Infrastruktur med möjligheter

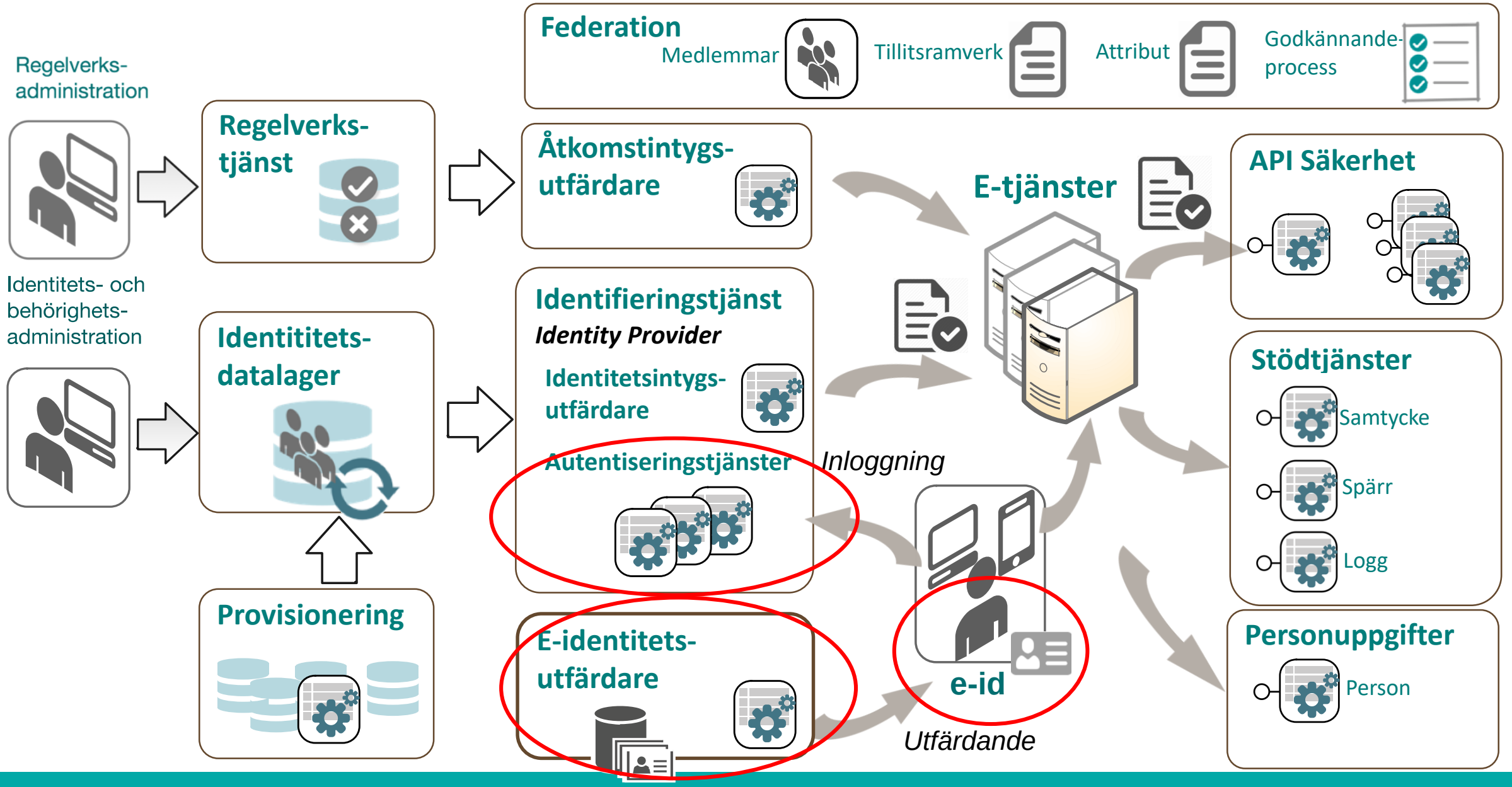
Anvisning Autentisering (dokumentet är i status 1.0 RC1)

Bengt-Göran Andersson, Inera

IT Säkerhetsansvarig

2017-09-28

Följer Referensarkitektur för Identitet och åtkomst



Bakgrund till Anvisningen

- Startade med krav från Ineras certifiering av 3-parts applikationer som vill ansluta mot de tjänster som Ineras tillhandahåller med patientinformation.
- Certifieringen har ett starkt behov av ett tydligt bedömningsunderlag för att utvärdera vald autentiseringsteknik i våra tjänster och 3-partsprodukter

Mål med Anvisning Autentisering

- Anvisning ska beskriva de krav Inera har på autentisering för att användare ska få ta del av patientinformation.
- Ett annat mål är att vårdsverige signalerar ett starkt behov av ett förenklat autentiseringsförfarande för användare i verksamheten.
- Tydlighet i bedömningen av en autentiseringsteknik
  - Grönt är godkänd nivå
  - Gult är acceptabel nivå
  - Rött är inte acceptabel nivå.

Workshops och grottforskning

- Initierades med ett antal workshop runt autentisering
- Anvisningen bygger mycket på eIDAS tillitsramverk för utgivning och själva autentiseringstekniken

Foto: Eneko Bidegain

Autentisering och Auktorisering

- Många blandar ihop begreppen:
  - Autentisering (identifiering)
  - Auktorisering (behörighet)
- Autentisering är att jag vill veta vem du är, med olika tillitsgrader
- Socialstyrelsens har krav på stark autentisering

Vad är stark autentisering?

Socialstyrelsen och EU Kommissionen har tagit fram begrepp och definitioner för stark autentisering

- HSLF-FS 2016:40. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.
  - 2 kap Definitioner:
  - **Stark autentisering**: kontroll av identiteten på två olika sätt

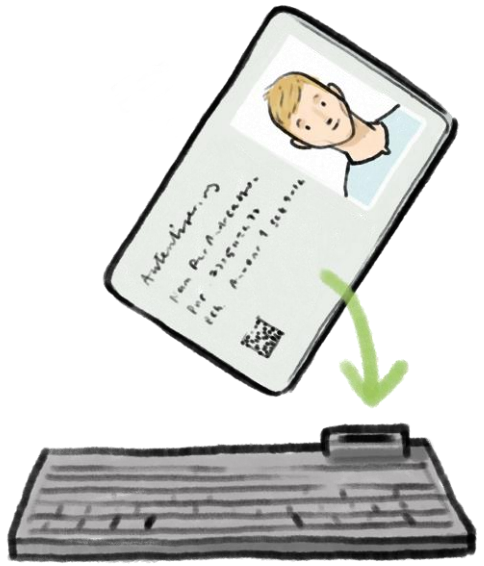
Stark autentisering enligt Socialstyrelsen

HSLF-FS 2016:40

Öppna nät

3 kap 15 § Om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att

1. överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dom, och
2. elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av **stark autentisering**.

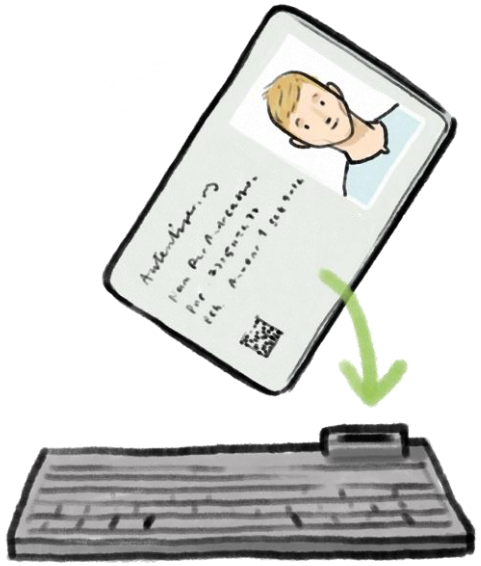


Stark autentisering enligt Socialstyrelsen

HSLF-FS 2016:40

Direktåtkomst till uppgifter om den enskilde själv

- 4 kap 11 § Vårdgivaren ska ansvara för att en enskilds direktåtkomst till uppgifter om sig själv och till dokumentation om åtkomst tillåts endast efter att den enskildes identitet har säkerställts genom **stark autentisering**.



Stark autentisering enligt eIDAS?

- EU:s förordning om gränsöverskridande elektronisk legitimering (eIDAS-förordningen).
  - Började tillämpas 1 juli 2016 men den 29 september 2018 krävs också att svenska offentliga myndigheter erkänner utländska e-legitimationer i svenska e-tjänster.
- KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2015/1502
  - Om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Autentiseringsfaktorer, Tillämpliga definitioner

- **Autentiseringsfaktor**: en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier:

  a. *innehavsbaserad autentiseringsfaktor:*

     en **autentiseringsfaktor** som personen måste kunna visa att den **innehar**.

  b. *kunskapsbaserad autentiseringsfaktor:*

     en **autentiseringsfaktor** som personen måste kunna visa att den har **kunskap** om.

  c. *egenskapsbaserad autentiseringsfaktor:*

     en **autentiseringsfaktor** som utgår från en **kroppslig egenskap** hos en fysisk person, som denne måste kunna visa att den har.

Harmonisering av tillitsnivåer

- E-Legitimationsnämnden pekar på ISO 29115 med fyra LoA, ”Level of Assurance” nivåer
  - 1 – Low, ”Little or no confidence in the asserted identity”
  - 2 – Medium, ”Medium Some confidence in the asserted identity”
  - 3 – High, “High confidence in the asserted identity”
  - 4 – Very high, “Very high confidence in the asserted identity”
- eIDAS säger tre tillits nivåer:
  - Låg
  - Väsentlig
  - Hög

eIDAS Tillitsnivå	Erforderliga beståndsdelar	Tillitsnivå (LoA) enligt ISO 29115
Låg	1. Medlet för elektronisk identifiering använder minst **en autentiseringsfaktor**. 2. Medlet för elektronisk identifiering är utformat så att utfärdaren vidtar **rimliga** åtgärder för att kontrollera att det endast används under ägarens kontroll eller innehav.	2 – Medium ”Medium Some confidence in the asserted identity”
Väsentlig	1. Medlet för elektronisk identifiering använder **minst två autentiseringsfaktorer från olika kategorier.** 2. Medlet för elektronisk identifiering är utformat så att det kan **antas** att det endast används under ägarens kontroll eller innehav.	3 – High “High confidence in the asserted identity”
Hög	**Nivå väsentlig,** samt 1. medlet för elektronisk identifiering skyddar mot kopiering och manipulering samt mot angripare med hög angreppskapacitet, 2. medlet för elektronisk identifiering är utformat så att ägaren på **tillförlitligt** sätt kan skyddas mot användning av andra.	4 – Very high “Very high confidence in the asserted identity”

Utfärdandeprocessen

Utfärdandeprocessen

- Även om en autentiseringsteknik i sig ses som väldigt säker så kan inte en teknik uppfylla en tillit om inte :
  - Styrkande och kontroll av identitet
  - Utfärdandet
  - Leverans
  - Aktiveringsprocessen

för att ställa ut medlet för den elektroniska identifieringen

Styrkande och kontroll av identitet

- eIDAS har tre tillits även nivåer på Styrkande och kontroll av identitet (fysisk person):
  - Låg
  - Väsentlig
  - Hög

Utfärdande, leverans och aktivering

- eIDAS har tre tillits även nivåer på Utfärdande, leverans och aktivering
  - Låg
  - Väsentlig
  - Hög

Utfärdandeprocessen

Viktigt:

- Utfärdandeprocessen av medlet för den elektroniska identifieringen måste alltid granskas och riskbedömas tillsammans med autentiseringstekniken för att ge en helhetsbild av lösningen.

Grundprinciper gällande åtkomst till patientinformation

inera

Grundprinciper gällande åtkomst till patientinformation

- Baserat på eIDAS Genomförandeförordning 1502/2015 är grundprincipen att en användares medel för elektronisk identifiering skall vara minst på **nivå Väsentlig** som så står i paritet med ISO 29115 Level of Assurance LoA 3 för att få åtkomst till patientinformation för tjänster som Inera tillhandahåller.

Giltighetstider och skärmlåsning

- Giltighetstiden för en stark autentisering
  - Sessionstid mot vårdsystem, basvärde 4 timmar
  - Tänjas till maximalt 12 timmar, beroende på verksamhet

- Låsning av skärm
  - För att förhindra obehörig åtkomst av patientinformation
    - Basvärde 1-2 minuter om obehöriga kan vistas i lokalen
  - Kontrollerad miljö
    - Operationssal, hela operationstiden.
    - Ambulans >30 minuter

Ärvda legitimationer

Ärvd legitimering = ID Växling (ELN)

- Förnya ett utgående certifikat
- Skapa mjuka certifikat till mobila enheter (P12:or)
- Icke certifikatbaserade enheter (kortlivade)

Förenklat autentiseringsförfarande

- Verksamheten har, under en arbetsdag, behov av att enkelt låsa och låsa upp en terminal
  - Efter krav på godkänd stark autentisering kunna ärva legitimationen till t.ex. en kontaktlös ID enhet.
  - Den förenklade får ej skapa nya ärvda legitimationer

Foto: Phil Hilfiker

Autentiseringsmetoder

- Certifikatbaserade, ”X.509” Smarta kort
- Certifikatbaserade, ”X.509” Mobila certifikat
- Engångslösenord (OTP, One-Time Password)
- Autentisering med OTP via SMS
- Certifikatbaserade, Bankkort/BankID
- Certifikatbaserade, Mobilt BankID
- Autentisering med Användarnamn och Lösenord

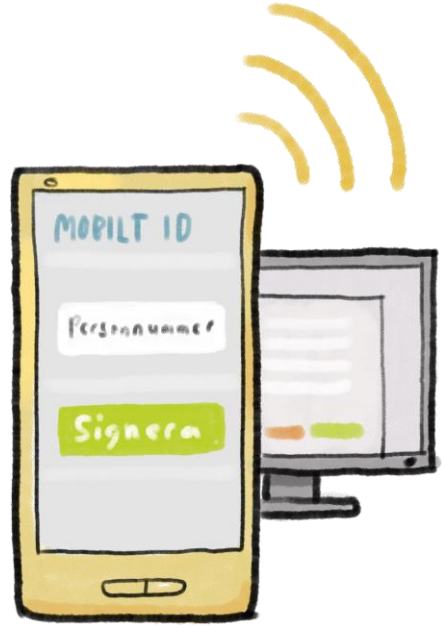
- Biometriska metoder
  - Då som ensam autentiseringsmetod

BankID

- Vad är avsikten med BankID?
  - ”Good enough” för access till den enskildes uppgifter
- Vad har vi för tillit till utgivningsprocessen?
- Vad har vi för tillit till bankernas CA dvs. certifikatutgivning?
- Vår bedömning **just nu** är:
  - BankID är ”Good enough” för MVK/Journalen dvs. för din egen journalinformation men i **dagsläget inte** för att få åtkomst till patientinformation för tjänster som Inera tillhandahåller.

Mobilt BankID

- Vad är avsikten med Mobilt BankID?
  - Att användas för autentisering till **Egen information** på Banken, Skatten, Försäkringsbolag
- Vem är kravställare för autentiseringstjänsten Mobilt BankID?
- Vem har granskat Mobilt BankID?
- ELN säger på sin hemsida om Svenska e-legitimationer
  - Övriga svenska e-legitimationer som är välspridda och allmänt accepterade inom Sverige
    - Mobilt BankID, BankID på kort och fil
    - Telia
- Vår bedömning **just nu** är:
  - Mobilt BankID är ”Good enough” för MVK/Journalen dvs. för din egen journalinformation men i **dagsläget inte** för att få åtkomst till patientinformation för tjänster som Inera tillhandahåller.



Biometriska metoder

- Referensarkitekturens styrande princip ”#IA10:
  - Vid användning av biometri för autentisering bör biometrisk data hållas nära användaren själv, helst endast inom användarens personliga eidentitetsbärare. Biometri bör inte användas som den enda faktorn i en autentiseringslösning.”
- Ineras bedömning
  - Bedömningsgrunden är alltså att t.ex. fingeravtrycks och irisskanning kan och ska endast användas som ersättning för PIN-kod och ska inte lagras centralt då det är svårt att revokera biometriskt baserad information.

Foto: Miguel Librero

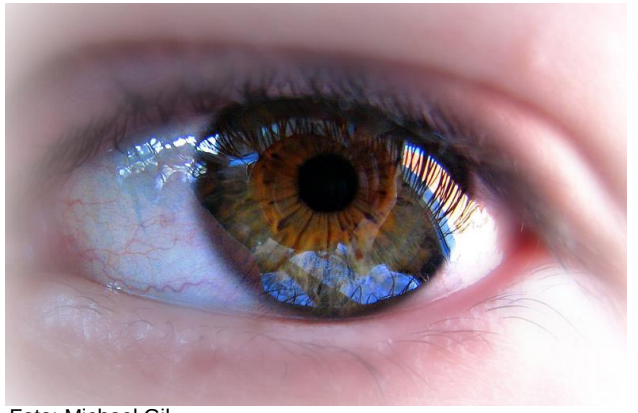


Foto: Michael Gil

Frågor?

Bengt-Göran Andersson

bengt-goran.andersson@inera.se

08-452 7132


inera