Kravunderlag inom området Identitet och Åtkomst

Specifik kravställning inom området identitets- och åtkomsthantering att utnyttja som underlag vid nyanskaffning av informationssystem.

Ett kompletterande dokument till *Referensarkitektur för Identitet och Åtkomst* (*IAM*).

Version 1.0 PA3

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Innehåll

1 Dokumentinformation

1.1 Revisionsinformation

Version	Datum	Beskrivning	Författare
1.0 PA1	2016-11-02	Arbetsmaterial (upp till version 1.3).	Arbetsgruppen IDA Access
1.0 PA2	2016-11-24	Byte av mall, redaktionella justeringar, inledning. Mindre justeringar av krav #2 och #5. För slutgranskning i arbetsgruppen.	Per M
1.0 PA3	2016-11-25	Justerad version för utskick.	Per M

1.2 Referenser[1]

Id	Referens/dokument
REF_IAM	Referensarkitektur - Identitet och åtkomst

[1] Övriga referenser anges primärt som fotnot i löpande text. Se även [REF_IAM] för ytterligare referenser.

2 Inledning

Detta dokument avser utgöra ett underlag för kravställning på informationssystem som nyttar tjänster inom området identitets- och åtkomsthantering. Underlaget är primärt tänkt att användas vid nyanskaffning av system. Används kraven vid vidareutveckling/anpassning av befintliga informationssystem kan kravnivåerna behöva anpassas till aktuella förutsättningar.

Kraven baseras på *Referensarkitektur för Identitet och Åtkomst,* vilken beskriver ett ramverk och tekniska krav för ett samverkande system för en ändamålsenlig identitets- och åtkomsthantering. För ytterligare förklaring/motivering av kraven samt använda förkortningar i detta dokument hänvisas till [REF_IAM].

Notera att detta dokument fokuserar på informationssystemet, dvs. systemet som slutanvändare nyttjar för informationsåtkomst. Referensarkitekturen ställer även krav på IT-infrastrukturen i form av förmågor och stödtjänster, vilket vidare beskrivs i [REF_IAM].

3 Kravställning

Med ”systemet” avses nedan ett informationssystem som tillhandahåller funktion och information till användare, exempelvis ett vårdinformationssystem eller administrativt informationssystem.

Kravnivån (ska respektive bör) är avpassad för nyanskaffning (upphandling/nyutveckling) av informationssystem. Kravnivån kan anpassas till det aktuella sammanhanget, t.ex. ett vidareutvecklingsuppdrag avseende ett befintligt system. I dessa fall rekommenderas att stämma av med huvuddokumentet [REF_IAM], för att säkerställa att kravnivåerna blir rätt avvägda.

3.1 Specifika krav inom Identitet och åtkomst

1. Systemet **ska** stödja en extern stödtjänst för federerad inloggning, här kallad *Identifieringstjänst* (även *Identity Provider, IdP*), vars ansvar är att identifiera och autentisera användare som begär åtkomst till systemet.

   Motiv: Underlättar att skapa en samordnad användarinloggning med hög igenkänningsfaktor och hög tillit. Ökar flexibiliteten och möjliggör att lägga till nya inloggningsmetoder som är anpassade för verksamheten utan att påverka anslutna e-tjänster. Skapar även grundförutsättningar för en samlad administrationspunkt, federativa lösningar och återanvändning av investeringar i säkerhetsteknik. Minskar inlåsningseffekterna mot viss hårdvara och mjukvara.

2. Systemet **ska** ansluta till Identifieringstjänst för federerad inloggning enligt något av följande alternativa standardprotokoll:

   - *SAML 2.0 samlp*[2]
     - *Web Browser SSO Profile*
       - SP-initierad SSO: Redirect/POST Binding.
       - IdP-initierad SSO: POST Binding.
     - Följsamhet till implementionsprofilerna eGov 2.0[3] samt saml2int[4]

[2] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

- *OpenID Connect 1.0*[5]
  - enligt *OpenID Connect Conformance Profiles*[6], minst stöd för en av *Basic Relying Party* respektive *Implicit Relying Party*.

Motiv: Ger en lös och standardiserad koppling mellan e-tjänsterna och de generella funktionerna för identitet och åtkomst. Produktanpassningar blir applicerbara på en global marknad, och bättre förutsättningar för att marknadens produkter kommer anslutningsklara från början.

3. Inloggningsmetod (autentiseringsmetod) **ska** kunna anpassas och förändras utan krav på förändring av systemet, genom att inloggningen delegeras till Identifieringstjänst.

   Motiv: Gränssnittet mot e-tjänsten blir stabilare över tid då det inte påverkas av nya användarkrav på inloggningsfunktionen eller den senaste autentiseringstekniken, vilket ger ökad förvaltningsbarhet och minskade kostnader för IT-säkerhetslösningar. E-tjänsten kan i första hand fokusera på den verksamhetsfunktion den ska leverera.

4. Systemet **ska** ha en för användaren tydlig utloggningsfunktion. Denna utloggningsfunktion ska avsluta användarens session i systemet samt skicka en utloggningsbegäran till Identifieringstjänsten.
   - För SAML 2.0: SAML Logout (Front-channel, POST-binding rekommenderad)
   - För OpenID Connect: Front-channel/Back-channel Logout

   Motiv: Tydlighet mot användaren hur hen avslutar sin session är viktigt. Utloggningsbegäran syftar till att inte en etablerad SSO-session ska kunna missbrukas, dvs. att det avkrävs en ny autentisering för att logga in på nytt i

---

[3] http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf

[4] http://saml2int.org/profile/current

[5] http://openid.net/developers/specs/

[6] http://openid.net/wordpress-content/uploads/2015/02/OpenID-Connect-Conformance-Profiles.pdf

systemet.

5. Systemet **ska** kunna göra en grundläggande behörighetsutvärdering[7] baserat på attribut i en digital biljett (intyg) utfärdad av Identifieringstjänst (intygsutfärdaren) enligt standarderna *Json Web Tokens* (*JWT*) respektive *SAML 2.0*.

   Motiv: en gemensam bas för identitet och behörighet skapar förutsättning för god skalbarhet och minskad administrativ börda i verksamheterna. Möjligheter skapas för att konsolidera huvuddelen av Identitets- och behörighetsadministrationen till en funktion där en användare samlat kan ges grundläggande rättigheter att arbeta med de IT-system och den information som hens arbete kräver. Även borttag av rättigheterna (t.ex. när medarbetare slutar anställning) underlättas.

6. System med behov av säker åtkomst till skyddade integrationsgränssnitt (api:er), **bör** ha möjlighet att använda en av följande profiler för att utgående från ett tidigare erhållet identitetsintyg erhålla åtkomstintyg från en *åtkomstintygsutfärdare* enligt *OAuth2.0*:
   - *SAML 2.0 Bearer Assertion* - RFC 7522[8] (för att integrera med existerande identitetssystem.)
     alternativt
   - *JWT Bearer Assertion* - RFC 7523[9] (för att integrera med existerande identitetssystem.)

   Motiv: Vid implementering av säker åtkomst till bakomliggande api:er bör standarder som är ämnade för detta syfte följas. Om funktionen dessutom kan nyttja autentisering utförd av Identifieringstjänsten, kan användaren få en upplevelse av singelinloggning (SSO) dvs. ytterligare autentisering av användare kan undvikas.

[7] Notera att systemet kan utföra kompletterande utvärderingar av behörighet baserat på andra underlag av betydelse för systemet. Se även [REF_IAM] för mer information.

[8] http://tools.ietf.org/html/rfc7522

[9] http://tools.ietf.org/html/rfc7523

7. Systemet **bör** kunna nyttja samtliga övriga implementerade tjänster beskrivna i den nationella referensarkitekturen för identitet och åtkomst [REF_IAM].

   Motiv: Anpassning mot referensarkitekturens stödtjänster och principer skapar förutsättning för att erhålla alla de tänkta positiva effekterna inom området.

8. Om systemet har eget identitetsdatalager **bör** systemet erbjuda ett öppet (dokumenterat och tillgängligt för kund) integrationsgränssnitt för att skapa, uppdatera, radera användarprofiler.
   - Rekommenderat protokoll: *SCIM*[10], se vidare [REF_IAM].

   Motiv: Möjliggör konsolidering av Identitets- och behörighetsadministration. Minskad administrativ börda i verksamheterna.

3.2 Generella krav på nätverkskommunikation

Nedan krav avser skydd av den nätverkskommunikation som sker i samband med kommunikation mellan systemet och externa stödsystem. Kraven kan ses som generella, men är också en nödvändig förutsättning för att uppnå avsedd skyddsnivå med de säkerhetsprotokoll som är kravställda.

9. Systemet **ska** möjliggöra kommunikation enligt standarden *HTTP1.1*.

   Motiv: grundläggande underliggande protokoll för interoperabilitet i enligt med aktuella standardval.

10. All nätverkskommunikation mellan parterna (system och stödtjänster) **ska** skyddas med *TLS* på transportnivå i enlighet med *RFC 7525*[11] som efterlever kraven enligt *oWasp* rekommendationer[12].

    Motiv: Följsamhet till säkerhetskrav som är obligatoriska i aktuella val av standardprotokoll (SAML 2.0, OpenID Connect respektive OAuth2.0)

[10] https://tools.ietf.org/html/rfc7644

[11] https://tools.ietf.org/html/rfc7525

[12] https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet