Logningspolitik

For den fællesoffentlige log-in-løsning

Version 1.0.

Dette dokument beskriver den fællesoffentlige føderations minimumskrav til logning hos Service og Identity Providere.

Målgruppen for dokumentet er projektledere, IT arkitekter og IT teknisk personale hos serviceudbyderen (eller dennes it-leverandør), som skal planlægge og opsætte logning i test- og produktionsmiljø.

IT- & Telestyrelsen

>

Logningspolitik
For den fællesoffentlige log-in-løsning

Udgivet af:
IT- og Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Indholdsfortegnelse

1 Dokumenthistorik

>

Version	Dato	Initialer	Ændringer
0.9	13-11-2007	TG	Oprettet
0.91	07-03-2008	TG	Reference til vejledning og signatur- og systembeviser tilføjet.
1.0	12-09-2008	TG	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.
1.0.1	17-09-2008	TG	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.

2 Formål og afgrænsning

>

Formålet med denne publikation er at beskrive den fællesoffentlige føderations minimumskrav til logning hos Service og Identity Providere (SP'ere og IdP'ere).

Det antages at læseren er bekendt med opbygningen af den fællesoffentlige føderation; for detaljer henvises til [GUIDE].

Kravene i dette dokument skal sikre:

- At roller og ansvar for logning placeres hos føderationens medlemmer.
- At lovgivningsmæssige krav opfyldes, herunder persondataloven.
- At oplysninger relevante for sporbarhed og sikkerhed er tilgængelige, herunder at efterforskningsmæssige hensyn tilgodeses. I tilfælde af uautoriseret adgang hos en serviceudbyder skal det således være muligt via logningen at fastslå hvilke akkreditiver, der har været anvendt, resultater af valideringen samt hvilke serviceudbydere, der efterfølgende er givet adgang til, samt hvornår brugeren er logget ud.
- At der sikres konsistens på tværs af føderationen med hensyn til hvilke typer logs, der genereres, samt indholdet af disse. Hvis der ikke er konsistens f.eks. i forhold til logningen af identifikatorer, kan det blive en næsten umulig opgave at sammenstille logs fra forskellige organisationer med henblik på at kortlægge hændelsesforløb fra den fællesoffentlige log-in-løsning (IdP'en) til en serviceudbyder (SP'en).

Ovenstående udgør således de primære formål med logningen.

Logningen rummer data som dokumenterer:

- hvilke systemer en bruger har fået adgang til via den fællesoffentlige log-in-løsning (NemLog-in)
- valideringen af brugerens akkreditiver ved log-in (digital signatur og certifikat)
- hændelsesforløb som strækker sig fra brugerens log-in via den fælles løsning til brugeren får adgang til en applikation hos en serviceudbyder.

Derimod rummer logningen *ikke* oplysninger om, hvad en bruger har foretaget sig i serviceudbyderens forretningsapplikation.

2.1 Afgrænsning

Politikken afgrænser sig til de funktionelle områder, der varetages af føderationen, herunder:

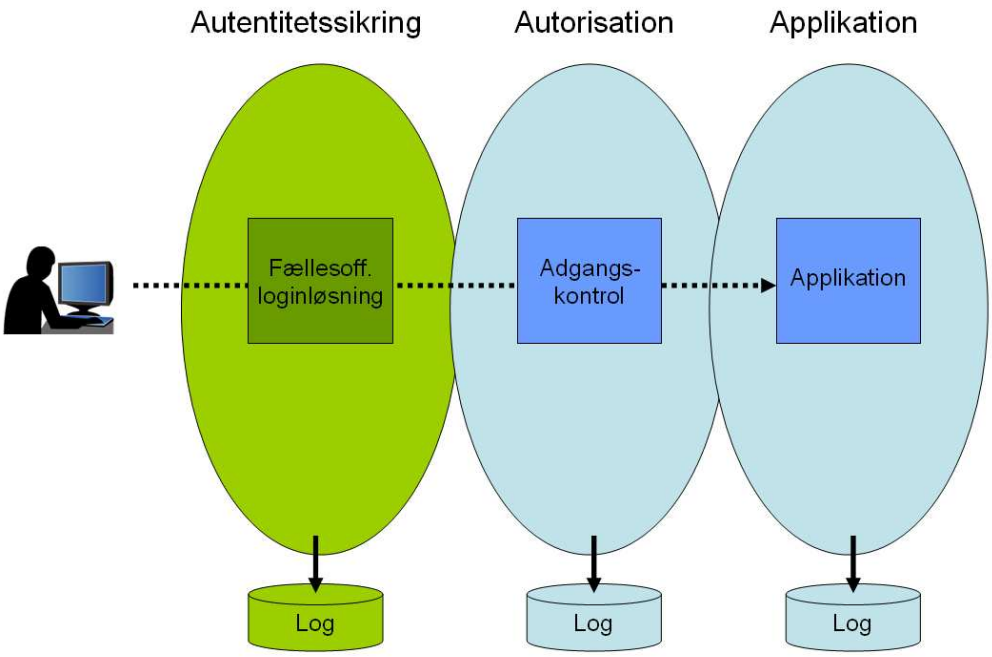
- Autentitetssikring af brugere
- Forespørgsler på attributter for brugere

Der behandles således *ikke* logningsforhold vedrørende:

- Forretningsapplikationer.
- Adgangskontrolsystemer der på baggrund af brugerens identitet foretager autorisationsbeslutninger.

>

Afgrænsningen er illustreret på nedenstående figur, hvor nærværende politik drejer sig om den med grønt markerede log, mens de øvrige logs er Service Providerens eget ansvar:



3 Organisatoriske krav

>

Medlemmerne af føderationen skal udpege en person, der er overordnet ansvarlig for logning, herunder at kravene i denne politik er opfyldt. Personens navn og kontaktoplysninger skal oplyses til operatøren i forbindelse med tilslutning til føderationen.

Opfyldelse af politikkens krav sker dels under etableringen af systemet i forbindelse med tilslutning, dels ved periodisk / løbende at udføre en række aktiviteter.

Den logningsansvarlige skal tilse, at organisationen (evt. dennes driftsleverandør) etablerer, dokumenterer og efterlever procedurer indenfor flg. områder:

- Personfølsomme data i logs skal håndteres i overensstemmelse med persondataloven.
- Der skal etableres en procedure for, hvad der skal foretages, 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. Dette er afgørende med henblik på at logdata kan fremlægges (og tillægges værdi) i en retssag.
- Der skal tages periodisk backup af logdata, så tilgængeligheden sikres.
- Logdata skal destrueres efter forældelse i overensstemmelse med politikken.
- Loggen skal løbende overvåges for kritiske hændelser som f.eks. forsøg på uautoriseret adgang.
- 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. Opgaverne kan derfor med fordel delegeres til drifts- og sikkerhedsorganisationen i virksomheden.

4 Lovgivningsmæssige krav

>

Dette kapitel har til formål at belyse kravene til logning i føderationen hidrørende fra persondataloven samt anden relevant lovning.

Som udgangspunkt skal en serviceudbyder i henhold til persondatalovens § 43 anmelde til Datatilsynet, at Økonomistyrelsen via den fællesoffentlige log-in løsning optræder som databehandler på dennes vegne.

Derudover skal en serviceudbyder vurdere, om anvendelse af den fællesoffentlige log-in-løsning giver anledning til behandling af personoplysninger, der skal anmeldes til Datatilsynet i henhold til lov om behandling af personoplysninger. I udgangspunktet vil logning af data og hændelser defineret i denne politiks appendiks A ikke medføre anmeldelsespligt for offentlige myndigheder. Eksempelvis giver logning af CPR nummer hos offentlige myndigheder alene ikke anledning til krav om anmeldelse (jævnfør § 44 i persondataloven).

Derimod vil logning i serviceudbydernes forretningsapplikationer kunne medføre et krav om anmeldelse i henhold til persondataloven, og dette skal derfor vurderes af den enkelte serviceudbyder. Dette er dog helt uafhængigt af anvendelse af den fællesoffentlige log-in-løsning.

5 Tekniske krav

>

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

5.1 Typer af logs

Denne politik opererer primært med én type af log, nemlig en såkaldt *opfølgningslog*. En sådan log indeholder sikkerhedsrelaterede hændelser, afvigelser og brugeraktiviteter [DS-484].

Opfølgningsloggen kan fysisk deles over flere filer eller databaser, såfremt det er hensigtsmæssigt, men informationen i de enkelte filer skal altid kunne sammenstilles, således at relationen mellem hændelser fremgår.

Ofte vil et system operere med andre typer logs, herunder trace/informationslogs, der anvendes til vedligeholdelse og fejlfinding af systemer, transaktionslogs, der viser opdateringer til systemers underliggende datamodel, forbrugslog, der viser ressourceforbrug, samt logs hørende til svartids- og performancemålinger. Alle disse typer af logs er uden for rammerne af logningspolitikken.

Dog skal man være opmærksom på, hvis nogle af de andre typer logs også indeholder personfølsomme data. I givet fald vil de så skulle håndteres efter bestemmelserne i persondataloven. Et eksempel kunne være, hvis driftspersonalet under en fejlfinding i systemet konfigurerer et højt informationsniveau i traceloggen, der så bevirker, at SAML assertioner indeholdende følsomme attributter logges.

5.2 Adgang til logfiler

Filerne med opfølgningsloggen skal sikres mod uautoriseret adgang, herunder sletning, modifikation eller fabrikation. Dette skal blandt andet sikre, at loggens indhold kan fremlægges som bevis ved domstolene. Vejledningen [SIG-BEV] indeholder praktiske anvisninger på, hvorledes logfilers integritet kan sikres.

5.3 Tidssynkronisering

Serverne i føderationen, der foretager logning, skal have synkroniseret deres tid. Enhver logning skal være forsynet med nøjagtigt tidsstempel.

I henhold til føderationens tidspolitik skal serverne hente deres tid fra en tidsserver, som er stratum 2 eller højere (se evt. http://en.wikipedia.org/wiki/Network_Time_Protocol), samt endvidere resynkronisere så ofte, at tiden højst afviger et millisekund.

5.4 Signaturbevis

I forbindelse med validering af signaturer fra føderationens parter (eksempelvis på SAML assertioner) skal der genereres og logges bevisdata i opfølgningsloggen, der dokumenterer den digitale signaturs gyldighed.

Det tilrådes at anvende kryptografiske signaturbeviser, systembeviser eller hybrider af disse to metoder. For detaljer se vejledningen [SIG-BEV] om sikring af digitale signaturers bevisværdi.

>

5.5 Arkivering og destruktion

Serviceudbyderne skal etablere en procedure for, hvor længe logdata gemmes, der tager højde for evt. krav persondataloven. Det anbefales, at slette log data efter seks måneder med mindre der er gode grunde til at forlænge perioden.

5.6 Maskinel behandling

Logfilerne bør have et format, der gør dem velegnede til 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.

6 Appendiks A: Loghændelser og -data

>

Dette appendix beskriver en række hændelser med tilhørende data, det er obligatorisk at logge i opfølgningsloggen. Føderationens parter kan vælge at logge flere informationer samt benytte andre logs, men skal i givet fald være opmærksomme på, hvis personfølsomme data optræder og foretage de nødvendige foranstaltninger.

6.1 Generelle log-attributter

Nedenstående tabel beskriver en række hyppigt forekommende attributter, der kan logges. Der refereres til disse attributter i den efterfølgende gennemgang af log-hændelser.

Felt	Information	Eksempel
Maskinidentifikation	IP på afsendersystemet	10.0.0.1
Afsenderidentifikation	Afsenderens ID som angivet i meta data	http://myprovider.dk/client
Tidspunkt	Tidspunkt for logning	2007-09-28T14:42:32
Serviceidentifikation	Navn på den service / operation der udføres	AuthnRequest
Systemidentifikation	Navn på det it-system der logger	IdP
Transaktions-ID	ID fra SAML assertion	2738492938475463282387
Sessions ID	Identifikationen af en session	2768764092873648723646

Det bemærkes, at ID fra SAML assertionen benyttes som den nøgle, der kan sammenknytte logninger på tværs af organisationer. Eksempelvis kan den sammenknytte de logninger, der er sket hos en Identity Provider vedr. brugerautentifikation med den session, der efterfølgende er oprettet hos en Service Provider.

Det er i det følgende underforstået, at detaljer om alle fejl skal logges, herunder SAML fejl samt fejl i signatur- eller certifikatvalideringer. Endvidere er det underforstået, at alle hændelser tidsstemples i loggen.

6.2 Basic Service Access with Authentication

Skemaet nedenfor skitserer flowet i DK-SAML profilen [DKSAML20], hvor der ikke er oprettet en tidligere session. For detaljer i protokollen henvises til [DKSAML20] afsnit 2.1:

#	Hændelse	Ansvar	Data som skal logges
BSA1	Brugeren tilgår en ressource hos en SP uden at have en session	SP	• ID på ressourcen (f.eks. URL) • Brugerens IP adresse • ID på AuthnRequest
BSA 2	SP re-dirigerer brugeren til IdP med AuthnRequest	SP	

>

BSA 3	IdP modtager AuthnRequest	IdP	• Signaturbevis • Brugerens IP adresse • ID på SP • ID på AuthnRequest
BSA 4	IdP autentificerer brugeren	IdP	• Valgt autentifikationsmetode • Valideringsresultat og -delresultater. For OCES inkluderer det certifikatets spærrestatus og gyldighed • ID på bruger som angivet i credentials. For OCES logges hele brugerens certifikat. • Intern brugeridentitet hos IdP (hvis forskellig fra credential ID) • Level of Authentication (1-4) • Unikt ID på IdP session • Timeout værdi for session
BSA 5	IdP laver SAML assertion og redirigerer brugeren tilbage til SP	IdP	• Den oprettede assertion
BSA 6	SP validerer SAML assertion	SP	• Brugerens IP adresse • Signaturbevis • ID på request der svares på (fra InResponseTo) • ID på Identity Provider (dvs. Issuer fra Assertion) • Assertion ID • Level of Authentication (1-4) • Resultat af validering af <Response> meddelelse og <Assertion> • Bruger ID fra assertion (dvs. Subject NameID fra assertion) • Identifikation af den interne brugerkonto som relateres til SAML assertionen.
BSA 7	SP danner session og autoriserer brugeren[1]	SP	• Unikt ID på SP session • Timeout værdi for session
BSA 8	SP returnerer ressourcen	SP	• ID på ressourcen (f.eks. URL)

[1] Bemærk at autorisationsbeslutninger er udenfor scope af føderationen og denne logningspolitik, se evt. afgrænsningen i begyndelsen af dokumentet.

>

6.3 Service Access with Single Sign-On

I et scenarium, hvor en bruger allerede er logget på føderationen, men ikke har en session med den pågældende SP, optræder nedenstående hændelser:

#	Hændelse	Ansvar	Data som skal logges
SSO1	Brugeren tilgår en ressource hos en SP og har allerede en tidligere session med IdP'en, men ikke med SP.	SP	• ID på ressourcen (f.eks. URL) • Brugerens IP adresse
SSO2	SP redirigerer brugeren til IdP med AuthnRequest	SP	
SSO3	IdP modtager AuthnRequest	IdP	• Signaturbevis • Brugerens IP adresse • ID på SP • ID på AuthnRequest
SSO4	IdP ser at brugeren allerede har en aktiv session.	IdP	• Unikt ID på IdP session • Intern brugeridentitet hos IdP • Aktuelt level of Authentication (1-4) • Timeout værdi for session
SSO5	IdP laver SAML assertion og redirigerer brugeren tilbage til SP	IdP	• Den oprettede assertion
SSO6	SP validerer SAML assertion	SP	• Brugerens IP adresse • Signaturbevis • ID på Identity Provider. • Assertion ID • Level of Authentication • Resultat af validering af <Response> meddelelse og <Assertion> • Bruger ID fra assertion • Identifikation af den interne brugerkonto som relateres til SAML assertionen.
SSO7	SP danner session og autoriserer brugeren	SP	• Unikt ID på SP session • Timeout værdi for session
SSO8	SP returnerer ressourcen	SP	• ID på ressourcen (URL)

>

6.4 Single Logout

Når en bruger ikke længere ønsker at være logget på føderationen og foretager et Single Log Out, afføder det følgende behov for logning. For detaljer i protokollen henvises til [DKSAML20] afsnit 2.4:

#	Hændelse	Ansvar	Data som skal logges
SLO1	Brugeren vælger SLO hos en SP	SP	• At SLO er ønsket • Brugerens ID • ID på SP session • Assertion ID
SLO2	SP kontakter IdP for at anmode om single logout	SP	
SLO3	IdP modtager anmodning om logout og checker hvilke andre SP brugeren har session med	IdP	• Angivelse af de SP'er der logges af fra • Brugerens IP adresse • Signaturbevis for signeret request • ID på SP • ID på IdP Session
SLO4	SP og andre SP'er modtager anmodning om logout	SP	• Signaturbevis • ID på bruger som logges ud • ID på SP session der termineres • Assertion ID hørende til session • Status på om session blev termineret
SLO5	IdP terminerer session med bruger og returnerer en bekræftelse til brugeren.	IdP	• Status fra SP'ere om hvorvidt logout lykkedes • Status på om IdP session blev termineret

6.5 Access via a Portal and Attribute Retrieval

En serviceudbyder har mulighed for at lave et attributopslag mod en attributservice. I flowet nedenfor antages det at serviceprovideren har gennemgået autentifikationen som beskrevet ovenfor og har en SAML assertion om brugeren. For detaljer om protokollen se [DKSAML20] afsnit 2.3:

#	Hændelse	Ansvar	Data som skal logges
ATT1	SP har brug for flere oplysninger om brugeren f.eks. til autorisation og sender en anmodning til	SP	• Angivelse af de ønskede attributter • Logning af brugerens samtykke

>

	attributservicen		
ATT2	Attributservicen autentificerer afsenderen og laver et opslag hvis svar sendes tilbage til SP	AS	• Signaturbevis for request • ID for SP • Brugerens ID • Logning af consent ID • Angivelse af de ønskede attributter • Logning af de udleverede attributværdier
ATT3	SP validerer svar og udtager attributter	SP	• Signaturbevis for svar. • Status på om de ønskede attributter er returneret (men ikke attributværdier!).

6.6 Federation using Persistent Pseudonyms

En alternativ log-in-mekanisme anvender persistente pseudonymer til at sammenkæde en assertion med en lokal brugerkonto. I dette scenarium autentificerer brugeren sig 2 gange, først mod IdP'en og efterfølgende mod SP, hvorpå der laves en kobling mellem de to akkreditiver, der efterfølgende kan anvendes til SSO. I efterfølgende autentifikationer skal der derfor kun afgives akkreditiver mod IdP'en. Se [DKSAML20] afsnit 2.5 for yderligere information.

#	Hændelse	Ansvar	Data som skal logges
PP1	Brugeren tilgår en ressource hos en SP uden at have en session	SP	• ID på ressourcen (f.eks. URL) • Brugerens IP adresse
PP2	SP redirigerer brugeren til IdP med AuthnRequest	SP	
PP3	IdP modtager AuthnRequest	IdP	• Signaturbevis • Brugerens IP adresse • ID på SP • ID på AuthnRequest
PP4	IdP autentificerer brugeren	IdP	• Valgt autentifikationsmetode • Valideringsresultat og -delresultater. For OCES inkluderer det certifikatets spærrestatus og gyldighed • ID på bruger som angivet i credentials. For OCES logges hele brugerens certifikat. • Intern brugeridentitet hos IdP (hvis forskellig fra credential ID) • Level of Authentication (1-4) • Unikt ID på IdP session • Timeout værdi for session
PP5	IdP laver SAML	IdP	• Den oprettede assertion

>

	assertion med persistent identifier og redirigerer brugeren tilbage til SP		
PP6	SP validerer SAML assertion	SP	• Brugerens IP adresse • Signaturbevis • ID på Identity Provider • Assertion ID • Bruger ID fra assertion (pseudonym) • Resultat af validering af <Response> meddelelse og <Assertion>
PP7	SP autentificerer brugeren mod den interne konto og mapper til den persistente identifier.	SP	• Valgt autentifikationsmetode • Level of Authentication (1-4) • Valideringsresultat og -delresultater. • ID på SP session • Timeout værdi for session • Identifikation af den interne brugerkonto • Sammenhængen mellem pseudonym og intern konto
PP8	SP danner session og autoriserer brugeren.	SP	• Unikt ID på SP session • Timeout værdi for session
PP9	SP returnerer ressourcen	SP	• ID på ressourcen

7 Referencer

>

[PERSLOV] ”Persondataloven”, Datatilsynet. http://www.datatilsynet.dk/lovgivning/persondataloven/

[DS484] ”DS484 Standard for informationssikkerhed”, Nyt Teknisk Forlag, ISBN 978-87-571-2478-1. [Findes ikke tilgængelig på Internettet]

[POLSIK] ”Quick guide til optimering af efterforskningsmuligheder når systemet er kompromitteret og forholdsregler inden det går galt.”, Tom Engly Henriksen, kriminalassistent, CPSA, Rigspolitiets Kriminaltekniske Afdeling - IT-sektionen, [Ikke tilgængeligt på internettet]

[SIKVEJL] ”Sikkerhedsvejledning (Vejl. nr. 37 af 2. april 2001)”, 16/4/2001, http://www.datatilsynet.dk/lovgivning/vejledninger/

[DKSAML20] ”SAML Profile for SSO in Danish Public Sector V2.0”, IT- og Telestyrelsen, 2007 http://oiosaml.info

[SIG-BEV] ”Signatur- og Systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi”, IT- og Telestyrelsen, 2008. http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/signatur-og-systembeviser

[GUIDE] ”Tilslutningsguide. Håndbog for serviceudbyderen som ønsker at tilslutte sig den fællesoffentlige log-in-løsning”, Brugerstyringssekretariatet, Økonomistyrelsen. www.digst.dk/Digitale-loesninger/NemLogin