Anvisning Autentisering

Principer och rekommendationer för åtkomst till patientinformation för tjänster som Inera tillhandahåller

V1.1

Reviderat och godkänt av Petter Könberg

Datum
2018-10-15

Innehåll

1. Dokumentinformation

1.1 Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2017-11-01	BGA/FR	Beslut att sätta anvisningen till v1.0
1,1	2018-08-01	BGA	Punkten 5.1.2 Automatisk utloggning vid inaktivitet tillagd. Efos kort finns nämnt tillsammans med SITHS. Referenslista och Förkortningar är uppdaterad och placerad sist i dokumentet. Förkortningar flyttat till början av dokumentet.

1.2 Revidering

Anvisning Autentisering ska revideras årligen eller när skäl finns att uppdatera hela eller delar av dokumentet. Revisionsinformation dvs. nuvarande status på anvisningen finns på första sidan.

Ineras Informations- och IT-säkerhetsfunktion är ägare av denna Anvisning.

Det åligger varje e-tjänsteförvaltning att följa denna anvisning.

2. Förkortningar

Ett urval av använda förkortningar/beteckningar.

CA	Certificate Authority
OTP	One-Time Password
IdP	Identity Provider
SS7	Signalling System No. 7. En uppsättning protokoll som beskriver kommunikationen mellan system och enheter i nätverk för mobiltelefoner.
HSA	Katalogtjänst https://www.inera.se/tjanster/katalogtjanst-hsa/
EMV	Europay, Mastercard och Visa. Betalningsmetod baserad på teknisk standard för betalning med smarta kort.

NFC	Near Field Communication. Överföringsmetod för kontaktlöst utbyte av data på korta sträckor.
PKCS	Public Key Cryptography Standards. https://en.wikipedia.org/wiki/PKCS
NPÖ	Nationell patientöversikt https://www.inera.se/tjanster/nationell-patientoversikt-npo/
SITHS	Identifieringstjänst https://www.inera.se/tjanster/identifieringstjanst-siths/
FIDO	FIDO Alliance är en icke vinstdrivande organisation med syfte att adressera interoperabilitet och användbarhet för autentiseringslösningar. https://fidoalliance.org
X.509	ITU-standard och ramverk inom X.500 för autentisering definierar även en standard för digitala certifikat inom PKI, Public Key Infrastructure
NIST	National Institute for Standards and Technology

3. Bakgrund

Denna anvisning ligger till grund för de generella krav som Inera ställer på autentiseringslösningar och legitimeringar för att få tillgång till patientinformation genom de tjänster som Inera tillhandahåller.

Autentiseringsanvisningen ska också ge ett tydligt underlag för kunna testa, granska och certifiera applikationer som ska anslutas mot tjänster som Inera tillhandahåller. Nya tjänster behöver en tydlig autentiseringsanvisning som vägleder utvecklare och leverantörer av e-tjänster vilka krav Inera ställer gällande autentisering och e-legitimationer för att uppfylla lagar och förordningar.

4. Mål med Anvisningen

Ett viktigt mål med denna Anvisning är att 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 verksamhetenen. Rutinen idag är att användaren alltid loggar in i t.ex. NPÖ med sitt SITHS kort eller kommande Efos kort och att kortet alltid ska vara tillgängligt för applikationen. Målsättningen för att förenklat autentiseringsförfarande är att ge användaren en möjlighet att ärva en stark autentisering till en terminal eller mobil enhet eller en alternativ och godkänd ID enhet. Vid autentiseringen väljer användaren att koppla sin starka autentisering till vald ID enhet.

Följande färgmarkeringar visar Ineras rekommendationer i detta dokument:

Grönt är godkänd nivå för att få tillgång till patientinformation genom de tjänster som Inera tillhandahåller.

Gult är acceptabel nivå för att få tillgång till patientinformation genom de tjänster som Inera tillhandahåller, men det ska finnas en i tiden rimlig avvecklingsplan.

Rött är en icke acceptabel nivå för att få tillgång till patientinformation genom de tjänster som Inera tillhandahåller och ska Ej användas utan avvecklas snarast.

5. Referensmaterial

5.1 Styrande principer

Dokument ska följa Referensarkitektur för Identitet och Åtkomst [R1] och dess styrande principer som har med syfte att säkerställa spårbarhet, skalbarhet, flexibilitet och interoperabilitet i IT-system.

IA2 (3.2 i Referensarkitekturdokumentet) och hanteringen av ärvda e-legitimationer.

5.2 Stark autentisering och tillitsnivåer

Socialstyrelsen och EU Kommissionen har tagit fram begrepp och definitioner för stark autentisering som beskrivs under rubrik 4.3 och 4.4

5.3 Stark autentisering enligt Socialstyrelsen

Följande står i HSLF-FS 2016:40. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården [R5].

2 kap Definitioner:

stark autentisering: kontroll av identiteten på två olika sätt

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.

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.

5.4 Stark autentisering enligt eIDAS

5.4.1 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 [R3].

2 Tekniska specifikationer och förfaranden

De tekniska specifikationer och förfaranden som beskrivs i denna bilaga ska användas för att fastställa hur de krav och kriterier som avses i artikel 8 i förordning (EU) nr 910/2014 ska tillämpas för medel för elektronisk identifiering som utfärdats inom ramen för ett system för elektronisk identifiering.

Nedanstående tabell är ett utdrag från eIDAS Genomförandeförordning 1502/2015 [R2]. Tillitsnivåer för medel för elektronisk identifiering med Ineras föreslagna korrelation till e-Legitimationsnämndens tillitsnivåer som baseras på ISO 29115, Information technology – Security techniques – Entity authentication assurance framework [R4].

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”

5.4.2 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.

5.5 E-legitimering definitioner

Enligt eSam ”Juridisk vägledning för införande av e-legitimering och e-underskrifter” [R6] hämtar vi följande Definitioner:

- Med e-legitimering menas att innehavaren av en e-legitimation använder den för att visa vem han eller hon är.
- Med e-identifiering menas en kontroll av vem som legitimerat sig.
- Med identitetsintyg menas en elektronisk handling, som kan användas endast vid ett visst tillfälle, där utställaren intygar vem som har legitimerat sig.

E-legitimering för olika syften och kan ske för till exempel:

1. tillträde, i syfte att elektroniskt få tillgång till uppgifter som får lämnas ut till den person som legitimerat sig och få skydd mot att någon annan släpps in under sken av att vara den som legitimerat sig,
2. uppgiftslämnande, för att lämna uppgifter elektroniskt och få skydd mot att någon annan lämnar uppgifter under sken av att vara uppgiftslämnaren, eller
3. indirekt underskrift, för att ställa ut en elektronisk handling som är skyddad mot förfalskning och förnekande av underskrift på motsvarande sätt som om handlingen hade undertecknats på papper.

Beroende på den typ av e-tjänst användaren nyttjar och informationsinnehållet i tjänsten kan en viss minsta skyddsnivå krävas för e-legitimationen och tillhörande identifiering.

5.6 Utfärdandeprocessen

Även om en autentiseringsteknik i sig ses som väldigt säker så kan inte en teknik uppfylla en tillit om inte utfärdandet, leverans och aktiveringsprocessen, för att ställa ut medlet för den elektroniska identifieringen, är till fylles. Nedanstående tabeller 2.1.2 och 2.2.2 som är ett utdrag från eIDAS Genomförandeförordning 1502/2015 visar vilka krav EU ställer för tillitsnivåerna Låg, Väsentlig och Hög.

”2.1.2 Styrkande och kontroll av identitet (fysisk person)”

eIDAS Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Personen kan antas inneha bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten. 2. Beviset kan antas vara äkta eller existera enligt en tillförlitlig källa, och beviset förefaller vara giltigt. 3. Enligt en officiell källa existerar den påstådda identiteten, och det kan antas att den person som åberopar denna identitet är en och samma person.
Väsentlig	Nivå låg, samt ett av de alternativ som anges i punkterna 1–4 måste vara uppfyllt: 1. Kontroll har skett av att personen innehar ett bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten, och beviset kontrolleras för att fastställa att det är äkta, eller enligt en tillförlitlig källa existerar det och avser en verklig person, och åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 2. en identitetshandling uppvisas under ett registreringsförfarande i den medlemsstat där handlingen utfärdades, och handlingen tycks avse den person som uppvisar den, och åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att handlingen har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 3. om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig de förfaranden som anges i avsnitt 2.1.2 för tillitsnivån väsentlig, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008(1) eller av ett likvärdigt organ, eller 4. om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån väsentlig eller hög, och riskerna för ändring i personidentifieringsuppgifterna beaktas, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån väsentlig eller hög bekräftas av det organ för

	bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ.
Hög	Kraven i punkt 1 eller 2 ska uppfyllas: 1. Nivå väsentlig, samt ett av de alternativ som anges i leden a–c måste vara uppfyllt: a) När en person har kontrollerats och befunnits inneha fotografiskt eller biometriskt identifieringsbevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, och den bevisningen avser den påstådda identiteten, kontrolleras beviset för att fastställa om det är giltigt enligt en tillförlitlig källa. **och** Sökanden har identifierats som den påstådda identiteten genom jämförelse av en eller flera fysiska egenskaper hos personen med en tillförlitlig källa, **eller** b) Om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig med de förfaranden som anges i avsnitt 2.1.2 för tillitsnivån hög, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och åtgärder vidtas för att styrka att resultaten från tidigare förfaranden fortfarande är giltiga, **eller** C) Om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån hög, och riskerna för ändring i personidentifieringsuppgifterna beaktas, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, **och** åtgärder vidtas för att styrka att resultaten av detta tidigare förfarande för utfärdande av ett anmält medel för elektronisk identifiering fortfarande är giltiga, **ELLER** 2. om den sökande inte lägger fram något erkänt fotografiskt eller biometriskt identifieringsbevis, ska samma förfaranden som används på nationell nivå i medlemsstaten av den enhet som ansvarar för registreringen för att erhålla sådant erkänt fotografiskt eller biometriskt identifieringsbevis tillämpas.

”2.2.2 Utfärdande, leverans och aktivering”

eIDAS Tillitsnivå	Erforderliga beståndsdelar
Låg	Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken medlet kan antas nå endast den avsedda personen.
Väsentlig	Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken det kan antas att medlet levereras endast till ägaren.
Hög	Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren.

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

Ovanstående utdrag från eIDAS Genomförandeförordning 1502/2015 ska användas vid bedömningen av den kontrollen av identitet av användaren i samband med utfärdandet av medel för elektronisk identifiering står i paritet med autentiseringstekniken dvs. om autentiseringstekniken bedöms vara på nivå Väsentlig ska även identitetskontrollen vid utfärdandet var vara på nivå Väsentlig enligt ovan.

6. 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.

6.1 Giltighetstiden för en stark autentisering

Giltighetstid för en från stark autentisering ska normalt sett gälla i 4 timmar men kan, under vissa arbetsmässiga förhållanden, tänjas till 12 timmars giltighetstid innan en ny stark autentisering ska ske. En stark autentisering etablerats via godkänd och betrodd Identifieringstjänst, IdP som normalt sett genererar ett identitetsintyg som levereras till den tjänst (SP) som begärt en autentisering. Därefter sätts en session upp, mellan klienten och tjänsten, baserat på erhållet identitetsintyg.

För att vara tydlig, vi identifierar ett par olika sessionstider:

- En Single Sign-On, SSO sessionstid som default är 60 minuter dvs. tiden som en IdP kan generera en ny SAML biljett till en SP utan krav på om autentisering.

- En sessionstid för en autentiserad session mot ett vårdsystem. För tjänster som Inera tillhandahåller gäller att sessionstid default, som är kopplad till den starka autentiseringen enligt inledningstexten ovan av rubrik 5.1, ska vara maximalt 4 timmar innan en ny stark autentisering krävs. Denna tid ska vara anpassad för en normal förmiddags och eftermiddagspass inom verksamheten. Default tiden kan dock, beroende på verksamhet och efter riskanalys, även kunna tänjas till maximalt 12 timmar innan en ny stark autentisering erfordras.

6.1.1 Låsning av skärm vid inaktivitet

Även om giltighetstiden för stark autentisering enligt Ineras norm är 4 timmar så ställs krav på att obehöriga inte ska kunna ta del av ev. patientinformation som visas på skärmen. Vid inaktivitet eller att användaren lämnar sin terminal ska ett automatiskt skärmlås träda in som antingen är tidsstyrt eller, vilket är Ineras rekommendation, via en närvaroavkänning av användaren som kan vara baserad på en NFC ID enhet eller t.ex. en biometrisk identifiering, typ ansiktsidentifiering.

Vid användandet av tidsstyrt skärmlås så är terminalens placering avgörande för hur länge en inaktiv terminal kan stå olåst. I en väl kontrollerad miljö t.ex. i en operationssal med begränsad access för obehöriga kan tiden för skärmlås förmodligen vara den tid operationen varar och i en ambulans säkerligen mer än 30 minuter. I en mer publik miljö där obehöriga kan röra sig bör tiden för skärmlås vid inaktivitet inte vara längre än 1–2 minuter.

Om avsteg från detta görs, ska det ske efter en dokumenterad behovs- och riskanalys. Syftet med denna analys att erhålla ett värde som uppfyller verksamhetens krav samtidigt som säkerheten upprätthålls, i det fall en användare förlorar sin enhet. Det åligger sedan kundens informationssäkerhetsorganisation att säkerställa att denna tid hålls.

6.1.2 Automatisk utloggning vid inaktivitet

Normalt sett ska en användare alltid logga ut från nationella tjänster t.ex. NPÖ om man planerar att inte använda sig av tjänsten mer under dagen eller lämnar sin arbetsplats för möten osv. Tjänsten ska hantera en automatisk utloggning vid inaktivitet för att förhindra att andra användare, avsiktligt eller oavsiktligt, kan komma in på en redan inloggad session detta utifall att en användare glömmer att logga ut. Tiden för den automatiska utloggningen beror på typ av arbetsplats.
Riktvärden för automatisk utloggning bör vara default 15 minuter, men sessionstiden kan utökas eller minskas beroende på om användaren har en personlig dator eller om en riskanalys visar att 15 minuter är för lång tid. Vid eventuella avsteg från ovanstående riktvärde ska de tider som valts under rubriken ovan, "Låsning av skärm vid inaktivitet", tas i beaktande.

6.1.3 Förenklat autentiseringsförfarande

Inom ovanstående tidsram kan, efter krav på stark autentisering, en ärvd legitimering **(se Ärvd legitimering rubrik 5.2 nedan**) i ett s.k. förenklat autentiseringsförfarande, under en begränsad tidsperiod, hantera in och utloggning till vald e-tjänster och då även upplåsning av användarens tidigare av låst terminal eller mobil enhet.

Det förenklade autentiseringsförfarandet kan då vara en icke certifikatbaserad ID enhet t.ex. en NFC baserad ID dosa som kopplas till användaren i samband med den starka autentiseringen.

En PIN-kod alternativt en biometrisk identifiering ska normalt sett kopplas till den förenklade autentiseringen. Efter tre felaktiga PIN-kodsförsök bör den förenklade autentiseringen låsas och att användaren avkrävs en ny stark autentisering.

Om avsteg från detta görs, ska det ske efter en dokumenterad behovs- och riskanalys.

Två typer av förenklad autentisering har identifierats:

1. Centralt baserad. Användaren kan av verksamheten få en godkänd ID-enhet tillagd i en attributkälla eller att någon annan teknik används som knyter den starka autentiseringen med vald ID-enhet
2. Lokalt baserad. Den ärvda legitimationen är helt baserad till den lokala arbetsplatsen. Kopplingen sker med hjälp av arbetsplatsens CSP som hanterar dialogen med t.ex. det Smarta kortet och vald ID-enhet.

OBS. Det förenklade autentiseringsförfarandet dvs. en ärvd legitimering från en tidigare stark autentisering, får **aldrig**, i tjänster som Inera tillhandahåller, användas till en ny ärvd legitimering. En ärvd legitimering med tillit till åtkomst i tjänster med patientinformation, som Inera tillhandahåller, ska primärt alltid utgå från en stark autentisering.

6.1.4 Spårbarhet

Krav på spårbarhet ska finnas i en central lösning enligt alternativ 1 ovan, som ska visa hur kopplingen mellan den ursprungliga starka autentiseringen och den ärvda legitimationen har etablerats.

För den lokalt baserade lösningen, enligt alternativ 2 ovan, kan det vara svårt att uppfylla en spårbarhet som kan återspeglas i en central loggfunktion.

6.2 Ärvd legitimering

Begreppet ärvd legitimering (Ärvd legitimering ska **likställas** med E-legitimationsnämnden, ELN:s begrepp **ID växling**) är, enligt Referensarkitektur IA, att t.ex. förnya ett giltigt men snart utgående X.509-certifikat på ett smart kort eller att utfärda ett nytt certifikat, en ny ärvd e-legitimation, till en mobil e-legitimationsbärare med stöd av ett giltigt certifikat t.ex. på ett smart kort. En CA kan utfärda ett mjukt certifikat en s.k. P12 fil (se rubrik 6.2, Mjuka certifikat) som kan placeras på en mobil enhet t.ex. sin mobiltelefon eller surfplatta.

Inom ramen för ärvd legitimering kan även icke certifikatbaserade ID enheter falla in som medlet för elektronisk identifiering. Den ärvda legitimationen kan i sig ha lägre tillitsnivå än den ursprungliga men i samband med att användaren genomför en stark autentisering kan en ärvd legitimation tillfälligt och kortlivat erhålla samma tillitsnivå (se rubrik 5.1.2 Förenklat autentiseringsförfarande). Enligt ”Referensarkitektur Identitet och åtkomst” kan en ärvd legitimation aldrig gälla längre eller med högre tillit än den som användes vid utfärdandet samt att, enligt ELN, kan aldrig den ärvda legitimeringen nå högre tillitsnivå än Väsentlig.

6.2.1 Distribution av ärvda legitimationer

För att säkerställa att ärvda legitimationer, baserade på mjuka certifikat s.k. P12-filer, placeras på avsedd terminal/mobil enhet krävs någon form av Device Management, DM lösning som på

ett tillförlitligt och säkert sätt hanterar distributionen (även kallad provisionering) och lagring till vald terminal/mobil enhet.

6.2.2 Rekommendation gällande ärvd legitimering

En certifikatbaserad ärvd legitimation kan ärvas i flera led och bibehålla sin tillit om den görs enligt ett fastställt regelverk som är beskrivet i certifikatutfärdarens (CA) CPS, Certification Practice Statement.

En ärvd legitimation kan aldrig få en högre tillitsnivå än det ursprungliga medlet för elektronisk identifiering, den ärvda legitimeringen kan heller inte, enligt ELN, aldrig nå högre tillitsnivå än Väsentlig.

En ärvd legitimation som inte är certifikatbaserad, som beskrivs under rubrik 5.1.2 i ett s.k. förenklat autentiseringsförfarande kan hantera in och utloggning till vald e-tjänst i den tidsram som en stark autentisering anses giltig enligt rubrik 5.1 Giltighetstiden för en stark autentisering.

En viktig bedömningsfaktor gällande ärvda legitimationer och dess tillit t.ex. gällande mjuka certifikat som är skyddade av en tillfällig PIN-kod ska vara att betrakta som en enfaktorautentisering om flera användare kan dela på samma enhet samtidigt. Denna bedömning medför då att det ärvda mjuka certifikatet endast får användas som ett förenklat autentiseringsförfarande dvs. tillfälligt och kortlivat under en del av dag eller i vissa fall hel dag efter att en stark autentisering genomförts.

En riskanalys ska, som ett tilläggskrav, alltid ske som avgör att den ärvda e-legitimationen kan bibehålla tilliten på den nivå som tjänsten faktiskt kräver.

7. Autentiseringsmetoder

Punkterna 1–5 ovan beskriver bakgrund, lagar och förordningar som Inera baserat nedanstående bedömning av autentiseringsmetoder med tillhörande e-legitimationer.

7.1 Certifikatbaserade, ”X.509” Smarta kort

Ett Smart kort byggs upp kring ett antal standarder och säkerhetsprofiler som tillsammans skapar det säkra Smarta kortet. De viktigaste är:

1. Chip ska minst uppfylla Evaluation Assurance Level 4+ (EAL 4+), kraven för Common Criteria Protection Profile Secure Signature Creation Device (SSCD) och Protection Profile Java card eller minst uppfylla FIPS 140–2 level 2 samt i det senare fallet användas i FIPS-mode.
2. Slumptalsgeneratorn som används vid generering av nyckelmaterial direkt på chippet (on-board) för både ordinarie och tillfälliga kort ska implementeras enligt NIST SP 800-90A revision 1 eller senare.
3. Kortprofil ska följa ISO 7816–15 och om annat inte nämns, vara implementerad enligt Svensk Standard SS 614 332

En e-legitimation baserad på Smarta kort enligt ovan beskrivna standarder är med dagens norm den bästa och säkraste tekniken för att identifiera en användare. Den privata nyckeln, som är kopplad till den publika nyckeln i certifikatet, är helt skyddad och endast indirekt åtkomlig från den inbyggda CPU:n på chippet. Den privata nyckeln kan endast användas med att man anger rätt PIN-kod dvs. det är i praktiken omöjligt att röja eller kopiera den privata nyckeln.

Till det Smarta kortet skickar man alltid in det som ska krypteras/signeras tillsammans med att man måste skicka med sin PIN-kod. Det är alltid CPU:n i Smarta kortet med tillhörande asymmetrisk kryptoalgoritm som utför den matematiska kalkylationen, utan att den privata nyckeln lämnar kortet. Resultatet dvs. den krypterade/dekrypterade strängen skickas därefter tillbaka från det Smarta kortet till den anropande applikationen/gränssnittet.

En nackdel med ett normalt Smart kort typ SITHS eller Efos kort är att de ur ett skalbarhetsperspektiv inte fungerar i en servermiljö då de inte klara mer än ett antal krypteringar/dekrypteringar per sekund.

7.1.1 Rekommendation gällande Smarta kort

Med referens till rubrik 4.6 Utfärdandeprocess och eIDAS tillitsnivåer som beskrivits under rubrik 4.4.1 ovan uppfyller Smarta kort minst nivå Väsentlig dvs. tillräckligt hög för att autentiseringstekniken uppfyller de krav Inera ställer för att en användare, beroende på medarbetaruppdrag, kan få nå patientinformation inom tjänster som Inera tillhandahåller. Nivå Hög kan uppnås om utfärdandeprocessen följer de rekommendationer som beskrivs under rubriken 4.6 Utfärdandeprocessen.

7.2 Certifikatbaserade, ”X.509” Mobila certifikat

Mobila certifikat t.ex. PKCS#12 (P12) filer (resonemanget gäller konceptuellt även t.ex. Java Key Store/JKS filer och likvärdiga filbaserad lagring) är en DER/PEM kodad arkivfil som normalt sett innehåller ett certifikat, en krypterad privat nyckel och ett CA certifikat, dvs. motsvarande information som normalt sett också lagras i ett Smart kort. En stor skillnad mellan ett Smart kort och en P12-fil är att P12-filen relativt enkelt kan kopieras om den inte lagras i en sluten container. En annan viktig skillnad är också att hela den matematiska kalkylationen av den asymmetriska kryptoalgoritmen måste ske i en mjukvara/applikation i terminalen. Terminalen måste få tillgång till en dekrypterad kopia av den privata nyckeln från P12-filen samt att applikationen också har tillgång till den nyckel/PIN-kod som öppnar den krypterade privata nyckeln i P12-filen. Sammantaget så finnas det flera attackvektorer mot P12-filer.

7.2.1 Sårbarheter och risker med Mobila certifikat

1. P12-filen dvs. det mobila certifikatet kan kopieras om den inte skyddas i en säker container.
2. Den privata nyckeln kan röjas genom att applikationen måste öppna dvs. dekryptera den privata nyckeln från filen och lagra/cacha den i arbetsminnet så att kryptobiblioteket kan utföra signering/kryptering av efterfrågat anrop.
3. En serverapplikation måste alltid ha tillgång till P12-filens krypteringsnyckel/PIN-kod till den privata nyckeln i P12-filen, vilket medför att även den också behöver skyddas

från utomståendes access i en servermiljö. I en klientmiljö knappar användaren in sin PIN-kod när det efterfrågas, dvs. den behöver inte lagras.

I en servermiljö använder man som regel alltid P12/JKS filer beroende på de prestandabegränsningar som beskrivits ovan.

7.2.2 Distribution av Mobila certifikat

För att säkerställa att mobila certifikat, P12-filer, placeras på avsedd terminal/mobil enhet **krävs** någon form av Device Management, DM lösning som på ett tillförlitligt och säkert sätt hanterar distributionen (även kallad provisionering) och lagring till vald terminal eller mobil enhet.

7.2.3 Rekommendation gällande Mobila certifikat

Med referens till rubrik 4.6 Utfärdandeprocess och eIDAS tillitsnivåer som beskrivits under rubrik 4.4.1 **kan** mobila certifikat uppfylla nivå Väsentlig dvs. tillräckligt hög för att autentiseringstekniken ska uppfylla de krav Inera ställer för att en användare, beroende på medarbetaruppdrag, kan nå patientinformation inom tjänster som Inera tillhandahåller.

Mobila certifikat **kan Inte** nå eIDAS tillitsnivå Hög då en P12-fil i sin natur kan kopieras och finnas i flera kopior utan att användare och utfärdare har någon möjlighet att kontrollera detta.

7.2.4 Behov av riskanalys för Mobila certifikat

I och med ovanstående sårbarheter och risker för mobila certifikat som beskrivits under punkten 6.2.1, krävs att en Riskanalys genomförs för varje nyutvecklat system och tjänst som ska anslutas mot tjänster som Inera tillhandahåller som belyser att eventuella risker och konsekvenser i hanteringen av de mobila certifikaten ligger under den nivå som kan bedömas rimligt för att godkänna systemet.

7.3 Certifikatbaserade, Bankkort/BankID e-legitimation

Det finns två olika Bankkort/Inloggningskort som ges ut av banker för att användarna ska kunna göra sina bankaffärer över Internet.

Den ena typen är bankernas Betalkort/Bankkort, som idag oftast är s.k. Java kort, innehåller oftast flera profiler/applets med olika funktioner. En av profilerna i ett EMV (Europay, Mastercard, Visa standarden) kort som är anpassad för att fungera tillsammans med handelns betalterminaler och kan inte helt jämföras med Smarta kort som beskrivs under rubrik 6.1. Normalt sett finns även en ID profil som fungerar i paritet med Smarta kort.

Sedan har vi bankernas s.k. Inloggningskort som är ett PKCS#15 kompatibelt kort (som är jämförbara med Smarta kort som är beskrivet under rubrik 6.1) som kan läsas av t.ex. OpenSC men profilen på kortet är inte kompatibelt för Secmakers NetID.

7.3.1 Sårbarheter och risker med Bankkort baserade på EMV tekniken

Utfärdandeprocessen för en kund som ansöker om ett bankkonto med tillhörande Bankkort/BankID hanteras i banken regi som har sin egen rutin för identifiering och verifiering av kunden.

Konto och Bankkort/BankID är utfärdat enkom för att ge kunden möjlighet access till sitt eget konto och för egna affärer i handeln.

Det finns sårbarheter i kommunikationsprotokollet mellan en betalterminal och kortets EMV-profil. Den allvarligaste är att man kan få kortet att signera en transaktion utan att användaren behöver ange sin PIN-kod men den sårbarheten finns inte i ID profilen som normaltsett används för autentisering och signering av transaktioner mot t.ex. bankens webbtjänster. För att få full tillit till alla Bankkort med EMV profil krävs en djupare analys för att verifiera att ingen bank använder EMV profilen för autentisering.

Bankerna utfärdar sina certifikat till kundens Bankkort och BankID från sin egna CA som inte är verifierats eller godkänts av svenska myndigheters tillitsramverk.

Ett för Inera tydligt sätt att erkänna Bankkort/BankID (gäller även Mobilt BankID) på minst nivå Väsentlig dvs. tillräckligt hög för att autentiseringstekniken uppfyller de krav Inera ställer för att en användare, beroende på medarbetaruppdrag kan få nå patientinformation inom tjänster som Inera tillhandahåller, är att bli godkänd av E-legitimationsnämnden, ELN som e-legitimationsutfärdare för kvalitetsmärket Svensk e-legitimation.

7.3.2 Sårbarheter och risker med Bankernas inloggningskort

Utfärdandeprocessen för en kund som ansöker om ett bankkonto med tillhörande Bankkort/BankID hanteras i banken regi som har sin egen rutin för identifiering och verifiering av kunden.

Konto och Bankkort/BankID är utfärdat enkom för att ge kunden möjlighet access till sitt eget konto och för egna affärer i handeln.

Bankernas PKCS#15 kompatibla Inloggningskort inte är utsatta för den sårbarhet som är beskriven under rubriken 6.3.1 dvs. i EMV kortet.

Se ovan punkten 6.3.1

7.3.3 Rekommendation gällande Bankkort

Det finns en osäkerhet i utfärdande och tillitsprocessen för Bankkort/BankID i dagsläget, tekniken bedöms endast lämplig för access till Invånartjänster som t.ex. Journalen där en användare endast kommer åt sin egen patientinformation. Bankkort/BankID ska inte användas som e-legitimation för att nå patientinformation inom tjänster som Inera tillhandahåller.

7.3.4 Rekommendation gällande Bankerna inloggningskort

Bankerna Inloggningskort ska inte användas som e-legitimation för att nå patientinformation inom tjänster som Inera tillhandahåller

7.4 Certifikatbaserade, Mobilt BankID

Autentiseringen med Mobilt BankID är en s.k. Out-of Band teknik som ägs av Finansiell ID-Teknik. Tyvärr så är väldigt lite tekniskt material publicerat om tjänstens uppbyggnad, därav har vi, i denna anvisning, tvingats att göra vissa antaganden om funktionalitet och teknik i Mobilt BankID och dess autentiseringstjänst.

En för mobil autentiseringsteknik med mjuka ärvda certifikat som lagras i en ”säker” container inom Appen Mobilt BankID. Ett certifikat för Mobilt BankID skapas i ett webbaserat gränssnitt hos Din bank mha. att användaren autentiserar sig med en bankdosa eller sitt Bankkort/BankID. I bankens webbgränssnitt kopplar man också ihop sitt mobiltelefonnummer och den installerade Appen Mobilt BankID och efter ett signerat godkännande från användaren skickas ett mobilt certifikat (i paritet med en P12-fil) över till mobilen. Vid en inloggning till en tjänst, efter att man angett sitt personnummer, informeras användaren om att starta sin App Mobil BankID, samtidigt som tjänsten skickar en autentiseringsbegäran vidare till Mobilt BankID. Mobilt BankID klienten på användarens mobil startas och etablerar en session till Mobilt BankID som därefter skickar över information till Appen att tjänsten A begär en autentisering (gäller även signering av transaktioner) och användaren knappar in sin PIN-kod som då signerar autentiseringsbegäran som skickas tillbaka till Mobilt BankID. Mobilt BankID verifierar signeringen och skickar en bekräftelse om godkänd autentisering tillbaka till den begärande tjänsten.

7.4.1 Sårbarheter med Mobilt BankID

- En bank kan öppna ett bankkonto med tillhörande Bankkort/BankID baserat på en lägre grad av tillit för utfärdandet.
- Ett Mobilt BankID är en ärvd e-legitimation (se rubrik 5.2) baserad på kundens Bankkort/BankID som då också knyts till en mobil enhet vars utfärdandeprocess Inera inte har kontroll över.

7.4.2 Rekommendation gällande BankID/Mobilt BankID

Under rubrik ”**5 Grundprinciper gällande åtkomst till patientinformation**” ovan, säger Inera ”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 genom tjänster som Inera tillhandahåller”.

Bedömning av tillit till en autentiseringsteknik omfattar både teknik (se rubrik 4.4) och utfärdandeprocessen (se rubrik 4.6). I och med att Finansiell ID-Teknik inte publicera hur tekniken är byggd så anser Inera att det är svårt att bedöma att helheten ligger på minst tillitsnivå Väsentlig.

Mobilt BankID bedöms i dagsläget i första hand endast lämplig för access till Invånartjänster som t.ex. Journalen där en användare endast kommer åt sin egen information.

BankID/Mobilt BankID ska inte användas som e-legitimation för att nå patientinformation inom tjänster som Inera tillhandahåller, om inte teknik och utfärdandeprocessen tydligt kan redovisas och intygas från utfärdare och tjänsteleverantör. Se även punkten 6.3.1

7.5 Engångslösenord (OTP, One-Time Password)

7.5.1 Autentiseringsdosor

Det finns flera typer av autentiseringsdosor som genererar tidskodade engångslösenord med eller utan tangentbord t.ex. RSA SecurID, Vasco DIGIPASS och SafeNet MobilePASS. En

autentiseringsdosa med sifferdisplay men utan tangentbord har en inbyggd teknik som genererar en ny tidssynkroniserad siffersträng som vid autentiseringstillfället ska matchas mot det värde som autentiseringsservern förväntar att användarkontots autentiseringsdosa är kopplat mot. För att få en tvåfaktorsautentisering finns ett par möjligheter t.ex. att antingen förstärks den från dosans genererade siffersträng med att användaren lägger till en egen kopplad PIN-kod som vid autentiseringen/inloggningen till ett system/tjänst eller så anger man loggar man in sitt användarnamn och lösenord tillsammans med ett tredje inmatningsfält för autentiseringsdosans siffersträng.

En autentiseringsdosa med tangentbord kan även hantera en s.k. ”Challenge-Response” autentisering på motsvarande sätt som autentisering med ett Smart kort. Användaren startar med att ange sitt användarnamn och lösenord som kontrolleras av autentiseringsservern. Autentiseringsservern kontrollerar inloggningen och skickar sedan ut en ”Challenge” sekvens som matas in i dosan tillsammans med en PIN-kod. Resultatet av den tidssynkroniserade kalkylationen visas på dosans display som användaren därefter matar in som en ”Response” tillbaka till autentiseringsservern.

SecurID, DIGIPASS, MobilePASS och förmodligen andra autentiseringsdosor finns även som Appar till mobiltelefoner med motsvarande funktionalitet som ovan.

7.5.2 Sårbarheter och risker, OTP med Autentiseringsdosor

Ovan beskrivna autentiseringsdosor är baserad på proprietär och hemlig teknik. RSA fick för ett antal år sedan ett intrång där kritisk information runt deras teknik röjdes som gjorde att en hackare kunde räkna ut siffersekvensen för en viss dosa. En ganska osannolik risk men bör ändå nämnas i sammanhanget. Autentiseringsdosor är dock en vitt spridd och vedertagen teknik som används frekvent av både företag och myndigheter världen över.

7.5.3 Rekommendation gällande OTP med Autentiseringsdosor

Autentiseringsdosor i form av Appar behöver initieras i någon form. Detta kräver en säker utgivningsprocess med en säker identifiering och leverans av ”initieringstoken” till användaren enligt eIDAS Genomförandeförordning 1502/2015 med referens till rubrik 4.6 i detta dokument.

Om utfärdandeprocessen för autentiseringsdosan följer eIDAS nivå Väsentlig så bedöms tekniken vara på nivå Väsentlig dvs. acceptabel för att nå patientinformation inom tjänster som Inera tillhandahåller.

7.6 Autentisering med OTP via SMS

Autentisering med OTP över SMS är en teknik där användaren initialt autentiserar sig (loggar in) med sitt användarnamn och lösenord mot tjänstens autentiseringsserver. Till användarkonto har ett attribut kopplats med användarens mobiltelefonnummer. Vid en godkänd initial autentisering skickar autentiseringsservern ut ett SMS innehållande ett engångslösenord till användarens mobiltelefon. Användaren får på inloggningsskärmen upp ytterligare ett lösenordsfält där det mottagna SMS lösenordet skall skrivas in.

Autentiseringsservern måste ha någon form av kopplingen till en mobiloperatörs SMS tjänsten antingen via ett direktabonnemang från autentiseringsservern eller via en 3e part som vidarebefordrar SMS:et till användarens mobila enhet.

7.6.1 Sårbarheter och risker med OTP via SMS

- En självadministrationsportal med återställningsrutinen för spärrat konto kan missbrukas.
- Utfärdandet/utgivningsprocessen av SIM-kort från mobiloperatören till användaren är en svag länk som många gånger ligger utanför Ineras kontroll, se rubrik 4.6 Utfärdandeprocessen.
- Otydligheter kan finnas till vem som har skrivrättigheter till den katalogtjänst (AD/HSA) som innehåller användarens mobiltelefonnummer dvs. hur fungerar uppdateringsprocessen för användarinformationen i katalogtjänsten?
- Sårbart för ”Man In The Middle” Attacker dvs. en angripare som lyckats avlyssna överföringen av SMS kan hinna logga in i ett system och använda engångslösenordet före användaren. Sannolikheten för att lyckas med denna attack är attackeraren dessutom måste ha tillgång till användarens initiala inloggningsuppgifter.
- Sårbarheter har nyligen utnyttjats i SS7-protokollet i mobiloperatörer core-nät där tjuvar/hackare lyckats omdirigera bankers engångskoder (mTAN, mobile Transaction Authentication Numbers) i form av sms till egna mobilenheter.

7.6.2 Rekommendation gällande OTP via SMS

Inera rekommendera inte längre engångslösenord via SMS som en säker autentiseringsmetod med tanke på ovanstående beskrivna sårbarheter och risker. SMS baserad autentisering bör inom ett rimligt tidsperspektiv avvecklas som autentiseringsmetod för att användare som ska nå patientinformation via tjänster som Inera tillhandahåller.

7.7 Autentisering med Användarnamn och Lösenord

Autentiseringen baseras enbart på att en användare anger sitt användarnamn och lösenord vid inloggning till en tjänst som då verifieras mot en autentiseringsserver eller internt i applikationen/tjänsten

7.7.1 Sårbarheter och risker med Användarnamn och lösenord

Öppet för ”Brute Force” attacker [R8] dvs. har användaren för dålig lösenordskvalitet dvs. att lösenordet är ett vanligt ord som finns i en ordlista eller en omskriven variant på vanliga ord. Alternativt kan en attackerare via ”Social engineering” genom t.ex. användarens sociala nätverk hitta/gissa sig till tänkbara lösenord baserat på en koppling till användaren.

Många användare använder samma kontouppgifter, dvs. samma användarnamn t.ex. en mailadress och samma lösenord, till många system vilket innebär att om ett av systemen blir hackat och konto- och hashade lösenordsfiler kommer i orätta händer finns det en mängd verktyg idag som kan knäcka enkla lösenord i hashade lösenordsfiler.

7.7.2 Rekommendation gällande Användarnamn och lösenord

Användarnamn och lösenord är att betrakta som enfaktors autentisering och får inte användas för att ge användare access till tjänster som Inera tillhandahåller med patientinformation.

7.8 Biometriska metoder

Här hänvisas helt till Referensarkitektur – Identitet och åtkomst [R2] 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.”

7.8.1 Rekommendation gällande biometriska metoder

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.

7.9 FIDO Alliance

Beskrivs i Referensarkitektur IA dokumentet men behandlas inte i denna utgåva av Ineras Anvisning Autentisering.

8. Autentisering och IdP

Från Referensarkitektursdokumentet kan man läsa:

”Identifieringstjänst (Identity Provider, IdP) – Tjänst i IT-infrastrukturen som utför autentisering av användare på begäran, och via en ***Identitetsintygsutfärdare*** vidarebefordrar ***identitetsintyg*** till e-tjänst med uppgifter om en identifierad användare. Identifieringstjänst ingår i flera säkerhetsarkitekturer med lite olika benämningar. Typiskt är att uppgifterna paketeras i s.k. ***intyg*** även kallade ***biljetter*** och ***tokens***.”

Att beskriva Identifieringstjänstens funktion och relations till autentisering **ingår inte** i denna utgåva av Anvisning Autentisering.

För federationer och tillit mellan IdP:er hänvisas till SAMBI [R7] och dess arbete.

9. Loggning och spårbarhet

Krav på spårbarhet ska finnas i en central lösning som ska visa hur kopplingen mellan den ursprungliga starka autentiseringen och en ärvd legitimation har etablerats.

För en lokalt baserade lösning med ärvd legitimering finns vissa svårigheter för att uppfylla en spårbarhet som kan återspeglas i en central loggfunktion.

10. Referenslista

Ref	Dokumentnamn	Dokument
R1	Referensarkitektur – Identitet och åtkomst	http://rivta.se/documents/ARK_0046/
R2	eIDAS Genomförandeförordning 1502/2015	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002
R3	Förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden nr 910/2014	https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0910&from=EN
R4	ISO 29115, Informationsteknik - Säkerhetstekniker - Tillit för objektsautentisering	https://www.iso.org/standard/45138.html
R5	HSLF-FS 2016:40, Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.	http://www.socialstyrelsen.se/sosfs/2016-40
R6	eSam, är ett medlemsdrivet program för samverkan mellan 24 myndigheter och SKL för att underlätta och påskynda digitaliseringen av det offentliga Sverige	http://esamverka.se/
R7	SAMBI, möjliggör en säker åtkomst till digitala tjänster för hela sektorn vård, hälsa och omsorg.	http://www.sambi.se
R8	Brute-force attack	https://en.wikipedia.org/wiki/Brute-force_attack