Anvisningar för användare vid användning av e-Tjänster

Anvisningar och rekommendationer för användare av 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.

Dokumentet ska tjäna som ett stöd för e-tjänsternas användaranvisningar.

Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	2013-12-16	Björn Skeppner	Första utgåva
0.2	2013-12-17	Björn Skeppner	Smärre justeringar
0.9	2013-12-18	Björn Skeppner	Justerad efter synpunkter
1.0	2014-01-23	Björn Skeppner	Justerad efter första remissomgång

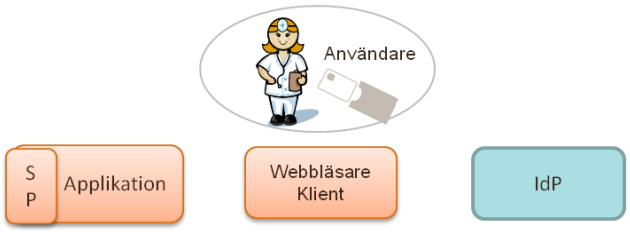
Bidragande till detta dokument har varit (alfabetisk ordning):

Namn	Organisation/Företag
Ewa Jerilgård	CeHis
Ulf Palmgren	Cesam

Sammanfattning

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

- Användaren
- e-Arbetsplats (PC, läsplatta etc)
- Identitetsutfärdaren (IdP:n)
- e-Tjänsten (applikationen, SP:n)



Användarens ansvar

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

e-Arbetsplatsens ansvar

- Är att tillse att kommunikationen med e-Tjänsten och 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 e-Tjänster 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 vilka krav som ställs på en användare av e-Tjänster som levereras av Inera.

Bakgrund

Detta dokument är ett av tre dokument som levereras såsom en leverans av uppdraget:
” Uppdrag - Hantering av säkerhetsaspekter vid inloggning med SITHS-kort” [R1] 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” [R2].

De två andra dokumenten som uppdraget levererar är:

- Anvisningar för e-Arbetsplats som används vid inloggning med smarta kort/certifikat [R3]
- Anvisningar för användare vid användandet av e-Tjänster [R4]

Uppdraget skall således hantera riktlinjer & krav på följande delar:

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

Avgränsningar

Detta dokument syftar endast till att ge förvaltningar/leverantörer av e-Tjänster underlag till anvisningar och användarkrav till de användare som är brukare av e-Tjänsten.

Förutsättningar

Lagstiftningar

Patientdatalagen SFS 2008:355 [R1]

4 kap. Grundläggande bestämmelser om inre sekretess och elektronisk åtkomst inom en vårdgivares verksamhet
Inre sekretess
1 §
Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

Författningssamlingar

SOSFS 2008:14 [R2]

Hälso- och sjukvårdspersonalens och andra befattningshavares ansvar
20 § Den hälso- och sjukvårdspersonal, entreprenör, uppdragstagare eller annan som arbetar för en vårdgivare eller som har slutit avtal med en vårdgivare ska

1. ansvara för att personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för obehöriga,
2. ansvara för att datorer eller andra informationsbärare som har använts inte lämnas utan att patientuppgifterna är skyddade från obehörig åtkomst, och
3. endast ta del av patientuppgifter, om han eller hon deltar i vården av patienten eller av något annat ändamål som anges i 2 kap. 4 och 5 §§ patientdatalagen (2008:355) behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

Rekommendationer på krav som bör ställas på användaren

- Att användaren inte ska lämna en e-Arbetsplats obevakad då användaren är inloggad på en e-Tjänst med patientinformation
- Att om användaren lämnar e-Arbetsplatsen tillfälligt ska användaren antingen logga ut ur alla e-Tjänsten eller aktivera personligt lösenordsskyddad skärmsläckare eller motsvarande samt avlägsna sin e-legitimation (ex SITHS-kortet)
- Att då användaren loggar ut ur e-Tjänsterna för att lämna sin e-Arbetsplats även avslutar samtliga webläsarfönster samt avlägsna sin e-legitimation (ex SITHS-kortet)
- Att användaren inte får ändra inställningarna på e-Arbetsplatsen som rör hantering av e-tjänstekort, exempelvis inställningar för smartkortsläsare och Net iD
- Att användaren bara använder e-Arbetsplatsen i enlighet med verksamhetens regelverk
- Att användaren rapporterar misstänkta incidenter som kan tänkas påverka e-Arbetsplatsens skyddsnivå
- Att e-Arbetsplatsen endast får vara ansluten till av verksamheten godkända nätverk
- Att användaren ska skydda och ej avslöja PIN-koden till sin e-legitimation (ex SITHS-kortet)

Referenslista

Ref	Dokumentnamn	Dokument
R1	Patientdatalagen SFS 2008:355	http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdatalag-2008355_sfs-2008-355/
R2	Socialstyrelsens	http://www.socialstyrelsen.se/sosfs/2008-14
R3	Riktlinje för klientdator som används vid inloggning med smarta kort/certifikat	URL
R4	Riktlinjer för användare vid användandet av e-Tjänster	URL