DIGITALISERINGSSTYRELSEN

NemLog-in

Logningspolitik for tjenesteudbydere tilsluttet NemLog-in

Version 1.4

Indholdsfortegnelse

1 Dokumenthistorik

Date	Version	Change description	Initials
12-09-2008	1.0	• Referencer opdateret; versionsnummer sat til 1.0. Følgende logningsregler er opdateret: • Under SLO4 er tilføjet ID på bruger, som logges ud. • Under BSA6 er det præciseret at ID på Identity Provider er Issuer fra Assertion, og bruger ID er Subject NameID fra Assertion. I BSA1 er tilføjet ID på request og under BSA6 er der tilføjet ID på det request, der svares på.	TG
17-09-2008	1.0.1	• Opdateret med nye kommentarer. • Referencer til integrationsguide er indført. • Formålet med logningen er udbygget. • Krav til tidssynkronisering er blevet præciseret. • Afsnit om persondatalov er opdateret. Afsnit om kryptering af data er fjernet.	TG
21-12-2012	1.2	• Opdateret til Digitaliseringsstyrelsens dokumentlayout. • Referencer opdateret. • Krav til logning af privilegier beskrevet. • Opdateret beskrivelser af dataansvar.	TG
11-02-2013	1.3	Opdateret logningskrav til at omfatte hele <SignatureProof> elementet som følge af interne designændringer (EMC Centera).	TG
17-09-2021	1.4	Omskrevet og simplificeret, så politikken kun gælder tjenesteudbydere, da NemLog-in's egen log er håndteret gennem kontraktkrav.	TG

2 Formål og afgrænsning

Formålet med denne politik er at beskrive krav til den logning, der skal udføres hos tjenesteudbydere, der anvender NemLog-in3. Politikken udgør et bilag til de tekniske krav til tjenesteudbydere, der videre indgår i vilkår for private tjenesteudbydere [VIL] samt bekendtgørelse for offentlige tjenesteudbydere [BKG].

Politikken er henvendt til tekniske personer hos tjenesteudbydere, der skal konfigurere logning i selvbetjeningsløsninger, der er tilsluttet NemLog-in. Det forudsættes, at læseren er bekendt med de tekniske snitflader til NemLog-in3 herunder [OIOSAML].

Kravene i logningspolitikken har til formål at sikre:

- At tjenesteudbyderes roller og ansvar for logning er veldefinerede.
- At oplysninger relevante for sporbarhed og sikkerhed er tilgængelige i logs, herunder at efterforskningsmæssige hensyn tilgodeses. Dette indebærer eksempelvis at hændelsesforløb på tværs af NemLog-in og tjenesteudbydere kan følges, hvis de relevante logninger stilles til rådighed for efterforskning.
- At der sikres konsistens på tværs af NemLog-in's føderation med hensyn til logning.

Derimod stiller logningspolitikken *ikke* krav til logning af oplysninger om, hvad en bruger har foretaget sig i tjenesteudbyderes selvbetjeningsløsninger.

En tjenesteudbyder kan desuden have egne forretningshov eller være underlagt regulering, som afføder behov for yderligere logning end hvad denne politik tilsiger.

2.1 Afgrænsning

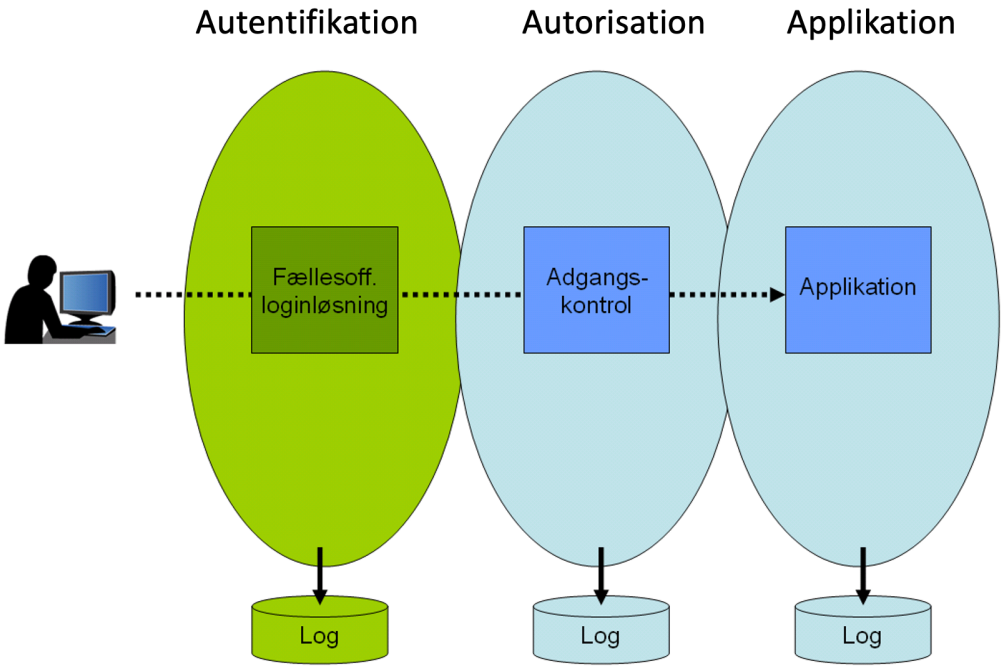
Politikken afgrænser sig til de funktionelle områder, der er relevante for interaktionen med NemLog-in, herunder:

- Autentifikation af brugere.
- Brugeres rettigheder og fuldmagter (for offentlige tjenesteudbydere).
- Signering af dokumenter via NemLog-in's signeringstjeneste.
- Forespørgsler på attributter for brugere.

Der behandles således *ikke* logningsforhold vedrørende:

- Forretningsapplikationer (selvbetjeningsløsninger).
- Adgangskontrolsystemer der på baggrund af brugerens identitet og medsendte rettigheder foretager autorisationsbeslutninger i forretningsapplikationer.

Afgrænsningen er illustreret på nedenstående figur, hvor nærværende politik adresserer den med grønt markerede log, mens de øvrige logs ikke er omfattet af denne politik:



3 Organisatoriske krav

Ved tiltrædelse af NemLog-in's vilkår forpligter private tjenesteudbydere sig til at overholde denne logningspolitik; for offentlige tjenesteudbydere følger forpligtelsen til at overholde logningspolitikken af '*Bekendtgørelse om offentlige myndigheders og offentligretlige organers anvendelse af MitID-løsningen og NemLog-in' [BKG].*

Tjenesteudbyderen skal etablere, dokumentere, vedligholde og efterleve procedurer indenfor flg. områder:

- Personoplysninger i logs skal håndteres i overensstemmelse med databeskyttelsesreguleringen.
- Der skal etableres en procedure for, hvilke handlinger der skal udføres, såfremt logningerne indikerer sikkerhedsbrud, herunder om og hvornår eksterne parter (som f.eks. politiet) involveres.
- Der skal etableres en procedure for adgang til logdata, som sikrer integritet og autenticitet af disse.
- Der skal tages periodisk backup af logdata, så tilgængeligheden sikres.
- Der skal etableres sletteprocedurer som sikrer, at logdata slettes, når de ikke længere er relevante.
- Log-systemets driftsstatus skal overvåges, så eksempelvis forstyrrelser detekteres og håndteres.

En række af disse områder vil således have relation til driftsmæssige procedurer, mens andre vil relatere sig til sikkerhedsmæssige politikker og -procedurer.

3.1 Dataansvar

En tjenesteudbyder er selvstændigt dataansvarlig for personoplysninger logget i egne systemer, herunder som modtages fra NemLog-in.

4 Tekniske krav

I dette kapitel beskrives en række overordnede tekniske krav til logningen. De specifikke hændelser med tilhørende data er beskrevet i appendiks.

4.1 Adgang og integritet

Logdata skal sikres mod uautoriseret adgang, herunder sletning, modifikation eller fabrikation af logninger. Disse tiltag til sikring af loggens integritet skal blandt andet sikre, at loggens troværdighed og bevisværdi.

4.2 Tidssynkronisering

Servere, der foretager logning, skal have synkroniseret deres tid med en nøjagtig kilde. Enhver logning skal være forsynet med nøjagtigt tidsstempel.

Serverne bør således hente deres tid fra en tidsserver, som er stratum 2 eller højere (se evt. http://en.wikipedia.org/wiki/Network_Time_Protocol) og bør endvidere resynkronisere så ofte, at tiden højst kan afvige et millisekund.

4.3 Sletning

Som tidligere nævnt skal Tjenesteudbydere skal etablere en sletteprocedure for logdata, der tager højde for databeskyttelsesreguleringen. Logninger i medfør af denne politik opbevares i mindst 6 måneder for bl.a. at sikre efterforsknings-hensyn – eksempelvis i situationer hvor en digital identitet misbruges.

4.4 Maskinel behandling

Logfilerne bør have et format, der gør dem velegnede til automatisk / maskinel behandling - herunder sammenstilling, filtrering og udsøgning af relevant information. Det skal således være muligt at adskille de enkelte felter i en logning, og en logning skal forsynes med passende nøgler / identifikatorer, der muliggør sammenstilling af hændelsesforløb, der er spredt over mange enkeltlogninger.

5 Appendiks A: Logningskrav ved brugerautentifikation

Dette appendiks beskriver en række hændelser med tilhørende data, som er obligatoriske at logge i forbindelse med brugerautentifikation via NemLog-in.

Tjenesteudbydere kan vælge at logge yderligere informationer samt benytte andre logs, men skal i givet fald være opmærksomme på, hvis personoplysninger optræder og foretage de nødvendige foranstaltninger.

Detaljer om alle fejl skal logges, herunder SAML fejl samt fejl i signatur- eller certifikatvalideringer.

5.1 Autentifikationsanmodninger

Tjenesteudbydere skal som minimum logge flg. data:

- ID på SAML <AuthnRequest> sendt til NemLog-in

Dertil kan tjenesteudbydere overveje at logge IP-adresse for slutbruger.

5.2 Autentifikationssvar

Tjenesteudbydere skal som minimum logge flg. data:

- ID på SAML <AuthnResponse> fra NemLog-in
- Sikringsniveau angivet i Assertion
- ID på request der svares på (fra InResponseTo)
- Resultat af validering af <Response> meddelelse og <Assertion> (herunder signaturvalidering)
- Bruger ID fra assertion (dvs. Subject NameID fra assertion)
- Identifikation af den interne brugerkonto som relateres til SAML assertionen.
- Rettigheder og/eller fuldmagtsprivilegier indeholdt i Assertion.
- Unikt ID på lokal session, som dannes på baggrund af autentifikationssvaret.

Dertil kan tjenesteudbyder overveje at logge IP-adresse for slutbruger.

5.3 Single Logout initieret fra en Tjenesteudbyder

Tjenesteudbydere skal som minimum logge flg. data, når der sendes et SAML <LogoutRequest> til NemLog-in:

- Markering af at brugeren har valgt logout
- ID på SAML <LogoutRequest> sendt til NemLog-in
- NameID i <LogoutRequest>
- Værdi af <SessionIndex> i <LogoutRequest>
- Svarstatus fra NemLog-in i <LogoutResponse>

De krævede felter i request er markeret med rødt i nedenstående eksempel:

Figur 1: Eksempel på felter i logout request som skal logges

5.4 Single Logout fra anden Tjenesteudbyder

Tjenesteudbydere skal som minimum logge flg. data, når der modtages et SAML <LogoutRequest> fra NemLog-in:

- ID på SAML <LogoutRequest> sendt fra NemLog-in
- ID på bruger som logges ud
- Markering af at lokal session er blevet termineret

5.5 Attributforespørgsler

En tjenesteudbyder har mulighed for at lave et attributopslag (SAML Attribute Query) mod NemLog-in's attributservice. I den forbindelse skal tjenesteudbydere som minimum logge flg.:

- ID på bruger
- Angivelse af de ønskede attributter
- ID på request sendt til NemLog-in
- Svarstatus fra NemLog-in

6 Appendiks B: Logningskrav i forbindelse med signering

Dette appendiks beskriver logningskravene for tjenesteudbydere, som anvender NemLog-in's signeringstjenester.

NemLog-in har to signeringstjenester: en legacy-signering, som understøtter signering med NemID, og en kvalificeret signeringstjeneste, som understøtter signering med MitID.

Tjenesteudbydere skal som minimum logge nedenstående oplysninger ved brug af NemLog-in's signeringstjenester:

a) Signeringstekst som ønskes signeret af brugeren og gives som input til NemLog-in.
b) ID på request til NemLog-in.
c) Modtaget svar fra NemLog-in med signatur og statuskode.
d) Resultat af signaturvalidering af svar.
e) Resultat af validering af, at signeringsteksten indlejret i den genererede signatur matcher den forventede signeringstekst (punkt a).
f) Resultat af validering af, at den forventede bruger har skrevet under (evt. output fra kald til NemLog-in's match tjenester).

Der henvises til den tekniske dokumentation for signeringstjenesterne for detaljer om de sikkerhedsmæssige valideringer, en tjenesteudbyder forventes at foretage ved anvendelse af signeringstjenesten.

6.1 Validering via signeringstjenesternes web services

For tjenesteudbydere, som anvender signeringstjenestens web service grænseflade, anbefales at logge både request og response meddelelse, der udveksles.

7 Referencer

[OIO-SAML2] "OIO Web SSO Profile V2.0.9", Digitaliseringsstyrelsen. http://digitaliser.dk/resource/2377872

[OIO-SAML3] "OIO Web SSO Profile V3.0.2", Digitaliseringsstyrelsen. https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/oiosaml-302/

[SIG-BEV] "Signatur- og Systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi", IT- og Telestyrelsen, 2008. http://digitaliser.dk/resource/250820

[VIL] "Vilkår til Tjenesteudbydere tilsluttet NemLog-in Broker", Digitaliseringstyrelsen. https://www.nemlog-in.dk/tu/privat/vilkaar/

[BKG] "Bekendtgørelse om tilrådighedsstillelse og anvendelse af MitID-løsningen og NemLog-in for offentlige myndigheder og offentligretlige organer".