Anvisning
Autentisering

inera
Ett företag inom SKR

Syfte

Denna anvisning är en del av Ineras Riktlinje för informationssäkerhet. Anvisningen ligger till grund för de generella krav som Inera ställer på autentiseringslösningar och legitimeringar för att få tillgång tjänster med eller utan patientinformation

Berörda

Anvisningen gäller alla anställda och konsulter inom Inera. Ineras chefer är ansvariga för att alla anställda och konsulter har god kännedom och efterföljer Ineras ledningssystem och arbetar utifrån anvisningen.

Beskrivning

Bedömda autentiseringsmetoder för åtkomst i tjänster med patientinformation

Färgmarkering för godkända autentiseringsnivåer för tjänster med patientinformation

Följande färgmarkeringar gäller som visar Ineras krav för tjänster **med** patientinformation:

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

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.

Smarta kort

Smarta kort är godkända om utgivningen uppfyller minst tillitsnivå Väsentlig eller LOA3. Tillitsnivå Hög kan uppnås om utfärdandeprocessen följer de krav som eIDAS ställer på detta

Exempel på Smarta kort är SITHS-korten

Av DIGG godkända e-legitimationer

Alla e-legitimationer som är godkända av DIGG på minst tillitsnivå Väsentlig/LoA 3 enligt kvalitetsmärket Svensk E-legitimation är per automatik godkända.

På DIGGs hemsida finns listat vilka e-legitimationer som är godkända på tillitsnivå 3. Exempel är SITHS

BankID

BankID som e-legitimation är granskad av DIGG och godkänd som Svensk e-legitimation. BankID bör dock som huvudregel inte användas i tjänsten då det är en privat e-legitimation

Av DIGG godkänd mobila e-legitimationer

Alla mobila e-legitimationer som är godkända av DIGG på minst tillitsnivå Väsentlig/LoA 3 enligt kvalitetsmärket Svensk E-legitimation är per automatik godkända.

På DIGGs hemsida finns listat vilka e-legitimationer som är godkända på tillitsnivå 3.

Mobilt BankID

Mobilt BankID som e-legitimation är granskad av DIGG och godkänd som Svensk e-legitimation. BankID bör dock som huvudregel inte användas i tjänsten då det är en privat e-legitimation

OTP (One-time password) med Autentiseringsdosor

Autentiseringsdosor behöver initieras i någon form. Detta kräver en säker utgivningsprocess med en säker identifiering och leverans av ”initieringstoken” till användaren enligt eIDAS Genomförandeförordning.

Om utfärdandeprocessen för autentiseringsdosan följer eIDAS tillitsnivå Väsentlig/LoA 3 så bedöms tekniken vara på tillitsnivå Väsentlig/LoA 3 dvs. acceptabel för att nå patientinformation inom tjänster som Inera tillhandahåller.

Autentiseringsappar

Autentiseringsappar behöver initieras i någon form. Detta kräver en säker utgivningsprocess med en säker identifiering och leverans av ”initieringstoken” till användaren enligt eIDAS Genomförandeförordning.

Bedömning av tillit till en autentiseringsteknik omfattar både teknik och utfärdandeprocess. I och med att ovanstående teknik inte är granskad så är bedömningen att det är svårt att säkerställa att helheten ligger på minst tillitsnivå Väsentlig/LoA 3.

Engångslösenord via SMS

Engångslösenord via SMS ska inte anses vara en säker autentiseringsmetod med tanke på sårbarheter och risker.

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

Biometriska metoder

Bedömningsgrunden är att till exempel fingeravtrycks- och irisskanning endast ska användas som ersättning för PIN-kod och inte lagras centralt då det är svårt att revokera biometriskt baserad information.

Autentiseringsmetoder för Ineras interna it-system

Informationsklassificering som grund

Ineras Anvisning informationsklassificering anger fyra klassificeringsnivåer som ligger till grund för nedanstående bedömning av autentiseringsmetodernas applicerbarhet i de tjänster som Inera tillhandahåller. Primärt är det Informationsklassningen för Konfidentialitet (K) som behöver bedömas när det gäller krav på autentiseringsmetod. Vid höga krav på Riktighet krävs dock motsvarande autentisering för att kunna ändra på informationen.

Multifaktorautentisering (MFA) - huvudregel

Huvudregeln är att åtkomst till information som ur konfidentialitets- eller riktighetsperspektivet klassas som Nivå 2 (Betydande) eller Nivå 3 (Allvarlig) ska föregås av inloggning med multifaktorautentisering (MFA). Vilka autentiseringsmetoder som är godkända är listat i kommande kapitel.

Åtkomst till information som ur ett konfidentialitets- eller riktighetsperspektiv klassas som Nivå 0 (Försumbar) eller Nivå 1 (Måttlig) kan föregås av en inloggning med användarnamn och lösenord. Det är dock ingen nackdel att multifaktorsautentisering används även här.

Nivå	Konfidentialitet (K)	Riktighet
3. Allvarlig	Information med mycket högt skyddsvärde	Information där riktigheten aldrig ska kunna gå att ifrågasättas. Det ska inte gå att göra fel.
2. Betydande	Skyddsvärd information av högre känslighet som kräver att åtkomst begränsas. till exempel sekretessbelagda personuppgifter	Information som kräver att skyddet för riktighet är högt och att avsevärd vikt läggs på att upprätthålla riktigheten
1. Måttlig	Information där visst behov finns att kunna begränsa åtkomsten.	Information där riktigheten ska finnas men som inte kräver mer än periodvisa kontroller
0. Försumbar	Ej känslig information	Information som inte i efterhand kräver kontroll av om den förändrats

För mer information om själva informationsklassificeringen se Ineras Anvisning för informationsklassificering

Godkända autentiseringsmetoder vid nivå Allvarlig och Betydande:

- **Certifikatsbaserade smarta kort:** Till exempel SITHS-kort.

- **Av DIGG godkända e-legitimationer:** Alla e-legitimationer som är godkända av DIGG kvalitetsmärket Svensk E-legitimation. På DIGGs hemsida finns listat vilka e-legitimationer som är godkända på tillitsnivå 3, ett exempel är SITHS-kort.

- **BankID på kort:** Är granskad av DIGG och är godkänd som svensk e-legitimation. BankID bör dock som huvudregel inte användas i tjänsten då det är en privat e-legitimation.

- **Engånglösenord med Autentiseringsdosor:** Autentiseringsdosor är godkända under förutsättning att tilldelningen innefattar en utgivningsprocess med en säker identifiering och leverans av ”initieringstoken” till användaren.

- **Freja eID+:** Är granskad av DIGG och är godkänd som svensk e-legitimation. Freja eID+ bör dock som huvudregel inte användas i tjänsten då det är en privat e-legitimation

- **Mobilt BankID:** Är granskad av DIGG och är godkänd som svensk e-legitimation. Mobilt BankID bör dock som huvudregel inte användas i tjänsten då det är en privat e-legitimation.

- **Autentiseringsappar:** Är godkända under förutsättning att tilldelningen innefattar en utgivningsprocess med en säker identifiering och leverans av ”initieringstoken” till användaren

Godkända autentiseringsmetoder vid nivå Måttlig:

- Alla autentiseringmetoder som är godkända för nivå Allvarlig och Betydande, enligt ovan

- **Användarnamn och lösenord:** Är att betrakta som enfaktorsautentisering och ska följa Ineras regelverk med avseende på lösenordslängd, bytesintervall och komplexitet.

- **Autentisering via telefontjänst:** Ska som huvudregel inte användas för inloggning men bedömningen är att om möjlighet ges i en autentiseringsmetod att återställa ett ”Glömt lösenord” via en uppringningstjänst, kan detta vara ett av stegen för att identifiera rätt medarbetare.

- **Biometriska metoder:** Till exempel fingeravtrycks- och irisskanning, ska endast användas som ersättning för PIN-kod och inte lagras centralt då det är svårt att revokera biometriskt baserad information. Exempel är för upplåsning av dator om den initiala inloggningen skett via en godkänd multifaktorautentisering.

- **Engångslösenord via SMS:** Ska som huvudregel inte användas, men kan för information som inte bedöms så känslig vara en möjlighet för viss höjning av säkerheten.

Autentiseringmetoder vid nivå Försumbar

- Åtkomst till information som är klassad enligt Nivå Försumbar kräver som regel ingen autentisering. Om bedömning görs att autentisering ändå ska införas är samtliga ovan nämnda autentiseringsmetoder godkända.

Tilläggsinformation gällande autentisering

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.

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, 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.

Förstärkta autentiseringsmetoder med QR koder
En autentiseringsmetod i autentiseringstjänsten ska kunna förstärkas med ett tillägg för att säkerställa att användaren och autentiseringsklienten finns på samma fysisk plats. Detta för att förhindra obehörig inloggning från annan plats som kan ta över en användares pågående inloggning eller lura till sig en inloggning från en obetänksam användare.

Förstärkningen ska kunna aktiveras genom att ange detta i anropet från IdP till autentiseringstjänsten.

Förstärkningen innebär att till exempel en ”autostarttoken” genereras av autentiseringstjänsten som sedan autentiseringsklienten måste överföra till autentiseringstjänsten i samband med autentisering.

Detta ska innebära att

- Om användaren använder samma enhet för autentiseringsklienten, ska ”autostarttoken” i första hand överföras automatiskt via Appväxling.

- Om användaren använder annan enhet för autentiseringsklienten, ska användaren kunna läsa in ”autostarttoken” i form av en QR-kod som till exempel publiceras i användarens webbläsare och som läses av mha kameran från autentiseringsapplikationen. QR-koden ska som huvudregel vara rörlig och inte statisk.

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 helst via en närvaroavkänning av användaren som kan vara baserad på en NFC ID enhet eller till exempel 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 till exempel i en operationssal med begränsad access för obehöriga kan tiden för skärmlås förmodligen vara den tid en operation 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.

Automatisk utloggning vid inaktivitet

Normalt sett ska en användare alltid logga ut från inloggade tjänster när denne planerar att inte använda sig av tjänsten mer under dagen eller lämnar sin arbetsplats för möten osv.
Tjänsten ska hantera automatisk utloggning vid inaktivitet i syfte att förhindra att andra användare, avsiktligt eller oavsiktligt, kan komma in på en redan inloggad session om 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.

Förenklat autentiseringsförfarande

Inom giltighetstiden för en stark autentisering kan, efter krav på stark autentisering, en ärvd legitimering i ett s.k. förenklat autentiseringsförfarande hantera in och utloggning till vald e-tjänst. Förenklat autentiseringsförfarande kan även hantera upplåsning av användarens tidigare låsta terminal eller mobila enhet.

Det förenklade autentiseringsförfarandet kan vara en icke certifikatbaserad ID enhet till exempel 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 till exempel det Smarta kortet och vald ID-enhet.

OBS. Det förenklade autentiseringsförfarandet dvs. en ärvd legitimering från en tidigare stark autentisering, får aldrig användas till en ny ärvd legitimering. En ärvd legitimering ska primärt alltid utgå från en godkänd stark autentisering.

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.

Ärvd legitimering

Begreppet ärvd legitimering, likställt med DIGG:s begrepp ID växling, är att exempelvis förnya ett giltigt men snart utgående certifikat på ett smart kort. Alternativt att utfärda ett nytt certifikat, en ny ärvd e-legitimation, till en mobil e-legitimationsbärare med stöd av ett giltigt certifikat på ett smart kort. En CA kan utfärda ett mjukt certifikat som kan placeras på en mobil enhet till exempel 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. En ärvd legitimation kan dock aldrig gälla längre eller med högre tillit än den som användes vid utfärdandet samt att, enligt DIGG, kan aldrig den ärvda legitimeringen nå en högre tillitsnivå än Väsentlig.

Krav på 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 DIGG, nå en högre tillitsnivå än Väsentlig.

En ärvd legitimation som inte är certifikatbaserad kan hantera in och utloggning till vald e-tjänst i den tidsram som en stark autentisering är giltig.

En viktig bedömningsfaktor gällande ärvda legitimationer och dess tillit till exempel 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.