DIGITALISERINGSSTYRELSEN

National eID-gateway

Marts 2022
Version 1.1

Logningspolitik

Dette dokument beskriver minimumskrav til logning hos Tjenesteudbyder ved anvendelse af den danske eID-gateway.

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

Indholdsfortegnelse

1. Formål og afgrænsning

Formålet med denne publikation er at beskrive, når den danske eID-gateway har minimumskrav til logning hos tjenesteudbydere, der anvender komponenten DK eIDAS Connector i den nationale eID-gateway.

Kravene i dette dokument skal sikre:

- At tjenesteudbyder er bekendt med kravene til logning.
- At lovgivningsmæssige krav opfyldes, herunder EU's databeskyttelsesforordning og den danske databeskyttelseslov vedtaget den 17. maj 2018.
- At oplysninger relevante for sporbarhed og sikkerhed er tilgængelige, herunder at efterforskningsmæssige hensyn tilgodeses. I tilfælde af uautoriseret adgang hos en tjenesteudbyder skal det således være muligt via logningen at fastslå hvilke akkreditiver, der har været anvendt, resultater af valideringen, samt hvilken tjenesteudbyder, der efterfølgende har modtaget autentificering og evt. attributter fra den danske eID-gateway, samt hvornår tjenesteudbyder har lukket sessionen.
- At der sikres konsistens mellem tjenesteudbyder og den danske eID-gateway med hensyn til hvilken log, der genereres, samt indholdet af disse.

Ovenstående udgør således de primære formål med logningen.

1.1 Afgrænsning

Politikken afgrænser sig til den logning, der skal finde sted, når den danske eID-gateway anvendes til autentifikation af brugere og evt. forespørgsler på attributter for brugere gennem den danske eID-gateway via DK eIDAS Connector.

Der behandles således ikke logningsforhold vedrørende:

- Tjenesteudbyders forretningsapplikationer.
- Tjenesteudbyders adgangskontrolsystemer foretager adgangskontrol og giver adgang til tjenesteudbyders forretningsapplikationer på grundlag af den autentificering, som den danske eID-gateway foretager af brugerens identitet.

Logningen rummer således data, som dokumenterer:

- Valideringen af brugerens akkreditiver ved log-in (digital signatur og certifikat).
- Hændelser i kommunikationen mellem tjenesteudbyder og den danske eID-gateway.

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

2. Organisatoriske krav

Tjenesteudbyder 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 Digitaliseringsstyrelsen i forbindelse med tilslutning til den danske eID-gateway.

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 inden for følgende områder:

- Logs i kommunikationen med DK eIDAS Connector må ikke rumme persondata. Virksomhedscertifikat ID eller funktionscertifikat ID vil kunne identificere tjenesteudbyder i loggen.
- 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 fx 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.

Implementeringen af logningspolitikken skal baseres på klare målemetoder (KPI´er) med henblik på regelmæssigt at vurdere og evaluere kvalitet, effektivitet og sikkerhedsniveau.

Valg af kontroller skal indeholde vægtning af de enkelte risikofaktorer, og tage afsæt i de identificerede og vurderede risici.

Kontroller af de generelle driftsprocesser og sikkerhedsprocedurer skal baseres på verificeret dokumentation, som gennemføres ud fra internationale anerkendte standarder fx ISO27001 og rammeværk for sikkerhedskontroller fx SANS CIS.

Tilsyn, revision, auditering og rapportering (SLA) skal udføres på grundlag af det aftalte kontrolmiljø for at skabe gennemsigtighed og sikre gensidig efterlevelse/overholdelse af de fastlagte krav i aftalen.

3. Lovgivningsmæssige krav

Logning skal overholde kravene hidrørende fra EU's databeskyttelsesforordning og den danske databeskyttelseslov vedtaget den 17/5 2018. Disse er beskrevet i tilslutningsaftalens Bilag A: Detaljerede sikkerhedskrav.

4. Tekniske krav

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

4.1 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.

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 persondata. I givet fald vil de så skulle håndteres efter bestemmelserne om persondata. 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.

4.2 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.

4.3 Tidssynkronisering
Den server hos tjenesteudbyder, der foretager logning, skal have synkroniseret sin tid med serveren hos den danske eID-gateway, som logger hændelser og kommunikationen med tjenesteudbyders it-system. Enhver logning skal være forsynet med nøjagtigt tidsstempel.

Derfor skal tjenesteudbyders server, der foretager logning, hente sin tid fra en tidsserver, som er stratum 2 eller højere[1] samt endvidere re-synkronisere så ofte, at tiden højst afviger et millisekund.

4.4 Signaturbevis
I forbindelse med validering af signaturer fra den danske eID-gateway (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.

4.5 Arkivering og destruktion
Tjenesteudbyderne skal etablere en procedure for, hvor længe logdata gemmes, der tager højde for evt. krav i databeskyttelsesloven. Det anbefales at slette log data efter seks måneder med mindre, der er gode grunde til at forlænge perioden.

4.6 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.

[1] Se evt https://en.wikipedia.org/wiki/Network_Time_Protocol

5. Appendiks A: Loghændelser og -data

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

5.1 Generelle log-attributter

Nedenstående tabel beskriver de generelle attributter, der skal logges. Der refereres til disse attributter, og der nævnes flere konkrete 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 tjenesteudbyders metadata	https://sp.myndighed.dk/
Tidspunkt	Tidspunkt for logning	2018-05-28T14:42:32
Serviceidentifikation	Navn på den service / operation der udføres	AuthnRequest
Systemidentifikation	Navn på det it-system der logger	Tjenesteudbyders it-system
Transaktions-ID	ID fra SAML assertion	2738492938475463282387
Sessions ID	Identifikationen af en Session	2768764092873648723646
Response resultat	Oplysning om resultatet af AuthnRequest	Success /Succes med attributter overført / Fejl med Fejl-ID

Det bemærkes, at ID fra SAML-assertionen benyttes som den nøgle, der kan sammenknytte logninger på tværs af tjenesteudbyder og den danske eID-gateway.

Alle fejl skal logges, herunder SAML-fejl samt fejl i signatur- eller certifikatvalideringer. Alle hændelser (response resultater) skal tidsstemples.

5.2 Basic Service Access with Authentication

Skemaet nedenfor skitserer flowet i OIOSAML-profilen [OIOSAML], hvor der skal foretages en autentifikation af den danske eID-gateway. Tjenesteudbyder er forkortet som TU, og DK eIDAS Connector er forkortet med eIDC. For detaljer i standarden henvises til [OIOSAML]:

#	Hændelse	Ansvar	Data som skal logges
BSA1	Brugeren vælger at tilgå eIDC	TU	
BSA 2	TU redirigerer brugeren til eIDC med AuthnRequest	TU	• ID på AuthnRequest • ID på TU
BSA 3	eIDC modtager AuthnRequest	eIDC	• Signaturbevis • ID på TU • ID på AuthnRequest
BSA 4	eIDC autentificerer brugeren	eIDC	• 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 eIDC (hvis forskellig fra credential ID) • Level of Authentication (1-4) • Unikt ID på eIDC session • Timeout værdi for session
BSA 5	eIDC indhenter landevalg fra bruger og videresender til eIDAS service, der tilbagesender svaret	eIDC	• Landevalg • Hvis tjenesteudbyder *ikke* ønsker attributter, dannes en assertion med en unik ID på den danske eID-Gateway • I modsat fald dannes en assertion med en unik ID på den danske eID-Gateway *og* de af tjenesteudbyder valgte attributter.
BSA 6	eIDC redirigerer brugeren tilbage til TU	eIDC	• Den oprettede assertion

BSA 7	TU validerer SAML assertion	TU	• 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)
BSA 8	TU danner session og tildeler brugeren adgangsprivilegier[2]	TU	• Unikt ID på TU session • Timeout værdi for session

6. Referencer

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

[SIGBEV] "Signatur- og systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi", Digitaliseringsstyrelsen. https://www.digitaliser.dk/resource/250820

7. Versionshistorik

Version	Dato	Initialer	Indhold /ændringer
1.0	29-06-2018	OSBUH	Første version til offentliggørelse
1.1	09.03.2022	IDAWI	Mindre tilpasninger i anvendt terminologi.

[2] Bemærk at tjenesteudbyders adgangskontrol er uden for scope af den danske eID-gateway og denne logningspolitik, se evt. afgrænsningen i begyndelsen af dokumentet.