DIGITALISERINGSSTYRELSEN

7. november 2012

Timeout-politik for den fællesoffentlige føderation

Dette dokument beskriver en politik for timeout af brugersessioner i den fællesoffentlige føderation, der er obligatorisk at overholde for føderationens medlemmer. Politikken definerer, hvor længe brugersessioner kan opretholdes (timeout perioden), før de skal fornys. Formålet med politikken er at sikre en hensigtsmæssig og ensartet brugeroplevelse relateret til, hvornår brugere bliver bedt om at logge ind.

Dokumentet henvender sig til teknisk personale, der skal konfigurere IT systemer således, at den herunder beskrevne politik overholdes.

Dokumenthistorik

Version	Dato	Initialer	Indhold /ændringer
1.0	9.9.2008	TG	Første version udarbejdet.
1.1	7.11.2012	TG	Opdateret med Digitaliseringsstyrelsen som afsender samt nye links.

Indholdsfortegnelse

Introduktion

I den fællesoffentlige føderation anvendes NemLog-in løsningen til log-in af brugere. Under et log-in-forløb etableres såkaldte *sessioner* med brugeren hos såvel log-in-løsningen som hos serviceudbydere. En session har til formål at sikre, at en applikation kan genkende browserens forskellige forespørgsler som kommende fra samme bruger. Et af de primære effekter ved dette er, at brugeren kan nøjes med at logge på applikationen én gang og efterfølgende kan tilgå løsningen kontinuerligt. Som et velkendt eksempel kan næves Internetbanker, hvor brugeren efter logi-n kan udføre forskellige handlinger som f.eks. tilgå kontooversigter, se rentevilkår, tilgå pensionsoversigter etc.

Af sikkerhedsmæssige grunde bør brugerens sessioner blive lukket (timeout), hvis brugeren ikke har været aktiv i en given tidsperiode (timeout periode). Hvis dette sker, bliver brugeren normalt tvunget til at logge på igen.

Som det er velkendt fra enkeltstående applikationer, opererer den fællesoffentlige føderation ligeledes med timeout af sessioner. Imidlertid er problemstillingen mere kompleks, idet der anvendes en ekstern loginløsning (NemLog-in), så opførslen skal koordineres mellem forskellige systemer. I det følgende beskrives, hvorledes timeout af sessioner skal håndteres, og de forskellige valg belyses.

Loginforløb

For at illustrere sessionsbegrebet i en føderation er de vigtigste hændelser i et log-in-forløb skitseret nedenfor. For detaljer henvises til [OIO-SAML].

Scenarie 1: Første log-in efter browseren er åbnet

1. Brugeren tilgår en web applikation hos en serviceudbyder, der kræver log-in.
2. Da serviceudbyderen ikke kender brugeren, sendes brugerens browser over til NemLog-in-løsningen.
3. NemLog-in kontrollerer, om den har en session med brugeren (f.eks. hvis brugeren har logget på for nylig), hvilket ikke er tilfældet.
4. Brugeren skal nu logge på NemLog-in med sin digitale signatur. NemLog-in opretter herefter en session med brugeren for at kunne genkende denne næste gang, han kommer "forbi".
5. NemLog-in sender brugerens browser tilbage til serviceudbyderen med informationer om brugerens identitet.
6. Serviceudbyderen opretter nu en session med brugeren, så de næste forespørgsler fra browseren kan genkendes som kommende fra samme bruger.
7. Brugeren kan efterfølgende tilgå de forskellige sider i serviceudbyderens applikation uden at skulle logge på igen; han bliver genkendt via sin session.

Som det fremgår af ovenstående, bliver der i forløbet oprettet to sessioner; én hos serviceudbyderen og én hos NemLog-in.

Scenarie 2: næste login (med single sign-on)

Når brugeren tilgår en ny løsning hos en anden serviceudbyder, er sekvensen følgende:

1. Brugeren tilgår en ny web applikation hos en anden serviceudbyder, der ligeledes kræver log-in.
2. Da serviceudbyderen ikke kender brugeren, sendes brugerens browser over til NemLog-in løsningen.
3. NemLog-in kontrollerer, om den har en session med brugeren. I dette tilfælde har brugeren lige logget på (scenarie 1), og derfor har han en aktiv session. Han behøver således ikke logge på hos NemLog-in igen.
4. NemLog-in sender brugerens browser tilbage til serviceudbyderen med informationer om brugerens identitet.
5. Serviceudbyderen opretter nu en session med brugeren, så de næste forespørgsler fra browseren kan genkendes som kommende fra samme bruger.

I ovenstående sekvens bevirker den eksisterende session hos NemLog-in, at brugeren ikke behøver at logge på igen, og der kan oprettes en session hos den nye serviceudbyder uden brugerens direkte involvering. Dette kaldes for single sign-on.

Timeout politik (normativ)

Nedenstående retningslinjer gælder for alle serviceudbydere i den fællesoffentlige føderation; retningslinjerne gælder for såvel selvstændige applikationer, der afvikles fra myndighedernes egne sites, som applikationer, der er indlejret på portaler (f.eks. via iFrame integrationsformen).

I den fællesoffentlige føderation skal medlemmerne konfigurere deres systemer, så sessioner udløber ved inaktivitet efter højst

- **30 min for serviceudbydere**
- **60 min for NemLog-in (Identity Provider)**

Det er valgfrit, om timeoutperioden nulstilles, hver gang brugerens browser tilgår en serviceudbyders løsning, eller om den er uafhængig af brugeraktivitet (fast timeout periode).

Efter timeout hos en serviceudbyder skal brugerens browser ved næste http forespørgsel sendes over til NemLog-in løsningen med en anmodning om log-in (et såkaldt SAML `<AuthnRequest>`; se [OIO-SAML] for detaljer).

Det skal bemærkes, at timeout hos en serviceudbyder ikke nødvendigvis medfører, at brugeren bliver tvunget til at logge på NemLog-in. Hvis brugeren har en aktiv session hos NemLog-in, kan denne svare på forespørgslen fra serviceudbyderen uden brugerdialog (dvs. foretage single sign-on). Brugeren vil dermed ikke opdage, at sessionen bliver fornyet (bortset fra at hans browser måske lige "blinker" et kort øjeblik).

Hvis en serviceudbyder af sikkerhedsmæssige grunde vil sikre sig, at brugeren bliver påtvunget aktiv log-in i NemLog-in løsningen, kan man sætte parameteren `ForceAuthn="true"` i kaldet til NemLog-in (se [OIO-SAML] for detaljer). Det anbefales ikke at benytte denne mekanisme, med mindre det er strengt nødvendigt, idet brugeroplevelsen forringes grundet gentagne log-ins. Som et alternativ kan det anbefales at lade brugerne signere transaktioner med deres digitale signatur på kritiske steder i applikationen, hvor man eksempelvis ønsker at få genbekræftet brugerens identitet og/eller samtykke. Denne fremgangsmåde kendes eksempelvis fra de fleste Internetbanker, hvor brugeren skal underskrive en betaling, før den effektueres.

Hvis en serviceudbyder ikke ønsker, at NemLog-in viser en brugergrænseflade i forbindelse med log-in / sessionsfornyelse, kan man sætte flaget `IsPassive="true"` i kaldet til NemLog-in. Dette medfører, at NemLog-in kun kan honorere forespørgslen om log-in, hvis brugeren har en eksisterende session. Hvis NemLog-in ikke har en brugersession, vil løsningen returnere en fejl til serviceudbyderen, idet aktiv log-in så vil være nødvendigt.

Bemærk at `IsPassive` og `ForceAuthn` flagene ikke begge må sættes på en forespørgsel.

Timeout i loginløsningen
Ved timeout i loginløsningen (NemLog-in) vil brugeren skulle foretage aktivt log-in, næste gang en serviceudbyder viderestiller en bruger for log-in (via et SAML `<AuthnRequest>`). Lokale sessioner hos serviceudbydere kan vedblive med at være aktive (såfremt brugeren holder dem i live), selvom NemLog-in's session timer ud. Bemærk at NemLog-in således *ikke* sender beskeder til serviceudbydere om, at de skal logge brugerne ud (såkaldt "single logout").

Samspil med portaler (ikke normativ)

Det er værd at bemærke, at offentlige portaler (borger.dk og virk.dk) kan stille yderligere krav til timeoutopførslen for applikationer, der er indlejret via iFrame integrationsformen [OIM].

Det kan således være hensigtsmæssigt, hvis indlejrede applikationer fornyr deres sessioner hos NemLog-in efter en fast periode (dvs. uanset brugeraktivitet), da man ellers kan risikere, at brugeren uventet bliver afkrævet log-in i portalerne. Retningslinjer for samspil med portaler ligger uden for denne politiks ansvarsområde, og der henvises til den fællesoffentlige integrationsmodel [OIM] og analysen [IFRAME-AN] for detaljer. Det skal yderligere bemærkes, at [OIO-SAML] profilen ikke foreskriver brug af `SessionNotOnOrAfter` attributten på `<AuthnStatement>` elementet, som kan anvendes til dette formål, men at samme effekt kan opnås via politikker udstukket af portalerne eller integrationsmodellen.

Referencer

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

[GUIDE] "Tilslutningsguide. Håndbog for serviceudbyderen som ønsker at tilslutte sig den fællesoffentlige log-in-løsning", Digitaliseringsstyrelsen. http://www.digst.dk/Loesninger-og-infrastruktur/NemLogin/Tilslutning-til-NemLogin/Materiale-til-IT-leverandoerer

[LOGPOL] "Logningspolitik for den fællesoffentlige log-in-løsning", Digitaliseringsstyrelsen. http://www.digst.dk/Loesninger-og-infrastruktur/NemLogin/Tilslutning-til-NemLogin/Tekniske-krav

[SIGBEV] "Signatur- og systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi", IT & Telestyrelsen. http://digitaliser.dk/resource/250820

[OIM] "Den fællesoffentlige integrationsmodel", Den Digitale Taskforce. http://oim.modernisering.dk/StartSide

[IFRAME-AN] "Analyse af udfordringer ved iFrame integrationsformen", Den Digitale Taskforce. http://digitaliser.dk/resource/2272443