Scheme för ackreditering, godkännande och auktorisering för åtkomst till säkerhetsrelaterad reparations- och underhållsinformation (RMI)

SERMI operations group
May 2016

Innehållsförteckning

1. Tillämpningsområde

Detta system är grunden för ackreditering, godkännande och auktorisering av IO: er som kräver åtkomst till säkerhetsrelaterade fordon RMI och tjänster.

Den specificerar i detalj processen och de organ som krävs för att godkänna och auktorisera IO: er att få tillgång till säkerhetsrelaterat fordon RMI enligt följande föreskrifter:

För lätta personbilar och kommersiella fordon (Euro 5 och Euro 6):

- Förordning (EG) nr 715/2007
- Förordning (EG) nr 692/2008 ändrad genom (EU) 566/2011

För tunga fordon (Euro VI):

- Förordning (EG) nr 595/2009
- Förordning (EU) nr 582/2011, ändrad genom förordning (EU) 64/2012

Systemägaren är föreningen “Forum för åtkomst till säkerhetsrelaterad information om reparation och underhåll av fordon”, i förkortad form ”SERMI”.

2 Normativa referenser

Följande refererade dokument är oumbärliga för att förstå och tillämpa detta dokument. För daterade referenser gäller endast den citerade utgåvan. För odaterade referenser gäller den senaste utgåvan av det refererade dokumentet (inklusive eventuella ändringar).

ISO 18541-1: 2014, *Vägfordon - Standardiserad tillgång till fordons-RMI - Del 1: Allmän information och definition av användningsfall*

ISO 18541-2: 2014, *Vägfordon - Standardiserad tillgång till fordons RMI - Del 2: Tekniska krav*

EN ISO / IEC 17011: 2004, *Bedömning av överensstämmelse - Allmänna krav för ackrediteringsorgan som ackrediterar organ för bedömning av överensstämmelse*

EN ISO / IEC 17020: 2012, *Bedömning av överensstämmelse - Krav för drift av olika typer av organ som utför inspektion*

Europaparlamentets och rådets direktiv 1999/93 / EG om *en gemenskapsram för elektroniska signaturer*

ETSI TS 102 042, *Elektroniska signaturer och infrastrukturer (ESI); Policykrav för certifieringsmyndigheter som utfärdar offentliga nyckelcertifikat*

3 Termer, definitioner, symboler och förkortade termer

3.1 Termer och definitioner

3.1.1 Ackreditering

intyg från ett nationellt ackrediteringsorgan (NAB) att ett organ för bedömning av överensstämmelse (CAB) uppfyller kraven i harmoniserade standarder och, i förekommande fall, eventuella ytterligare krav, inklusive de som anges i relevanta sektoriella system, för att utföra en specifik verksamhet för bedömning av överensstämmelse.

OBS Antagen från förordning (EG) 765/2008

3.1.2 Godkännande

process baserad på inspektionen utförd av CAB som bedömer ett IO-företag utgör ett legitimt kommersiellt företag för att bedriva säkerhetsaktiviteter och det och deras enskilda anställda uppfyller kraven i detta dokument.

3.1.3 Auktorisering

process baserad på CAB: s inspektion som bedömer en enskild anställd i ett godkänt IO-företag har rätt att få tillgång till säkerhetsrelaterat RMI. Den enskilda medarbetaren tilldelas en säker hårdvarutoken som innehåller ett personligt digitalt certifikat och en PIN-kod utfärdad av ett utsett Trust Center.

3.1.4 Digitalt certifikat

digitalt certifikat som använder en digital signatur från det utfärdande Trust Center för att binda en offentlig nyckel till IO-anställdas identitet enligt standarden ISO 20828. Det digitala certifikatet ska lagras i en säker hårdvarutoken med åtkomst- och kopieringsskydd. Identifieraren skapas av CAB och den fysiska personens identitet är endast känd för CAB.

3.1.5 Säker hårdvaru-Sign

kort eller USB-enhet skyddad av en PIN-kod mot obehörig åtkomst eller kopiering.

3.1.6 Certifieringsdatabas

databas som innehas av respektive Trust Center för att hantera det digitala certifikatets giltighet och identifierarna för auktoriserade IO-anställda.

3.1.7 Säkerhetsrelaterad information om reparation och underhåll

erforderlig information, programvara, funktioner och tjänster för att reparera och underhålla de funktioner som ingår i ett fordon av tillverkaren för att förhindra att fordonet blir stulet eller kört bort och för att spåra och återställa fordonet.

Reparation och underhåll av säkerhetsrelaterade funktioner inkluderar:

a. uppdatera en funktionellt sammanhängande programvara när den programvaran utför funktioner för att förhindra att fordonet blir stulet eller körs bort

b. köpa delar som förhindrar att fordonet blir stulen eller bogseras eller som kan användas av obehöriga för att ge fordonet en ny identitet.

Fordonstillverkare ska utforma funktionerna för att förhindra att fordon blir stulna i enlighet med FN-ECE-föreskrift 116 om enhetliga tekniska bestämmelser om skydd av motorfordon mot obehörig användning. De ska utforma dessa funktioner på ett sådant sätt att det inte gör oberoende operatörers rätt att få tillgång till reparations- och underhållsinformation för funktioner som inte är säkerhetsrelaterade.

3.1.8 Auktoriseringsdatabas
databas som innehas av respektive Trust Center som innehåller behörighetsuppgifterna för de anonymiserade auktoriserade IO-anställda.

3.1.9 Det europeiska samarbetet för ackreditering (EA)
det organ som erkänns av Europeiska kommissionen enligt artikel 14 i förordning (EG) 765/2008

3.1.10 Det nationella ackrediteringsorganet (NAB)
det enda organ som utsetts i varje medlemsstat enligt förordning (EG) 765/2008

3.1.11 Organet för bedömning av överensstämmelse (CAB)
Det organ som ansvarar för inspektion av IO: er och deras respektive IO-anställda och för att utfärda inspektionsintyg enligt detta schema, så att IO: er och deras respektive IO-anställda kan godkännas och bemyndigas att bedriva säkerhet inom bilsektorn. CAB ansvarar också för att utreda påståenden om missbruk och för att kommunicera resultatet till TC om behörigheten och godkännandet skulle återkallas. CAB ska vara fri från intressekonflikter (typ A), särskilt när det gäller ekonomiska, personliga eller familjeband med alla intressenter som använder eller tillhandahåller RMI.

3.1.12 Oberoende operatör (IO)
IO-företag enligt definitionen i förordning (EG) 715/2007 som lämnar in en ansökan till CAB för godkännande för att engagera anställda i säkerhetsrelaterad reparations- och underhållsinformation.

3.1.13 IO juridisk ombud
fysisk person som har befogenhet att lagligen representera IO i alla aspekter av tillgången till fordonets RMI.

3.1.14 IO-anställd
den anställde av den godkända IO som är auktoriserad som enskild person att delta i säkerhetsrelaterad reparations- och underhållsinformation (RMI) och som tillhandahålls av CAB med nödvändigt säkert hårdvarutoken och digitalt certifikat.

3.1.15 Fordonstillverkare (VM)
fordonstillverkare enligt definitionen i förordning (EG) 715/2007 och vars ansvar inom systemet är att ge tillgång till säkerhetsrelaterat RMI och funktioner till alla auktoriserade IO-anställda och som kommunicerar med Trust Center för att verifiera den pseudonymiserade identitets- och auktoriseringsstatusen för IO-medarbetaren som söker tillgång.

3.1.16 Trust Center (TC)
organ som ansvarar för att hantera de digitala certifikaten och auktoriseringsstatusen för IO-anställda och för att tillhandahålla CAB nödvändiga säkra hårdvarutoken för auktoriserade IO-anställda. TC är också ansvarig för att förse VM med information om den aktuella statusen för en anställds certifikat och auktorisering.

3.1.17 Forum för tillgång till säkerhetsrelaterat fordon RMI (SERMI)
systemägaren som ansvarar för definitionen, driften och underhållet av ackrediteringssystemet. Detta ansvar behandlas i EA-reglerna som systemägande. Medlemmarna i SERMI ska företräda intressenterna i processen för tillgång till säkerhetsrelaterat fordon RMI.

3.1.18 Relevanta myndigheter (RA)
offentliga myndigheter med lagligt mandat att agera inom området skydd av fordonssäkerhetsbrott, utredning och lagföring.

3.2 Förkortning - Definition

ACEA	European Automobile Manufacturers Association
AFCAR	Alliance for the Freedom of Car Repair in the EU
CAB	Organ för bedömning av överensstämmelse
CABUID	Organ för bedömning av överensstämmelse unik identifierare
CIRCA	kommunikations- och informationsresurscenteradministratör
CSP	Cryptographic Service Provider
DPA	Data Protection Act
EA	Europeiskt samarbete för ackreditering
EG	Europeiska gemenskapen
EN	Europeisk norm
SERMI	Forum för åtkomst till säkerhetsrelaterad information om reparation och underhåll av fordon
HW	Hårdvara
IO	Oberoende operatör
IOEUID	Oberoende operatör anställd unik identifierare
IOUID	Oberoende operatör unik identifierare
NAB	Nationella ackrediteringsorgan
OCSP	Online Certificate Status Protocol enligt RFC 2560
PIN	kod för personlig identifiering
PKCS # 11	Public Key Cryptography Standard

RA	Relevant myndighet
RMI	Reparations- och underhållsinformation
SOAP	Simple Object Access Protocol (Authorization Web Service)
TC	Trust Center
VM	Fordonstillverkare

4. Dokumentöversikt och struktur

En övergripande beskrivning av systemet och sammanhanget för åtkomst till säkerhetsrelaterat fordon RMI ges i kapitel 5.

Systemet specificeras i detalj i kapitel 6, där de organ som är inblandade i processen beskrivs med avseende på deras roll, ansvar, institutionella legitimitetskriterier och funktionella driftskrav.

Krav på implementering av tekniska system specificeras i kapitel 7.

5 Allmän information

Kontexten för IO-åtkomst till säkerhetsrelaterad RMI består av två processer. En process är utformad för att ge IO och dess anställda ett godkännande och tillstånd för åtkomst. Den andra processen visar åtkomst till säkerhetsrelaterad RMI i ett VM RMI-system.

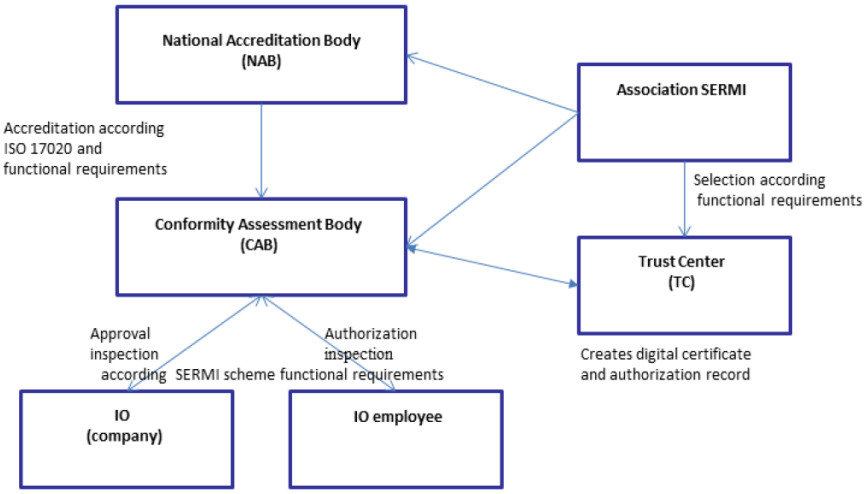
5.1 Godkännande och godkännande av IO

Processen kräver att NAB i medlemsstaterna är beredda att ackreditera CAB enligt det schema som föreslås i denna rapport som har validerats av EA. Det krävs också att CAB: er är ackrediterade av NAB i sina medlemsstater.

IO måste ansöka om godkännande och inspektion av arbetstagarbehörighet till en CAB som är ackrediterad i den stat där den anställde bor. När inspektioner för IO-godkännande och för en enskild IO-anställningstillstånd har utförts med ett positivt resultat, informerar CAB TC. TC skapar en auktoriseringspost och utfärdar en säker hårdvarutoken och ett digitalt certifikat som innehåller detaljer som gör att IO-anställd kan identifieras unikt på VM RMI-webbplatsen. Den säkra hårdvarutoken med det digitala certifikatet tillhandahålls den enskilda IO-anställda via CAB. Registrering av IO-medarbetaren för åtkomst till VM RMI-webbplatsen och betalning av IO i enlighet med VM RMI-webbplatsens villkor krävs för att kunna komma åt säkerhetsrelaterad RMI som beskrivs i nästa avsnitt.

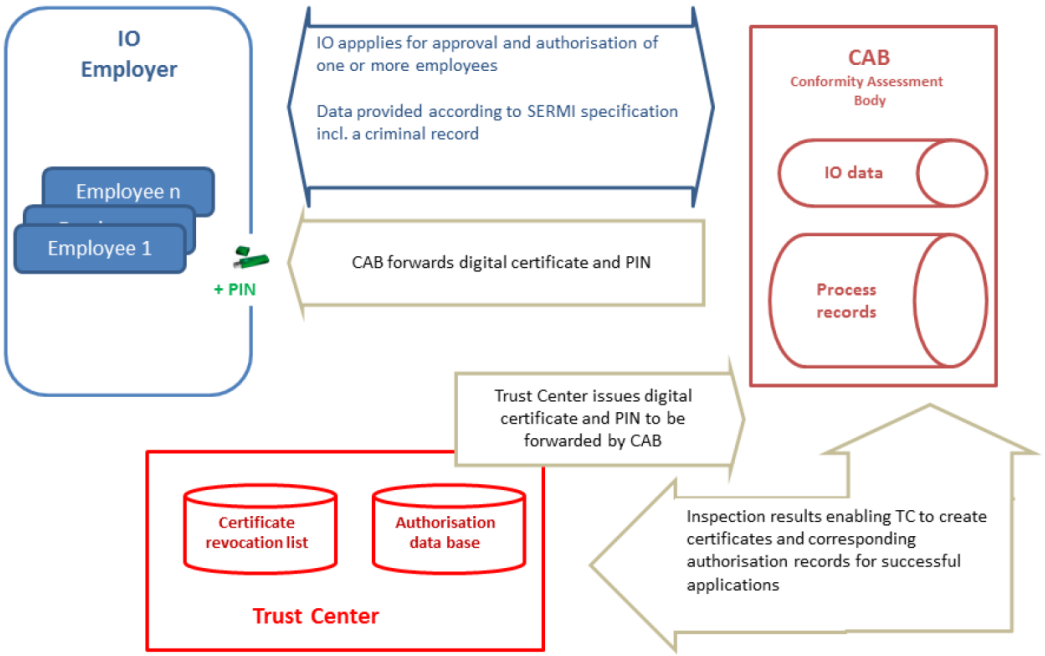
All digital dataöverföring mellan IO, TC och CAB sker via affär till affär (B2B) -transaktioner i rätt tid med säkra protokoll.

Följande bild visar de organ som är inblandade i systemet och deras förhållande.



Figur 1: De organ som är inblandade i systemet och deras relationer

Följande bild beskriver IO-godkännandeprocessen och IO-godkännandeprocessen.



Figur 2: IO-godkännande och IO-godkännandeprocess

5.2 Översiktsåtkomst till säkerhetsrelaterad RMI

Tillgång till säkerhetsrelaterat RMI ska tillhandahållas av den VM via dess RMI-webbplats (RMI) förutsatt att IO-medarbetaren är auktoriserad och IO för vars räkning han arbetar är godkänd av lämplig CAB.

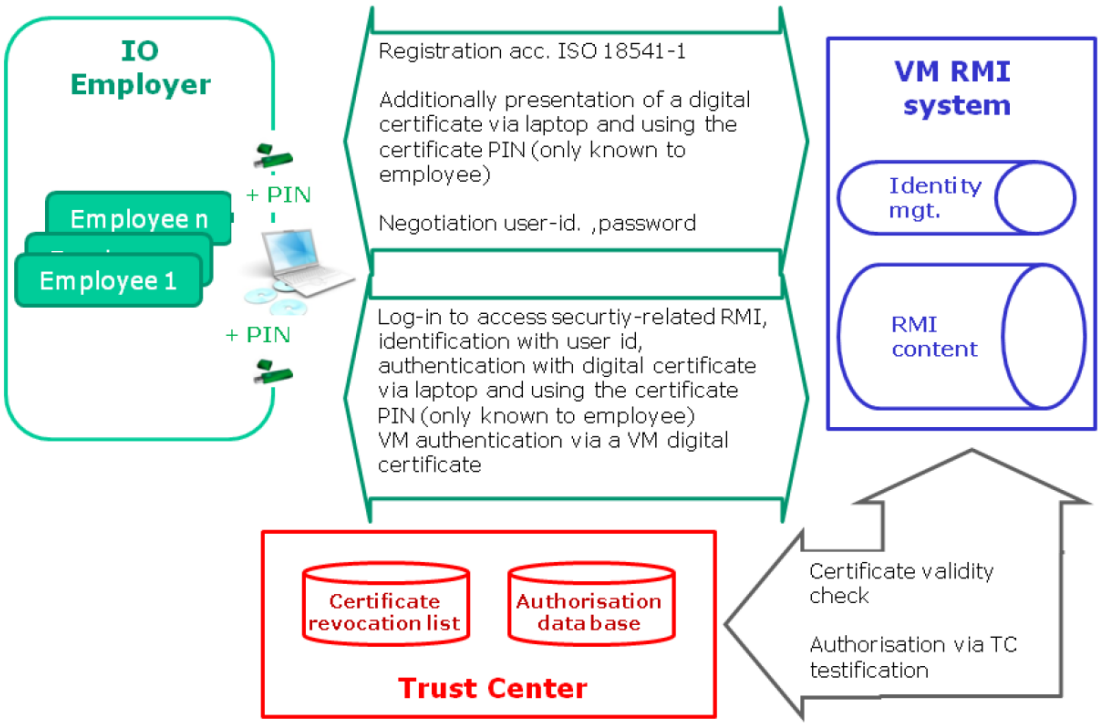
Tillverkare kan erbjuda en online-beställning facilitet för säkerhetsrelaterade delar med hjälp av en specialapplikation länkad till RMI-webbplatsen, vilket kräver att IO-medarbetaren är auktoriserad och IO för vars räkning han arbetar godkänns av lämplig CAB. Alternativt kan säkerhetsrelaterade delar erhållas från agenter / auktoriserade återförsäljare där för närvarande etablerade autentiseringsförfaranden finns (dvs. inga digitala certifikat krävs). Under alla omständigheter ska säkerhetsrelaterade delar levereras av VM och / eller deras ombud / auktoriserade återförsäljare i rätt tid till IO:erna.

För att kunna logga in och få åtkomst till säkerhetsrelaterad RMI krävs registrering av IO-medarbetaren hos VM för åtkomst till RMI-webbplatsen och betalning av IO för säkerhetsfunktionen.

En auktoriserad och registrerad IO-anställd kommer vid behov att logga in på VM RMI-webbplatsen och begära åtkomst till säkerhetsrelaterad RMI eller inköp av delar, moduluppdatering eller nyckeldriftsättning.

Vid mottagandet av begäran kommer VM-webbplatsen att kräva identifiering genom IO-medarbetarens unika identifierare och lämplig autentisering och auktorisering. Lämplig autentisering av IO-medarbetaren görs uteslutande med det digitala certifikatet. Vid mottagandet av det digitala certifikat, kommer VM RMI-webbplatsen att verifiera IO-anställdas unika identifierare och den aktuella statusen för certifikatet och auktorisationen genom att kommunicera med lämpligt Trust Center som anges i certifikatet.

All digital dataöverföring mellan IO, VM, TC och CAB sker via affär till affär (B2B) - transaktioner i rätt tid med säkra protokoll. När IO-anställdas unika identifierare och auktoriseringsstatus för IO-medarbetaren har verifierats ska VM RMI-webbplatsen ge åtkomst till den nödvändiga säkerhetsrelaterade funktionen.



Figur 3: Tillgång till säkerhetsrelaterad RMI

6 Schemaspecifikation

6.1 Specifikation av SERMI-rollen

Föreningen SERMI är systemansvarig som ansvarar för definition, drift och underhåll av ackrediteringssystemet. Föreningen SERMI har fått ett mandat från Europeiska kommissionen att bli det legitima organet för urvalsprocessen för Trust Center (TC).

6.1.1 Ansvar och krav

1) SERMI ska hantera begäran om ändringar av ackrediteringsprocessen och ska övervaka harmoniseringen av nationella implementeringar mellan medlemsstaterna.

2) SERMI ska skapa kriterier för val av TC och välja TC (er).

3) SERMI ska ansvara för att fastställa riktlinjer för teknisk implementering för interaktion mellan enheter i processen.

4) SERMI ska följa EA: s normer och riktlinjer för systemägare.

6.1.2 Funktionskrav: användningsfall

UC SE1. SERMI ska hantera begäran om systemändring och ska övervaka harmoniseringen av nationella implementeringar mellan medlemsstaterna

Aktör	AFCAR, ACEA, CAB
Mål	Aktörer kan (med goda skäl) göra en begäran om att ändra systemet
Case - Indata	En begäran om ändring av schemat för att ta emot säkerhetsrelaterat RMI
Case - Utdata	uppdaterat schema för att ta emot säkerhetsrelaterat RMI där så är lämpligt
Kort beskrivning	SERMI ska hantera förfrågningar om systemändringar. Medlemmarna ska utvärdera och uppdatera systemet.

UC SE2. SERMI ska välja Trust Center (TC)

Aktör	TC
Mål	För att aktivera och utse TC.
Case - Indata	TC: s ansökan till SERMI som ska bedöma att TC uppfyller alla funktionella och tekniska krav.
Case - Utdata	Godkänd eller avvisad TC-ansökan. Uppdaterad vald TC-lista.
Kort beskrivning	SERMI ska behandla förfrågningar från TC som ansöker om urval enligt kriterierna i avsnitt 6.1.3. SERMI ska skapa och uppdatera den valda TC-listan.

UC SE3. SERMI ska ansvara för att ställa in implementeringsguiden för interaktion mellan enheter i processen (t.ex. med OCSP, SOAP ...)

Aktör	SERMI
Mål	Fordonstillverkare och TC ska använda implementeringsguiden för att uppnå korrekt implementering av de nödvändiga (OCSP och SOAP) standarderna.
Case - Indata	Information och kända standarder.
Case - Utdata	Implementeringsguide som ger all information som krävs för kommunikationsgränssnitten.
Kort beskrivning	SERMI kommer att skapa och underhålla implementeringen med tanke på förbättrade säkerhetskrav och förbättrad teknik över tid.

6.1.3 Val av förtroendecenter

TC väljs av systemägaren SERMI.

Den valda TC ska uppfylla standarden ETSI TS 102 042, uppfylla kraven enligt direktiv 1999/93 / EG "kvalificerad elektronisk signatur" och de krav som beskrivs i kapitel 6.6.

Dessutom ska TC uppfylla kriterierna nedan:

- Förslagets tekniska fördel
- Trustcentrets förmåga att uppfylla kraven inklusive teknisk och ledningskompetens, ekonomisk bärkraft och relevant erfarenhet, med bevisad meritlista
- Relevant kompetens, erfarenhet och tillgänglighet för nyckelpersoner
- Kapaciteten av Trust centerts förmåga att verka över hela den europeiska scenen (EU 28)
- Förekomsten av en kvalitetssäkringsprocess på operativ nivå

6.2 Specifikation av NAB-roll

NAB, det enda organ som utsetts i varje medlemsstat enligt förordning (EG) nr 765/2008, ansvarar för ackrediteringen av organ för bedömning av överensstämmelse (CAB) som deltagare i systemets tillgång till säkerhetsrelaterade fordon RMI.

6.2.1 Ansvar och krav

NAB: s ansvar och krav definieras i förordning (EG) 765/2008

6.2.2 Funktionskrav: användningsfall

UC NA1. Ackreditering av en CAB

Aktör	CAB
Mål	Ackrediterad CAB.

Case - Indata	Ansökningsformulär från en CAB för att behandlas av NAB.
Case - Utdata	CAB är antingen ackrediterat eller inte ackrediterat. NAB-ackrediteringsrapport från CAB.
Kort beskrivning	Ackrediteringsformulär som tillhandahålls av NAB för komplettering av CAB. Ackrediteringsformuläret ska fyllas i av den organisation som ansöker om att bli CAB. NAB ska bedöma att organisationen uppfyller alla angivna krav. Ackrediteringsförfarandet ska säkerställa att CAB bedöms som "Bedömning av överensstämmelse - Krav för drift av olika typer av organ som utför inspektion" (ISO / IEC 17020) som inspektionsorgan typ A, och de ytterligare kriterier som beskrivs i avsnitt 6.2.3. CAB ska begära ackreditering enligt reglerna i artikel 7 i förordning (EG) nr 765/2008.

UC NA2. Behandling av klagomål mot CAB

Aktör	IO, TC, VM, relevanta myndigheter.
Mål	Att hantera klagomål.
Case - Indata	Klagomål mot en CAB.
Case - Utdata	Lösning av klagomål mot CAB.
Kort beskrivning	Det förväntas generellt att klagomål löses på lokal nivå mellan CAB och den klagande. Klagomål som inte löses på lokal nivå kan hänvisas till NAB för vidare övervägande. I sådana fall ska NAB hantera klagomål enligt etablerade rutiner enligt ISO 17011: 2004, sek. 5.9. Ackrediteringsorganet a) ska besluta om klagomålets giltighet, b) ska vid behov se till att ett klagomål angående ett ackrediterat CAB först behandlas av CAB, c) vidta lämpliga åtgärder och bedöma deras effektivitet, d) ska registrera alla klagomål och vidtagna åtgärder, och e) ska svara på den klagande. Under klagomålsprocessen via NAB förblir alla befintliga IO-godkännanden (papperscertifikat) och alla anställda auktorisationer (digitala certifikat) som har utfärdats av detta CAB giltiga. Om NAB beslutar att återkalla CAB-ackrediteringen måste alla IO-godkännanden (papperscertifikat) och alla arbetstagarbehörigheter (digitala certifikat) som har utfärdats av denna CAB krävas förnyas. SERMI ska informeras om detta beslut av NAB. CAB ska sedan omedelbart informera den godkända IO om detta beslut genom en så kallad slutförsäljningsanmälan. Om en av aktörerna anser att källan till klagomålet har att göra med systemdefinitionen ska detta hänvisas till systemägaren SERMI enligt användningsfall SE1.

UC NA3. NAB-lista över ackrediterade CAB

Aktör	NAB
Mål	NAB ska ha en uppdaterad lista över alla ackrediterade CAB.
Case - Indata	Ackrediterade CAB
Case - Utdata	En landsspecifik lista över ackrediterade CAB för detta land
Kort beskrivning	NAB ska skapa, underhålla och publicera en landsspecifik lista över alla ackrediterade CAB.

6.2.3 Kriterier för CAB-ackreditering

CAB ska ackrediteras som ett inspektionsorgan av typ A i enlighet med ISO / IEC 17020. Alternativ A för ledningssystemkravet ska tillämpas. Som ett inspektionsorgan av typ A måste CAB uppfylla de högsta kraven på oberoende.

Dessutom ska CAB: s förmåga att uppfylla de ansvarsområden och krav som beskrivs i avsnitt 6.3.1 och funktionskraven som beskrivs i avsnitt 6.3.2 bedömas av NAB under ackrediteringsprocessen.

Den personal som ansvarar för IO-inspektioner ska ha en kunskapsnivå inom reparations- och underhållsverksamheten för fordonsfordon och bilspecifikationer som är lämpliga för de uppgifter de utför.

6.3 Specifikation av CAB-rollen

CAB ska ansvara för att godkänna IO-kommersiella företag och bemyndiga associerade IO-anställda att delta i åtkomst till säkerhetsrelaterad information om reparation och underhåll av fordon.

6.3.1 Ansvar och krav

1) CAB ska upprätta en säker kommunikationskanal mellan CAB och TC.

2) CAB ska acceptera eller avvisa inspektionsansökningar från IO: s juridiska representanter och IO-anställda från de medlemsstater vars NAB det har ackrediterats.

3) CAB ska bedöma ansökningar om godkännande från lämpliga IO-företrädare och utfärda ett inspektionsintyg till IO-företrädare som uppfyller godkännandekriterierna så att TC kan behålla dem i auktoriseringsdatabasen under en period av 60 månader eller avslå ansökningar som inte uppfyller godkända kriterier.

4) CAB ska meddela IO: er sex månader innan godkännandet upphör.

5) CAB ska bedöma ansökningar om förnyelse av ett godkännande där så är lämpligt och utfärda ett nytt inspektionsintyg för IO som uppfyller godkännandekriterierna så att TC kan behålla dem i auktoriseringsdatabasen under ytterligare en period på 60 månader.

6) CAB ska behålla IO-uppgifterna om certifiering.

7) CAB ska meddela inspektionsresultat till TC så att IO-godkännanden återkallas där så är lämpligt.

8) CAB ska bedöma ansökningar om tillstånd för lämpliga IO-anställda och utfärda ett inspektionsintyg till IO-anställda som uppfyller auktoriseringskriterierna så att TC kan behålla dem i auktoriseringsdatabasen under högst 60 månader. Denna period kan inte vara längre än den återstående giltighetsperioden för respektive IO-godkännande.

9) CAB ska meddela IO-anställda 6 månader innan auktorisationen upphör att gälla.

10) CAB ska bedöma ansökningar om förnyelse av ett tillstånd där så är lämpligt och utfärda ett inspektionsintyg till IO-anställda som uppfyller auktoriseringskriterierna så att TC kan behålla dem i auktoriseringsdatabasen under ytterligare en period på högst 60 månader. Denna period kan inte vara längre än den återstående giltighetsperioden för respektive IO-godkännande.

11) CAB ska hålla IO-anställdas uppgifter om auktorisationer.

12) CAB ska utfärda ett negativt inspektionsintyg så att TC kan återkalla auktorisationen för en IO-anställd där så är lämpligt.

13) CAB ska undersöka påståenden om missbruk och bedöma om tillstånd och godkännande ska återkallas.

14) CAB ska fungera som ett gränssnitt till alla IO: er som godkänts av det CAB: n för ansökningar och klagomål.

15) CAB ska endast samla in och använda de uppgifter som krävs för godkännande / auktoriseringsprocessen som definieras här.

16) CAB ska behandla IO-data konfidentiellt.

17) CAB ska kommunicera inspektionsresultat till TC för att utfärda nödvändig säker hårdvaru-sign med ett digitalt certifikat för auktoriserade IO-anställda.

18) CAB ska tillhandahålla lämplig statistik till systemägaren SERMI.

19) CAB kommer endast att upprätta en affärsrelation med den ursprungligen valda TC för alla medlemsstater.

20) I framtiden ska CAB endast upprätta en relation med TC som certifierats av systemets ägare.

21) CAB ska spara säkra register över godkännande- och auktorisationsinspektioner under en period av fem år och i enlighet med lagen om dataskydd.

22) CAB ska informera alla andra CAB i sin medlemsstat om negativa inspektionsresultat av en IO.

23) CAB ansvarar för att de uppgifter som tillhandahålls under inspektioner av godkännande och godkännande överensstämmer med kraven, t.ex. säkerställa att all data är identisk med originaldokumentationen.

24) CAB är ansvarigt om de uppgifter som tillhandahålls av en auktoriserad anställd inte överensstämmer med kraven för auktorisationsinspektioner, t.ex. kopior och värden är inte desamma.

25) CAB ska göra slumpmässiga och oanmälda kontroller på plats av IO inom 60 månaders giltighetsperiod. Varje godkänd IO ska genomgå minst en slumpmässig kontroll på plats under 60 månaders giltighetsperiod. Ett negativt inspektionsresultat ska leda till återkallande av IO-godkännandet och IO-anställdas auktorisationer.

26) CAB ska tidigast göra en kontroll på plats på IO-begäran, sex månader före giltighetsfristen. Ett positivt inspektionsresultat krävs för förnyelse av ett godkännande.

6.3.2 Funktionskrav: användningsfall

UC CA1. CAB inrättar en affärsrelation med Trust Center

Aktör	CAB
Mål	CAB ska upprätta en affärsrelation med en vald TC som publiceras i SERMI vald TC-lista.
Case - Indata	Kontakt med utvalda TC ur listan över godkända TC publicerade av SERMI.
Case - Utdata	Ett undertecknat avtal mellan CAB och TC ska upprättas.
Kort beskrivning	CAB ska ha en affärsrelation med en vald TC enligt den publicerade SERMI-listan (se UC SE2) för att: a) Skapa digitala certifikat och auktoriseringsposter. b) Behåll godkännande och auktoriseringsstatus (skicka ut "nytt" certifikat vid behov). c) Skicka det digitala certifikatet och PIN-koden som ska skickas till IO-medarbetaren av CAB. En CAB ska bara skapa en affärsrelation med en TC.

UC CA2. CAB inspekterar IO för godkännande

Aktör	IO
Mål	Godkännande av IO så att en IO kan namnge medarbetare för behörighet att få tillgång till säkerhetsrelaterat RMI.
Case - Indata	Fyllt i ansökningsformulär enligt krav från CAB. Ansökningsformuläret ska åtminstone innehålla kriterierna i kapitel 6.3.3.
Case - Utdata	Papperscertifikat med IO-inspektionsresultat.
Kort beskrivning	IO: s juridiska ombud ska skicka ansökningsblanketten och alla nödvändiga handlingar till CAB på granskningsbara sätt. CAB ska kontrollera dokumenten och kontrollera om IO redan har inspekterats av en annan CAB. Om kriterierna för IO-godkännande (se 6.3.3) är uppfyllda ska CAB skicka pappersinspektionsintyget till IO: s juridiska representant. CAB ska på granskningsbara sätt meddela de andra CAB: erna i respektive land om IO inte klarar CAB-kontrollen. CAB ansvarar för inkonsekventa uppgifter. Varje IO-anställd hos en IO som blir auktoriserad för åtkomst till säkerhetsinformation ska registreras på samma CAB och TC. Varje godkänd IO ska underkastas oanmälda slumpmässiga kontroller minst en gång under godkännandets giltighetsperiod. Schema

UC CA3. CAB kontrollerar IO på plats

Aktör	CAB
Mål	Minst en slumpmässig och oanmäld kontroll på plats av varje godkänd IO under giltighetsperioden och en IO begärde kontroll på plats under de sista sex månaderna av giltighetsperioden ska säkerställa att den information som ges under ansökan är korrekt och att förfarandekraven implementeras och praktiseras i daglig verksamhet som anges av IO i ansökan om godkännande.
Case - Indata	Oanmälda besök i IO-lokaler. Besök i IO-lokaler på IO-begäran.
Case - Utdata	IO-godkännande bekräftas eller återkallas. Om IO-godkännandet återkallas återkallas IO-medarbetarens auktorisationer och TC uppmanas att återkalla motsvarande digitala certifikat.
Kort beskrivning	Kvalificerad CAB-personal besöker IO och kontrollerar på plats kriterierna i avsnitt 6.3.3 och implementering och beaktande i den dagliga driften av kriterierna i avsnitt 6.3.4. Enligt resultaten under kontrollen bekräftas eller återkallas IO-godkännandet. CAB kan besluta att låta IO granska korrekt korrigera mindre brister under en definierad tidsperiod efter kontrollen på plats för att undvika godkännande. Ett slutligt negativt inspektionsresultat ska resultera i att IO återkallar IO-godkännandet, IO-medarbetarbehörigheter och IO-anställdas digitala certifikat från TC.

UC CA4. CAB inspekterar IO för förnyelse av godkännande

Aktör	IO
Mål	Förnyelse av IO-godkännande.
Case - Indata	Slutförd ansökan enligt kravet från CAB. Ansökningsformuläret ska åtminstone innehålla kriterierna i kapitel 6.3.3. Positivt resultat av en IO som begärts på platsinspektion av CAB under de sex månaderna före tidsfristen för godkännandets utgång.
Case - Utdata	Pappersintyg med inspektionsresultat för förnyelse av ett IO-godkännande. Utgången av IO-godkännande, IO anställdes auktorisering och återkallande av de digitala certifikaten i händelse av ett negativt inspektionsresultat eller avslag på förnyelsebegäran.
Kort beskrivning	Efter en tidsperiod på 60 månader ska godkännandet förnyas. Innan godkännandet upphör ska IO: s juridiska företrädare underrättas av CAB om den väntande utgången. Denna anmälningsperiod ska vara sex månader innan godkännandet upphör. IO: s juridiska representant begär en inspektion på plats av CAB. CAB utför inspektionen på plats. Om inspektionsresultatet är negativt ska CAB återkalla IO-godkännandet och IO-anställdas auktorisationer. CAB instruerar TC att återkalla IO-anställningscertifikaten. IO: s juridiska representant ska skicka alla handlingar på granskbar väg till CAB två månader innan godkännandet upphör. CAB ska kontrollera dokumenten och kontrollera om IO redan har godkänts eller avvisats av en annan CAB. Om kriterierna för IO-godkännande (se 6.3.3) uppfylls ska CAB skicka certifikatet för inspektionspapper till IO: s juridiska representanter. CAB ska meddela de övriga CAB: erna i respektive land på granskningsbart sätt om IO inte klarar CAB-kontrollen. CAB ansvarar för inkonsekventa uppgifter. Varje anställd hos en IO som blir auktoriserad för åtkomst till säkerhetsinformation efter auktoriseringsinspektionen som beskrivs i användningsfall CA6 ska registreras på samma CAB och TC.

UC CA5.CAB underhåll av IO-data

Aktör	IO
Mål	IO-data ska vara korrekta.
Case - Indata	IO ska begära respektive CAB att ändra IO-uppgifterna. IO: s juridiska ombud ska fylla i lämpligt ändringsformulär och överlämna det till CAB.
Case - Utdata	Uppdaterad IO-data.
Kort beskrivning	IO: s juridiska representant ska skicka alla nödvändiga dokument till CAB på granskningsbara sätt. CAB ska kontrollera dokumenten. Om kraven uppfylls ska CAB utfärda pappersintyget till IO: s juridiska representanter.

UC CA6. CAB inspekterar IO-anställda för auktorisering

Aktör	IO - Anställd
Mål	Auktorisering av en IO-anställd eller en grupp av IO-anställda.
Case - Indata	Fyllt i ansökningsblankett för inspektion enligt krav från CAB. Ansökningsformuläret ska åtminstone innehålla kriterierna i kapitel 6.3.5.
Case - Utdata	Inspektionsresultat till TC för att: 1) utfärda ett elektroniskt HW-certifikat för denna IO-anställd, 2) skapa IO-anställdas auktoriseringsregister i databasen.
Kort beskrivning	IO-medarbetaren ska skicka ansökan och alla nödvändiga dokument till CAB på granskningsbart skick. CAB ska kontrollera om IO-medarbetaren hade ställt ett tidigare krav som avvisats av CAB själv eller någon annan CAB på europeisk nivå. CAB ska kontrollera dokumenten. Om kriterierna för IO-anställdas auktorisation (se 6.3.5) är uppfyllda ska CAB informera TC för att utfärda ett elektroniskt HW-certifikat (användningsfall TC1). Varje IO-anställd hos en IO som söker tillstånd ska registreras hos CAB och TC där IO: s godkännande är registrerat. Förkontroll av riktigheten och fullständigheten av information som lämnats av en IO-juridisk representant för dess anställda täcks av ISO 17020: 2012 klausul 7.1.6 och avsnitt 6.3.

UC CA7. Pseudonymisering av personuppgifter i CAB

Aktör	CAB
Mål	Pseudonymisering av personuppgifter från IO-anställda.
Case - Indata	Förnamn, efternamn på IO-medarbetaren.
Case - Utdata	IO-anställd unik identifierare som ska användas som i det digitala certifikatet.
Kort beskrivning	Förnamn, efternamn på IO-medarbetaren överförs till en IO-anställd unik identifierare som kommer att användas under hela processen för åtkomst till säkerhetsrelevant RMI. Användningsfallet säkerställer att behandlingen av personuppgifter sker i enlighet med EU-regler som skyddar individers grundläggande rättigheter och friheter, särskilt direktiv 95/46 / EG och direktiv 2002/58 / EG.

UC CA8. CAB informerar TC för att utfärda ett digitalt certifikat

Aktör	CAB
Mål	Att förse IO-medarbetaren med ett digitalt certifikat.
Case - Indata	CAB-inspektionsresultat till TC för en auktoriserad anställd.
Case - Utdata	Säker hårdvaru.sign med ett digitalt certifikat och en separat PIN-kod för IO-medarbetaren som skickas till CAB. IO-medarbetaren ska ta emot PIN-koden som är associerad med det digitala certifikatet som vidarebefordras av CAB på granskningsbara sätt.
Kort beskrivning	CAB ska skicka all nödvändig data till TC så att TC kan producera det digitala certifikatet, den säkra hårdvarutoken och PIN-koden.

UC CA9. CAB-inspektion av en IO-anställd för förnyelse av auktorisation

Aktör	IO-anställd
Mål	Förnyelse av anställningstillstånd
Case - Indata	Fyllt i ansökningsblankett för inspektion enligt krav från CAB. Ansökningsformuläret ska åtminstone innehålla kriterierna i kapitel 6.3.5.
Case - Utdata	Resultat för förnyelsekontroll av en IO-anställningstillstånd.
Kort beskrivning	Auktorisationen ska gälla under en bestämd period efter vilken tid auktorisationen upphör att gälla och måste förnyas. CAB ska informera IO om det datum då anställdas auktorisation upphör att gälla, sex månader före det faktiska datumet för auktorisationens utgång. IO-anställd ska skicka alla handlingar på granskningsbar väg till CAB 2 månader innan auktorisationen upphör att gälla. Processen för godkännandekontroll som beskrivs i användningsfall CA6 ska utföras.

UC CA10. CAB - underhåll av anställdas data

Aktör	IO - Anställd
Mål	Informationen om IO-anställda är korrekt
Case - Indata	Begär till respektive CAB att uppdatera IO-anställdas data. Lämpligt formulär ska fyllas i och undertecknas av IO-medarbetaren och IO: s juridiska ombud innan de skickas till CAB.
Case - Utdata	Uppdaterad IO-anställd.
Kort beskrivning	IO-anställda ska skicka alla nödvändiga dokument till CAB på granskningsbara sätt. CAB ska kontrollera dokumenten. Om uppdateringsförfrågan påverkar data lagrade i det digitala certifikatet ska CAB informera TC för att utfärda ett nytt digitalt certifikat (användningsfall TC1).

UC CA11. CAB-förfarande för klagomål och överklagande

Aktör	CAB
Mål	CAB ska ha en dokumenterad process för att ta emot, utvärdera och fatta beslut om klagomål och överklaganden. denna process ska respektera respektive nationell lagstiftning.
Case - Indata	Regler, standarder och SERMI-schema.
Case - Utdata	Dokumenterad process för klagomål och överklaganden.
Kort beskrivning	CAB måste utveckla och dokumentera en process för hantering av klagomål och överklaganden enligt EN ISO / IEC 17020: 2012 (7.5). Parter som vill representera en uppfattad systemfråga ska kunna kontakta respektive CAB med all nödvändig information.

UC CA12. CAB behandlar ett klagomål rörande ett IO-godkännande

Aktör	VM, TC, RA
Mål	CAB ska behandla klagomål och överklaganden rörande ett IO-godkännande. IO-godkännande ska återkallas eller bekräftas efter processresultatet. Godkännandedatabasen ska vara uppdaterad.
Case - Indata	Klagomål eller överklagande med nödvändig information enligt processen i UC CA11.
Case - Utdata	Avslag på klagomålet eller överklagandet. Eller Beslut om att återkalla ett IO-godkännande till följd av ett klagomål eller en överklagandeprocess: 1) Dokumenterad återkallelse av IO-godkännande och IO-godkännande klassificerad som återkallad i godkännandedatabasen. 2) IO - godkännande återkallas.
Kort beskrivning	CAB undersöker klagomålet eller överklagandet. Om skälen till klagomålet eller överklagandet inte kan bekräftas ska klagomålet eller överklagandet avslås. Om orsakerna bekräftas ska IO-godkännandet återkallas. I händelse av återkallande ska CAB: 1) informera IO: s juridiska ombud om att godkännandet ska återkallas, 2) informera respektive TC för att omedelbart dokumentera godkännandet som återkallats och återkalla alla digitala certifikat och auktorisationer från IO-anställda för respektive IO, 3) 3) informera alla CAB i sin medlemsstat om återkallelsen.

UC CA13. CAB behandlar ett klagomål angående en IO-anställds auktorisation

Aktör	VM, IO, TC, RA
Mål	CAB ska behandla klagomål och överklaganden rörande en IO-medarbetares auktorisation. IO-anställdas auktorisation ska återkallas eller bekräftas av TC efter processresultatet. Listan över återkallande av digitala certifikat och databasen för auktorisationer ska vara uppdaterad.
Case - Indata	Klagomål eller överklagande med nödvändig information enligt processen i UC CA11.
Case - Utdata	Avslag på klagomålet eller överklagandet. Eller Information om TC för att återkalla IO-anställdas auktorisation efter ett klagomål eller överklagandeprocess: 1) IO-anställdas digitala certifikat registrerat som ogiltigt. 2) IO-anställdas auktoriseringsstatus uppdaterad som ogiltig.
Kort beskrivning	CAB undersöker klagomålet eller överklagandet. Om skälen till klagomålet eller överklagandet inte kan bekräftas ska klagomålet eller överklagandet avslås. Om orsakerna är bekräftade ska IO: s medarbetartillstånd återkallas. CAB ska informera respektive TC för att omedelbart återkalla arbetstagarens digitala certifikat och medarbetarens auktorisation. CAB ska informera IO: s juridiska ombud om återkallelsen av IO-anställda.

UC CA14. CAB tillhandahåller statistik

Aktör	CAB
Mål	Övervakning av CAB.
Case - Indata	Resultat av godkännande, tillstånd och inspektioner på plats.
Case - Utdata	CAB ska tillhandahålla en rapport kvartalsvis under det första året av CAB-verksamhet och därefter årligen till systemägaren SERMI (publiceras på SERMI-webbplatsen)
Kort beskrivning	CAB analyserar resultaten av godkännandeprocessen och ger en rapport med: • Antal utredningar. • Kvot: godkännanden / ansökningar • Kvot: behörigheter / applikationer • Vanligaste (minst 3) skäl för att vägra godkännande • Vanligaste (minst 3) skäl för att vägra tillstånd • Antal och utfall av kontroller på plats under rapportperioden • Vanligaste (minst 3) orsaker till återkallande av IO-godkännande • Dessutom kan SERMI lägga till andra Key Performance Indicators (KPI)

6.3.3 Kriterier för IO-godkännande

CAB ska kontrollera följande för godkännande av IO: s juridiska representant eller under inspektion på plats under godkännandets giltighetsperiod.

1) Dokumenterat ägande av IO, namn på verkställande direktör och juridisk ombud.
2) Giltigt landsspecifikt identitetskort (t.ex. ID-kort / pass) för IO: s juridiska representant.
3) Listan som tillhandahålls av IO över anställda som bör auktoriseras. Kontrollen ska innehålla information om de anställdas ansvar och funktion.
4) Att IO har ansvarsförsäkring. Lägsta täckningsbelopp: 1 miljon euro för kroppsskada och 0,5 miljoner euro för skada på egendom.
5) Att IO inte är föremål för en tidigare återkallelse på grund av missbruk.
6) Bevis på verksamhet inom fordonsområdet (t.ex. medlemskap i en relevant förening, medlemskap i en nationell handelsorganisation).
7) Laglig affärsverksamhet enligt nationella definitioner.
8) IO-adress.
9) IO: s juridiska ombuds namn mot straffregister.
10) Förklaring undertecknad av IO: s juridiska ombud om att dataskyddsförordningen ska respekteras.

11) Förklaring undertecknad av IO: s juridiska ombud att överensstämmelse med de procedurkrav som anges i avsnitt 6.3.4 säkerställs för all verksamhet som rör fordonssäkerhet.

12) Åtagande att ge relevanta myndigheter, t.ex. polisen all information om en säkerhetsrelaterad operation på deras begäran.

13) Förpliktelse att informera CAB när företaget är upplöst eller upphör med handeln inom bilindustrin

14) Åtagande att omedelbart meddela alla ändringar av information om och tillstånd för IO-anställda (dvs hemvist, anställningsförhållande) till CAB.

6.3.4 Procedurkrav för säkerhetsrelaterad verksamhet

Allmänt beteende

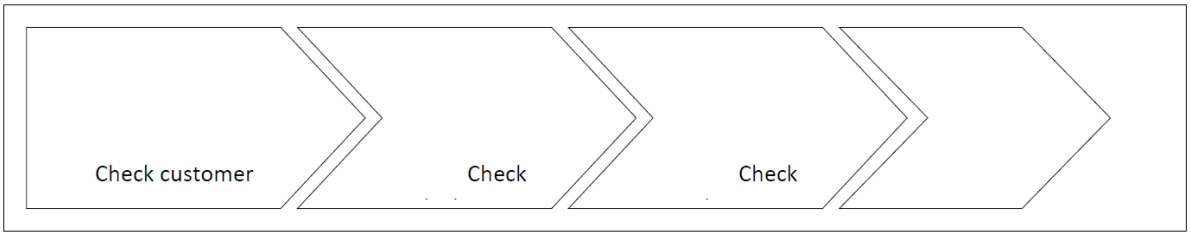
Endast IO-anställda i den godkända IO, som har godkänts framgångsrikt och har ett giltigt elektroniskt hårdvaruintyg (HW) utfärdat av motsvarande Trust Center, kommer att få tillgång till säkerhetsrelaterat RMI.

Den anställde tar personligt ansvar för korrekt användning av hårdvarucertifikatet och PIN-koden.

IO: erna och deras anställda ska följa procedurerna för att hantera slutanvändaranordningen (PC, bärbar dator, etc.) enligt ISO 18541-2 och i bilagan till IO-klientkrav som upprätthålls av SERMI.

Procedur för att utföra en säkerhetsrelaterad operation

Om en anställd utför en säkerhetsrelaterad mjukvaruuppdatering (t.ex. uppdatering eller utbyte av en elektronisk styrenhet (ECU)) eller behöver annan säkerhetsrelaterad reparations- och underhållsinformation för en fordonsdrift ska följande procedur följas.



Figur 4: Grundläggande beskrivning av proceduren för att utföra en säkerhetsrelaterad operation

Kontrollera kunden

IO-medarbetaren ska kontrollera kundens identitet som ska vara närvarande med fordonet. Möjliga identifieringskällor:

- Identitetskort, pass, körkort eller Medlemskort

Oavsett vilken mekanism som används ska det vara ansvaret att registrera identitetsinformationen på ett sätt som kan granskas.

Registreringsdokument för fordon	
Data (del I)	Fält (del I)
Efternamn eller företagsnamn	C.1.1
Andra namn eller initialer (i förekommande fall)	C.1.2
Adress i registreringsmedlemsstaten den dag då dokumentet utfärdas	C.1.3
Data (del II)	Fält (del II)
Efternamn eller företagsnamn	C.3.1 och C.6.1
Andra namn eller initialer (i förekommande fall)	C.3.2 och C.6.2
Adress i registreringsmedlemsstaten den dag då dokumentet utfärdas	C.3.3 och C.6.3

Figur 5: Fältreferens för kundkontroll från fordonets registreringsbevis

- Kundens efternamn och efternamn
- Identitetskortnummer eller nummer på vägkortets medlemskort

Om tillämpligt och om känt ska IO-medarbetaren notera följande uppgifter:

- Vagnparkhantering eller företagets hyrbil
- Kontaktnamn för respektive företag
- Adress till respektive företag
- Telefonnummer till respektive företag
- Förarens företagsidentifikation

Denna ytterligare information krävs under de omständigheter där kunden inte har fordonsregistreringsdokument, t.ex.

1) Fleet management

2) Hyrbilar

3) Lånprogram

Kontrollera fordonet

IO-anställda ska se till att fordonets identifikationsnummer (VIN) på fordonet är detsamma som VIN på registreringsdokumenten.

Registreringsdokument för fordon	
Data (del I)	Fält (del I)
Fordonets identifieringsnummer	E

Figur 6: Gemenskapskoder från registreringsdokumenten för fordonskontrollen

Kontrollera myndighet

Befogenheten att utföra arbete på fordonet ska fastställas och den mekanism som används ska vara granskbar och omfattas av nationell lagstiftning.

Kundens bemyndigande att tillåta reparationen ska kontrolleras med hjälp av ett autentiserat bemyndigandebrev för den begärda åtgärden från den registrerade ägaren eller ett motsvarande förfarande.

Om myndigheten inte upprättas genom en granskbar process ska bilen inte repareras förrän nödvändigt bevis har framställts.

Sluta bearbeta

Om det finns skäliga skäl för misstankar bör inte arbetstagaren gå vidare. Om möjligt och lämpligt bör situationen rapporteras till berörda myndigheter.

Utfärda reparationsorder

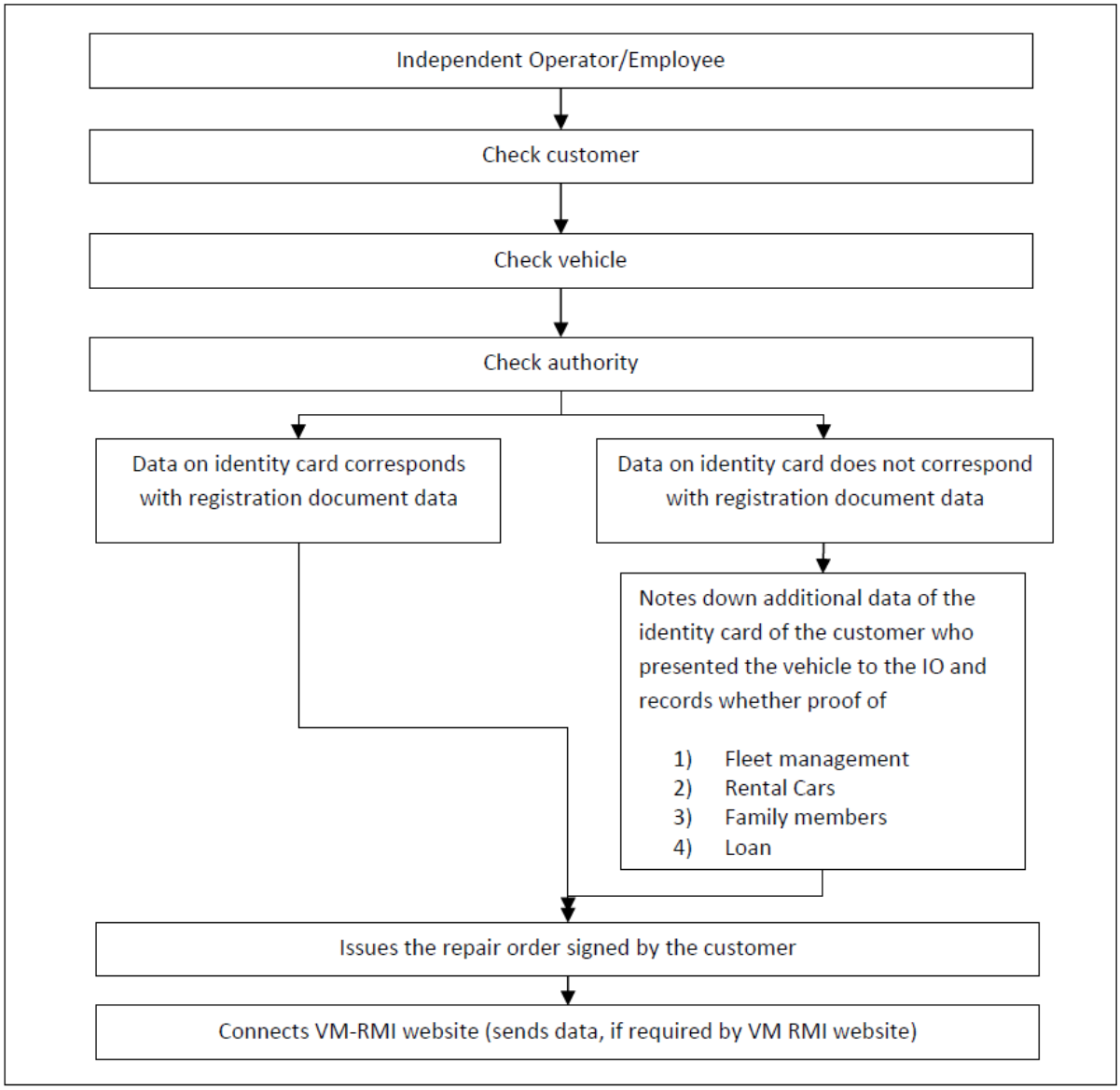
Nästa steg är att utfärda reparationsorder med hjälp av ett återförsäljarhanteringssystem (eller något liknande). Reparationsordern ska innehålla åtminstone data från figur 6 och all information som används för att identifiera kunden och deras auktoritet.

Registreringsdokument för fordon	
Data	Fält
Fordonets identifieringsnummer	A
Göra	D.1
Typ, variant, version	D.2

Figur 7: Gemenskapskoder från registreringsdokumenten för utfärdande av en reparationsorder

Det aktuella värdet på vägmätaren och anledningen till reparationen ska noteras och reparationsordern ska undertecknas av kunden (ägare och / eller den person som tar med fordonet till IO). Följande bild beskriver proceduren för IO och anställd.

Undertecknade reparationsorder måste hållas i minst 5 år av IO.



Figur 8: Procedurkrav för IO

6.3.5 Kriterier för IO anställdas auktorisation

CAB ska kontrollera följande för auktorisation för den anställde eller under inspektion på plats under godkännandets giltighetsperiod:

1) Att den anställde inte är föremål för ett tidigare återkallande på grund av missbruk.
2) Den anställdes hemadress.
3) Arbetstagarens namn mot kriminella register som utarbetats och presenterats av IO.
4) Anställning av respektive anställd hos IO.
5) Att den anställde har undertecknat ett avtal för att följa förfarandekraven specificeras i avsnitt 6.3.4.
6) Godkännande av IO där den anställde är godkänd.
7) Kopiera (båda sidor) av ett giltigt landsspecifikt identitetskort eller motsvarande (t.ex. ID kort / pass).

6.4 Specifikation av IO-rollen

IO-handelsföretaget ska lämna in en ansökan till CAB och begära godkännande för att bedriva säkerhetsrelaterat RMI.

6.4.1 Ansvar och krav

1) IO ska begära godkännandeinspektion från CAB.

2) IO ska registrera sig vid varje VM som han / hon vill göra affärer med.

3) IO ska informera CAB om ändringar av dess data och omständigheter (t.ex. adressändring).

4) IO ska informera CAB när dess verksamhet är upplöst.

5) IO ska kunna beställa alla delar som rör säkerhetssystem.

6) IO ska använda den säkra hårdvarutoken som tillhandahålls av TC.

7) IO ska ha lämpliga register för alla säkerhetsrelaterade RMI-transaktioner och operationer på granskningsbara sätt.

8) IO ska informera CAB i händelse av att en auktoriserad anställd avslutar sin anställning.

9) IO ska rapportera alla misstankar om en brottslig avsikt eller handling i samband med att säkra RMI till berörda myndigheter om det är lämpligt.

10) IO ska se till att de anställda är korrekt auktoriserade och att de anställda endast använder sina egna certifikat på granskningsbara sätt.

11) IO ska se till att den anställde använder säkerhetsrelaterade data i enlighet med de procedurkrav som anges i avsnitt 6.3.4 och i synnerhet föra register i granskningsbara medel för fordon, kund, myndighet, ägare och arbetsorderregister.

12) IO ska se till att dataskyddsföreskrifterna respekteras av alla anställda.

13) IO ska också se till att alla avgifter relaterade till arbetstagarens auktorisation betalas.

14) IO ska se till att alla auktoriserade anställda är lämpligt utbildade för underhåll, omprogrammering och reparation av säkerhets- och säkerhetsfunktioner.

15) IO ska begära en inspektion på plats av CAB under sex månader före godkännandets giltighetstid.

6.4.2 Funktionskrav: användningsfall

UC IO1. IO: s juridiska ombud begär godkännande

Aktör	IO juridisk representant.
Mål	IO: s juridiska representant ska uppfylla alla krav som ställts av SERMI, så att den godkända IO-juridiska representanten kan arbeta med säkerhetsrelaterat RMI.
Case - Indata	Alla nödvändiga dokument och ansökningsformulär (enligt CAB) i granskningsbart format.
Case - Utdata	Godkännande av IO: s juridiska ombud Eller icke godkännande av IO: s juridiska ombud
Kort beskrivning	IO: s juridiska representant ska använda NAB: s webbplats för att få en lista över ackrediterade CAB. IO: s juridiska ombud ska kontakta respektive CAB. IO: s juridiska ombud ska erhålla ansökningsformuläret från CAB. IO: s juridiska ombud ska fylla i ansökningsformuläret och skicka ansökningsblanketten och alla nödvändiga handlingar till CAB på granskningsbar väg. När CAB har inspekterat IO: s juridiska representant ska CAB registrera godkännandeinspektionsresultatet i sin databas för att CAB i framtiden ska kunna kontrollera om en IO-ansökan tidigare har inspekterats med ett negativt resultat. Varje anställd hos en IO-företrädare ska vara registrerad vid samma CAB. Icke godkännande av IO kommer att meddelas av CAB till alla andra CAB inom deras respektive NAB: s jurisdiktion.

UC IO2. IO-registrering på VM
(se EN / ISO 18541-1, användningsfallskluster 1)

UC IO3. IO- Upphörande av handel

Aktör	IO
Mål	Godkännandedatabasen uppdateras av CAB.
Case - Indata	Informationen om IO och dess upphörande av handeln eller IO informerar CAB om avveckling av verksamheten.
Case - Utdata	En uppdatering av godkännandedatabasen tillsammans med återkallandet av alla relaterade certifikat och auktorisationer som utfärdats till den IO.
Kort beskrivning	CAB ska få information om IO-handelsstopp. CAB ska informera TC för att återkalla alla certifikat och auktorisationer som utfärdats till den IO.

UC IO4. Beställning av delar

Aktör	IO
Mål	Leverera en beställd del till IO.
Case - Indata	Autentisering av IO-anställd. Säkerhetsrelaterad reservdelsbeställning.
Case - Utdata	Säkerhetsrelaterad del.
Kort beskrivning	VM ska erbjuda säkerhetsrelaterade beställningsanordningar för delar för auktoriserade IO-anställda. Tillverkare ska antingen erbjuda en onlinebeställningsanläggning för säkerhetsrelaterade delar med hjälp av det digitala certifikatet för att bekräfta identiteten på den person som kräver delen. Alternativt kan de kräva att säkerhetsrelaterade delar erhålls från auktoriserade återförsäljare där för närvarande etablerade autentiseringsförfaranden finns. Säkerhetsdelar ska levereras av VM eller deras ombud / auktoriserade återförsäljare i god tid till IO

UC IO5. IO tar emot säker hårdvaru-sign

Aktör	CAB
Mål	IOs juridiska representant får säker hårdvaru.sign med ett digitalt certifikat.
Case - Indata	Säker hårdvaru-sign med ett digitalt certifikat vidarebefordrat av CAB.
Case - Utdata	Säker hårdvarut-sign med ett digitalt certifikat mottaget av IO: s juridiska representant.
Kort beskrivning	Den juridiska representanten för IO ska få ett elektroniskt HW-certifikat från TC. Den juridiska representanten för IO ska leverera det elektroniska HW-certifikatet till respektive IO-anställd (se UC EM6).

UC IO6. IO-registreringskrav

Aktör	IO juridisk representant
Mål	Granskningsbar registrering av transaktioner som hålls av IO.
Case - Indata	Dokument / information från reparationsorder.
Case - Utdata	Granskning (ådit) och detaljer om reparationsjobbet.
Kort beskrivning	IO ska lagra data som krävs enligt lag, dvs. återförsäljarhanteringssystem (DMS) för revision / juridiska ändamål. Nationell lagstiftning måste beaktas. Innan utfärdandet av en reparationsorder ska IO se till att följande information samlas in: 1) Identifiering av kunden 2) Identifiering av fordonet (Fordon på plats) 3) Bevis på kundens befogenhet att begära arbetet till fordonet. Se procedurkrav 6.3.4.

UC IO7. Avslutande av anställning av en IO-anställd vid en IO

Aktör	IO juridisk representant
Mål	Godkännande- / auktoriseringsdata på CAB hålls uppdaterade
Case - Indata	Information om avslut på kontrakt med IO-anställd
Case - Utdata	Uppdaterad auktoriseringsdatabas och begäran till TC om att återkalla respektive digitalt certifikat.
Kort beskrivning	Den juridiska representanten för IO ska informera CAB om anställningsbytet inom tre arbetsdagar. CAB ska informera TC för att uppdatera auktoriseringsdatabasen och återkalla respektive digitala certifikat. IO ska informeras om ändringarna.

6.5 Specifikation av IO-medarbetarrollen

IO-anställd för den godkända IO som är auktoriserad som enskild person att bedriva säkerhet och som förses med nödvändig maskinvara och elektroniskt maskinvarudigitalcertifikat får tillgång till VM RMI-systemet för att få säkerhetsrelaterad information och utför säkerhetsrelaterade reparations- och underhållsaktiviteter.

6.5.1 Ansvar och krav

1) IO-medarbetaren ska begära tillstånd. Detta ska vara i samband med IO.

2) IO-medarbetaren ska registrera sig på VM RMI-systemet.

3) IO-medarbetaren ska få åtkomst till säker RMI enligt ISO 18541.

4) IO-medarbetaren ska ladda ner programvara (drivrutin för maskinvara för att läsa den säkra programvarutoken med det digitala certifikatet) eller ges åtkomst till identitetsprogramvaran på annat sätt av hårdvaruleverantören, dvs. Trust Center.

5) IO-medarbetaren ska få en PIN-kod från TC.

6) IO-medarbetaren ska få ett elektroniskt hårdvaruintyg från IO: s juridiska representant.

7) IO-medarbetaren får maskinvara för att läsa elektroniskt maskinvaruintyg från IO: s juridiska representant.

8) IO-medarbetaren ska erkänna att alla register över säkerhetsrelaterade RMI som laddats ner från VM RMI-systemet endast får lagras så länge det är nödvändigt att utföra den operation för vilken informationen behövdes. Efter operationen måste uppgifterna definitivt förstöras.

9) IO-medarbetaren ska informera sin IO-arbetsgivare om det digitala certifikatet inte längre krävs.

10) IO-medarbetaren ska rapportera, enligt sitt / hans IO-avtal, till polisen om alla åtgärder som rör RMI som är misstänkta och kan vara kriminella.

11) IO-medarbetaren ska förvara den säkra hårdvaru-sign med det digitala certifikatet och PIN-koden på en plats som är skyddad mot stöld och inte lämna den lätt åtkomlig för en obehörig användare.

12) IO-medarbetaren får inte skicka den strikt personliga säkra programvaru-sign med det digitala certifikatet och / eller PIN-koden till någon tredje part. PIN-koden är strikt personlig och ska under inga omständigheter kommuniceras till tredje part.

13) Den anställde ansvarar för att korrekt använda det personliga säkra programvaru-sign och PIN-koden.

14) Den anställde ska informera sin IO om eventuella förändringar av omständigheter som har att göra med auktorisation under auktoritetsperiodens giltighetstid (dvs. hemvist, anställningsförhållande).

15) Den anställde ska informera IO och TC om eventuell förlust eller missbruk av den säkra hårdvaru-sign med det digitala certifikatet inom 24 timmar på granskbar väg.

16) IO-medarbetaren ansvarar för att tillhandahålla all auktoriseringsrelevant information och alla efterföljande ändringar (dvs. hemvist, anställningsförhållande) omedelbart till CAB.

6.5.2 Funktionskrav: användningsfall

UC EM1. IO-anställd begär tillstånd

Aktör	IO - Anställd
Mål	IO-anställd får tillstånd att arbeta med säkerhetsrelaterat RMI.
Case - Indata	IO-anställd uppfyller alla krav som anges av SERMI. IO-anställd fyller i ansökningsformuläret från CAB.
Case - Utdata	Auktorisering av en IO-anställd, så att IO-medarbetaren kan ta emot det digitala certifikatet för åtkomst till säkerhetsrelaterat RMI.
Kort beskrivning	IO-medarbetaren kommer att få ansökningsformuläret från CAB om IO: s juridiska representant har begärt tillstånd från respektive anställd. IO-medarbetaren fyller i ansökningsformuläret och skickar ansökningsblanketten och alla nödvändiga dokument till CAB på granskningsbar väg. CAB ska kommunicera det positiva inspektionsresultatet till TC för att skapa en auktoriseringspost och utfärda ett digitalt certifikat för denna IO-anställd. CAB ska också hålla koll på IO-anställdes avslag om inspektionen inte lyckas.

UC EM2. IO-anställdes registrering på en VM
(se EN / ISO 18541-1 användningsfallskluster 1)

UC EM3. Anställdas tillgång till säkerhetsrelaterat RMI
(se EN / ISO 18541 alla delar)

UC EM4. IO anställd nedladdning av programvara (drivrutin för maskinvara för att läsa elektroniskt HW-certifikat)

Aktör	IO - Anställd
Mål	IO-anställda laddar ner programvaran / drivrutinen så att han / hon kan använda det elektroniska HW-certifikatet på den persondator som beskrivs i ISO 18541-2.
Case - Indata	IO-anställds begäran till TC.
Case - Utdata	Drivrutin-programvara
Kort beskrivning	Den anställde ska endast ladda ner och installera TC-programvaran och använda hårdvaran från respektive TC.

UC EM5. Mottagning av PIN-koden från CAB

Aktör	CAB
Mål	Tillhandahålla IO-anställd PIN-koden för den säkra hårdvarutoken med det digitala certifikatet.
Case - Indata	PIN från TC.
Case - Utdata	PIN-brev levererat till IO-anställd
Kort beskrivning	CAB förbereder en PIN-bokstav med PIN-koden som tillhandahålls av TC för denna identitet och skickar den till IO-anställdas hemadress på granskningsbar väg.

UC EM6. IO-anställd får det digitala certifikatet från IOs juridiska representant

Aktör	IO juridisk representant, IO anställd
Mål	Leverera det elektroniska HW-certifikatet till IO-medarbetaren.
Case - Indata	Elektroniskt HW-certifikat.
Case - Utdata	IO-anställd får det elektroniska HW-intyget från IO: s juridiska representant.
Kort beskrivning	IO-medarbetaren ska få det elektroniska HW-certifikatet från IO: s juridiska ombud med motsvarande identitet.

6.6 Specifikation av rollen Trust Center

TC ska skapa och skicka elektroniska hårdvarucertifikat till IO via respektive CAB när IO: s juridiska representant har godkänts och IO-anställda som begär ett certifikat har godkänts. TC ska upprätthålla en databas med giltighet av auktorisation för IO-anställda. TC ska tillhandahålla ett gränssnitt för användning av VM för att verifiera certifikatens status (via OCSP) och statusen för behörigheter för IO-anställda.

6.6.1 Ansvar och krav

1) TC ska skapa och digitala certifikat och leverera dem till IO-anställda via CAB.

2) TC ska ha en databas (OCSP) med återkallande av digitala certifikat.

3) TC ska upprätthålla en databas med anställdas auktorisationer.

4) TC ska avbryta digitala certifikat när så är lämpligt.

5) TC ska tillfälligt avbryta IO-medarbetarbehörigheter där så är lämpligt.

6) TC ska tillhandahålla programvaran för att använda de digitala certifikaten.

7) Valfritt: TC ska tillhandahålla en miljö för att testa beredskapen för ett certifikat och den programvara som tillhandahålls av TC.

8) TC ska tillhandahålla ett gränssnitt med VM i enlighet med de tekniska implementeringsriktlinjerna från Forum Secure RMI.

9) TC ska förse "testanvändare" med testcertifikat för att validera kommunikationen mellan VM och TC för att begära status för auktorisering och autentisering av IO: er och anställda.

10) TC ska ladda ner testprotokollen från SERMI-webbplatsen (t.ex. OCSP & SOAP).

11) TC ska fungera i enlighet med funktionskraven i avsnitt 6.6.2 och tekniska krav i kapitel 7 i denna rapport.

12) TC ska fungera dygnet runt.

13) TC ska stödja följande tekniker: CSP / PKCS # 11, OCSP, SOAP.

14) TC ska kunna använda "kvalificerad elektronisk signatur" i enlighet med direktiv 1999/93 / EG.

15) TC ska uppfylla standarden ETSI TS 102 042.

16) En TC ska etablera en affärsrelation inklusive nödvändigt gränssnitt med ett ackrediterat CAB.

17) TC ska tillämpa de förfaranden och specifikationer som definieras i SERMI: s riktlinjer för teknisk implementering.

6.6.2 Funktionskrav: användningsfall

UC TC1. Trust Center skapar och levererar certifikat

Aktör	CAB
Mål	CAB tar emot certifikat och PIN-kod för distribution till IO-anställda
Case - Indata	Begäran om skapande av ett digitalt certifikat.
Case - Utdata	Digitalt certifikat och PIN.
Kort beskrivning	CAB ska kontakta TC (se användningsfall CA11 för procedur). TC ska skapa det digitala certifikatet och tillhandahålla det till CAB för distribution till IO-medarbetaren genom att använda följande procedur: 1) TC ska skicka det personliga digitala certifikatet till CAB på granskningsbara sätt. 2) 2) PIN-koden ska skickas separat på granskningsbara sätt separat till CAB.

UC TC2. Trust Center bedömer giltigheten av det digitala certifikatet

Aktör	VM
Mål	Validering av status för ett digitalt certifikat.
Case - Indata	Serienummer för digitalt certifikat.
Case - Utdata	Status som tillhandahålls av TC är följande: 0 - Avstängd 1 - Ok 2 - Återkallad 3 – Okänd
Kort beskrivning	VM ska be om status för anställdas digitala certifikat för autentisering med hjälp av den kommunikation som definieras i OCSP-standarden. TC ska svara angående OCSP-svararens status. TC upprätthåller för detta ändamål en återkallningsdatabas enligt OCSP-standarden.

UC TC3. Trust Center tillhandahållande av IO-auktoriseringsstatus

Aktör	VM
Mål	Validering av tillståndsstatus med SOAP.
Case - Indata	Digitalt certifikats serienummer och attribut.
Case - Utdata	Status svarad av TC är följande: Giltighet IOEUID IOUID KABUID
Kort beskrivning	VM ska be om tillståndsstatus för IO-anställda. TC ska svara om tillståndsstatusen.

UC TC4. Trust Center upphävande av utfärdade certifikat

Aktör	VM, IO, CAB, RA
Mål	Avstängning av digitalt certifikat för att förhindra framtida missbruk av en certifikatägare vid upptäckt missbruk.
Case - Indata	Utlöses av en lämplig anställd hos aktören med t.ex. serienummer eller på annat sätt för att identifiera certifikatet.
Case - Utdata	Avstängning av certifikat, status OCSP uppdaterad. TC skickar information till CAB. Information till IO-anställd om orsaken till det digitala certifikatets upphävande.
Kort beskrivning	Lämplig anställd hos respektive deltagare, t.ex. en anställd på en CAB som är ansvarig för avstängningen skickar ett meddelande till TC på granskningsbar väg. Meddelandet ska åtminstone innehålla: - Brevhuvud för respektive deltagare. - Serienummer eller annat sätt att identifiera certifikatet. - Transaktionsnummer från respektive deltagare, vid behov. Avstängningen ska behandlas omedelbart efter mottagandet av begäran om avstängning. TC ska kontrollera meddelandets ursprung och ha bekräftat meddelandets äkthet: - TC ska avbryta det digitala certifikatet (uppdaterad OCSP). - TC ska informera CAB om avstängningen för att inleda klagomål och överklagande i skriftlig eller elektronisk form.

UC TC5. Trust Center upphävande av godkännande av en IO

Aktör	VM, CAB, RA
Mål	Avstängning av auktorisationen för alla anställda för en specifik IO (plus alla behörigheter som tillhör den IO) för att förhindra framtida missbruk av anställda av en IO vid upptäckta missbruk.
Case - Indata	Begärs av arbetstagarrepresentant för en auktoriserad aktör (dvs. med ett lämpligt certifikat) t.ex. en anställd hos en CAB som är ansvarig för avstängningen med IO: s unika identifierare eller på annat sätt för att identifiera IO.
Case - Utdata	Avstängda auktorisationer har uppdaterats. dvs auktoriseringsdatabasen uppdateras. TC skickar information till CAB
Kort beskrivning	Autentiserad anställd från respektive skådespelare skickar ett meddelande till TC på granskningsbar väg. Meddelandet ska åtminstone innehålla: - Brevhuvud för respektive deltagare. - IO unik identifierare eller annat sätt att identifiera IO. - Transaktionsnummer från respektive deltagare, vid behov. Avstängningen ska behandlas omedelbart efter mottagandet av begäran om avstängning. TC ska kontrollera meddelandets ursprung. TC ska avbryta alla behörigheter som tillhör IO. TC ska informera CAB om avstängningen för att inleda klagomål och överklagande i skriftlig eller elektronisk form.

UC TC6. Trust Centers avbryter bemyndigandet från IO-anställda

Aktör	VM, IO, CAB, relevanta myndigheter
Mål	Avstängning av auktorisation för en IO-anställd för att förhindra framtida missbruk vid upptäckt missbruk.
Case - Indata	Begärs av en juridisk representant för en autentiserad deltagare.
Case - Utdata	Avstängning av auktorisation, uppdaterad auktoriseringsdatabas. Avstängningsmeddelande till CAB. Information till IO-anställd om orsaken till tillståndsavstängningen.
Kort beskrivning	Autentiserad anställd hos respektive deltagare, t.ex. en anställd på ett CAB som ansvarar för avstängningen ska skicka information till TC (med en vanlig metod). Informationen ska åtminstone innehålla: - Brevhuvud för respektive deltagare. - IO unik identifierare. - Unik identifierare för IO-anställd. - Transaktionsnummer från respektive aktör, vid behov. Avstängningen ska behandlas omedelbart efter mottagandet av begäran om avstängning. TC ska kontrollera informationens ursprung. TC ska avbryta ett tillstånd som tillhör en anställd. TC ska informera CAB om avstängningen för att inleda klagomål och överklagandeförfarandet i skriftlig eller elektronisk form.

UC TC7. Trust Centers återkallar IO-godkännande

Aktör	CAB
Mål	Godkännandedatabasen hålls uppdaterad.
Case - Indata	CAB meddelar beslutet att återkalla IO-godkännandet.
Case - Utdata	IO-godkännande klassificerat som återkallat i databasen.
Kort beskrivning	TC uppdaterar godkännandedatabasen omedelbart efter mottagandet av CAB-meddelandet om beslutet att återkalla en viss IO. IO-godkännandet klassificeras som återkallande. De digitala certifikaten och behörigheterna för alla IO-anställda vid denna IO klassificeras omedelbart som återkallade i motsvarande databaser.

UC TC8. Trust Centers återkallar IO-anställdas auktorisation

Aktör	CAB
Mål	Databaser för digitalt certifikat och auktorisering hålls uppdaterade.
Case - Indata	CAB meddelar beslutet att återkalla IO-auktorisationen.
Case - Utdata	IO: s digitala certifikat klassificerat som återkallat. IO-anställdas auktorisation klassificerad som återkallad.
Kort beskrivning	TC kommer att uppdatera det digitala certifikatet och behörighetsdatabaserna omedelbart efter mottagandet av CAB-meddelandet om beslutet att återkalla en viss IO-anställd. Det digitala certifikatet och bemyndigandet för IO-anställda vid denna IO klassificeras omedelbart som återkallade i motsvarande databaser.

UC TC8. Trust Center tillhandahållande av programvaran för att hantera ett certifikat (CSP och PKCS # 11)

Aktör	IO, IO-anställd (valfri VM)
Mål	IO-anställd är operativ och har tillgång till säker RMI.
Case - Indata	TC-webbplats öppnas för att ladda ner det nödvändiga programvarupaketet och information om hur du installerar programvaran.
Case - Utdata	Anställd ska vara i en operativ miljö för att hantera det elektroniska HW-certifikatet.
Kort beskrivning	TC ska tillhandahålla all nödvändig programvara för att använda det elektroniska HW-certifikatet samt information om minimikrav på systemet. Programvaran ska innehålla en kryptografisk tjänsteleverantör (CSP) för Windows-operativsystem (t.ex. Windows 7, Windows 8.1 och Windows 10) och en Public Key Cryptography Standard # 11 (PKCS # 11) -modul för Windows.

UC TC9. Trust Center tillhandahåller en miljö för att testa beredskapen för ett certifikat och den TC-tillhandahållna programvaran

Aktör	IO-anställd
Mål	Bekräftelse till IO-medarbetaren att det elektroniska HW-certifikatet fungerar.
Case - Indata	IO-anställdes elektroniska HW-certifikat + PIN och programvara på klientdator.
Case - Utdata	Testa ok / inte ok. Meddelande med felinformation om inte ok.
Kort beskrivning	Den anställde ska ansluta till TC: s webbplats. IO-medarbetaren ska logga in på TC-testwebbplatsen med sitt elektroniska HW-certifikat. IO-medarbetaren ska se resultatet av testet (ok / inte ok.) TC ska logga in åtgärder för ytterligare supportprocesser (t.ex. VM).

UC TC10. TC tillhandahåller ett gränssnitt angående specifikationerna för användningsfall CA1

Aktör	TC
Mål	TC-stöd för standardkommunikationsgränssnitt mellan TC och CAB (webbtjänst).
Case - Indata	Information och kända standarder för att utveckla ett kommunikationsgränssnitt (webbtjänst).
Case - Utdata	Kommunikationsgränssnitt mellan TC och CAB.
Kort beskrivning	TC ska utveckla och driva ett standardkommunikationsgränssnitt för CAB. CAB ska använda detta standardkommunikationsgränssnitt t.ex. för att beställa det digitala certifikatet.

UC TC11. TC ger testanvändare testcertifikat för att validera kommunikationen (OCSP & SOAP)

Aktör	VM
Mål	Den funktionella kommunikationen mellan en VM och en TC.
Case - Indata	Begäran till TC-gränssnittet.
Case - Utdata	Testdata: testanvändare, testcertifikat, innehåll för testautorisationsdatabas.
Kort beskrivning	VM-begäran om testdata på alla lämpliga språk för alla lämpliga marknader. TC ska skicka information (testanvändare / testcertifikat) som täcker alla möjliga testresultat till VM.

6.7 Specifikation av VM-roll

Fordonstillverkarens roll är att ge tillgång till säkerhetsrelaterad reparations- och underhållsinformation till alla godkända IO och auktoriserade IO-anställda. Virtuella maskiner ska kommunicera med Trust Center för att verifiera auktoriserings- och autentiseringsstatus för den IO-anställde som söker åtkomst.

6.7.1 Ansvar och krav

1) Fordonstillverkare ska inleda en undersökning av ett IO-godkännande om så är lämpligt.

2) Fordonstillverkare ska inleda en utredning av en anställds auktorisation om så är lämpligt.

3) Fordonstillverkare ska blockera en IO om så är lämpligt.

4) Fordonstillverkare ska blockera en IO-anställds tillgång till säker RMI om så är lämpligt.

5) Fordonstillverkaren ska begära upphävande av IO-godkännandet vid misstänkt missbruk. Alla auktorisationer för alla anställda som tillhör denna IO ska avbrytas vid behov.

6) Fordonstillverkaren ska begära avstängning av IO-anställningstillståndet vid misstänkt missbruk.

7) Fordonstillverkare ska identifiera en juridisk representant som är behörig att begära att ett IO-anställningstillstånd upphävs.

8) Fordonstillverkare får kontrollera giltigheten för en IO-anställdas digitala certifikat.

9) Fordonstillverkare får kontrollera en anställds auktorisationsstatus.

10) Fordonstillverkare ska ladda ner den tekniska specifikationen från SERMI-webbplatsen.

11) Fordonstillverkare ska tillhandahålla ett granskningsspår till berörda myndigheter.

12 VM måste stödja de överenskomna teknikerna i denna rapport (t.ex. OCSP, SOAP, PKCS # 11).

6.7.2 Funktionskrav: användningsfall

UC VM1. Undersökning av ett IO-godkännande

Aktör	VM
Mål	Att undersöka om ett befintligt godkännande ska förbli giltigt.
Case - Indata	VM märker eventuellt missbruk / indikation på missbruk.
Case - Utdata	Eventuellt missbruk eller indikation på missbruk bekräftas eller avvisas.
Kort beskrivning	Om VM märker missbruk ska den virtuella personen rapportera denna indikation på missbruk av en IO till CAB (under normal kontorstid) och blockera IO-anställda internt. VM kan starta klagomålsprocessen genom att informera respektive CAB. VM är fri att meddela polisen, om tillämpligt.

UC VM2. Undersökning av arbetstagarbehörighet

Aktör	VM
Mål	Att undersöka om ett befintligt godkännande ska förbli giltigt.
Case - Indata	VM märker eventuellt missbruk / indikation på missbruk.
Case - Utdata	Eventuellt missbruk eller indikation på missbruk bekräftas eller avvisas.
Kort beskrivning	Om VM märker missbruk ska den VM rapportera dessa indikationer på missbruk till CAB (vid normal kontorstid) och blockera IO-medarbetaren internt.

	VM kan starta klagomålsprocessen genom att informera respektive CAB. VM är gratis att meddela polisen, om tillämpligt.

UC VM3. VM blockerar IO

Aktör	VM
Mål	IO (och alla anslutna IO-anställda) nekas åtkomst till säkerhetsrelaterad information.
Case - Indata	VM registrerar felaktigt beteende för IO angående villkoren.
Case - Utdata	Tillgång till säkerhetsinformation blockerad för IO (och alla IO-anställda).
Kort beskrivning	Den VM ska blockera IO-åtkomsten internt. VM ska använda samma kriterier för att blockera IO som han använder för att starta motsvarande åtgärder i sin egen organisation. VM kan be om upphävande av IO-godkännande och starta klagomålsprocessen genom att informera respektive CAB.

UC VM4. VM blockerar IO-anställd

Aktör	VM
Mål	VM ska ha möjlighet att blockera en IO-anställd från åtkomst till säkerhetsrelaterad RMI.
Case - Indata	VM registrerar anledning att blockera IO-anställd.
Case - Utdata	Tillgång till säkerhetsinformation blockerad för IO-medarbetaren.
Kort beskrivning	Den VM ska blockera den anställdes åtkomst internt. Det digitala certifikatet för IO-medarbetaren som blockeras av VM förblir giltigt. VM ska använda samma kriterier för att blockera IO-anställda som han använder för att starta motsvarande åtgärder i sin egen organisation. Den VM kan begära avstängning av IO-medarbetarbehörighet och starta klagomålsprocessen genom att informera respektive CAB.

UC VM5. VM kontrollerar auktoriseringsstatus för en anställd

Aktör	VM
Mål	VM ska kontrollera auktoriseringsstatusen när den anställde använder certifikatet för autentisering för att komma åt säkerhetsrelaterat RMI.
Case - Indata	Innehållsinformation för den anställdes elektroniska HW-certifikat.
Case - Utdata	Auktoriseringsstatus
Kort beskrivning	Den VM ska kontrollera certifikatets giltighet (TC, OCSP.) Den VM ska kontrollera om den anställde är blockerad (intern intern). Den VM ska kontrollera giltigheten för medarbetarbehörigheten: - VM ska kontakta TC genom att använda innehållsinformationen i anställdes elektroniska HW-certifikat. - TC ska svara med aktuell autentiseringsstatus.

UC VM6. VM-nedladdning av implementeringsguiden från SERMI-webbplatsen (för närvarande OCSP & SOAP)

Aktör	VM
Mål	Överensstämmande check IO anställdes elektroniska HW-certifikat och auktorisering
Case - Indata	Begäran om implementeringsguide.
Case - Utdata	Nedladdad implementeringsguide.
Kort beskrivning	Nedladdning av implementeringsguiden från SERMI-webbplatsen. VM ska kontrollera IO-anställdas elektroniska HW-certifikat och auktorisering genom att använda implementeringsguiden (OCSP, SOAP).

UC VM7. VM levererar information till lokala myndigheter

Aktör	VM
Mål	Kunden kontaktar lokala myndigheter.
Case - Indata	Förfrågan från relevanta myndigheter via manuell process (ingen ytterligare IT-tjänst krävs).
Case - Utdata	Information om fordonet (t.ex. historik över åtgärder som utförts på ett specifikt VIN).
Kort beskrivning	Kunden rapporterar brott / ger VIN eller transaktionsinformation. En relevant myndighet, som t.ex. polisen kontaktar en specifik fordonstillverkare med en förfrågan angående ett specifikt VIN. VM, IO returnerar information om granskningsspår till relevant myndighet. Om det stulna fordonet återställs informerar RA VM och fordonets status återställs till det normala (granskningsspåret innehåller information om händelse).

6.7.3 Procedurkrav för VM

Innan begäran om säker RMI av en IO-anställd besvaras av VM ska den VM uppfylla följande procedurkrav:

- Procedurkrav för stulna fordon
- Förfarandekrav för "Audit trail"

Stulna fordon

VM ska hålla ett register över fordon av sina märken som rapporterats stulna av myndigheter.

VM ska vidta lämpliga åtgärder för ett rapporterat stulet fordon i enlighet med lokal lag: t.ex. kommunicera till myndigheter, neka reparation, reparera och rapportera till myndigheter.

Verifieringskedja

Det är viktigt att spåra och åtgärda fel eller missbruk av systemet i händelse av ett stulet fordon med hjälp av information som tillhandahålls till en oberoende operatör (IO).

Granskningssystemet måste tillhandahålla tydlig spårbarhet och ansvarsskyldighet som gör det möjligt för berörda myndigheter att spåra uppgifterna som tillhandahålls av fordonstillverkaren (VM) till IO-medarbetaren som använder den för det senare stulna fordonet.

Fordonstillverkaren bör utan onödigt dröjsmål tillhandahålla tillgängliga uppgifter på begäran av berörda myndigheter inom arbetsdagar. Data tillgänglig som visar när en IO besökte VM-RMI-webbplatsen. Detta krav ersätter inte på något sätt befintliga processer och procedurer som för närvarande överenskommits mellan VM och relevanta myndigheter.

Följande information för varje åtkomst till säkerhetsrelaterad reparations- och underhållsinformation ska lagras av respektive fordonstillverkare.

- Fordonets identifieringsnummer (VIN)
- Datum för transaktionen
- Typ av information
- Certifikatinformation som kan identifiera certifikatägaren.
- Fordonsregistreringsnummer (om möjligt)
- Typvariant, version av respektive fordon (om möjligt)

VM ska lagra dessa data under en tidsperiod på 5 år.

Relevanta myndigheter t.ex. polisen ska ha tillgång till denna information genom att kontakta respektive fordonstillverkare.

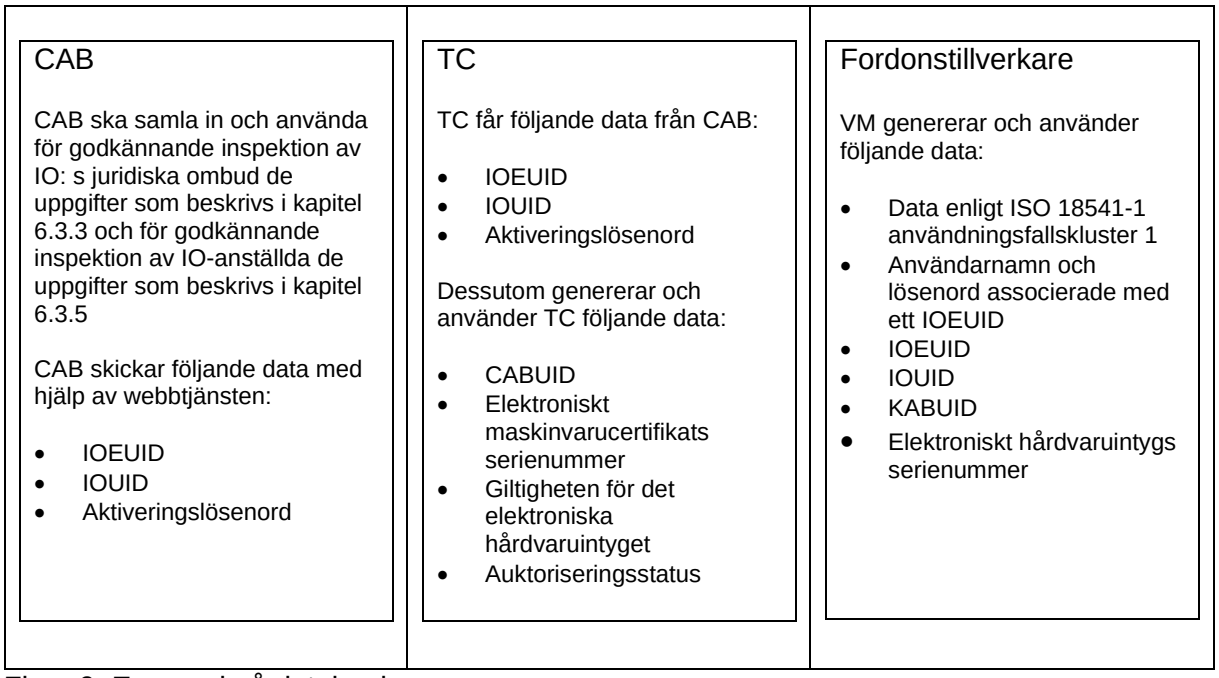
7 Tekniska krav

7.1 Säkra kommunikationskrav

All digital kommunikation eller överföring av identifierings-, godkännande- och auktoriseringsdata mellan CAB, TC och VM ska ske på ett säkert sätt, dvs med användning av https-ssl / tls och ömsesidig autentisering baserad på X.509-certifikat.

7.2 Beskrivning av datahantering

I SERMI-schemat samlar endast CAB in och använder personlig information: Följande diagram beskriver inte en databasimplementeringsmodell men definierar en minimal uppsättning attribut som måste lagras i varje enhetsinformationssystem för att kunna implementera definierade processer och användningsfall. Schema SERMI Sida 53



Figur 9: Exempel på datalagring

Attributbeskrivning

1) IO-anställd unik identifierare (IOEUID): Strängen som genereras av CAB som strikt identifierar IO-anställd.
2) IO unik identifierare (IOUID): Det värde som genereras av CAB och som strikt identifierar IO som en juridisk enhet.
3) CAB unik identifierare (UID): Det värde som genereras av Trust Center som strikt identifierar CAB.
4) Serienummer: Innehåller X509-certifikatets serienummer, vilket är unikt för varje certifikat och genereras automatiskt under certifikatutfärdandet.

Auktorisation X / Status Auktorisering X: Beskriv auktorisation (er) och motsvarande status för en användare.

7.3 Certifikatdesign

X509.V3-certifikatstandarden (RFC 5280) definierar en lista över vanliga fält och värden som ska fyllas i ett elektroniskt certifikat.

Det digitala certifikatet ska uppfylla BSI: s säkerhetskrav (http://www.bsi.de) angående nyckellängd och kryptografialgoritmer. Tidpunkten för att tillämpa BSI-kraven måste fastställas av Forum Secure RMI.

När man ansluter till en server med ett digitalt certifikat kontrollerar servern ett standardfält med namnet 'Subject DN' som gör det möjligt att göra en länk till identiteten för IO i det interna VM-systemet.

Följande bild visar ett utdrag av innehållsfält som krävs för identifiering av ett VM-system. Den fullständiga x509.V3-certifikatstrukturen som definieras i RFC 5280 visas inte här.

Fält	Värde	Kommentarer
Serienummer	XXX	Certifikatets serienummer.
Emittent	XXX	TC: s namn.
Giltighet	X år (från / till dags dato)	Certifikatets livslängd från certifikatutfärdandet till dess att giltigheten upphör.
Ämne DN	IOEUID = <UserUniqueIdentifier>, IOUID = <IOUniqueIdentifier>, CABUID = <CABUniqueIdentifier>,	Information kontrollerad av VM-systemet efter autentiseringssteg för att identifiera användaren.
Offentliga nyckeln	RSA-kryptering 4096 bitar	Algoritm och värde för den offentliga nyckeln i certifikatet.
Tillgång till myndighetsinformation	http: // XXX	OCSP-serverplats som kommer att definieras av TC.

Figur 10: Innehållsfält i det elektroniska hårdvaruintyget

Giltighet

Giltighetsperiod enligt definitionen i detta schema. Varje elektroniskt hårdvaruintyg ska vara giltigt i högst 36 månader. Denna period kan inte vara längre än den återstående giltighetsperioden för det anställde IO-godkännandet.

Ämne distinguished name (DN)

1) IOEUID: Innehåller ett värde genererat av CAB som representerar IO-anställdas identitet. Detta värde ska vara unikt för en auktoriserad användare: om en användare begär ett nytt elektroniskt hårdvarucertifikat från samma CAB eller en annan CAB (efter en förnyelse eller återkallelse), måste han / hon vara associerad med samma UID.

   IOEUID: n är uppbyggd enligt följande: <ISO-3166-1-LAND-KOD AV PLATSEN FÖR HUSET / NAMN PÅ CAB / KARAKTER ALFANUMERISK KOD>

   Exempel: DE / NEOCERT / 1234567890A

   Detta värde ska ha högst 64 bitar.

2) IOUID: Innehåller ett värde genererat av CAB som representerar IO-lagliga namn, adress och momsnummer.

   EXEMPEL: <IO LEGALNAME: NEO / ADRESS: MAINSTRASSE34BONN53129 / VAT: DE12345678910

3) CABUID: Innehåller ett värde genererat av TC som ska vara unikt för ett ackrediterat CAB. Detta värde ska ha högst 64 bitar.

   CAB har ansvaret för att hantera unika identifierare för användare. TC har ansvaret för att hantera unika identifierare IO: s juridiska enheter och CAB.

Information om publik nyckelinformation

Definierar algoritmen och längden på den offentliga nyckeln i det elektroniska hårdvaruintyget. För att säkerställa tillräckligt förtroende för algoritmens styrka ska en nyckellängd på 4096 bitar användas.

Tillgång till myndighetsinformation

Trust Center ska ge OCSP-åtkomst till certifikatåterkallningslistan för att ge automatisk åtkomst till certifikatets återkallningsstatus. OCSP-tjänsten ska tillhandahålla 24/7 dagar.

7.4 Auktoriseringskontroll Webbtjänst baserad på SOAP

VM-systemet ska kunna kontrollera behörighetsstatusen för användaren som begär åtkomst till säkerhetsinformation.

Denna kontroll ska tillhandahålla en standard SOAP XML-tjänst baserad på HTTPS-protokoll. Tillgång till denna tjänst ska verifieras med ett elektroniskt certifikat. Begäran på TC-servern ska baseras på följande information:

Indata		
Fält	Värde	Kommentarer
IO Employee Unique Identifier (IOEUID)	<UserUniqueIdentifier>	
IO Unique Identifier (IOUID)	<IOUniqueIdentifier>	
Auktoriserings-ID	<AuthorizationUniqueIdentifier>	

Figur 11: Inmatningsdata Schema SERMI Sida 56

Utdata		
Fält	Värde	Kommentarer
Användarstatus	**0 - Avstängd** **1 - Ok** **2 - återkallad** **3 - Okänd**	
IO-anställd unik identifierare	<UserUniqueIdentifier>	

Figur 12: Hämtning av information om användarinformation för utdata under registrering baserat på SOAP

Denna kontroll ska tillhandahålla en standard SOAP XML-tjänst baserad på HTTPS-protokoll. Ett VM-specifikt elektroniskt maskinvaruintyg ska autentisera åtkomst till den här tjänsten.