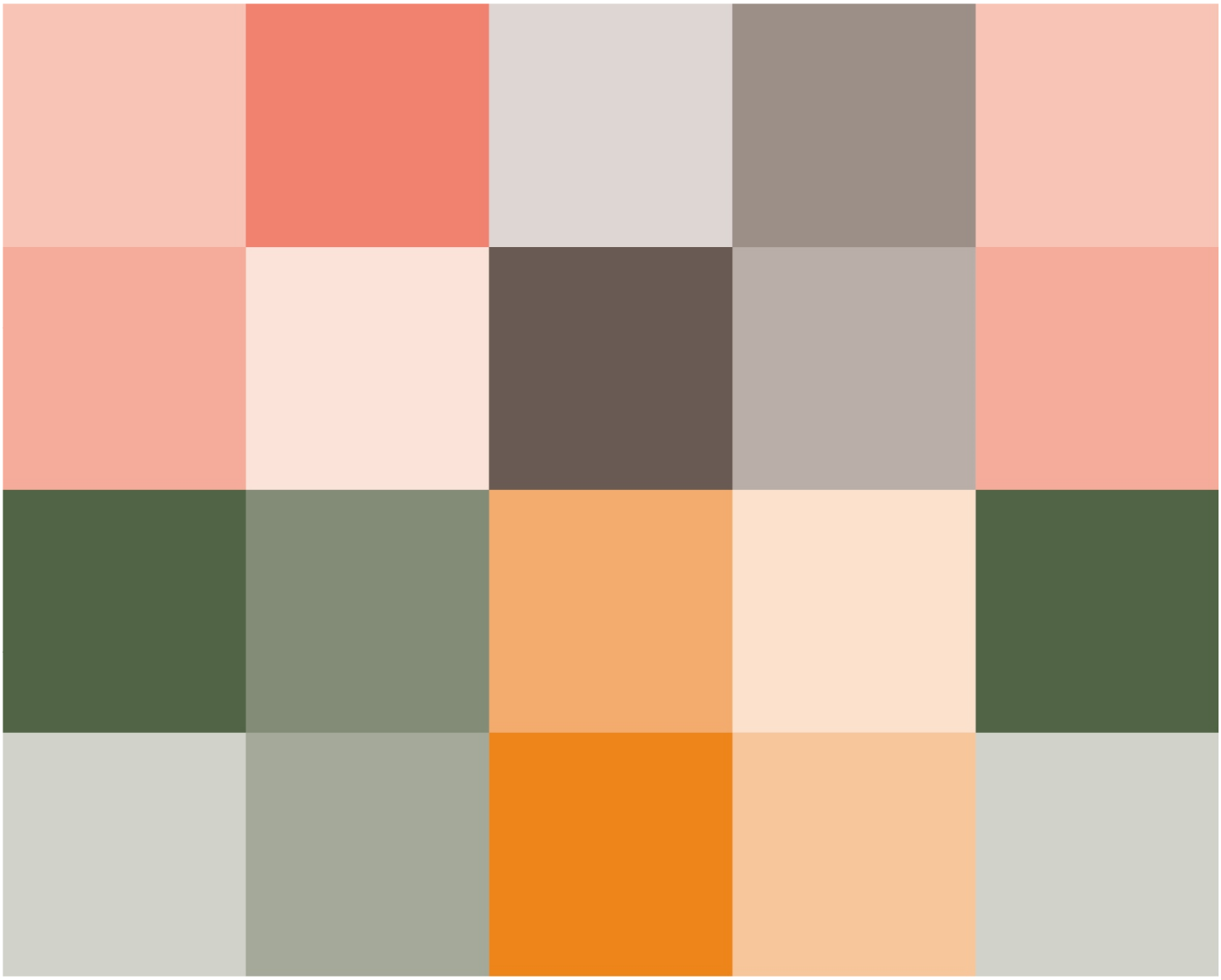


Plattform – Informationssäkerhet och tillitsmodell

Beskrivning av informationssäkerhets- och tillitsmodell som gäller för Plattform för eDelivery

Version: 2022-12-09

Målgrupper: Alla

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Sammanfattande beskrivning av plattformens modell för informationssäkerhet- och tillit.

Plattformen för eDelivery och dess federationer stödjer utbyte av informationssäkerhetsklassad information och meddelanden. Utbytet är baserad på egenskaper, funktioner och tjänster med fokus på hög säkerhet och tillit med principen att skapa trygghet och förtroende för alla anslutna och agerande aktörer.

Plattformens övergripande informationssäkerhets- och tillits-modell omfattar flera dimensioner såsom aktörsroller, organisation, rutiner, teknik, säkerhetsåtgärder samt servicenivåer.

Informations- och IT- säkerhetsarbetet inom plattformen och dess federationer bedrivs systematiskt och riskbaserat enligt modeller och metoder som utgår från ISO27000-serien samt MSB's föreskrifter och vägledningar som gäller för statliga myndigheter.

Ansvarsförhållanden regleras via avtal som beskrivs i plattformens avtalsmodell samt gemensamma regler och rutiner som definieras i ramverket för plattformen per aktörsroll.

En federation tillhandahåller specifika regler och rutiner per aktörsroll vilka beskrivs i federationens federationsdeklaration för dess miljöer.

Behandling av information är en åtgärd eller kombination av åtgärder beträffande informationshantering som varje aktör ansvarar själva för att etablera och dokumentera enligt egna rutiner och processer.

Informationssystem omfattar anslutna informationssystem samt i anslutning agerande tekniska IT-system och verktyg som används av aktör för teknisk lagring och överföring av information inom miljöer i Plattformen och dess federationer.

Informationssäkerhets och tillitsmodellen är baserad på följande övergripande principer:

- aktörer ansvarar själva för att utforma och etablera ett systematiskt och riskbaserat informationssäkerhetsarbete för behandling av information.
- aktörer ansvarar själva för att dokumentera egna rutiner och processer för behandling av information i anslutna och agerande informationssystem.
- aktörer i samverkan och tillsammans med andra aktörer agerar så snabbt som möjligt för support, fel och avvikelser samt incidenter i Plattformen och dess federationer.

Innehållsförteckning

1. Inledning

Säker transport av meddelanden mellan aktörer

Plattformens övergripande funktioner för informationssäkerhet och IT-säkerhet för skapande av tillit mellan aktörer inom plattformen och dess federationer beskrivs genom ansvar, syfte, principer samtrekommendationer.

- Regler och rutiner definieras per aktörsroll.
- Uppfyllnad av regler kontrolleras enligt gällande anslutningsförfarande per aktörsroll samt följs upp och efterlevnadskontrolleras i produktionsmiljöer.
- Ramverket för Plattformen gäller som grund för tolkningsordning inom Plattformen.

Har aktör andra lagar, förordningar och föreskrifter för hantering och behandling av information samt informationssystem så är det varje enskild aktörs eget ansvar att hantera detta inom egen verksamhet.

Huvudsyftet med tillit inom plattformen och federation är att säkerställa att aktörerna har förmågan att hantera information och behandling av information i anslutna och agerande informationssystem och tekniska IT-system på ett verifierbart och tillfredställande sätt.

Informations- och IT-säkerhetsarbetet inom plattformen och dess federationer bedrivs systematiskt och riskbaserat enligt modeller och metoder som utgår från ISO27000-serien samt MSB's föreskrifter och vägledningar för att skapa systemisk tillit mellan alla aktörer.

Ansvarsförhållanden per aktörsroll beskrivs övergripande omfattande behandling av information samt hantering av Informationssystem och IT-system och regleras via avtal som beskrivs mer detaljerat i plattformens avtalsmodell. Om aktörer tecknar avtal mellan varandra aär det varje enskild aktörs eget ansvar att hantera att avtalen uppfyller plattformens gällande regler.

En federation tillhandahåller specifika regler och rutiner per aktörsroll vilka beskrivs i federationens federationsdeklaration för dess miljöer.

Behandling av information är en åtgärd eller kombination av åtgärder beträffande informationshantering, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Informationssystem omfattar till Plattformen anslutna och agerande tekniska IT-system och stödsystem samt verktyg som används av aktör för teknisk lagring och överföring av information inom miljöer i Plattformen och dess federationer.

Transportmodell Utökad Bas inom Plattformen är dimensionerad för att svara upp mot de krav och risker som gäller för allvarlig konsekvensnivå 3 (konfidentialitet och riktighet) enligt MSB's informationssäkerhetsklassningsmodell.

1.1 Målgrupper och intressenter

Detta dokument är ett beskrivande dokument som syftar till att öka medvetenhet och skapa förståelse kring Informationssäkerhet och tillit inom Plattformen samt anslutning av Federationer för samtliga intressenter oavsett roll.

1.2 Dokumentstruktur

Detta dokument innehåller för Plattformen följande delar:

- Ansvarsförhållande och tillit
- Vägledande principer
- Transportinfrastruktur, Miljöer och Certifikat
- Säkerhetsdomäner och tillit
- Informationssäkerhet
- Teknisk IT-säkerhet
- Grundkrav för servicenivåer
- Säkerhetsåtgärder

1.3 Referenser

Dokumentet "Ramverk för Plattform för eDelivery" innehåller en förteckning över alla dokument som *styr och beskriver* Plattform och dess federationer vid en viss given tidpunkt och beskriver hela plattformens dokumentstruktur.

2. Ansvarsförhållande inom Plattformen

Huvudsyftet med ansvar och tillit inom plattformen och anslutna federationer är att säkerställa att aktörerna har bevisade förmågor att hantera information och behandling av information i anslutna och agerande informationssystem på ett verifierbart och tillfredställande sätt. Anslutningsresan i Plattformen omfattar även granskningskriterier.

2.1 Bevisade förmågor och anslutning för aktörer

Plattformen har även förutsättningar att i framtiden via transportinfrastrukturen hantera informationsutbyte mellan olika federationer och då uppkommer även ett behov av tillit mellan flera olika federationer inom plattformen.

Gemensamma regler och rutiner för olika aktörsroller för anslutning, teknik, administration samt identifiering ger förutsättningar att skapa systemisk tillit för en trygg och effektiv digital samverkan för dom aktörer som är ansluta till och agerar i plattformen och anslutna federation och dess miljöer.

Aktörsroller i Plattformens som omfattas av tillit och ansvar är

- Plattformsansvarig,
- Accesspunktsoperatör,
- Federationsägare,
- Federationsoperatör,
- Deltagare,
- Tjänsteleverantör av Meddelandetjänster

Plattformens gemensamma regler och rutiner per aktörsroll finns beskrivet i plattformen samt i federationers egna regelverk och dessa gäller som grund för tolkningsordning inom Plattformen.

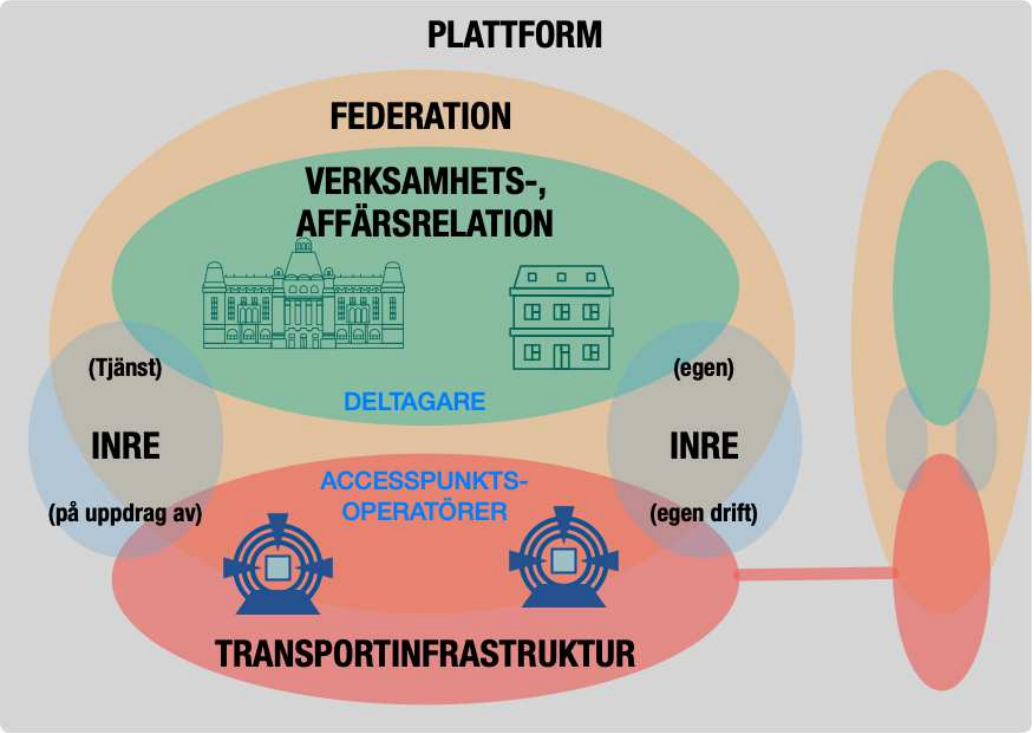
Plattformens avtalsmodell gäller som grund för tillit mellan olika aktörsroller. För att säkerställa efterlevnaden av ramverkets olika delar tecknas avtal mellan olika aktörer. Avtalen reglerar ansvar för åtkomst till information och behandling av information samt administration och personuppgiftsbehandling.

Tillit inom Plattform och Federation verifieras mot dokumenterad Federationsdeklaration avseende uppfyllnad, anpassningar, avgränsningar och tillägg av Federationsägare som granskas, verifieras samt godkänns av plattformsansvarig.

Accesspunktsoperatörer ansluts till Plattformen samt Federationens olika miljöer genom en anslutningsresa som finns beskriven i Plattformen där följsamhet verifieras som ett plattformsgodkännande av plattformsansvarig.

Accesspunktsoperatör godkänns även av federationsägare för anslutning till och agerande i federationens produktionsmiljö.

Deltagare ansluts till Federation enligt gällande regelverk inom federation och aktuell Federationsdeklaration där följsamhet och tillit mot andra aktörer verifieras genom en självdeklaration för de aktörer som är ansluta till och agerar i en federation och dess miljöer.



Figur : Illustration av tillit

2.2 Samtliga aktörers ansvar

Samtliga aktörer ansvarar själva för att vara uppdaterad i vad som gäller gällande styrande principer, regler samt rutiner för aktörens gällande roller i anslutning och agerande i Plattformen och anslutna federationer, se Plattformens styrande dokument per aktörsroll.

Ansvar och styrande principer, regler och rutiner beskrivs även i federationers regelverk och federationsdeklaration.

Samtliga aktörer ansvarar själva för att kontinuerligt analysera, bedöma och vidta de säkerhetsåtgärder som lagar och förordningar ställer på den egna verksamheten som agerar och är ansluten till Plattformen och dess federationer.

Aktörer som är statliga myndigheter ska uppfylla styrande föreskrifter om

- informationssäkerhet enligt MSBFS2020:6.
- säkerhetsåtgärder i informationssystem och IT-system enligt MSBFS 2020:7.

Samtliga aktörer ansvarar för att etablera och dokumentera egna regler och rutiner och att informationssäkerhetsarbetet bedrivs systematiskt och riskbaserat enligt styrande principer, rekommendationer och regler i Plattformen och anslutna federationer. Vi rekommenderar tekniska stöd för upprätthållande och uppdatering av dokumentation.

Samtliga aktörer ansvarar för att genomföra egen informationssäkerhetsklassning för att säkerställa kvalitet och trygghet i skydd och tillgång av information och behandling av information i den egna verksamheten utifrån identifierande risker, hot, och sårbarheter.

Samtliga aktörer ansvarar för analys och bedömning av egen verksamhet utifrån säkerhetsskydd, samhällsviktig verksamhet samt beredskapsperspektiv, tex. NIS-förordning, samt personuppgiftsbehandling enligt gällande Dataskyddsförordning.

- Plattformsansvarig ansvarar övergripande för helheten i Plattformen
- Federationsägare ansvarar övergripande för helheten i Federationen

Samtliga aktörer ansvarar för att vid utveckling, anskaffning eller utkontraktering säkerställa och dokumentera att regler på säkerhet och säkerhetsåtgärder uppfylls av anslutna och agerande informationssystem i Plattform och dess federationer.

Samtliga aktörer ansvarar för att innan driftsättning och inför förändring som kan påverka säkerheten anslutna och agerande informationssystem i Plattform och dess federationer och genomföra egna säkerhetstester och granskning samt kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet.

Samtliga aktörer ansvarar för att informera berörda andra aktörer vid driftsättning och förändringar samt att det finns nödvändig dokumentation för drift och förvaltning för dom egna informationssystemen.

Samtliga aktörer ansvarar för hantering och mottagning av meddelanden från andra anslutna aktörer inom Plattform och anslutna federationer där aktören är ansluten under förutsättning att gällande regler och rutiner samt tekniska specifikationer följs.

Samtliga aktörer ansvarar för egen efterlevnad och följsamhet för behandling av information och agerande i samt anslutna informationssystem utifrån ställda regler i plattformen och dess federationer. Mer information om efterlevnad finns i Plattformens ramverk.

Samtliga aktörer ansvarar för att stödja andra anslutna aktörer vid behov av support, felhantering, driftavbrott samt incidenthantering och kontakta närmaste berörda aktörer inom Plattformen och dess anslutna federationer.

3. Vägledande principer

Plattformen är uppbyggd kring många vägledande principer men utifrån informations-säkerhet och tillit bygger dessa på deltagares efterfrågan på tekniska möjligheter för digital samverkan, tillit och säkerhet som möter plattformens och federationers utbud såsom

- Deltagares efterfrågan möter en federations utbud
- Systemisk tillit inom Federation
- Deltagares eget ansvar för information och informationshantering

Vägledande principer för Plattformen utgår från :

- Informationssäkerhet och teknisk IT-säkerhet är baserat på standarder inom ISO 27000-serien som gäller övergripande för Plattformen och dess federationer.
- Plattformen omfattar väl dokumenterade principer, regler och rutiner samt rekommendationer vilka beskrivs i gällande Ramverk för Plattformen.

Avtalsmodell som reglerar ansvar, åtagande och befogenheter för aktörsrollerna plattformsansvarig, federationsägare, federationsoperatör, deltagare, accesspunktoperatör, och tjänsteleverantörer.

- Accesspunktsoperatörer följs upp och utvärderas kontinuerligt avseende regelefterlevnad enligt gällande ramverk och avtal.
- Federationer med anslutna deltagare följs upp och utvärderas kontinuerligt avseende regelefterlevnad enligt godkänd federationsdeklaration.

Tillitsmodell som beskriver hur tillit skapas mellan aktörer i tillitscirklar och säkerhetsdomäner finns beskrivet i detta dokument samt plattformens regler och rutiner.

Anslutningsmodell där deltagare och accesspunktsoperatörer systematiskt ansluts till federation respektive plattformens transportinfrastruktur.

- Plattformsansvarig ansvarar för accesspunktsoperatörer som ansluts till Plattform (kundkännedom) samt att följa upp dessa.
- Federation ansvarar för deltagare och tjänsteleverantörer som ansluts till Federation (kundkännedom) samt att följa upp dessa.

Accesspunktsoperatör

- Accesspunktsoperatörer i en federation bildar en tillitscirkel och kan därmed lita på att även andra accesspunktsoperatörer är godkända.

Federationer som organiserar och förvaltar gemenskaper av deltagare.

- En federation inbegriper organisatoriska roller och avtalstecknare, federationsägare och federationsoperatör.

Deltagarmodell beskriver och reglerar deltagares ansvar.

- Deltagare ska informationssäkerhetsklassa sin egen information innan utbyte.
- Deltagare ska granska och godkänna de informationssäkerhetsåtgärder som realiseras i en federation innan egen anslutning.
- Deltagare etablerar tillitcirklar mellan varandra genom verksamhetsrelationer och eventuellt genom egna överenskommelser

4. Transportinfrastruktur, miljöer och certifikat

Plattformen stödjer transport och utbyte av information och meddelanden med fokus på hög säkerhet och tillit med principen att skapa trygghet och förtroende för alla aktörer i plattformen.

4.1 Transportinfrastruktur i plattformen

Meddelanden utbyts inom en federations transportinfrastruktur och dess miljöer genom olika transportmodeller med transport via accesspunktsoperatörer mellan deltagare.

Dokumenterade specifikationer för teknisk kommunikation där gällande dokument för transportinfrastruktur, transportmodeller, transportprofiler, kuverteringsprofiler samt komponentspecifikationer som omfattar

- Transportmodeller som beskriver och reglerar hur meddelanden utbyts.
- Meddelandemodeller som beskriver och reglerar hur meddelanden struktureras, signeras och krypteras,

Transportinfrastrukturen är realiserad i reglerade och väl dokumenterade miljöer som har tydliga syften och egenskaper.

- Plattformsansvarig äger, styr och förvaltar utgivning av certifikat för accesspunkts-operatörer per miljö.
- Accesspunktsoperatörer granskas och godkänns av plattformsansvarig innan anslutning till produktionsmiljön efter test, granskning och godkännande att accesspunktsoperatör har påvisat förmågor och följsamhet gentemot regelverk och specifikationer.
- Deltagare granskas och godkänns av federationsägare innan anslutning till produktionsmiljön enligt gällande federationsdeklaration.

4.2 Miljöer i plattformen

En miljö innehåller plattformstjänster och federationstjänster som är reglerade och väl dokumenterade.

- En miljö är tekniskt avskild från andra miljöer och varje miljö inbegriper en egen och avskild certifikatsutgivning för accesspunktsoperatörer.
- En kvalitetsäkringsmiljö-QA, som efterliknar produktionsmiljön, används av accesspunktoperatörer och deltagare för att kvalitetssäkra egna system.
- Vissa komponenter utvecklas, driftsätts, förvaltas av plattformsansvarig som plattformstjänster.
- Vissa komponenter utvecklas, driftsätts, förvaltas av federationsägare som federationstjänster.
- Varje komponent skall ha väl dokumenterade servicenivåer och säkerhetsåtgärder.

4.3 Transportmodeller i plattformen

Plattformen innehåller följande transportmodeller som finns beskrivna i ramverket

- ”Transportmodell – Bas” som tekniskt beskriver och reglerar hur meddelanden utbyts mellan aktörer i plattformen och federationer.
- ”Transportmodell – Utökad bas ” som tekniskt beskriver och reglerar hur meddelanden utbyts mellan organisationer där deltagare signerar och krypterar meddelanden med privata nycklar mellan meddelandetjänster hos deltagare.

4.4 Certifikathantering plattformen

En viktig beståndsdel i Plattformens utbud av säkerhetsåtgärder är användningen av PKI/Certifikat. Transportmodellen bestämmer specifikt hur denna typ av säkerhetsåtgärd tillämpas. I transportinfrastrukturen används PKI/Certifikat på bland annat följande sätt.

- ***Funktionscertifikat*** är kopplad till en tjänst och dess tjänsteinstanser och kan bland annat används för att kryptera och/eller signera kommunikation mellan förmedlingstjänster (såsom accesspunktstjänster).
  - *Ett **TLS/(SSL) -certifikat*** är ett funktionscertifikat som används för att etablera säkra anslutningar över internet och som en del i skalskydd.
  - Ett ***AP-certifikat*** är ett funktionscertifikat (AS4) som används för autentisering av accesspunktstjänster och auktorisationskontroll vid godkännande av en accesspunktstjänst för att kunna agera i en federations miljö.
  - Ett ***informations-certifikat*** är ett funktionscertifikat (AS4) som används för att signera den information som en tjänst administrerar och tillhandhåller.
  - Ett ***deltagar-certifikat*** är ett funktionscertifikat (XHE) som är utgiven till en Deltagare och som används för att kryptera och signera meddelanden och nyttolaster mellan Deltagarnas verksamhetssystem.
- ***Användarcertifikat*** används främst för användare och administration i plattformen i samband med inloggning, kryptering samt signering av informationsmängder

Certifikatutfärdare styrs enligt ramverket och

- **Accesspunktsoperatörs (AP-certifikat)** utfärdas av plattformsansvarig per miljö och federation.

- **TLS/(SSL) Certifikat,** som utfärdas av betrodd certifikatsutgivare finns reglerade i tillämplig transportprofil och som del i skalskydd och enligt rekommendationer från plattformsansvariga och federationsägare.
- **Deltagares** funktions-certifikat utfärdas av extern certifikatsutgivare enligt gällande ramverk för federation.

5. Säkerhetsdomäner och tillit inom Plattformen

Plattformen stödjer utbyte av informationssäkerhetsklassad information och meddelanden och är baserad på egenskaper och funktioner med fokus på hög säkerhet och tillit med principen att skapa trygghet och förtroende för alla aktörer i plattformen.

Tillit och förtroende skapas mellan olika aktörer inom plattform och federationer för följande tillitscirklar och säkerhetsdomäner för miljöer och styrs av ramverket för plattformen omfattande gällande förutsättningar, principer, regler, rutiner samt avtal.

5.1 Tillit inom Plattformen

Styrs av ramverket för plattformen gällande förutsättningar, principer, regler, rutiner omfattande Plattformen samt Accesspunktsoperatör.

- Standardiserad kommunikation Accesspunktsoperatör till Accesspunktsoperatör via Transportinfrastrukturens miljöer och plattformstjänster samt miljöer
- Plattformsansvarig godkänner Accesspunksoperatör – Kundkännedom och avtal
- Användning av standardiserade komponenter för Plattformstjänster
- Användning av separata och avskilda miljöer (Test, QA, Produktion)
- Indirekt via tillit till plattformsansvarig

5.2 Tillit inom Federationer och Deltagarsäkerhet

Styrs av ramverket för plattformen gällande förutsättningar, principer, regler, rutiner omfattande Federation samt Deltagare.

- Skall beskrivas i Federationsdeklaration och ansvaret ligger på Federationsägare.
- Federationsägare godkänner Deltagare – Kundkännedom och avtal
- Användning av standardiserade komponenter för Federationstjänster
- Användning av separata och avskilda miljöer (Test, QA, Produktion)

- Indirekt via tillit till federationsägare

5.3 Tillit och inre säkerhet i plattformen

Styrs av ramverket och skall beskrivas i federationsdeklaration och ansvaret ligger på samtliga aktörer i federationer och plattformen.

- Deltagare – Tjänsteleverantör – Federationsägare – Plattformsansvarig
- Tjänsteleverantör agerar på uppdrag av Deltagare eller Deltagare agerar som Tjänsteleverantör
- Indirekt via administrativ hantering och identifiering i plattform och federationer

5.4 Tillit och säkerhet för Deltagare till Deltagare

Styrs av ramverket och skall beskrivas i federationsdeklaration och ansvaret ligger på Deltagare/Tjänsteleverantörer i federationer utifrån gällande ramverk.

- Deltagare har yttersta ansvaret för den information som skickas via transportinfrastrukturen inom ramen för federation, både som avsändare och mottagare av digitala meddelanden.
- Via verksamhetsrelationer och verksamhetsavtal mellan Deltagare och tjänsteleverantörer samt Deltagare och Accesspunktsoperatörer
- Indirekt via systemisk teknisk tillit till federation och plattform

6. Informationssäkerhet i Plattformen

Detta avsnitt omfattar syften, principer, rekommendationer och regler för informationssäkerhet i Plattformen och dess federationer för samtliga aktörer gällande tillgång till information och behandling av information

Kontroll sker per aktörsroll genom anslutningsförfarande, övervakning och efterlevnadskontroll..

6.1 Administrativ och personell säkerhet

Syftet med administrativ och personell säkerhet är öka förtroendet för att egen eller inhyrd personal har rätt tillgång till information och behandlar information på ett säkert sätt.

6.1.1 Principer

[A] Interna rutiner och åtgärder för administrativ och personell säkerhet säkerställer att personal behandlar information på ett säkert sätt.

[B] Obehörig tillgång till information i aktörers lokaler försvåras genom skalskydd och fysisk säkerhet.

6.1.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva utveckla och upprätthålla åtgärder för att säkerställa att egen och inhyrd personal behandlar information på ett säkert sätt enligt egna interna rutiner.

Samtliga aktörer behöver själva identifiera och hantera behovet av skalskydd och fysisk säkerhet såsom tillträdesbegränsning för sina lokaler.

6.2 Informationssäkerhetsklassning

Syftet med informationssäkerhetsklassning är att säkerställa rätt säkerhetsnivå och skydd av information och behandling av information i den egna verksamheten utifrån gällande lagar, förordningar och föreskrifter.

6.2.1 Principer

[A] Informationssäkerhetsklassning utformas utifrån behov av skydd för informationen en aktör identifierar för den verksamhet som bedrivs.

[B] Informationssäkerhetsklassning bedöms genom analys och värdering av skyddsbehov för konfidentialitet, riktighet och tillgänglighet.

[C] Plattformen utgår från det metodstöd och rekommendationer som Myndigheten för samhällsskydd och beredskap (MSB 0040-09) tagit fram för informationssäkerhetsklassning.

6.2.2 *Rekommendationer enligt MSBFS2020:6. 6 §*

Samtliga aktörer bör

1. klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),

2. identifiera, analysera och värdera risker för sin information (riskbedömning),

3. utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och

4. utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.

6.2.3 Rekommenderad modell för informationssäkerhetsklassning

Informationssäkerhetsklassningen bör utföras av samtliga aktörer enligt denna eller motsvarande modell. Informationens skyddsvärde bestäms utifrån vilka konsekvenser som otillåten spridning av meddelanden och information inom verksamheten och plattformen riskerar att leda till.

Informationssäkerhetsklassningen bör göras till en tabell enligt nedan och se några exempel på frågor utifrån konsekvensnivåer och risker.

Information/Tjänst Komponent	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
Beskrivning	-Nivå	-Nivå	-Nivå

Konfidentialitet

- Vad blir konsekvensen om någon obehörig får tillgång till informationen?
- Vad händer om någon obehörig får tillgång till informationen?

Riktighet

- Vad blir konsekvensen om obehörig person eller process förändrar informationen?
- Vad blir konsekvensen om verksamheten inte upptäcker detta?

Tillgänglighet

- Vilken konsekvens får det om informationen inte alls kan användas på grund av bortfall av tillgänglighet?
- Vilken konsekvens får det om informationen kan användas, men endast i begränsad utsträckning?

6.2.4 Konsekvensnivåer och bedömningsgrunder för informationssäkerhetsklassning

Konsekvensnivåer kan värderas i Plattformen enligt nedan modell.

	Konfidentialitet	Riktighet	Tillgänglighet
4+ Synnerligen allvarlig (Sveriges säkerhet)	Hanteras separat	Hanteras separat	Hanteras separat
3. Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
2. Betydande	Information där förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
1.Måttlig	Information där förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
0. Ingen eller försumbar	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. Förekommer vid helt publik information.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.. Ytterst ovanlig nivå för information!	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. Relativt ovanlig nivå för information.

6.2.5 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva utforma och etablera i**nformationssäkerhetsklassning**

baserat på egna interna regler och arbetssätt för behandling av information samt informationssystem som ansluter och agerar i Plattformen och dess federationer.

Samtliga aktörer behöver själva löpande analysera, bedöma och vidta de åtgärder som lagar och förordningar ställer på den egna verksamheten hos respektive aktör/roll utifrån den informationssäkerhetsklassning och riskhantering som behöver göras för att säkerställa skyddsbehov och säkerhetsåtgärder för behandling av information med hänsyn till känslighetsnivå utifrån dataskydd och säkerhetsskydd.

6.3 Riskbaserat informationssäkerhetsarbete

Syftet med ett systematiskt och riskbaserat informationssäkerhetsarbete är att säkerställa kvalitet och trygghet i skydd av information och behandling av information i den egna verksamheten utifrån identifierande risker, hot, och sårbarheter.

6.3.1 Principer

[A] Ett informationssäkerhetsarbete utformas utifrån de risker, hot och sårbarheter en aktör identifierar för den verksamhet som bedrivs.

[B] Risker bedöms genom analys och värdering av skyddsbehov och säkerhetsåtgärder för information och behandling av information.

[C] Ett informationssäkerhetsarbete bedrivs baserat på egna interna regler som motsvarar de risker, hot, och sårbarheter som identifieras.

[D] Ett riskbaserat informationssäkerhetsarbete stödjer tillit för andra aktörer som är anslutna till och agerar i plattformen och berörd federation.

6.3.2 *Rekommendationer enligt MSBFS2020:6. 5 och 14§*

När aktörer utformar och etablerar informationssäkerhetsarbete bör den säkerställa att

1. informationssäkerhetsarbetet tilldelas nödvändiga resurser,
2. egna interna regler och arbetssätt upprättas,
3. egna interna regler och arbetssätt motsvarar identifierade och bedömda risker, hot och sårbarheter,
4. informationssäkerhetsarbetet följs upp och utvärderas regelbundet,
5. kontakt och eskaleringsvägar finns upprättade till berörda aktörer.

6.3.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva utforma och etablera ett systematiskt riskbaserat informationssäkerhetsarbete baserat på egna interna regler och arbetssätt som motsvarar identifierade och bedömda risker, hot och sårbarheter.

Samtliga aktörer behöver själva löpande bedriva ett systematiskt riskbaserat informationssäkerhetsarbete genom att analysera, värdera, hantera och följa upp risker, hot och sårbarheter samt vidta åtgärder.

6.4 Felhantering och support

Syftet med felhantering och support är att skyndsamt upptäcka fel och bedöma behov av support samt bedöma om fel skall rapporteras vidare.

6.4.1 Principer

[A] Hantering av fel säkerställs genom att skyndsamt upptäcka och bedöma fel och behov av support.

[B] Fel och behov av support hanteras, bedöms, klassificeras och eskaleras enligt egna regler samt lagar och förordningar.

[C] Fel och behov av support rapporteras vidare enligt utförda bedömningar och egna samt gemensamma rapporteringsvägar.

[D] Återkommande fel och behov av support utgör skäl till att genomföra översyn av säkerhetsåtgärder och motverka att det händer igen.

6.4.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva fastställa, dokumentera, införa, och kontinuerligt kontrollera och utvärdera förmågan att skyndsamt upptäcka och bedöma fel och behov av support samt bedöma om inträffat fel och behov av support behöver rapporteras externt.

6.5 Incidenthantering

Syftet med incidenthantering är att skyndsamt upptäcka och bedöma avvikelser, vid behov återställa samt bedöma om avvikelsen skall rapporteras vidare.

6.5.1 Principer

[A] Hantering av incidenter och avvikelser säkerställs genom att skyndsamt upptäcka och bedöma avvikelser och återställa manipulerad eller förlorad information.

[B] Incidenter och avvikelser hanteras, bedöms, klassificeras och eskaleras enligt egna regler samt lagar och förordningar.

[C] Incidenter och avvikelser rapporteras vidare enligt utförda bedömningar och egna samt gemensamma rapporteringsvägar.

[D] Återkommande incidenter och avvikelser utgör skäl till att genomföra översyn av säkerhetsåtgärder och motverka att det händer igen.

6.5.2 *Rekommendation enligt MSBFS2020:6, 11 §:*

Aktörer bör kunna

1. skyndsamt upptäcka och bedöma incidenter och avvikelser,

2. återställa manipulerad eller förlorad information, och

3. bedöma om inträffad incident ska rapporteras vidare enligt gällande kontaktvägar.

Rekommendation enligt MSBFS2020:6, 12 §:

Aktörer bör kunna identifiera grundorsaker till incidenter eller avvikelser och vidta åtgärder för att motverka att liknande incidenter och avvikelser inträffar på nytt.

6.5.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva fastställa, dokumentera, införa, och kontinuerligt kontrollera och utvärdera förmågan att skyndsamt upptäcka och bedöma incidenter och avvikelser, återställa manipulerad eller förlorad information, och bedöma om inträffad incident behöver rapporteras externt.

6.6 Spårbarhet och Logghantering

Syftet med loggning, spårbarhet och logghantering är att skapa bevis för inträffade händelser och producera en spårbarhetskedja som kan användas för analys, uppföljning och hantering av fel, avvikelser samt incidenter.

6.6.1 Principer

[A] Bevis för inträffade händelser säkerställs genom loggning som producerar en spårbarhetskedja som används för uppföljning och hantering av fel, avvikelser samt incidenter.

[B] Analys av loggar används för att kontinuerlig upptäcka och hantera incidenter och avvikelser samt fel.

6.6.2 Rekommendationer

Aktörer bör vid förfrågan från annan aktör vara behjälplig med att ta fram och lämna ut relevant logginformation, under förutsättning att den part som har efterfrågat logginformationen har ett berättigat intresse av dem och att aktören inte enligt lag eller annan författning är förhindrad att lämna ut dessa.

Aktörer bör logga minst följande informationsrelaterade händelser

1. Obehörig åtkomst och försök till obehörig åtkomst till information.
2. Åtkomst till information som bedömts ha behov av utökat skydd.

6.6.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva genom loggning skapa bevis för inträffade informationsrelaterade händelser som kan användas för analys, uppföljning och hantering av fel, avvikelser samt incidenter.

Samtliga aktörer behöver själva regelbundet analysera innehållet i säkerhetsloggarna för att kontinuerligt upptäcka och hantera incidenter och avvikelser samt fel.

6.7 Servicenivåer

Syftet med servicenivåer är att kunna mäta tillgänglighet i form av service och kvalitet enligt förväntade nivåer.

6.7.1 Principer

[A] Mätbara parametrar skapar möjlighet till servicenivåer för tillgänglighet

[B] Grundläggande servicenivåer finns för miljöer och komponenter i Plattformen

[C] SLA:er och ytterligare servicenivåer kan avtalas mellan aktörer vid behov

6.7.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva via egna interna rutiner fastställa, dokumentera, införa, och kontinuerligt mäta tillgänglighet för service och kvalitet för uppföljning av behandling av information samt informationssystem till Plattformen och dess anslutna federationer.

6.8 Kontinuitetshantering för informationssystem

Syftet med kontinuitet är att under och efter svåra situationer, incidenter och kriser kunna upprätthålla fungerande informationssystem för behandling av information enligt i förväg accepterad omfattning och servicenivåer.

6.8.1 Principer

[A] Förmågan att upprätthålla kontinuitet under och efter svåra situationer, incidenter och kriser säkerställs genom att förmågan fastställas, dokumenteras, införs, och kontinuerligt kontrolleras och utvärderas.

[B] Förmågan att upprätthålla kontinuitet som fastställs i konsekvensanalys beror på servicenivåer såsom Maximalt tolerabla avbrottsperioder, Mål för återställningstid och återställningspunkt.

6.8.2 Rekommendation enligt MSBFS2020:6, 13 §:

Aktörer bör i sitt kontinuitetsarbete

1. utvärdera och omhänderta tillgänglighetskraven från genomförd informationsklassning,
2. identifiera aktörens behov av uthållighet över tid,
3. beakta behovet av att tillämpa alternativa arbetssätt, och
4. tydliggöra hur beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normal verksamhet fattas.

6.8.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva fastställa, dokumentera, införa, och kontinuerligt kontrollera och utvärdera förmågan att upprätthålla kontinuitet under svåra situationer, incidenter och kriser enligt i förväg accepterad omfattning och servicenivåer.

Samtliga aktörer behöver själva utföra konsekvensanalys för att skapa en förståelse för hur svåra situationer, incidenter och kriser påverkar verksamhetens operativa förmåga och möjligheten att uppnå fastställda servicenivåer och verksamhetsmål. (BIA - ”Business Impact Analysis”).

6.9 Granskning av informationssäkerhetsåtgärder

Syftet med granskning av de informationssäkerhetsåtgärder som plattformen och berörd federation erbjuder är att säkerställa att den egna verksamhetens krav på informationssäkerhetsåtgärder uppfylls vid anslutning till och agerande i en federation.

6.9.1 Principer

[A] Krav på att informationssäkerhetsåtgärder uppfylls vid anslutning till och agerande i en federation säkerställs genom egen granskning av de informationssäkerhetsåtgärder som plattformen och berörda federation erbjuder.

6.9.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva granska av de informationssäkerhetsåtgärder som plattformen och berörda federationer erbjuder för att säkerställa att aktörens krav på informationssäkerhetsåtgärder uppfylls vid anslutning till och agerande i en federation.

6.10 Arkivering av dokumenterad information

Syftet med att arkivera dokumenterad information är att möjliggöra framtida användning samt att skydda den från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning.

6.10.1 Principer

[A] Dokumenterad information arkiveras och gallras i enlighet med författningsenliga, avtalsmässiga, verksamhetsmässiga krav samt servicenivåer.

[B] Dokumenterad information hanteras enligt av aktören utfärdade riktlinjer för lagring, arkivering, och gallring.

[C] Dokumenterad information arkiveras i form av säkerhetsrelaterade händelser, krypteringsnycklar samt datamängder som lagras och tillhandahålls i aktuell aktörs tjänster.

6.10.2 Rekommendationer enligt ISO 27002, 18.1.3:

Aktörer bör utfärda riktlinjer för lagring, arkivering, hantering och gallring av dokumenterad information;

6.10.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva arkivera och gallra dokumenterad information i enlighet med författningsenliga, avtalsmässiga, verksamhetsmässiga krav samt servicenivåer.

6.11 Avveckling av dokumenterad information och lagringsmedia

Syftet med avveckling dokumenterad information och lagringsmedia samt utrustning som informationssystem består av är att minimera risken för läckage av konfidentiell information till obehöriga personer.

6.11.1 Principer

[A] För att minimera risken för läckage avvecklas dokumenterad information och lagringsmedia med stöd av interna rutiner.

[B] För att minimera risken för läckage avvecklas utrustning som informationssystem består av med stöd av interna rutiner.

[C] Avveckling sker i proportion till bedömda risker för känslighet och konfidentialitet.

6.11.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva avveckla dokumenterad information och lagringsmedia på ett säkert sätt för att minimera risken för läckage av information till obehöriga personer med stöd av interna regler i proportion till bedömda risker för känslighet och konfidentialitet.

Samtliga aktörer behöver själva avveckla utrustning som informationssystem består av på ett säkert sätt för att minimera risken för läckage av information till obehöriga personer med stöd av interna regler i proportion till bedömda risker för känslighet och konfidentialitet.

7. Teknisk IT-säkerhet i Plattformen

Detta avsnitt omfattar syften, principer och rekommendationer och regler för agerande och anslutna informationssystem för samtliga aktörer gällande IT-säkerhet i Plattformen och dess federationer med målsättning att skapa tillit mellan aktörer.

Kontroll sker per aktörsroll genom anslutningsförfarande, övervakning och efterlevnadskontroll.

7.1 Uppdelning i nätverkssegment

Syftet med att placera informationssystem med olika funktioner i separata nätverks-segment är att förhindra spridning av incidenter och minska konsekvenser av angrepp.

7.1.1 Principer

[A] Informationssystem med olika funktioner placeras i separata nätverkssegment i produktionsmiljöer.

[B] Informationssystem med olika funktioner placeras i separata nätverkssegment även för utvecklings-, test- och utbildningsmiljö och hanteras separat av varje enskild aktör.

7.1.2 Rekommendationer enligt MSBFS2020:7, 4.1 §:

Följande funktioner i produktionsmiljön bör placeras i separata nätverkssegment:

1. Klienter för användare.
2. Klienter för administration.
3. Servrar.
4. Centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande.
5. Centrala stödfunktioner i form av skrivare, scanner och liknande.
6. Trådlösa nätverk.
7. Gästnätverk.
8. Externt åtkomliga tjänster.
9. Informationssystem som sammankopplas med informationssystem hos extern aktör.
10. Industriella informations- och styrsystem.
11. System som innehåller sårbarheter som inte kan hanteras.

7.1.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva förhindra spridning av incidenter och minska konsekvenser av angrepp genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö.

7.2 Filtrering av nätverkstrafik

Syftet med att filtrera nätverkstrafik är att förhindra spridning av incidenter och minska konsekvenser av angrepp.

7.2.1 Principer

[A] Nätverkstrafik filtreras mellan nätverkssegment i produktionsmiljöer.

7.2.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

7.3 Behörigheter, digitala identiteter och autentisering

Syftet med hantering av behörigheter är att säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljöer och att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver

7.3.1 Principer

[A] En digital identitet kopplas till en individ, organisation, funktion, eller tjänst.

[B] Digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö hanteras i olika kataloger skilda från kataloger för produktionsmiljön.

[C] Digitala identiteter som ger systemadministrativ behörighet tilldelas restriktivt.

[D] För identifiering av individer används flerfaktorsautentisering.

[E] Hantering av autentiseringsuppgifter utförs enligt interna regler.

7.3.2 Rekommendationer enligt MSBFS2020:7, 4.3 §:

Behörighetshanteringen bör säkerställa genom interna regler att

1. digitala identiteter i produktionsmiljön är unika,
2. digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem,
3. tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år,
4. behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat, och
5. olika digitala identiteter används vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.

7.3.3 Rekommendationer enligt MSBFS2020:7, 4.4 §:

Digitala identiteter som ger systemadministrativ behörighet bör endast användas för systemadministration och tilldelas restriktivt.

En digital identitet med systemadministrativ behörighet bör endast ges åtkomst till en begränsad del av produktionsmiljön.

7.3.4 Rekommendationer enligt MSBFS2020:7, 4.5 §:

Flerfaktorsautentisering bör användas vid

1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk,
2. systemadministrativ åtkomst till informationssystem, och
3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

7.3.5 Rekommendationer enligt MSBFS2020:7, 4.6 §:

Aktörer bör ha interna regler för hantering av autentiseringsuppgifter med krav på

1. längd och komplexitet,
2. när byte ska ske,
3. hur distribution ska ske, och
4. hur autentiseringsuppgifterna ska skyddas.

Tekniska system bör användas för att stödja efterlevnaden av reglerna avseende längd, komplexitet och byte.

7.3.6 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva säkerställa att endast behöriga användare och informationssystem inte har mer åtkomst till IT-system, informationssystem, och information än vad den behöver.

Samtliga aktörer behöver själva ha interna regler för behörighetshantering.

Samtliga aktörer behöver själva säkerställa att behörighetshantering utformas på ett sådant sätt att varje digital identitet inte har mer åtkomst till IT-system, informationssystem, och information än vad den behöver.

Samtliga aktörer behöver själva säkerställa att endast behöriga personer har åtkomst via stark autentisering med hjälp av flerfaktorsautentisering till de IT-system, informationssystem, och information som den behöver i produktionsmiljö.

7.4 Kryptering och nyckelhantering

Syftet med hantering av digitala nycklar och kryptering är att skydda information mot obehörig åtkomst och obehörig förändring vid användning, överföring och lagring.

7.4.1 Principer

[A] För att skydda information mot obehörig åtkomst och obehörig förändring vid användning, överföring och lagring används kryptering.

[B] Digitala nycklar hanteras på ett säkert sätt enligt interna regler.

[C] Säkra algoritmer såsom statistiskt säkerställd slumptalsgenerering används vid skapande av digitala nycklar.

7.4.2 Rekommendationer enligt MSBFS2020:7, 4.7 §:

Aktörer bör använda kryptering för att skydda

1. säkerhetsloggar mot obehörig åtkomst och obehörig förändring,
2. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring, och
3. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför myndighetens kontroll.

7.4.3 Rekommendationer enligt MSBFS2020:7, 4.9 §:

Aktörer bör ha interna regler för hantering av kryptering och hantering av digitala nycklar med krav på

1. hantering av krypteringsnycklar,
2. godkännande och förvaltning av krypteringslösningar, och
3. hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

7.4.4 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva identifiera behov av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Samtliga aktörer behöver själva hantera behovet och användning av kryptering och digitala nycklar.

Samtliga aktörer behöver själva ha interna regler för hantering med skydd av digitala nycklar under hela livscykel inklusive generering, lagring, arkivering, hämtning, distribution, återkallande och destruering av nycklar.

Samtliga aktörer behöver själva använda säkra algoritmer såsom statistiskt säkerställd slumptalsgenerering för skapande av digitala nycklar

7.5 Säkerhetskonfigurering

Syftet med säkerhetskonfigurering är att skydda IT-system och informationssystem mot obehörig åtkomst.

7.5.1 Principer

[A] IT-system och Informationssystem skyddas mot obehörig åtkomst genom att upprätthålla säker konfigurering.

[B] Utvecklings-, test- och driftmiljöer är separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

7.5.2 Rekommendationer enligt MSBFS2020:7, 4.10 §:

Aktörer bör, för att skydda IT-system och informationssystem mot obehörig åtkomst genom att

1. byta ut förinställda autentiseringsuppgifter,
2. stänga av, ta bort eller blockera systemfunktioner som inte behövs, och
3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

7.5.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva genom säker konfigurering av IT-system och informationssystem i produktionsmiljön skydda mot obehörig åtkomst.

7.6 Säkerhetstester och granskningar

Syftet med säkerhetstester och granskningar är att skapa en grund för identifiering av sårbarheter och risker i IT-system och information system.

7.6.1 Principer

[A] Sårbarheter och risker i IT-system och information system identifieras genom säkerhetstester och granskningar.

7.6.2 Rekommendationer enligt MSBFS2020:7, 4.12:

Aktörer bör ha interna regler för hur kontroll görs av att

1. informationssystemen är uppdaterade,
2. valda säkerhetsåtgärder är införda på korrekt sätt, och
3. genomförda säkerhetskonfigurationer är tillräckliga.

Automatiserade säkerhetstester och manuella granskningar bör kombineras vid kontroll av säkerheten i informationssystemen.

7.6.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva säkerställa att säkerhetstester och granskningar utförs för att identifiera av sårbarheter och risker.

7.7 Ändringshantering

Syftet med hantering av ändringar är att säkerställa att förändringar, uppgraderingar och uppdateringar i IT-system och informationssystem genomförs på ett strukturerat, spårbart och säkert sätt.

7.7.1 Principer

[A] Strukturerad och spårbar ändringshantering säkerställer att förändringar, uppgraderingar och uppdateringar i IT-system och informationssystem genomförs på ett säkert sätt.

7.7.2 Rekommendationer enligt MSBFS2020:7, 4.12:

Aktörer bör säkerställa att förändringar i IT-system och informationssystem genomförs på ett strukturerat och spårbart sätt.

Aktörer bör ha interna regler för ändringshantering med krav på

1. vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning,
2. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras,
3. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version,
4. hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål, och
5. hur risker ska hanteras när uppdatering eller uppgradering enligt punkt 3 och 4 inte kan genomföras.

Säkerhetsuppdateringar bör införas skyndsamt och behovet av att automatisera uppdateringar bör övervägas.

För att undvika störning vid förändring bör aktörer genomföra tester och ta fram en plan för återställning innan förändringen genomförs.

De interna reglerna bör tydliggöra hur risker för incidenter och avvikelser i samband med förändringar i utvecklings-, test- och utbildningsmiljö identifieras och hanteras.

7.7.1 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva säkerställa att förändringar i informationssystem genomförs på ett strukturerat, spårbart och säkert sätt.

7.8 Robust och korrekt tid

Syftet med att använda robust och korrekt tid i miljöer är att säkerställa korrekt kommunikation av information och meddelanden, samt korrekta och jämförbara händelseloggar och spårbarhetskedjor.

7.8.1 Principer

[A] Robust och korrekt tid används i alla miljöer genom tillämpning av koordinerad universell tid, UTC(SP).

7.8.2 Rekommendationer enligt MSBFS2020:7, 4.13 §:

Aktörer bör använda tidstjänsten Swedish Distributed Time Service på www.ntp.se.

Behovet av att använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras

7.8.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.

Samtliga aktörer behöver själva kontinuerligt övervaka tidsynkroniseringen.

7.9 Säkerhetskopiering

Syftet med säkerhetskopiering är kunna återställa information som förlorats eller förvanskats.

7.9.1 Principer

[A] Säkerhetskopiering används för att kunna återställa information som förlorats eller förvanskats.

[B] Vid bedömning av säkerhetskopieringens omfattning och intervall omhändertas även programvara, konfiguration utöver information och allt hanteras som en helhet.

7.9.2 Rekommendationer enligt MSBFS2020:7, 4.13 §:

Aktörer bör

1. minst en gång per dygn säkerhetskopiera information som behövs för aktörens förmåga att utföra sitt uppdrag, och

2. minst två gånger per år, eller vid större förändringar av produktionsmiljön, verifiera förmågan att, inom för aktörens godtagbara tidsperiod, återställa information från säkerhetskopior.
3. Behovet av säkerhetskopiering och förmåga till återställning av information i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras separat av varje enskild aktör.

7.9.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva regelbundet säkerhetskopiera sin information för att kunna återställa information som förlorats eller förvanskats.

Samtliga aktörer behöver själva förvara säkerhetskopior skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.

7.10 Säkerhetsloggning och tillhörande analys

Syftet med säkerhetsloggning är att säkerställa spårbarhet i Informationssystem och IT-system som kan användas för analys, uppföljning och hantering av fel, avvikelser samt incidenter.

7.10.1 Principer

[A] Loggning av säkerhetsrelaterade händelser tillämpas regelbundet enligt interna rutiner.

[B] Analys av säkerhetsloggar används för att kontinuerlig upptäcka och hantera incidenter och avvikelser samt fel.

7.10.2 Rekommendationer enligt MSBFS2020:7, 4.16 §:

Aktörer bör för att säkerställa spårbarhet i informationssystem, logga minst följande säkerhetsrelaterade händelse enligt interna rutiner:

1. Obehörig åtkomst och försök till obehörig åtkomst till IT-system och informationssystem.
2. Förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter.
3. Förändringar av behörighet för användare och informationssystem.

7.10.3 Rekommendationer enligt MSBFS2020:7,4. 17 §:

Aktörer bör analysera innehållet i loggarna för att upptäcka och hantera incidenter och avvikelser enligt interna rutiner. Loggarna kan

1. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten,
2. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar, och
3. vara tillgängliga för analys under fastställd bevarandetid.
4. bör innehålla uppgift om vem eller vad som agerat, vad som har skett och vid vilken tidpunkt.
5. skapa jämförbarhet genom att använda koordinerad universell tid, UTC(SP) för samtliga säkerhetsloggar.
6. samlas i ett för ändamålet avsett informationssystem.

7.10.4 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva för att säkerställa spårbarhet i informationssystem och IT-systemen logga säkerhetsrelaterade händelser regelbundet.

Samtliga aktörer behöver själva enligt interna rutiner dokumentera hur tekniska säkerhetsloggarna används samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de bevaras.

Samtliga aktörer behöver själva enligt interna rutiner skydda loggningsverktyg och logginformation mot manipulation och obehörig åtkomst.

Samtliga aktörer behöver själva regelbundet analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser.

7.11 Övervakning av nätverkstrafik

Syftet med övervakning av nätverkstrafik är att upptäcka och hantera incidenter och avvikelser.

7.11.1 Principer

[A] Berörd nätverkstrafik övervakas kontinuerligt.

7.11.2 Rekommendationer enligt MSBFS2020:7, 4.18 §:

- Behovet av intrångsdetektering och intrångsskydd bör bedömas för berörd nätverkstrafik och för aktörs produktionsmiljö i sin helhet.

- Behovet bör även bedömas för aktörs utvecklings- test- och utbildningsmiljö.

7.11.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva kontinuerligt övervaka berörd nätverkstrafik.

Samtliga aktörer behöver själva identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

Samtliga aktörer behöver själva identifiera och hantera behovet av realtidsövervakning av nätverkstrafik.

7.12 Övervakning av IT-system och informationssystem

Syftet med övervakning av IT-system och informationssystem är att upptäcka och hantera incidenter och avvikelser.

7.12.1 Principer

[A] Berörda IT-system och informationssystem övervakas kontinuerligt.

7.12.2 Rekommendationer enligt MSBFS2020:7, 4.18 §:

- Behovet av intrångsdetektering och intrångsskydd bör bedömas för berörda IT-system och informationssystem och för aktörs produktionsmiljö i sin helhet.

- Behovet bör även bedömas för aktörer utvecklings- test- och utbildningsmiljö.

7.12.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva kontinuerligt övervaka berörda IT-system och informationssystem.

Samtliga aktörer behöver själva identifiera och hantera behovet av realtidsövervakning av berörda IT-system och informationssystem.

7.13 Skydd mot skadlig kod

Syftet med skydd mot skadlig kod är att säkerställa att information och informationssystem skyddas mot intrång, inkommande skadlig kod, och spridning av skadlig kod.

7.13.1 Principer

[A] Information och informationssystem skyddas mot skadlig kod genom införande av upptäckande, förebyggande och återställande säkerhetsåtgärder.

[B] Användning av programvara som ger skydd mot skadlig kod.

7.13.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva ha ett uppdaterat eget skydd mot intrång, skydd mot inkommande skadlig kod samt skydd mot spridning av skadlig kod.

Samtliga aktörer behöver själva använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig behöver andra åtgärder vidtas som ger motsvarande skydd.

7.14 Skydd av utrustning

Syftet med skydd av utrustning är att förhindra förlust, skada, stöld, påverkan, eller obehörig åtkomst av den utrustning som informationssystem består av och hanterar information.

7.14.1 Principer

[A] Den utrustning som informationssystem består av och hanterar information skyddas mot förlust, skada, stöld, påverkan, eller obehörig åtkomst.

7.14.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva ha interna regler för hur utrustning skyddas.

Samtliga aktörer behöver själva skydda utrustning mot skador och obehörig åtkomst, genom att

1. placera utrustning i särskilda it-utrymmen,
2. tilldela behörighet till särskilda it-utrymmen restriktivt,
3. identifiera och hantera behovet av övervakning och larm i särskilda it-utrymmen,
4. registrera tillträde till särskilda it-utrymmen på individnivå,
5. placera och skydda utrustning för att minska riskerna för miljörelaterade hot och faror och möjligheter för obehörig åtkomst.

Lagringsmedia, informationssystem och IT-system behöver på ett säkert sätt avvecklas när de inte längre behövs med stöd av interna regler.

7.15 Redundans och återställning

Syftet med redundans och återställning är att säkerställa tillgänglighet till IT-system och informationssystem under och efter avvikelser eller incidenter enligt i förväg accepterad omfattning och servicenivåer.

7.15.1 Principer

[A] Tillgänglighet till IT-system och informationssystem vid avvikelser eller incidenter säkerställs genom tillräcklig redundans och förmåga till återställning.

7.15.2 Rekommendationer enligt MSBFS2020:7, 4.12, 4.22 §:

1. För att undvika störning vid förändring bör aktör genomföra tester och ta fram en plan för återställning innan förändringen genomförs.

2. Övning av återställning bör ske regelbundet och utifrån identifierat behov av tillgänglighet.

7.15.3 Rekommendationer inom Plattformen

Samtliga aktörer behöver själv,

1. ha tillräcklig redundans och förmåga till återställning för att uppfylla krav på tillgänglighet vid avvikelser eller incidenter enligt i förväg accepterad omfattning och servicenivåer.
2. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda IT-system och informationssystem,
3. öva återställning av informationssystem som är centrala för aktörens förmåga att utföra sitt uppdrag, och
4. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.

7.16 Kontinuitet för IT-system och utrustning

Syftet med kontinuitet är att under och efter svåra situationer, incidenter och kriser kunna upprätthålla fungerande IT-system med utrustning och lagringsmedia enligt i förväg accepterad omfattning och servicenivåer.

7.16.1 Principer

[A]Förmågan att upprätthålla kontinuitet under och efter svåra situationer, incidenter och kriser fastställs, dokumenteras, införs, och kontinuerligt kontrolleras och utvärderas.

7.16.2 Rekommendationer inom Plattformen

Samtliga aktörer behöver själva fastställa, dokumentera, införa, och kontinuerligt kontrollera och utvärdera förmågan att upprätthålla kontinuitet under svåra situationer, incidenter och kriser enligt i förväg accepterad omfattning och servicenivåer.

8. Grundkrav för servicenivåer

Detta avsnitt och vägledning kan användas som grund för samtliga aktörsroller.

Samtliga servicenivåer i Plattformens tjänster i miljöer beskrivs i plattformens olika funktioners beskrivningar, regler och rutiner som plattformsansvarig ansvarar för. Servicenivåer för federationstjänster ansvarar federationsägare för och dessa hanteras inom federationens regelverk samt federationens federationsdeklaration.

Övriga aktörsroller som AP-operatör och Deltagare kan utgå från följande grundkrav som en vägledning för servicenivåer inom Plattformen.

8.1 Plattformstjänster

Servicenivåer beskrivs mer detaljerat i komponentspecifikationer och miljöspecifikationer.

Kategori	**Aspekt på servicenivå**	**Grundnivåer**
Tillgänglighet	Plattformstjänster ska ha en tillgänglighet 24/7 räknat som ett genomsnitt per månad exkl. planerade avbrott)	99,5%
Tillgänglighet	Plattformstjänster är att anse som otillgänglig om den kontinuerligt inte går att nå på specificerat sätt under en period av	10 sekunder
Spårbarhet	Plattformsansvarig ska lagra alla händelseloggar för plattformstjänster	12 månader
IT-säkerhet	Backup och återläsningsprocedur ska finnas som medger återställning inom	24 timmar
Support och felhantering	Plattformsansvarig skall löpande stödja AP-operatör och federationsägare inkl. deltagare vid behov av support och felhantering via gällande supportkanaler.	Löpande helgfria arbetsdagar 9-16
Incident	Avbrott/störning eller intrång som klassas som incident som kan ha inverkan på Plattformstjänster, AP-operatörer, Federationstjänster samt Deltagare ska rapporteras från Plattformsansvarig till berörda inom	6 timmar

Incident	Vid inrapportering av incidenter från Access-punktsoperatör eller Deltagare ska Plattforms-ansvarig påbörja hantering enligt egna rutiner och etablerade kanaler för incidentrapportering	Nästa helgfria arbetsdag
Incidentrapportering	Avbrott/störning eller intrång som gäller under tillsyn skall rapporteras av Plattformsansvarig enligt gällande förordningar för t.ex. Dataskydd och NIS	Enl. förordning
Administrativ	Planerade avbrott(service fönster) ska annonseras till berörda i förväg med minst	5 helgfria arbetsdagar
Tillgänglighet(Ny)	Förmågan att upprätthålla kontinuitet fastställs i konsekvensanalys per aktörsroll och beror på servicenivåer såsom Maximalt tolerabla avbrottsperioder, Mål för återställningstid och återställningspunkt.	ToBeDefined

8.2 Servicenivåer som exempel för AP-operatör/AP-komponent

Servicenivåer enligt nedan kan fungera som vägledning för AP-operatörer i Plattformen och bör regleras i avtal mellan AP-operatör och Deltagare.

Kategori	**Aspekt på servicenivå**	**Grundnivåer**
Tillgänglighet	AP-funktionen ska ha en tillgänglighet 24/7 räknat som ett genomsnitt per månad exkl. planerade avbrott)	99,5%
Tillgänglighet	AP-funktionen är att anse som otillgänglig om den kontinuerligt inte går att nå på specificerat sätt under en period av	10 sekunder
Spårbarhet	AP-operatören ska lagra alla händelseloggar för AP-tjänsten i minst	12 månader
IT-säkerhet	Backup och återläsningsprocedur ska finnas som medger återställning inom	24 timmar

Support och felhantering	AP-operatör skall löpande stödja Deltagare och Plattformsansvarig vid behov av support och felhantering via gällande supportkanaler.	Löpande helgfria arbetsdagar 9-16
Incident	Avbrott/störning eller intrång som klassas som incident som kan ha inverkan på Plattformstjänster, andra AP-operatörer, Federationstjänster samt Deltagare ska incidenten rapporteras från AP-operatör till berörda inom	6 timmar
Incident	Vid inrapportering till AP-operatör av incidenter från Plattformsansvarig eller Deltagare ska AP-operatör påbörja hantering enligt egna rutiner och etablerade kanaler för incidentrapportering	Nästa helgfria arbetsdag
Incidentrapportering	Avbrott/störning eller intrång som gäller under tillsyn skall rapporteras av AP-operatör enligt gällande förordningar för t.ex. Dataskydd och NIS	Enl. förordning
Administrativ	Planerade avbrott i en AP-funktion ska annonseras till Plattformsansvarig samt ansluten Deltagare i förväg med minst	5 helgfria arbetsdagar
Tillgänglighet(Ny)	Förmågan att upprätthålla kontinuitet fastställs i konsekvensanalys per aktörsroll och beror på servicenivåer såsom Maximalt tolerabla avbrottsperioder, Mål för återställningstid och återställningspunkt.	

8.3 Servicenivåer för Federationstjänster

Servicenivåer för Federationstjänster kan utgå från grundläggande servicenivåer för Plattformstjänster som vägledning och kan ytterligare regleras inom federation och beskrivas i Federationsdeklaration.

8.4 Servicenivåer för Deltagare

Även servicenivåer för Deltagare utgår som grund från servicenivåer för Plattforms-tjänster samt Accesspunkts-operatör. Detaljer kring servicenivåer för Deltagare regleras av federationsägare i federationsdeklaration samt avtal inom Federation och med aktuell Accesspunktsoperatör.

9. Säkerhetsåtgärder i Plattformen

Samtliga i Plattformen centrala funktioner som plattformstjänster, miljöer, komponenter och transportmodeller ansvarar för att dokumentera vilka säkerhetsåtgärder som gäller för dess funktion. Federationer hanterar detta inom sitt eget regelverk och dokumenterar detta i federationens federationsdeklaration.

Se gällande säkerhetsåtgärder per funktion och som vägledning kan nedan förteckning av säkerhetsåtgärder användas.

9.1 Säkerhetsåtgärder som mall för Plattformen

Denna mall kan användas som vägledning för tjänster och tekniska specifikationer som etablerar en rad säkerhetsmekanismer i Plattformen och dess federationer.

Säkerhetsåtgärd	**Security Function (CEF/EU)**	**Definition/Omfattning**
Förändringsskydd under transport	Transport Integrity	
Identifiering/ Ursprungskontroll av avsändare	Authentication Sender	
Auktorisation av Sändning	Authorisation of Sending	
Identifiering av mottagare	Receiver Authentication	
Förändringsskydd av meddelande	Message Integrity	
Insynsskydd för kommunikation	Message Confidentiality – non-persistent	
Insynsskydd för lagrade meddelanden	Message Confidentiality – persistent	
Tidstämpel på meddelande	Message Timestamp	
Ursprungskontroll av (av)sändare	Addressee Identification / Party Identification	
Oavvislighet av meddelande	Non Repudiation of Origin	
Oavvislighet av kvittens	Non-Repudiation of Receipt	
Robust meddelandeutväxling	Reliable Message	

9.2 Säkerhetsåtgärder för Transportmodell Bas (kopia)

Denna transportmodell baseras på tjänster och tekniska specifikationer som etablerar en rad säkerhetsmekanismer. Detta avsnittet är kopierat från ”Transportmodell – Bas” som en vägledning i denna versionen av Plattformens ramverk men kommer tas bort i framtida uppdatering och då enbart finnas i ”Transportmodell – Bas”.

Säkerhetsåtgärd	**Security Function (CEF/EU)**	**Definition/Omfattning**
Förändringsskydd under transport	Transport Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS **Deltagares integration med sin AP** genom inre säkerhet
Identifiering/ Ursprungskontroll av avsändare	Authentication Sender	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP. **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt.
Auktorisation av Sändning	Authorisation of Sending	**AP till AP** genom att certifikat visar att AP är godkänd för aktuell federation och miljö **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt.
Identifiering av mottagare	Receiver Authentication	**AP till AP** genom att certifikat i tjänstemetadatat visar att AP är godkänd för aktuell federation och miljö. Kontroll

		av att den synkrona kvittensens signatur överensstämmer med certifikat från tjänstemetadata. **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt
Förändringsskydd av meddelande	Message Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS **Deltagares integration med sin AP** genom inre säkerhet *Inget obrutet förändringsskydd Deltagare till Deltagare*
Insynsskydd för kommunikation	Message Confidentiality – non-persistent	**AP till AP** genom AS4 kryptering samt TLS **Deltagares integration med sin AP** genom inre säkerhet
Insynsskydd för lagrade meddelanden	Message Confidentiality – persistent	*Nyttjas ej i Transportmodell Bas*
Tidstämpel på meddelande	Message Timestamp	**AP till AP** genom AS4 tidsstämpel (signerad av avsändande AP) **Deltagare till Deltagare** genom att kuvert är tidsstämplat *(ej signerad i denna Transportmodell)*
Ursprungskontroll av (av)sändare	Addressee Identification / Party Identification	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP.

		Deltagare till Deltagare genom slagning i SMP och tillit till att denna information är korrekt.
Oavvislighet av meddelande	Non Repudiation of Origin	**AP till AP** genom att meddelande signeras med avsändandes APs certifikat. **Deltagare till Deltagare** *ingen säkerhetsmekanism för oavvislighet i denna Transportmodell*
Oavvislighet av kvittens	Non-Repudiation of Receipt	**AP till AP** genom att transportkvittens signeras med mottagande APs certifikat. **Deltagare till Deltagare** *ingen säkerhetsmekanism för oavvislighet i denna Transportmodell*
Robust meddelandeutväxling	Reliable Message	**AP till AP genom** synkron transportkvittens **Deltagare till Deltagare** genom asynkron meddelandekvittens

9.3 Säkerhetsåtgärder för Transportmodell Utökad Bas(kopia)

Detta avsnittet är kopierat från ”Transportmodell – Utökad Bas” som en vägledning i denna versionen av Plattformens ramverk men kommer tas bort i framtida uppdatering och då enbart finnas i ”Transportmodell – Utökad Bas”.

Säkerhetsåtgärd	**Security Function (CEF/EU)**	**Definition/Omfattning**
Förändringsskydd under transport	Transport Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS

		Deltagare till Deltagare genom kryptering av nyttolast
Identifiering/ Ursprungskontroll av avsändare	Authentication Sender	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP. **Deltagare till Deltagare** genom avsändande Deltagares signatur och slagning i Certifikatspubliceringstjänsten för att verifiera att avsändaren använder rätt certifikat.
Auktorisation av Sändning	Authorisation of Sending	**AP till AP** genom att certifikat visar att AP är godkänd för aktuell federation och miljö **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt.
Identifiering av mottagare	Receiver Authentication	**AP till AP** genom att certifikat i tjänstemetadatat visar att AP är godkänd för aktuell federation och miljö. Kontroll av att den synkrona kvittensens signatur överensstämmer med certifikat från tjänstemetadata. **Deltagare till Deltagare** genom slagning i SMP och tillit till att denna information är korrekt samt genom slagning i Certifikatspubliceringstjänst för att verifiera mottagarens certifikat

Förändringsskydd av meddelande	Message Integrity	**AP till AP** genom AS4 kryptering och signering samt TLS **Deltagares integration med sin AP** genom inre säkerhet **Deltagare till Deltagare** genom kryptering av nyttolast
Insynsskydd för kommunikation	Message Confidentiality – non-persistent	**AP till AP** genom AS4 kryptering samt TLS **Deltagare till Deltagare** genom kryptering av nyttolast
Insynsskydd för lagrade meddelanden	Message Confidentiality – persistent	**Deltagare till Deltagare** genom kryptering av nyttolast
Tidstämpel på meddelande	Message Timestamp	**AP till AP** genom AS4 tidsstämpel (signerad av avsändande AP) **Deltagare till Deltagare** genom att kuvert är tidsstämplat (och signerat)
Ursprungskontroll av (av)sändare	Addressee Identification / Party Identification	**AP till AP** genom matchning av AP-certifikatet subjekt och transportkuvertets identifierare för avsändande AP. **Deltagare till Deltagare** genom slagning i Certifikatspubliceringstjänsten för att kontrollera att avsändarens signatur är i överenstämmelse avsändarens publicerade certifikat
Oavvislighet av meddelande	Non Repudiation of Origin	**AP till AP** genom att meddelande signeras med avsändandes APs certifikat.

		Deltagare till Deltagare genom att meddelandet är signerat
Oavvislighet av kvittens	Non-Repudiation of Receipt	**AP till AP** genom att transportkvittens signeras med mottagande APs certifikat. **Deltagare till Deltagare** genom att meddelandet är signerat
Robust meddelandeutväxling	Reliable Message	**AP till AP genom** synkron transportkvittens **Deltagare till Deltagare** genom asynkron meddelandekvittens