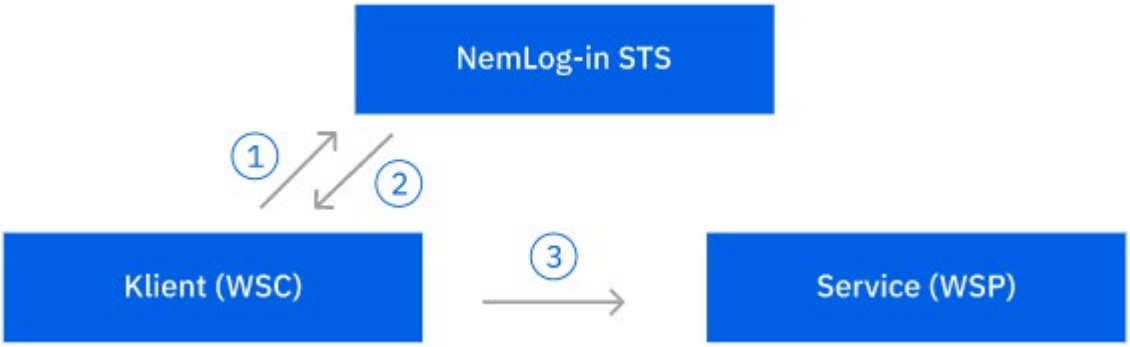
NemLog-in er udviklet i regi af Digitaliseringsstyrelsen og består af en række forskellige komponenter, der tilsammen udgør den fællesoffentlige brugerstyringsløsning. Løsningen blev oprindeligt etableret i 2008 og kører i dag i tredje generation med mere end 300 it-systemer tilsluttet.

I foråret 2014 blev NemLog-in's Security Token Service sat i drift. Denne løsning gør det muligt at foretage adgangsstyring til web services ved brug af såkaldte security tokens.

3 Grundscenarie

Den oprindelige NemLog-in løsning understøtter adgang til browser-baserede applikationer for personbrugere. Med introduktionen af NemLog-in's Security Token Service (STS) komponent er det nu også muligt at understøtte adgangsstyring til web services – baseret på udstedelse, præsentation og validering af security tokens (SAML Assertions).

Grundscenariet illustreret:



De er tre aktører i spil på figuren:

- En Web Service Provider (WSP) er det system, der udstiller en web service, som skal beskyttes.
- En Web Service Consumer (WSC) er det system / klient, som ønsker at kalde web servicen.
- NemLog-in's Security Token Service udsteder et security token (SAML Assertion) til WSC'en.

Som vist på figuren kalder WSC'en først NemLog-in for at få udstedt et security token (trin 1+2). Dette token medsendes herefter i servicekaldet til WSP'en (trin 3), som validerer tokenet, og giver adgang på baggrund af dets indhold.

Snitfladen til NemLog-in's Security Token Service er baseret på en dansk profil af WS-Trust protokollen (se [OIO-TRUST]). Her er anmodningen om tokenet (trin 1) specificeret i form af en `<RequestSecurityToken>`-besked og svaret som en `<RequestSecurityTokenResponse>`-besked.

Både WSP og WSC skal på forhånd være tilsluttet NemLog-in[1], og der er herved indgået et tillidsforhold (i form af en aftale) samt udvekslet certifikater mv. til brug for efterfølgende autentifikation. Ved at følge mønstret ovenfor opnås en arkitekturmæssig dekobling mellem WSC og WSP, så en WSP ikke behøver kende alle anvenderne af dens service (WSC'er), og så WSC'er får en ensartet måde at tilgå beskyttede web services. WSP'en skal således blot validere, at det modtagne token er digitalt underskrevet af NemLog-in's STS, samt at tokenet i øvrigt er gyldigt.

[1] Med undtagelse af WSC'er i signature case.

4 Introduktion til identitetsbaserede web services

NemLog-in's STS kan fungere på forskellige måder og indgå i en række forskellige scenarier. Fælles for dem alle er, at der tale om såkaldt "identitetsbaserede web services". Med dette menes, at WSC'en får udstedt et token til at agere på vegne af en personbruger – således at det efterfølgende web service kald sker i kontekst af denne brugers identitet samt evt. rettigheder. Dette er altså i modsætning til "systembrugerparadigmet", hvor systemer i sig selv er tildelt en adgang til en web service, der er uafhængig af personbrugere.

Et klassisk eksempel på brug af identitetsbaserede web services findes i scenarier, hvor en bruger logger på en portal, og portalen har brug for at hente brugerens data hos en ekstern web service. Her kan portalen som WSC få udstedt et token til at tilgå servicen og hente brugerens data – men tokenet gælder kun den pågældende personbruger. Hvis brugeren ikke var logget ind i portalen, har portalen ikke adgang til de pågældende data, så adgangen opnås altså i kraft af brugeren. Adgangen på vegne af en bruger benævnes nogen gange for "ActAs" for at tydeliggøre, at servicekaldet sker på vegne af en bruger.

NemLog-in understøtter pt. tre forskellige scenarier med identitetsbaserede web services:

- Bootstrap token case
- Signature case
- Local token case (udfaset med NemLog-in3)

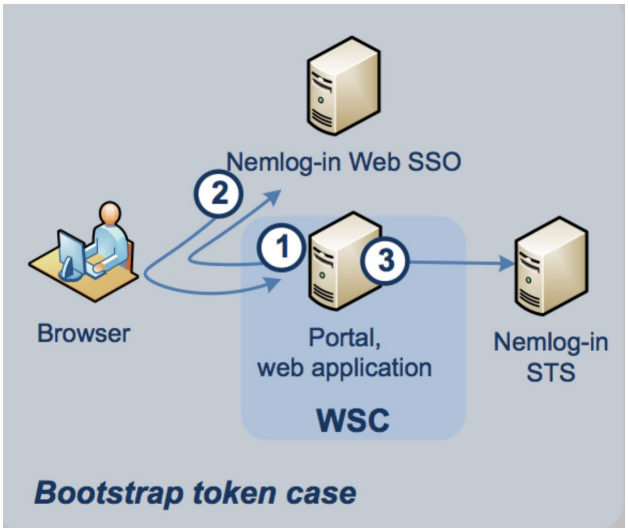
Den primære forskel mellem disse ligger i, hvordan WSC'en autentificerer sig mod NemLog-in's STS, samt hvordan brugerens identitet er fastslået. De tre scenarier gennemgås nedenfor.

4.1 Bootstrap token case

Det første scenarie dækker det klassiske behov i portaler. Det kan generelt benyttes af web løsninger, hvor brugeren er logget ind via NemLog-in Web SSO, og hvor der efterfølgende er behov for at kalde en ekstern, identitetsbaseret web service.

Ved tilslutning af en web løsning til NemLog-in kan det angives, at løsningen har brug for at kalde identitetsbaserede web services. Herved vil NemLog-in's Identity Provider indlejre et såkaldt "bootstrap token" i den SAML Assertion, der udstedes, når brugeren logger på løsningen via sin browser. Boostrap tokenet er en alm. SAML attribut indeholdende en base64-indkodet værdi. Web løsningen kan herefter udtage dette bootstrap token, veksle det i NemLog-in's STS (input til RequestSecurityToken besked), og modtage et nyt token (identity token), som til sidst kan anvendes mod web servicen.

Princippet er illustreret på nedenstående figur:

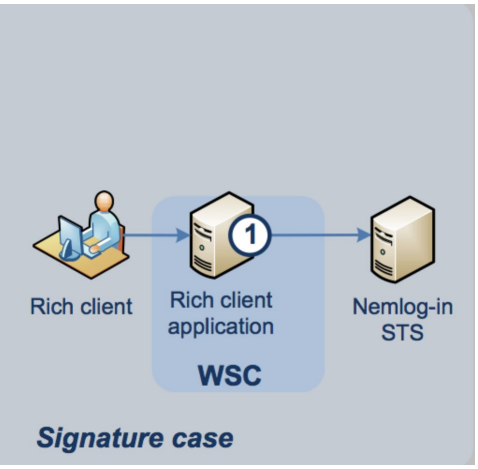


I scenariet sikres, at WSC'en kun kan få tokens udstedt af NemLog-in, når den har brugeren logget ind. Derudover kan en WSP under registrering hos NemLog-in indikere, at NemLog-in's STS skal kommunikere med NemLog-in IdP'en og kun udstede tokenet, hvis brugeren på det aktuelle tidspunkt har en gyldig session med IdP'en.

4.2 Signature case

Det næste scenarie anvendes typisk i forbindelse med "rige" klienter, hvor brugeren er logget ind i klienten uden om NemLog-in. I denne situation har klienten ikke noget bootstrap token, som beviser at brugeren er logget. I stedet kan klienten anmode NemLog-in's STS om et token mod en ekstern web service - og bede brugeren signere servicekaldet (inkl. tidsstempel) med sin digitale signatur (heraf navnet på scenariet). På den måde sikres, at klienten kun kan få udstedt tokens med brugerens aktive medvirken.

Scenariet er illustreret på nedenstående figur:



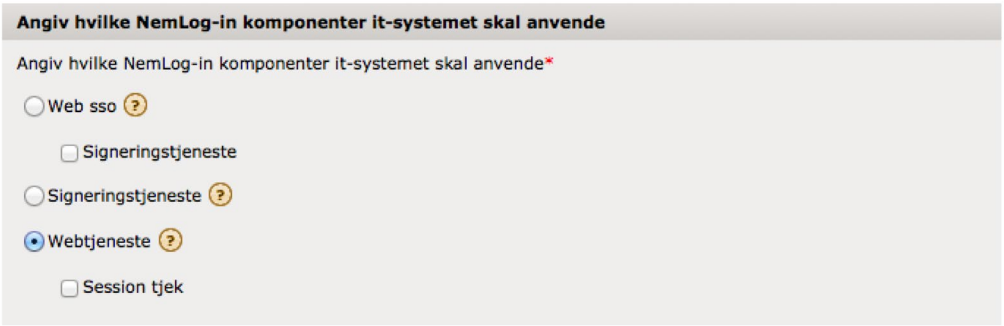
4.3 Local token case

Den sidste variant er "local token case", som er udfaset i NemLog-in3, da den ikke har været anvendt i praksis. Varianten er nævnt for komplethedens skyld, da den er beskrevet i tidligere materiale.

5 Tilslutning til NemLog-in's STS

Tilslutning og administration af WSC'er og WSP'er sker via NemLog-in Administrationen[2]. Manualen for administrationssystemet [ADM-MAN] forklarer processen med tilslutning, men herunder gives et overblik over de væsentligste scenarier for tilslutning.

Type af system	Tilslutning
WSC, bootstrap token case	Løsningen skal i første omgang tilsluttes som Web SSO løsning og skal i sine metadata angive en særlig attribut[3], der indikerer, at bootstrap token ønskes udstedt i SAML tokenet.
WSC, signature case	Alle systemer har adgang til at kalde NemLog-in's STS som signature case, og dette kræver derfor ikke forudgående registrering af WSC'en i NemLog-in.
WSP	En WSP tilsluttes NemLog-in som en "Webtjeneste" (se figur nedenfor). Efter systemet er oprettet, skal der uploades en XML fil med metadata, der beskriver hvilke attributter, WSP'en ønsker at modtage i det udstedte SAML token. I manualen for administrationssystemet [ADM-MAN] afsnit 4.4 findes et eksempel på formatet for metadatafilen, der er en variant af SAML metadata formatet. Bemærk at en WSP skal tage stilling til, om man ønsker tokens udstedt fra NemLog-in, hvor Subject er et X509SubjectName eller et persistent pseudonym.



Figur 1: Tilslutning af en Web Service Provider i administrationssystemet

Ved afkrydsning af "Session tjek" i ovenstående skærmbillede, vil STS'en som nævnt kontakte IdP'en og kun udstede tokenet til WSP'en, hvis brugeren har en aktuel session med IdP'en.

[2] https://administration.nemlog-in.dk

[3] https://data.gov.dk/model/core/eid/bootstrapToken i OIOSAML 3

6 Regler ved udstedelse af tokens

NemLog-in's STS foretager en lang række valideringer og opslag i forbindelse med udstedelse af security tokens. Herunder er fremhævet de vigtigste forhold, som kan være nyttige at kende for en WSC samt WSP til planlægningsformål.

6.1 Generelle forhold vedr. NemLog-in's STS:

- De tre scenarier ("boostrap case", "local token case" og "signature case") benytter hvert sit entityID, som angives eksplicit i WSC'ens request.
- Tokens udsteds til en specific WSP, som WSC'en angiver i sit request (via `<wst:AppliesTo>` elementet).
- SOAP-kaldet fra WSC'en skal signeres (både headere og `<body>`).
- Attributter i tokens udstedes i henhold til WSP'ens metadatafil (som angiver de ønskede attributter), og `<wst:Claims>` elementet i det indgående WS-Trust kald ignoreres derfor. Bemærk at WSP'en først i løbet af 2022 vil være i stand til at udstede tokens med OIOSAML 3 attributter, og at WSP metadatafiler derfor indtil videre må angive OIOSAML 2 attributter.
- Der understøttes både OCES attributprofilen og persistente pseudonymer i udstedte token (se OIOSAML for detaljer).
- NemLog-in henter privilegier fra FBRS og indlejrer dem i tokenet, hvis den pågældende bruger har privilegier til WSP'en.
- De udstedte identity tokens er konfigureret til at have en gyldighed på 8 timer fra udstedelsestidspunktet.

6.2 Boostrap token case:

- Anmodningen fra WSC til NemLog-in's STS skal signeres med det samme certifikat, som benyttes til Web SSO interaktion med NemLog-in's IdP.
- Tokenet fra STS'en vil blive udstedt som et "holder-of-key" token, således at WSC'en skal signere web servicekaldet mod WSP'en med samme certifikat/nøgle.

6.3 Signature case:

Brugeren skal underskrive med et medarbejdercertifikat, hvis CVR nummer svarer til en kendt / registreret brugerorganisation i NemLog-in.

7 Yderligere dokumentation

Leverandørens dokumentation af NemLog-in STS'en findes på tu.nemlog-in.dk. Heri findes XML eksempler på request / response beskeder, processeringsregler mv.

8 Snitflader og test

På NemLog-in's support-site (www.tu.nemlog-in.dk) findes vejledning, som beskriver snitflader, endpoints, bindings, fejlkoder mm. mod NemLog-in's STS i henholdsvis integrations- og produktionsmiljøerne. Dokumentet beskriver endvidere de testfaciliteter, der er tilgængelige i integrationstestmiljøet.

9 Referencer

[OIO-SAML] ”OIO Web SSO Profile V3.0”, Digitaliseringsstyrelsen.

https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/

[OIO-BPP] ”OIO Basic Privilege Profile”, Digitaliseringsstyrelsen.
https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/

[OIO-TRUST] ”OIO WS-Trust Profile”, Digitaliseringsstyrelsen.
https://www.digitaliser.dk/resource/5988041

[IDWS] ”OIO Identity-based web services”, Digitaliseringsstyrelsen.
https://www.digitaliser.dk/resource/5988041

[ADM-MAN] **Brugermanual til NemLog-in Administration**

Henvender sig til Teknisk administrator, Administrator for it-systemudbyder og Administrator for it-leverandør.

Åbn manual: https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/brugermanual-til-nemlog-in-administration/