

Kirsten Rothoff.

Fra: Finn Gronbak [GRONBAK@dk.ibm.com]
Sendt: 24. september 2007 08:42
Til: I-ITA - OIO Standarder
Cc: Søren Peter Nielsen; Sven-Erik Vestergaard; Jens Mikael Jensen
Emne: Fw: Kommentar til SAML høring - DEN RIGTIGE - GLEM DEN FORRIGE

Valg af SAML

At vælge SAML som standard for federeret single sign-on i den offentlige sektor er et godt valg, som falder i godt i tråd med IBM's omfattende support for SAML i IBM's Tivoli sikkerhedsprodukter.

Overordnet vedr. afgrænsning

Denne profil foretager nogle kraftige fravalg, samtidig med at den fokuserer meget på de krav der rejses fra offentlige portaler - specielt borger.dk. Den fremstår derfor som en pragmatisk, taktisk standard og det kunne måske være en fordel at markere det ved f.eks.

Slet ikke at anvende ordet "SAML" i profilens navn, men noget i retning af "Profil for offentlig fælles web login 1.0"
At ændre profilens navn til "DK-SAML 2.0 Web Browser SSO Profile"
Fremhæve denne fokusering i det indledende "prpose" afsnit.
Angive en mulig roadmap for kommende versioner eller profiler under "DK-SAML" - f.eks. "DK-SAML Web Services SSO Profile", DK-SAML WSRPPProfile",...

Afgrænsning til en national standard

Med kravet om anvendelse af OCES certifikater afgrænser standarden sig til at være en national standard, som udelukker herboende personer som ikke har eller kan få et OCES certifikat og udenlandske brugere samt udenlandske service providers, der skal udveksle OCES virksomhedscertifikater med ID provideren.

Det giver også problemer i forhold til internationale leverandører af sikkerhedsprodukter, som typisk holder sig til internationale standarder (en af grundene til at vi har dem). IBM's deltagelse i borger.dk proof-of-concept viste i casen med Rødovre Kommune, at dette godt kan lade sig gøre, men der skal foretages ekstra konfigurerings m.v. for at implementere den nødvendige nationale tilpasning.

Afsnit 2.3 om Access via portal

I det beskrevne scenarie fungerer portalen som en ren gennemstilling via et link eller en iframe til en service provider (SP). Portalen er imidlertid selv en SP, som har brug for autentificering af brugere, så de kan tilgå de portalrelaterede resourcer, som portalen er ansvarlig for - f.eks. portalsider, portlets på portalsider osv. Portalen kan sikkert også selv have brug for Attribute Services.

Afgrænsningen til borger.dk med fravalg af f.eks. WSRP virker lidt som en taktisk, "tilfældig", "pragmatisk" afgrænsning i forhold til at denne standard jo har et bredere sigte. Vedr. WSRP er IBM's support for denne standard i IBM's portalprodukter meget omfattende. WSRP vil sandsynligvis få stor betydning for distribuerede portaler med den kommende version 2, hvor der åbnes på for inter-portlet kommunikation,

Afgrænsning til point-to-point interaktion via https Da udgangspunktet i arkitekturen er en point-to-point interaktion via https bliver det aktørernes (IDP, SP) opgave eksplicit at tage hånd om sessioner (cookie baseret), ID provider adresser, og Attribute server adresser, hvor de sidste to via deres implementering som web service kald jo kunne routes igennem en broker, hvis der altså indgik denne mulighed i arkitekturen. På samme måde skal aktørerne også selv bidrage til transaktionsstyring ved, som det foreslås, anvendelse af Assertion ID som transaktionsidentifikator og logning af disse til auditformål. Igen opgaver som en brokerbaseret arkitektur kan håndtere - i brokeren.

I afsnit 11.3.1 nævnes noget om at publicere meta data lokationer i DNS records som en option???

Uklarhed omkring anvendelse af OCES virksomhedscertifikat eller lignende?
Flere steder nævnes det at der skal anvendes OCES virksomhedscertifikat eller lignende ("or equivalent").

Service Provider og IDP MUST forbindes via en SSL sikret linie med anvendelse af OCES Virksomhedscertifikat. Hvad menes der med "or equivalent" i afsnit 7.1.3 side 31? Er alle service providers virksomheder, der har et virksomhedscertifikat? Hvad med udenlandse service providers.

Afsnit 10.9 I starten (side 46) skrives at SP-Attr Service Provider skal anvende OCES eller lignende. Senere i afsnittet (side 47 tredje sidste afsnit) skal (MUST) der anvendes et OCES virksomhedscertifikat.

Afsnit 11.5.2 skrives det at OCES virksomhedscertifikatet "is generally mandatory", vil det sige overvejende, altså at undtagelser kan gøres.

Mapning af pseudonym og subject ID hosService Provider Afsnit 9.2 Mapningen mellem Persistent pseudonyme Attribute er det vel kun SP der skal mappe til det interne subject ID. Derfor ikke "Both Identity provider... and the mapping" sidste afsnit side 42.

Hvad er årsagen til at 'Transient pseudonym profile' ikke understøttes?

Med venlig hilsen
Finn Grønbæk
IT Architect

IBM Denmark, Software Group
Nymøllevej 91, DK2800 Lyngby
Mobile phone: +45 2880 8168
Email: gronbak@dk.ibm.com

----- Forwarded by Finn Gronbak/Denmark/IBM on 09/24/2007 08:40 AM -----

Finn
Gronbak/Denmark/I
BM

09/24/2007 08:37
AM

To
oiostandarder@itst.dk
cc
Søren Peter Nielsen <SPN@itst.dk>,
Sven-Erik
Vestergaard/Denmark/IBM@IBMDK, Jens
Mikael Jensen/Denmark/IBM@IBMDK
Subject
Kommentar til SAML høring

Der skal bruges omtanke og forsigtighed når vi 'skruer' lokale tilføjelser/profiler på såkaldte åbne standarder. Dels kan det give problem når kommunikation sker med 'kunder' uden for landets grænser, også med hensyn til COTS. Nu har IBM jo i tilfældet Rødovre Kommune vist at vi kan understøtte den danske SAML profil med standard software, så indtil nu er alting jo godt.

DK-SAML2.0 understøtter ' Federation using persistent pseudonym profile' der nævnes at det bl.a. kan ske af privacy hensyn. Hvad er årsagen til at 'Transient pseudonym profile' ikke understøttes?

Valg af SAML

At vælge SAML som standard for federeret single sign-on i den offentlige sektor er et godt valg, som falder i godt i tråd med IBM's omfattende support for SAML i IBM's Tivoli sikkerhedsprodukter.

Overordnet vedr. afgrænsning

Denne profil foretager nogle kraftige fravalg, samtidig med at den fokuserer meget på de krav der rejses fra offentlige portaler - specielt borger.dk. Den fremstår derfor som en pragmatisk, taktisk standard og det kunne måske være en fordel at markere det ved f.eks.

Slet ikke at anvende ordet "SAML" i profilens navn, men noget i retning af "Profil for offentlig fælles web login 1.0"
At ændre profilens navn til "DK-SAML 2.0 Web Browser SSO Profile"
Fremhæve denne fokusering i det indledende "prpose" afsnit.
Angive en mulig roadmap for kommende versioner eller profiler under "DK-SAML" - f.eks. "DK-SAML Web Services SSO Profile", DK-SAML WSRPProfile",...

Afgrænsning til en national standard

Med kravet om anvendelse af OCES certifikater afgrænser standarden sig til at være en national standard, som udelukker herboende personer som ikke har eller kan få et OCES certifikat og udenlandske brugere samt udenlandske service providers, der skal udveksle OCES virksomhedscertifikater med ID provideren.

Det giver også problemer i forhold til internationale leverandører af sikkerhedsprodukter, som typisk holder sig til internationale standarder (en af grundene til at vi har dem). IBM's deltagelse i borger.dk proof-of-concept viste i casen med Rødovre Kommune, at dette godt kan lade sig gøre, men der skal foretages ekstra konfigurerings m.v. for at implementere den nødvendige nationale tilpasning.

Afsnit 2.3 om Access via portal

I det beskrevne scenarie fungerer portalen som en ren gennemstilling via et link eller en iframe til en service provider (SP). Portalen er imidlertid selv en SP, som har brug for autentificering af brugere, så de kan tilgå de portalrelaterede resourcer, som portalen er ansvarlig for - f.eks.

portalsider, portlets på portalsider osv. Portalen kan sikkert også selv have brug for Attribute Services.

Afgrænsningen til borger.dk med fravalg af f.eks. WSRP virker lidt som en taktisk, "tilfældig", "pragmatisk" afgrænsning i forhold til at denne standard jo har et bredere sigte. Vedr. WSRP er IBM's support for denne standard i IBM's portalprodukter meget omfattende. WSRP vil sandsynligvis få stor betydning for distribuerede portaler med den kommende version 2, hvor der åbnes på for inter-portlet kommunikation,

Afgrænsning til point-to-point interaktion via https Da udgangspunktet i arkitekturen er en point-to-point interaktion via https bliver det aktørernes (IDP, SP) opgave eksplicit at tage hånd om sessioner (cookie baseret), ID provider adresser, og Attribute server adresser, hvor de sidste to via deres implementering som web service kald jo kunne routes igennem en broker, hvis der altså indgik denne mulighed i arkitekturen. På samme måde skal aktørerne også selv bidrage til transaktionsstyring ved, som det foreslås, anvendelse af Assertion ID som transaktionsidentifikator og logning af disse til auditformål. Igen opgaver som en brokerbaseret arkitektur kan håndtere - i brokern.

I afsnit 11.3.1 nævnes noget om at publicere meta data lokationer i DNS records som en option???

Uklarhed omkring anvendelse af OCES virksomhedscertifikat eller lignende?

Flere steder nævnes det at der skal anvendes OCES virksomhedscertifikat eller lignende ("or equivalent").

Service Provider og IDP MUST forbindes via en SSL sikret linie med anvendelse af OCES Virksomhedscertifikat. Hvad menes der med "or equivalent" i afsnit 7.1.3 side 31? Er alle service providers virksomheder, der har et virksomhedscertifikat? Hvad med

undenlandkse service providers.

Afsnit 10.9 I starten (side 46) skrives at SP-Attr Servie Provider skal anvende OCES eller lignende. Senere i afsnittet (side 47 tredje sidste afsnit) skal (MUST) der anvendes et OCES virksomhedscertifikat.

Afsnit 11.5.2 skrives det at OCES virksomhedscertifikatet "is generally mandatory", vil det sige overvejende, altså at undtagelser kan gøres.

Mapning af pseudonym og subject ID hosService Provider Afsnit 9.2 Mapningen mellem Persistent pseudonyme Attribute er det vel kun SP der skal mappe til det interne subject ID. Derfor ikke "Both Identity provider... and the mapping" sidste afsnit side 42.

Hvad er årsagen til at 'Transient pseudonym profile' ikke understøttes?

Med venlig hilsen

Finn Grønbæk
IT Architect

IBM Denmark, Software Group
Nymøllevej 91, DK2800 Lyngby
Mobile phone: +45 2880 8168
Email: gronbak@dk.ibm.com