inera

Rutiner för ID-administratörer

Identifieringstjänst SITHS

inera

Innehåll

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2019-03-15	SITHS Policy Authority	Fastställt
1.1	2019-04-11	SITHS Policy Authority	Tillägg av hjälpmedel för kontroll av ID-handlingar
1.2	2019-05-14	SITHS Policy Authority	Tillägg av fotoregler

1. Dokumentets syfte

Detta dokument är för dig som har rollen ID-administratör inom Identifieringstjänst SITHS. Dokumentet innehåller de rutiner för livscykelhantering av kort och certifikat inom SITHS som ska följas för att regelverket ska uppfyllas.

Detta dokument beskriver de normala utgivningsflödena.

2. Rutin för identifiering och verifiering av svensk ID-handling

Förutsättningar

Grunden för verifiering av en svensk ID-handling är ”De sju stegen” godkänd av Svenska Bankföreningen.

- Rutinen dokumenteras i organisationens rutiner
- Elektroniska identitetshandling med **tillitsnivå 2** kan bara ges till personer 15 år eller äldre
- Elektroniska identitetshandling med **tillitsnivå 3** kan bara ges till personer 18 år eller äldre
- Elektroniska identitetshandling med **tillitsnivå 3** kräver en folkbokföringsadress i Sverige

Rutinbeskrivning

1. Ta ut ID-handlingen ur ett eventuellt fodral
2. Gör en helhetsbedömning av personen
    a. Jämför fotot med innehavaren
    b. Jämför andra detaljer som t ex ålder
3. Gör en helhetsbedömning av ID-handlingen
    a. Titta och känn på ID-handlingen
    b. Kontrollera sista giltighetsdatum så att ID-handlingen fortfarande är giltig
        i. Sista giltighetsdatum får inte ha passerats
4. Kontrollera säkerhetsdetaljer

a. Vattenmärken och genomsiktsbild: Håll upp ID-handlingen mot ljuset.
b. Säkerhetstrådar
c. ID-handlingens yta och fotots integritet
    i. Känn, se och vippa på ID-handlingen. En bild eller tecken kan bli synlig eller förändras när man vippar på det.
    ii. Kontrollera mikro- och minitext gärna med förstoringsglas.
d. Intagliotryck - guilloché - mönster med tunna linjer
    i. Särskilda trycktekniker får bläcket att kännas upphöjt eller tjockare. För att känna ett upphöjt intagliotryck låt fingret löpa över det eller skrapa försiktigt på det med nageln.
e. Optiska säkerhetsdetaljer
    i. Kontrollera gärna med UV-lampa

5. Verifiera giltigheten för svenska pass och nationella ID-kort hos Polisen

Om du misstänker att ID-handlingen är ogiltig kontakta Ansvarig utgivare eller Säkerhetsansvarig. **Lämna inte ut kortet!**

Kompletterande hjälpmedel

Exempel på produkter som kan användas för kontroll av säkerhetsdetaljer:

- Authentiscan från företaget Keesing. Produkten kräver en licens.
- 365id från företaget 365id AB. Produkten kräver en licens

Länkar

Verifiera svenska pass och nationella ID-kort
https://etjanster.polisen.se/egid/giltighetskontroll/giltighetskontroll

De sju stegen https://desjustegen.se/

3. Fotoregler

- Fotot skall innehålla en välliknande bild på innehavarens ansikte.
- Ansiktet skall vara avbildat rakt framifrån. Bakgrunden skall vara vit. Ansiktet skall vara jämnt belyst och det får inte finnas skuggor i bakgrunden.
- Hela huvudet skall vara synligt och blicken skall vara riktad mot kamerans lins. Huvudbonad eller liknande skall inte bäras.
- Undantag från sist nämnda krav får medges för den som i dagligt bruk av religiösa eller medicinska skäl använder huvudbonad. Hela ansiktet måste dock vara synligt.
- Pupillerna skall synas tydligt. Reflexer får inte synas i glasögon. Mörka glasögon får inte bäras i annat fall än då detta påkallat av medicinska skäl.
- Avståndet mellan ögon (pupill) och hakspets skall vara 14 – 17 mm.
- Fotot ska vara utskrivet på fotopapper, vanligt skrivarpapper får inte användas.

4. Rutin för utgivning av Ordinarie kort (Tillitsnivå 3)

Förutsättningar
Utgivning av ordinarie kort (Tillitsnivå 3) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Personen kan identifiera sig med godkänd svensk ID-handling
- Identifiering och verifiering sker enligt godkänd rutin

Vid fotoförsett kort gäller dessutom

- Foto och signatur alltid lagras på en behörighetsskyddad lagringsplats och hämtas med hjälp av SIS Capture Station

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

För SIS gäller:

- Handläggare som hanterar SIS-kort, beställning och utlämning, ska vara godkänd av DNV
- Fotoautomat får användas vid förnyelse enligt dispens men inte vid nybeställning

4.1 Beställning

4.1.1 Kortbeställning med fotografering hos ID-administratör

1. Användaren kommer till kortkontoret
2. Användaren identifierar sig
3. ID-administratören verifierar mot beställningen att foto krävs för korttypen
4. ID-administratören väljer **HCC till nytt kort**
    a. Kortprodukt
    b. Verifierar ID-handling
    c. Anger underskriftskod
5. ID-administratören verifierar kundnummer, kortprodukt och kontor i SCS
6. ID-administratören fotograferar användaren och fångar eventuell namnteckning i SCS
7. ID-administratören anger sin underskriftkod och skickar beställningen till leverantör via SCS

4.1.2 Kortbeställning när foto finns på fil

1. ID-administratören verifierar mot beställningen att foto krävs för korttypen
2. ID-administratören väljer **HCC till nytt kort**
    a. Kortprodukt

b. Anger underskriftskod
3. ID-administratören verifierar kundnummer, kortprodukt och kontor i SCS
4. ID-administratören anger användarens personnummer i fältet för intyg
5. ID-administratören hämtar foto via SCS
6. ID-administratören anger underskiftskod och skickar beställningen till leverantör via SCS

4.1.3 Kortbeställning med fotografering i fotoautomat

1. Användaren går till fotoautomaten
2. Användaren tar del av regelverket som presenteras på skärmen
3. Användaren anger sitt personnummer eller HSA-id genom att antingen
   a. ange manuellt
   b. läs av från SITHS eID
4. Användaren tar, med hjälp av automaten, ett foto rakt framifrån som visar hela ansiktet
5. Användaren skriver under beställningen och att hen tagit del av regelverket genom att antingen
   a. ange pinkod för legitimering eller underskrift (i detta fall ska en kryptografisk kontroll av pinkodens korrekthet göras)
   b. skriva under på inbyggd skrivplatta
6. Fotot sparas ner till behörighetsskyddad lagringsplats tillsammans med underskriften och personnummer.
7. ID-administratören verifierar mot beställningen att foto krävs för korttypen
8. ID-administratören väljer **HCC till nytt kort**
   a. Kortprodukt
   b. Anger underskriftskod
9. ID-administratören verifierar kundnummer, kortprodukt och kontor i SCS
10. ID-administratören anger användarens personnummer i fältet för intyg
11. ID-administratören hämtar foto, eventuell signatur och personnummer från den behörighetsskyddade lagringsplatsen via SCS
12. ID-administratören skriver under och skickar beställningen till leverantör via SCS

4.1.4 Kortbeställning utan foto

1. ID-administratören verifierar mot beställningen att foto inte krävs för korttypen
2. ID-administratören väljer **HCC till nytt kort**
   a. Kortprodukt
   b. Anger underskriftskod
3. ID-administratören verifierar kundnummer, kortprodukt och kontor i SCS
4. ID-administratören anger användarens personnummer i fältet för intyg
5. ID-administratören fullföljer beställningen via SCS genom att gå förbi foto och namnteckning.
6. ID-administratören skriver under och skickar beställningen till leverantör via SCS

4.2 Utlämning

Förutsättningar
Utlämning av ordinarie kort (Tillitsnivå 3) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Personen kan identifiera sig med godkänd svensk id-handling
- Identifiering och verifiering sker enligt godkänd rutin
- Utlämning och mottagande sker i samma flöde

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

4.2.1 Lämna ut kort hos ID-administratör

1. Användaren kommer till kortkontoret
2. Användaren identifierar sig och bekräftar att hen har rätt pinkoder med sig
3. ID-administratören verifierar det levererade kortet mot användaren och användarens id-handling
4. ID-administratören kontrollerar kortnummer och lämnar ut kortet i SITHS Admin
5. ID-administratören anger vilken id-handling som använts
6. ID-administratören skriver under utlämnandet och överlämnar kortet
7. Användaren sätter det nya kortet i kortläsaren
8. Användaren läser och godkänner villkoren
9. Användaren skriver under mottagandet elektroniskt

5. Beställning av pukkod

Förutsättningar
Beställning av pukkod

- Rutinen dokumenteras i organisationens rutiner
- Användaren har ett aktivt ordinarie kort

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

Rutinbeskrivning

1. Användaren beställer en pukkod enligt intern rutin
2. ID-administratören verifierar att användaren har ett aktivt ordinarie kort
3. ID-administratören **Begär PUK till befintligt kort**
4. Pukbrevet skickas med REK till användarens folkbokföringsadress

6. Tilläggscertifikat till ordinarie kort

Förutsättningar

- Rutinen dokumenteras i organisationens rutiner
- Användaren har ett ordinarie kort. Kortet kan vara utfärdat av annan organisation.
- Det är tillåtet att lägga på tilläggscertifikat på kort utlämnat av annan organisation utan att hämta tillstånd från den utfärdande organisationen
    a. Kortinnehavaren ska upplysas om vad man gör och att det eventuellt kan ge problem vid återkomst till ursprungsorganisationen
    b. Kortinnehavaren avgör själv om befintligt kort ska användas
- Det är tillåtet att ta bort tilläggscertifikat från kort utfärdade av annan organisation
- Tillstånd behöver inte hämtas från den utfärdande organisationen
    a. Certifikat från den kortutlämnande organisationen bör inte tas bort

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

Rutinbeskrivning

1. Användaren beställer ett tilläggscertifikat enligt intern rutin
2. ID-administratören väljer att utfärda ett **HCC till befintligt kort**
3. Användaren loggar in i Självadministrationen
4. Användaren laddar ner certifikatet till sitt ordinarie SITHS-kort

7. Rutin för utgivning av Reservkort på plats (Tillitsnivå 2)

Förutsättningar

Utgivning av reservkort på plats (Tillitsnivå 2) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Personen kan identifiera sig
- Identifiering och verifiering sker enligt godkänd rutin

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

Rutinbeskrivning

1. Användaren kommer till kortkontoret
2. Användaren identifierar sig
3. ID-administratören verifierar att användaren har rätt att få ett reservkort

4. ID-administratören väljer **Begär HCC till reservkort** och
    a. Anger kortnummer
    b. Anger giltighetstid
    c. Anger underskriftskod
5. ID-administratören väljer **Lämna ut kort** och
    a. Väljer rätt kort/kortserienummer
    b. Verifierar ID-handling
    c. Anger underskriftkod
6. ID-administratören skriver ut kvittensen och den undertecknas av användaren
7. ID-administratören lämnar över reservkortskuvertet till användaren
8. Användaren använder Självadministrationen för nedladdning av HCC
9. Användaren läser och godkänner villkoren och skriver under med sin underskriftskod

8. Utgivning av Reservkort på distans (Tillitsnivå 2)

Förutsättningar

Utgivning av reservkort på distans (Tillitsnivå 2) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Identifiering och verifiering sker enligt godkänd rutin

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för KUR

Rutinbeskrivning

1. Användaren kommer till kortutlämnare
2. Kortutlämnaren tar fram ett reservkortskuvert
3. Användaren identifierar sig för eller är känd av kortutlämnaren
4. Kortutlämnaren överlämnar en kvittens som användaren fyller i, undertecknar och ger till kortutlämnaren
5. Kortutlämnaren undertecknar kvittensen och skickar in den
6. Kortutlämnaren ringer support
    a. meddelar kortnumret
    b. kortutlämnarens personnummer
10. ID-administratören väljer **Begär HCC till reservkort** och
    a. Anger kortnummer
    b. Anger giltighetstid
    c. Anger underskiftskod
11. ID-administratören väljer **Lämna ut kort** och
    a. Väljer rätt kort/kortserienummer
    b. Anger Intyg som ID-sätt och samt kortutlämnarens personnummer
    c. Anger underskriftskod

9. Utgivning av reservkort - identitetsverifiering med hjälp av arbetskamrater

Förutsättningar

- Rutinen dokumenteras i organisationens rutiner
- Organisationen har en lokal applikation som kan hantera flödet nedan

Rutinbeskrivning

1. Den person som behöver ett reservkort hämtar/får ett obrutet reservkortskuvert innehållande reservkort med tillhörande pinkod från enhetens förvaringsplats.
2. Reservkortsinnehavaren startar applikationen och anger sin identitet, till exempel lokalt användar-id eller HSA-id, identiteten kontrolleras mot lämplig källa och reservkortsinnehavarens namn presenteras som verifiering.
3. Reservkortsinnehavaren anger orsaken till varför ett reservkort behövs.
4. Reservkortsinnehavaren läser lokala villkor och markerar genom en kryssruta att det är gjort.
5. Reservkortsinnehavaren sätter in reservkortet i kortläsaren och applikationen läser av och visar upp kortnumret. Reservkortsinnehavaren tar sedan ut sitt kort.
6. Intygsgivare 1 sätter in sitt kort och läser igenom intygstexten. Texten ska innehålla en försäkran att personen som ska ha reservkortet är den vars identitet och namn står i texten. I texten ska också framgå reservkortsnumret. Om intygsgivaren anser att den kan gå i god för att personen som skall ha reservkortet är rätt person skriver denna under genom att använda sitt certifikat för signering eller identifiering.
7. Intygsgivare 2 gör samma sak som intygsgivare 1 ovan.
8. Intygsgivningen ska sparas, tillgängliga för utgivningsområdet, under 10 år som en verifierbar fil innehållande reservkortsnummer, reservkortsinnehavarens identitet, intygsgivarnas identiteter, datum och tid. Filen ska vara signerad av intygsgivarna. Signeringen ska vara av typen attached.
9. Tre meddelanden ska skickas av applikationen:
    a. Ett till reservkortsinnehavaren med uppmaning att reagera om det inte är hen som begärt ett reservkort.
    b. Ett till intygsgivare 1 med uppmaning att reagera om hen inte har intygat reservkortsinnehavarens identitet.
    c. Ett till intygsgivare 2 med samma uppmaning.
10. Ett meddelande går till utgivningsområdet. I meddelandet ska framgå reservkortsinnehavarens identitet, orsak till behov av reservkort, reservkortsnumret och vilka som verifierat identiteten. I SITHS Admin beställs **Begär HCC till reservkort** och reservkortet lämnas ut. Giltighetstiden för reservkortet ska anpassas efter den orsak som reservkortsinnehavaren angett. Är orsaken förlorat kort ska tidigare kort avregistreras.

11. Om så önskas kan reservkortinnehavaren nu få ett meddelande att beställningen är genomförd och att certifikatet nu kan laddas ner.
12. Reservkortinnehavaren laddar ner certifikat från SITHS Självadministration
13. Reservkortsinnehavaren skriver under en kvittens och skickar in den till utgivningsområdet. Kvittens kan inte göras elektroniskt med det certifikat som reservkortinnehavaren just fått.
14. ID-administratören lägger på bevakning att kvittens ska inkomma från reservkortsinnehavaren. Om kvittens inte inkommer inom skälig tid så ska certifikatet spärras
15. Den underskrivna och inskickade papperskvittensen arkiveras i 10 år.

Förutsättningar

Utgivning av reservkort med två intygsgivare (Tillitsnivå 3) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Identifiering och verifiering sker enligt godkänd rutin
- Båda intygsgivarna måste ha ordinarie SITHS-kort
- Båda intygsgivarna måste finnas i samma organisation i SITHS
- Datorn (där intygsgivare2 agerar) måste ha 2 kortläsare
- Användaren måste ha ett svenskt personnummer

För användare med skyddade personuppgifter

- Kräver att ID-administratören har tilläggsroll för sekretess

Rutinbeskrivning

1. Användaren förfogar över ett reservkort
2. Användaren identifierar sig för eller är känd av intygsgivarna
3. Intygsgivare1 loggar in i SITHS Admin
    a. anger kortnumret
    b. intygar identiteten
    c. anger giltighetstid utifrån internt regelverk beroende på orsak
4. Intygsgivare2 loggar in i SITHS Admin
    a. intygar identiteten
5. Användaren tar över tangentbord och skärm
6. Användaren läser och godkänner villkoren
7. Användaren väljer pinkoder
8. Användaren skriver under mottagandet

10. Utgivning av reservkort på distans utan kortutlämnare

Förutsättningar

- Rutinen ska användas i undantagsfall då en person som ska få reservkort befinner sig på distans och då det saknas behörig ID-administratör där personen befinner sig
- Rutinen dokumenteras i organisationens rutiner
- Reservkortskuvert innehållande reservkort med tillhörande pinkoder och reservkortskvittens skickas med rekommenderad post till personens arbetsplatsadress registrerad i HSA
- ID-administratör sparar kopia av underlaget på reservkortskvittensen för bevakning och utlämning

Rutinbeskrivning

1. ID-administratör skickar:
    a. Reservkortskuvert, manuell reservkortskvittens och informationsmaterial med rekommenderad post till personens arbetsplatsadress.
2. Personen skickar tillbaka ifylld reservkortskvittens
3. ID-administratör
    a. När underskriven kvittens mottagits skapar ID-administratör **Begär HCC för reservkort** och lämnar ut kortet i SITHS Admin med ID-sätt **Identifierad med rekommenderad post.**
4. Reservkortskvittensen arkiveras.
5. Personen laddar ner sitt certifikat via SITHS Självadministration

11. Identifiering vid utgivning av Reservkort till utländska personer med utländsk ID-handling (Tillitsnivå 2)

Förutsättningar

Identifiering vid utgivning av Reservkort till utländska personer med utländsk ID-handling (Tillitsnivå 2) förutsätter att

- Rutinen dokumenteras i organisationens rutiner
- Personen får inte ha registrerats med svenskt personnummer eller samordningsnummer.
- Denna rutin kan inte användas vid utfärdande på distans eftersom ID-administratören ska göra en fysisk kontroll av ID-handlingen.

- med ”ID-handling” menas i denna rutin alla pass och nationella id-kort som kan verifieras enligt nedan.
- ID-administratören ska vara väl införstådd med hur identifiering med hjälp av utländsk ID-handling ska gå till.

Rutinbeskrivning

1. Användaren kommer till kortkontoret
2. Användaren identifierar sig
3. ID-administratören verifierar att användaren har rätt att få ett reservkort
4. ID-administratören verifierar att födelsedatum och ID-handlingens nummer noterats i HSA
5. ID-administratören väljer **Begär HCC till reservkort** och
    a. Anger kortnummer
    b. Anger giltighetstid - verifiera att giltighetstiden på certifikatet/kortet inte överstiger giltighetstiden på uppdraget
    c. Anger underskriftskod
6. ID-administratören väljer **Lämna ut kort** och
    a. Väljer rätt kort/kortserienummer
    b. Verifierar ID-handling enligt någon av nedanstående metoder, se punkt 11.1 i detta dokument
    c. Genomför identifiering enligt punkt 2 i detta dokument
    d. Anger underskriftkod. **Därmed intygar ID-administratören att hen följt rutinen för verifiering av utländsk ID-handling**
7. ID-administratören skriver ut kvittensen och den undertecknas av användaren
8. ID-administratören lämnar över reservkortskuvertet till användaren
9. Användaren använder Självadministrationen för nedladdning av Crossbordercertifikat
10. Användaren läser och godkänner villkoren och skriver under med sin underskriftskod

11.1 Metoder för verifiering av utländsk ID-handling

Någon av följande metoder ska användas:

- ID-skanner
- ID-handlingsdatabas kombinerat med UV-lampa
- PRADO kombinerat med UV-lampa

11.1.1 ID-skanner

Exempel på produkter som kan användas för kontroll av säkerhetsdetaljer:

- Authentiscan från företaget Keesing. Produkten kräver en licens.
- 365id från företaget 365id AB. Produkten kräver en licens.

11.1.2 ID-handlingsdatabas kombinerat med UV-lampa

Hittills godkänd produkt: Documentchecker standard, webbtjänst från företaget Keesing. Här finns bilder av specificerade exemplar av ID-handlingar, funktion för att kontrollera att en MRZ-kod överensstämmer med övriga uppgifter samt helpdesk. Produkten kräver en licens.

Använd UV-lampa för att kontrollera de säkerhetsdetaljer i ID-handlingen som framträder vid UV-belysning.

11.1.3 PRADO kombinerat med UV- lampa

För ID-handling utfärdad av ett EU eller ESS-land kan PRADO användas. PRADO - ”Public Register of Authentic identity and travel Document Online” är ett offentligt register över äkta identitets- och resehandlingar online, vilken tillhandahålls av EU. I PRADO finns information om säkerhetsdetaljer på identitets- och resehandlingar.

Använd UV-lampa för att kontrollera de säkerhetsdetaljer i ID-handlingen som framträder vid UV-belysning.

http://prado.consilium.europa.eu/SV/homeindex.html