inera

Anvisningar e-Tjänster

Anvisningar och rekommendationer för
e-Tjänster i samverkan SAML & SSO

Innehåll

Målgrupp

Målgruppen för detta dokument är utvecklare och förvaltare av e-Tjänster som samverkar i en SAML SSO-miljö. Primärt för Inera's e-Tjänster som samverkar med Säkerhetstjänsternas SSO-miljö.

Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	2013-12-11	Björn Skeppner	Första utgåva
0.2	2013-12-14	Björn Skeppner	Justeringar & tillägg om bl.a SLO och dubbelriktad SSL
0.9	2013-12-15	Björn Skeppner	Lagt till sammanfattning och justeringar efter synpunkter
0.9A	2013-12-23	Björn Skeppner	Justerad och fastlagd efter kommentarer från Christoffer Johansson
0.91	2014-01-23	Björn Skeppner	Justerad efter remissomgång
1.0	2014-02-03	Björn Skeppner	Slutjusterad efter input från programstyrgrupp infrastruktur och Per Mützel
2.0	2014-03-19	Björn Skeppner	Infört anvisningar för Single logout, Signed request samt timeout
2.1	2014-03-28	Björn Skeppner	Testjusteringar efter slutsatser i Arkitekturrådet 2014-03-26
2.2	2017-11-20	Daniel Petersson	Borttag av SSL och uppdatering av referenser

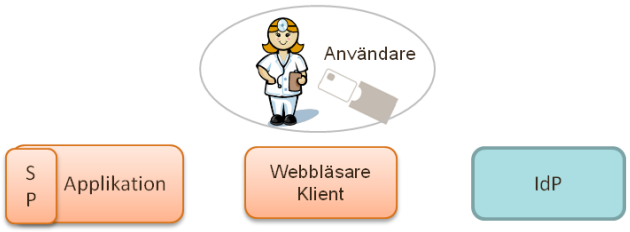
Bidragande till detta dokument har varit (alfabetisk ordning):

Namn	Organisation/Företag
Björn Gustavsson	Inera AB
Christoffer Johansson	Inera AB
Conny Balazs	Certezza AB
Jonas Öholm	SecMaker AB
Magnus Hoflin	Truzzt AB
Per Mützell	Alcesys AB
Roger Öberg	CGI
Ulf Palmgren	Cesam

Sammanfattning

Den sammantagna säkerheten i en Single Sign On-miljö (SSO) hänger på att alla medverkande parter uppfyller kraven, så att tillit till ingående parter uppnås. Parterna är:

- Användaren (aktören)
- E-Arbetsplatsen (PC etc)
- Identitetsutfärdaren (IdP'n)
- e-Tjänsten (applikationen, SP'n)



Användarens ansvar

- Är att följa lagar & föreskrifter som är applicerbara inom e-Tjänstens användningsområde
- Tillse att ingen obehörig har åtkomst till inloggad e-Tjänsten. Vilket t.ex innebär skyldighet att logga ut & stänga e-Tjänsten då e-Arbetsplatsen lämnas obevakad.

e-Arbetsplatsens ansvar

- Är att tillse att kommunikationen med e-Tjänsten samt IdP'n sker med förväntad säkerhet. För att detta ska kunna uppfyllas krävs att den är rätt konfigurerad och har erforderlig programvara installerad och uppdaterad

IdP'n ansvar

- Är att identifiera och autentisera en användare och utställa ett identitetsintyg (SAML-biljett) till de applikationer som aktören avser att nyttja

e-Tjänstens ansvar

- Är att validera riktigheten i identitetsintyget (SAML-biljetten) och utifrån dess behörighetsstyrande attribut tilldela/neka tillgång till funktioner inom e-Tjänsten.

Inledning

Syfte

Syftet med detta dokument är att klargöra minimikrav på de e-Tjänster som samverkar i en SAML SSO-miljö så att förväntad säkerhet uppnås i de samverkande miljöerna. Detta gäller både de e-tjänster som levereras från Inera och andra e-Tjänster som nyttjar Inera's infrastrukturtjänster.

Bakgrund

Detta dokument är ett av tre dokument som levereras såsom en leverans av uppdraget:
" Uppdrag - Hantering av säkerhetsaspekter vid inloggning med SITHS-kort" som i sin tur har sitt ursprung av de incidentrapporter *Inera-INC-22948* och *Inera-INC-22953* som inkom till Ineras servicedesk under september 2013 och resulterade i en rapport:
" Rapport Säkerhetsproblem - SSO 2013-09-12".

De två andra dokumenten som uppdraget levererar är:

- Anvisningar för e-Arbetsplats som används vid inloggning med smarta kort/certifikat [R1]
- Anvisningar för användare vid användandet av e-Tjänster [R2]

Uppdraget skall således hantera anvisningar & krav på följande delar:

- e-Arbetsplatsen –användarens arbetsstation
- e-Tjänsten –den applikation som användaren nyttjar
- Användarens ansvar och skyldigheter

Avgränsningar

Detta dokument hanterar endast krav och riktlinjer på e-Tjänster. Krav på e-Arbetsplatsen och användare beskrivs i andra dokument [R1, R2]. Dokumentet har ej heller ambitionen att vara heltäckande vad gäller parametersättningar, konfigureringar etc utan det förutsetts att en leverantör av en e-Tjänst (SP) har nödvändiga kunskaper i SAML, SSO, PKI & TLS/SSL, eGov2 samt saml2int. Se referens [R3] (SAMBI SAML profile).

Förutsättningar

Ineras leverans

Inera kommer inte att leverera en specifik klientprogramvara eller applikation för sina webbaserade e-Tjänster. GUI:et realiseras i en web-läsare för de e-Tjänster som Inera levererar. Dock ska de krav som ställs på en e-Tjänst också kunna uppfyllas av en rik klient.

Tillit

I en SAML SSO-miljö förutsätts det att det finns en viss form av tillit mellan de samverkande parterna. Parterna är:

- e-Arbetsplatsen (PC-klient etc), inklusive PKI-delen
- IdP'n (Identity Provider)
- SP (Service Provider, e-Tjänsten)
- Användaren
- Federationsoperatörer och dess metadata (aktuellt då tjänsterna är med i SAMBI)

Varje part har ett beroende till de övriga parterna för att säkerhetskedjan ska fungera enligt förväntan. Brister/fel i en av parterna kan medföra att säkerhetskedjan inte är intakt.

När en användare autentiserar sig till IdP'n, ex med sitt SITHS-kort, så krävs det att e-Arbetsplatsen är "relevant" säkerhetspatchad både vad gäller OS, Net iD samt webbläsaren för att förväntad funktionalitet och säkerhet ska uppnås.

IdP'n genomför autentiseringen genom att kräva klientcertifikatsbaserad TLS/SSL baserat på innehavet av certifikat från SITHS. IdP'ns challenge signeras av e-Arbetsplatsen om användaren kan ange rätt PIN-kod för sitt kort

IdP'n behöver även tillit till en spärrfunktion (OCSP-tjänst eller spärrlista) för att kontrollera att användarens certifikat (på t.ex SITHS-kort) är giltigt.

För att autentiseringen skall bli fullbordad krävs att IdP'n har tillgång och tillit till en identitetskälla (ex. HSA-katalogen) för att identifiera användaren och hämta ev behörighetsstyrande egenskaper för användaren.

SSO, Single Sign On

SSO förutsätter att man som användare har en inloggningssession i IdP'n. Dvs har genomfört en godkänd autentisering till IdP'n. Sessionstiden i IdP'n (den tid man har på sig att logga in i e-Tjänster utan att behöva autentisera sig igen) är konfigurerbar och är i Säkerhetstjänster satt till 60 minuter. Är man inloggad i en IdP så behöver man således inom denna tidsperiod inte ange sin PIN-kod på kortet igen, utan IdP'n utfärdar en SAML-biljett till e-Tjänsten via webbläsaren. Webbläsaren upprättar då en unik session mellan webbläsaren och e-Tjänsten. Denna session "lever" så länge som användaren är inloggad och aktiv i e-Tjänsten. För att avsluta denna session måste användaren aktivt logga ut ur e-Tjänsten (eller bli utloggad av e-Tjänsten genom

inaktivitet), alternativt stänga samtliga öppna webbläsare, vilket dock bara avslutar sessionen på klienten. Det är således webbläsaren som tillsammans med e-Tjänsten samverkar kring en SSO-session.

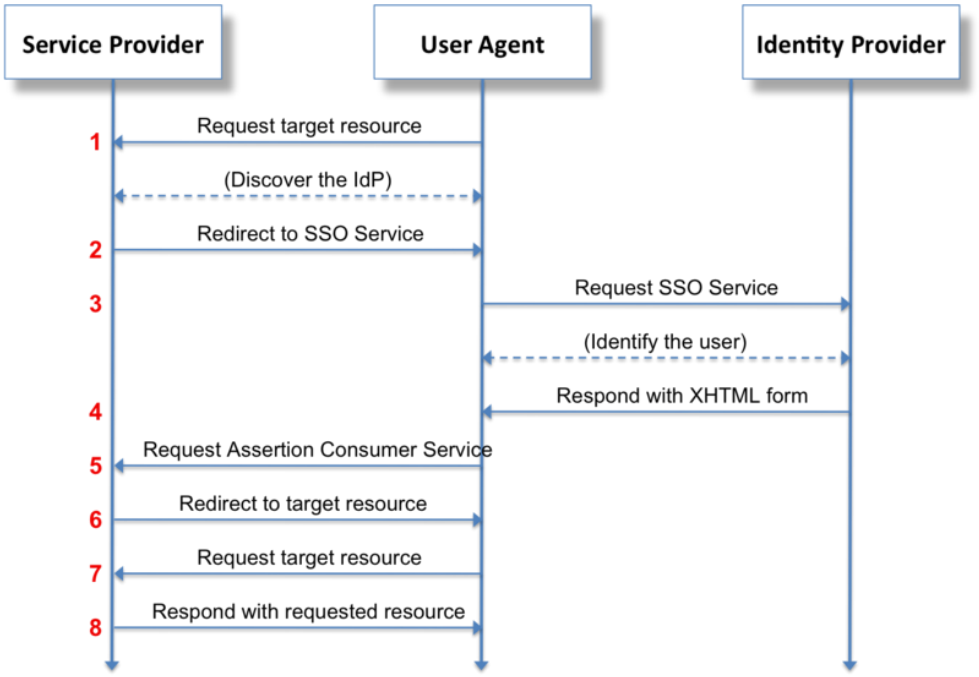
Det riktlinjer som finns i detta dokument ska inte påverka SSO. Dvs användaren ska inte behöva uppleva en försämring i en **pågående arbetssession** med krav på extra inloggningar och uppdragsval, SSO ska fungera som förväntat.

SLO, Single Logout

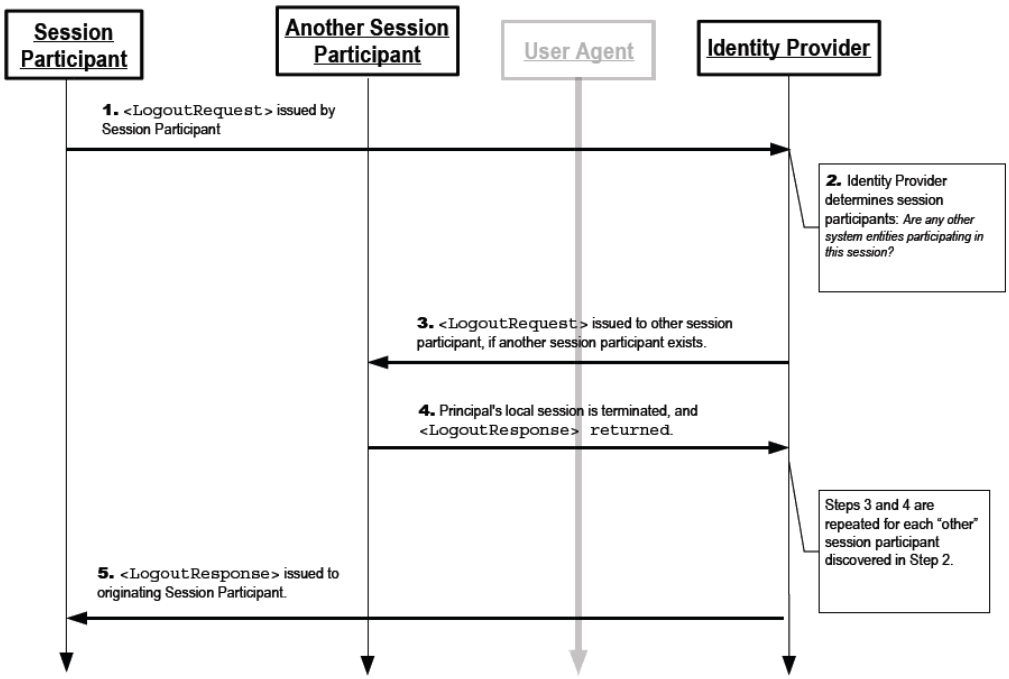
För att en användare på ett säkert sätt ska kunna avsluta sin användning av en e-Tjänst så behöver e-Tjänsten ha en logoutfunktion. Denna logoutfunktion skall avsluta användarens session i e-Tjänsten samt till inloggningstjänsten (IdP'n) skicka en utloggningsbegäran (SAML SLO request). e-Tjänstens medverkan i SAML SSO deklareras via SAML metadata.

Övriga förutsättningar

- Följsamhet till SAML2-standarden [R6]
- Följsamhet till SAMBI SAML profile [R3]
- Riktlinje för klientdator som används vid inloggning med smarta kort/certifikat [R1]
- Riktlinjer för användare vid användandet av e-Tjänster [R2]
- Kompabilitet med eGov2 samt saml2int (specificerat i SAMBI SAML profile [R3])
- Att man möter upp de krav i aktuella tillitsramverk vilka är applicerbara på en SP. För Inera's tjänster kommer detta att innebära SAMBI's tillitsramverk



Figur 1, SAML SSO (från Wikipedia)



Figur 2, SAML SLO

Krav på e-Tjänsten

Krav

Användardialoger

- Vid inloggning till e-Tjänsten bör tjänsten informera användaren om att den ska logga ut ur tjänsten när den avslutar arbetet
- Det ska i e-Tjänstens grafiska gränssnitt tydligt framgå vem det är som är inloggad
- Det ska i e-Tjänsten finnas en tydlig utloggningsfunktion (logoutknapp/meny). Denna funktion ska stänga sessionen och avsluta applikationen samt initiera en SLO-begäran till IdP'n. Lämplig text på en sådan knapp/meny är: "Logga ut"
- När användaren loggar ut ska det tydligt visas att sessionen mot tjänsten är avslutad. Om det är en webbapplikation bör användaren även uppmanas om att stänga alla webbläsare.
  Exempel från Inera's e-post: "Du har loggats ut från Outlook Web App. Skydda e-postkontot genom att stänga alla webbläsarfönster"
  Exempel från MVK: "Av tekniska skäl måste du stänga webbläsaren helt för att logga ut"

e-Tjänsten

- Ska använda etablerade ramverk för SAML-implementation, ex Open SAML [R5]
- Ska använda standardbibliotek för SSL/TLS (Open SSL, RSA BSAFE, MS-CAPI/CryptoAPI etc)
- Ska använda de senaste versionerna av TLS (helst TLS 1.2) [R4], bl.a beroende på vilka webbläsare man vill supporta
- Ska säkerställa robusthet mot BREACH/CRIME. Exempelvis genom att undvika TLS & http-komprimering (gZip etc) Se ref [R7]
- Ska säkerställa att nyckelhanteringen (certifikaten) hanteras säkert och skyddat
- Bör stänga av dåliga kryptoalgoritmer och versioner av SSL som man inte bör använda. (För mer information, se bilaga 1, SSL/TLS Cipher suites)
  Se exempel nedan:

  Exempel på konfigurering i Apache

  Se: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html

  Exempel på inställningar i IIS Webserver

  Se: https://msdn.microsoft.com/sv-se/library/dn786418(v=ws.11).aspx

- Ska tillse att klockorna är synkroniserade med IdP'n. Bl.a viktigt för validering av SAML-biljettens giltighet. Exempelvis genom en publik NTP-referens
- SAML-biljetten ska valideras. Framförallt vad gäller giltighet och signatur
- Ska ha "replay detection" för att man inte ska kunna återanvända en SAML-biljett
- Ska ha en XML-parser som är säkerställd mot XML injection [R8] samt XML signature wrapping attack (XSW) [R9]
- Bör ha stöd för LoA-filtrering istället för enbart autentiseringscontext (dvs. att SP:n kräver en viss LoA-nivå i SAML respons istället för autentiseringsmetod) `urn:sambi:names:attribute:levelOfAssurance`
- Ska ha stöd för Single Logout (både IdP-initierad och SP-initierad)
  För de e-Tjänster som av speciella undantagsskäl ej är lämpliga att medverka i SLO så ska detta hanteras genom explicit hantering via metadata. SLO förväntas hanteras via front channel.
- Bör ha stöd för Identity Provider Discovery Service Protocol Profile (IdPDisco)
- Ska ha stöd för subjectConfirmation method (bearer, senderVouches) samt den timer som kan sättas i detta element (tiden som en klient har på sig att etablera en SP-session med uppvisat intyg)
- Ska kontrollera att IdP'ns `<saml2:SubjectConfirmationData InResponseTo=>` motsvarar SP:ns `<samlp:AuthnRequest ID>`
- Bör undvika beroende till funktioner i Net iD som är beroende av programvarans konfiguration på klienten. Ett sådant exempel är Net iD plugin. Eventuella avsteg ska godkännas genom ett AB av arkitekturledningen
- Bör ha automatisk avslut av e-Tjänsten vid inaktivitet , ex >15 minuter. Ett sådant avslut ska ej resultera i en SLO request
- Ska minst utföra behörighetskontroll utifrån de behörighetsstyrande attribut som är specificerade i Sambi SAML-profile [R3] och relevanta för e-Tjänsten
- Ska EJ signera inloggningsbegäran (signed request) till IdP'n
- Ska föra logg över in- och utloggningar (minst: vem, när, inloggningsmetod, utloggning/avslut)

Tester

- För att säkerställa e-Tjänsten (SP) säkerhet så rekommenderas bl.a:
  https://kantarainitiative.org/confluence/display/certification/SAML+2.0+Full+Matrix+Test+Event
  Framförallt om e-Tjänsten är en nyutvecklad SAML-implementation

- Validering, härdning och penetrationstest av SP-funktion och tillhörande applikation, utförs lämpligen genom en oberoende testpartner.

Referenslista

Ref	Dokumentnamn	Dokument
R1	Anvisningar för klientdator som används vid inloggning med smarta kort/certifikat	https://www.inera.se/globalassets/tjanster/sakerhetstjanster/dokument/anvisningar-single-sign-on/anvisningar_for_klientdator_vid_inloggning_med_certifikat_pa_smarta_kort_v_1_1.pdf
R2	Anvisnngar för användare vid användandet av e-Tjänster	https://www.inera.se/globalassets/tjanster/sakerhetstjanster/dokument/anvisningar-single-sign-on/anvisningar_anvandare_av_e_tjanster_v_1_0.pdf
R3	SAMBI SAML profile	https://confluence.cgiostersund.se/display/ST/SAML+Profil
R4	SSL/TLS	http://en.wikipedia.org/wiki/Transport_Layer_Security
R5	Open SAML	https://wiki.shibboleth.net/confluence/display/OpenSAML/Home
R6	Security Assertion Markup Language (SAML) V2.0 Technical Overview	https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf
R7	A BREACH beyond CRIME	http://breachattack.com/
R8	Testing for XML Injection (OWASP-DV-008)	https://www.owasp.org/index.php/Testing_for_XML_Injection_(OWASP-DV-008)
R9	On Breaking SAML: Be Whoever You Want to Be	https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91.pdf