IT-säkerhetsbilaga till regelverk för anslutning till Säker digital kommunikation - Informationssäkerhet

Version 1.2 (2022)

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0 (2022)	220225	Malin Domeij	Beslutad version i 1.0 för tjänsten Säker digital kommunikation.
1.1 (2022)	220609	Marco de Luca	Avsnitt 1.3.2 – Översiktsbild uppdaterad Avsnitt 2.4 – Transportkryptering refererar ej till avsnitt 2.1
1.2 (2022)	221108	Marco de Luca	Avsnitt 2.2 – Omarbetning, SDK-anslutning förutsätter en plattformsgodkänd accesspunktsoperatör Avsnitt 2.3.1 – Förtydligande gällande krav på certifikat och nyckellängder

Innehållsförteckning

1. Inledning 4

1.1 Syfte 4
1.2 Definitioner 4
1.3 Bakgrund 7

2. Krav på skydd vid meddelandeöverföring 10

2.1 Generella kryptografiska krav samt säkerhetsprotokoll 10
2.2 Säkerhet i eDelivery transportinfrastruktur – skydd mellan accesspunkter 10
2.3 Certifikat för O2O-kryptering och signering av meddelanden – skydd vid meddelandeöverföring mellan användarorganisationer 11
2.4 Inre säkerhet – skydd mellan anslutande system och accesspunkt 12

3. Krav på skydd vid kommunikation med gemensamma komponenter 14

3.1 eDelivery transportinfrastrukturs gemensamma komponenter 14
3.2 SDKs gemensamma komponenter 15

4. Teknisk säkerhet 16

4.1 Felsökning 16
4.2 Tid 16

5. Referenser 17

1. Inledning

1.1 Syfte

Detta är en bilaga till Regelverk för anslutning till Säker digital kommunikation – Informationssäkerhet (hädanefter benämnt Regelverket). Bilagan innehåller krav som syftar till att upprätthålla en lämplig nivå på konfidentialitet och riktighet vid meddelandeöverföring inom Säker digital kommunikation (SDK). För att uppnå denna nivå används autentisering, kryptering och signering.

Bilagan tar upp krav såsom säkerhetsprotokoll, algoritmer och nyckellängder. Den innehåller också referenser till säkerhetsmekanismer och krav inom eDelivery transportinfrastruktur (Plattform för eDelivery) hos Myndigheten för digital förvaltning (DIGG). Detta eftersom SDK är en tillämpning av eDelivery transportinfrastruktur och med syftet att ange samtliga it-säkerhetskrav för kommunikation inom SDK.

För information om eDeliverys transportinfrastrukturs säkerhetsmekanismer hänvisas till ”DIGG Plattform - Informationssäkerhet och tillitsmodell”[1].

Dokumentet utgör den första versionen för tjänsten 2022 och ska kompletteras med ytterligare hänvisning till information från DIGG. Det kan komma att revideras ytterligare med anledning av förändrad säkerhetsmodell och förändrade ansvarsförhållanden mellan DIGG som ansvarig för eDelivery transportinfrastruktur respektive Inera som SDK-federationsägare- och operatör av SDK. Man bör förvänta sig att det kan bli mer frekventa uppdateringar de första åren när SDK införs hos användarorganisationer.

1.2 Definitioner

Följande definitioner används i detta dokument och kompletterar definitionerna i Regelverket. Definitioner som förväntas regleras i DIGG eDelivery definitionslista markeras med [2].

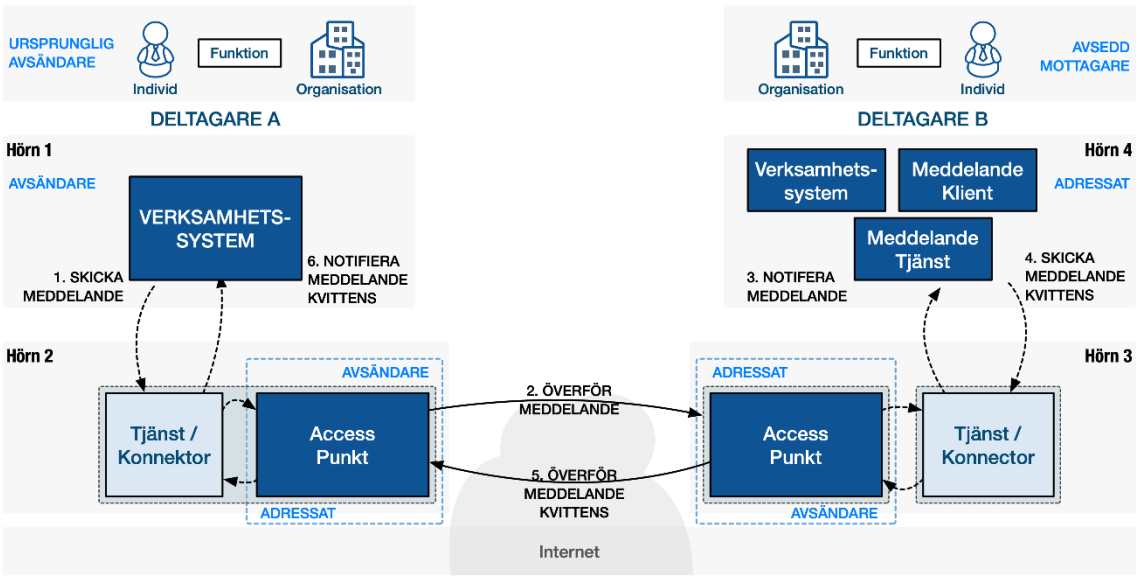
Förkortning	Term	Beskrivning
	Anslutande system	Ett samlingsbegrepp för Meddelandeklient och Meddelandetjänst; det system som användarorganisation tekniskt ansluter via en Accesspunkt till SDK. Anslutande system motsvarar Hörn 1 (C1) respektive Hörn 4 (C4) i eDelivery fyrhörningsmodell.
	Autentisering	Autentisering (authentication på engelska) innebär att bekräfta en användares eller systems verkliga identitet i avsikt att stödja konfidentialitet.
CA	Certificate Authority[2]	Certifikatutfärdare, organisation som utfärdar digitala certifikat.

Certpub	Certifikatspubliceringstjänst[2]	Gemensam komponent i eDelivery transportinfrastruktur. Certifikatspubliceringstjänst innehåller användarorganisationers publika certifikat som används för att hantera kryptering och signering av nyttolast.
	Kryptering	Kryptering skyddar information, d.v.s. att överförd information endast kan läsas av avsedd part.
MK	Meddelandeklient	Meddelandeklient utgör gränssnitt mot användare i meddelandehanteringen. Meddelandeklient hanterar funktioner som säker "brevlåda", säker inloggning, behörighetsstyrning, skapa/skicka/ta emot/besvara meddelande, notifiering av användare samt sortering i t.ex. konversationer (meddelandetrådar). Meddelandeklient kan vara ett fristående it-stöd eller ett verksamhetssystem som anpassas för kommunikation via SDK.
MT	Meddelandetjänst	Meddelandetjänst är det tekniska lagret av ett meddelandesystem hos en användarorganisation som deltar i meddelandeutbyte inom SDK. Användarorganisationens Meddelandetjänst möjliggör O2O-kryptering och signering. Meddelandetjänst ansvarar för att styra meddelandet till rätt meddelandeklient (s.k. internt vägval).
O2O	Organisation-till-organisation-kryptering och signering	O2O innebär säker meddelandeöverföring mellan användarorganisationers Meddelandetjänster som kommunicerar via SDK genom kryptering av nyttolast och signering av kuvert.
PKI	Public Key Infrastructure[2]	Ett ramverk för hantering av digitala certifikat, med privata och publika nycklar, för att bl.a. skapa tillit mellan parter.
	SDK Adressbok	Registerfunktion med organisatoriska adressuppgifter för respektive deltagande användarorganisation. Används primärt för att ange funktionsadresser inom organisation, samt beskrivningar och attribut att söka och filtrera på (verksamhetsadressering).
SML	Service Metadata Locator[2]	Gemensam komponent i eDelivery transportinfrastruktur. SML möjliggör att Accesspunkter dynamiskt kan hitta mottagande organisations Metadatatjänst enbart baserat på mottagande parts organisationsidentitet, samt vetskap om vilket typ av meddelandeutbyte som ska göras (i detta fall SDK meddelandeutbyte). SML kan ses som ett försystem som hjälper till att registrera organisationer som ska deltaga i ett meddelandeutbyte.

SMP	Metadatatjänst, Service Metadata Publisher[2]	Gemensam komponent i eDelivery transportinfrastruktur. Metadatatjänst håller mottagares tekniska kommunikationsmöjligheter (kapabiliteter) för kommunikation via eDelivery transportinfrastruktur. I SMP registreras accesspunktsoperatörers accesspunkter och dess deltagare. I SDKs fall motsvaras deltagare av användarorganisationer.
	Signering	Digital signering garanterar riktighet (integritet), d.v.s. att information inte otillbörligt kan förändras. Signering stödjer också en annan viktig egenskap, oavvislighet (”non-repudiation” på engelska), d.v.s. att avsändare/mottagare inte kan förneka att information skickats/tagits emot.

1.3 Bakgrund

Säker digital kommunikation är en tillämpning av eDelivery transportinfrastruktur. Lösningen utgår ifrån en s.k. fyrhörningsmodell (four-corner model) för säker robust transport. Se Figur 1 nedan.



Figur 1 – DIGGs fyrhörningsmodell (Four-corner model)

Förklaring av hörnen i modellen:

Hörn 1 (C1) / Hörn 4 (C4) är deltagares (användarorganisationers) anslutande system, där:

- Hörn 1 är avsändarens (sändande användarorganisations) Meddelandetjänst och Meddelandeklient
- Hörn 4 är adressatens (mottagande användarorganisations) Meddelandetjänst och Meddelandeklient

Hörn 2 (C2) / Hörn 3 (C3) är deltagares (användarorganisationers) anslutna Accesspunkter, där:

- Hörn 2 (C2) är avsändarens (sändande användarorganisations) Accesspunkt
- Hörn 3 (C3) är adressatens (mottagande användarorganisations) Accesspunkt

För mer information, se DIGGs dokumentation avseende eDelivery transportinfrastruktur.

1.3.1 Säkerhetsområden som reglerar skydd vid meddelandeöverföring

Inom fyrhörningsmodellen finns följande säkerhetsområden som reglerar skydd vid meddelandeöverföring:

Säkerhetsområde	Hörn	Beskrivning
Säkerhet i eDelivery transportinfrastruktur	C2 - C3	Fokuserar på säkerheten vid meddelandeöverföring mellan Accesspunkter. Detta område regleras av Ansvarig för eDelivery. För information om eDelivery transport-infrastrukturs säkerhetsmekanismer och skydd mellan accesspunkter, se ’DIGG eDelivery Informationssäkerhet och tillitsmodell’[1] samt ’DIGG eDelivery – Transportmodell – Utökad Bas’[3].
O2O-kryptering och signering inom SDK	C1 - C4	Fokuserar på säkerheten vid meddelandeöverföring mellan avsändarens (sändande användarorganisations) anslutna system (C1) och adressatens (mottagande användarorganisations) anslutna system (C4). Se närmare beskrivning i definitioner. Detta område regleras av SDK-federationsoperatör.
Inre säkerhet i lokala komponenter	C1 - C2 samt C3 - C4	Fokuserar på säkerheten vid meddelandeöverföring mellan anslutande system och Accesspunkt hos avsändare respektive adressat. Detta område regleras i tillämpliga delar av SDK-federationsoperatör.

Tabell 1 – Förklaring av säkerhetsområden

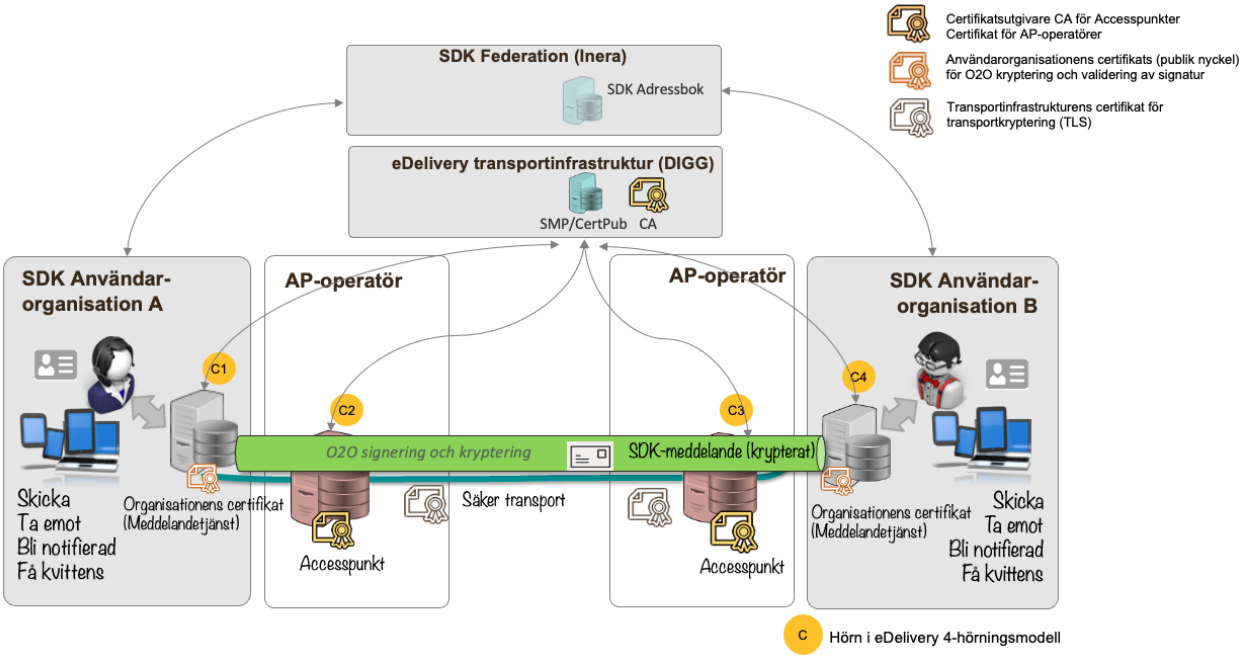
1.3.2 O2O-kryptering och signering

SDK tillämpar O2O-kryptering och signering för säker meddelandeöverföring mellan användarorganisationer.

Meddelanden som skickas inom SDK ska signeras och krypteras mellan Meddelandetjänst hos sändande respektive mottagande användarorganisation. Respektive användarorganisations Meddelandetjänst

ansvarar för att signera, kryptera, validera signatur och dekryptera meddelande. Detta innebär bland annat att Meddelandetjänst paketerar meddelandet enligt ’DIGG eDelivery kuverteringsprofil XHE’[4].

Användarorganisationens certifikat för kryptering och signering tillgängliggörs genom slagning mot DIGGs Certifikatspubliceringstjänst.



Figur 2 – Översikt säkerhetsmekanismer i SDK

2. Krav på skydd vid meddelandeöverföring

2.1 Generella kryptografiska krav samt säkerhetsprotokoll

För att skydda informationen vid meddelandeöverföring ställs krav på kryptering, signering och autentisering. Olika metoder används beroende på säkerhetsområde och vilket hörn i fyrhörningsmodellen som hanterar meddelandet.

Val av säkerhetsprotokoll, algoritmer och nyckellängder ska följa ”best practice guidelines”.

I praktiken innebär detta att för skydd av information vid meddelandeöverföring gäller nedanstående säkerhetsprotokoll, algoritmer och nyckellängder, vilka är de senast gällande vid tidpunkt för denna version av IT-säkerhetsbilagan.

Äldre säkerhetsprotokoll och algoritmer, som ej anses säkra[1], **SKA INTE** tillåtas.

2.2 Säkerhet i eDelivery transportinfrastruktur – skydd mellan accesspunkter

Säkerställer konfidentialitet och riktighet mellan accesspunkter (säkerhet i eDelivery transportinfrastruktur). Den som ansvarar för accesspunkten kallas för Accesspunktsoperatör och måste genomföra tester och godkännas av DIGG för att kunna delta och agera i SDK-federationen. Både offentliga aktörer och privata tjänsteleverantörer kan bli godkända som Accesspunktsoperatörer.

För att ansluta till SDK-federationen **ska** användarorganisationen använda sig av DIGG plattformsgodkänd accesspunktsoperatör. Detta innebär bl.a. krav på tillåtna säkerhetsprotokoll för transportkryptering, säkerhetsprotokoll för meddelandekryptering mellan accesspunkter, krypteringsalgoritmer och nyckellängder samt godkänd certifikatsutgivare.

I denna it-säkerhetsbilaga regleras de tilläggskrav som gäller för SDK.

2.2.1 Tillåtna säkerhetsprotokoll för transportkryptering

[1] Enligt ”Best practice guidelines”, t.ex. från följande källor:
Inera ”Tekniska anvisningar – Kryptering”
FMV CSEC – ”188 Scheme Crypto Policy SP-188”
NIST ”SP 800–131A Rev. 2”
ENISA – ”Algorithms, key sizes and parameters report”

Utöver DIGGs plattformsgodkännande för Accesspunktsoperatör gäller följande tillägg:

- Endast acceptera för SDK specificerade certifikatsutgivare (CA)
- Tillämpa autentiseringsmetod enligt SDKs specifikation
- Använda för SDK specificerade kommunikationsportar för SSL/TLS

Tillägg specificeras på tjänsten Säker digital kommunikations öppna informationsyta under Mer om tjänsten – Regelverk – Informationssäkerhet [5].

2.3 Certifikat för O2O-kryptering och signering av meddelanden – skydd vid meddelandeöverföring mellan användarorganisationer

Säkerställer konfidentialitet och riktighet mellan användarorganisationer (O2O-kryptering och signering).

Här gäller följande krav:

- Meddelandekryptering och signering enligt ’DIGG eDelivery – Transportmodell Utökad BAS’[3]

2.3.1 Krav på certifikat och nyckellängder

Krav på certifikat och nyckellängder enligt avsnitt ”2.4.2 Krav på krypteringsalgoritmer och nyckellängder”.

Anskaffande och förnyelsehantering:

- Användarorganisationen ansvarar för att vid var tid ha ett giltigt certifikat.
- Användarorganisationen ansvarar för att anskaffa certifikat samt registrera certifikatets publika nyckel i DIGGs Certifikatspubliceringstjänst enligt rutiner som anvisas av SDK-federationsoperatör.
- Användarorganisationen ansvarar för att vid byte av certifikat utan dröjsmål meddela SDK-federationsoperatör och uppdatera i DIGGs Certifikatspubliceringstjänst enligt rutiner som anvisas av SDK-federationsoperatör.

Kontroll av certifikatens giltighet vid meddelandeutbyte:

- Användarorganisationen ansvarar för att kontrollera certifikatens giltighet vid kryptering och dekryptering av meddelanden samt validering av signatur.
    - Certifikatens giltighet ska kontrolleras mot DIGGs Certifikatspubliceringstjänst enligt ’DIGG eDelivery – Certifikatspublicering – REST-bindning till SMP’[6]
    - Spärrhantering / revokeringskontroll ska göras enligt ’DIGG eDelivery – Kuverteringsprofil XHE’[4]

2.3.2 Godkända certifikatsutgivare (CA)

Godkända certifikatsutgivare är tills vidare:

- SITHS[7] e-id funktionscertifikat (Inera)
- E-identitet för offentlig sektor - Efos [8] (Försäkringskassan)
- ExpiTrust EID CA V4[9] (tidigare Steria AB e-Tjänstelegitimationer Kort CA v2 hos Expisoft AB)

2.3.3 Konfigurering av tillit till godkända CAs

Giltig signerad metadata i DIGGs Certifikatspubliceringstjänst utgör grund för tillit till certifikat.

Detta innebär att kontroll av tillit till godkända certifikatsutgivare ej bör tillämpas.

2.4 Inre säkerhet – skydd mellan anslutande system och accesspunkt

Säkerställer konfidentialitet och riktighet mellan anslutande system och accesspunkt (inre säkerhet).

Här gäller följande krav:

- Transportkryptering **och flerfaktorsautentisering av anslutande system.**
- Information kan hanteras okrypterat och konsumerande anslutna system behöver inte autentiseras i följande fall:
    - Inom en för användarorganisationen isolerad serverhall **eller** låst serverutrymme där ingen server eller nätverkskomponent delas med någon annan part, kan information inom en tjänst hanteras och transporteras okrypterad.
    - Inom dedikerade switchar i en väl skyddad miljö kan trafik transporteras okrypterad.

2.4.1 Tillåtna säkerhetsprotokoll för transportkryptering

- **TLS** version **1.2** eller nyare.
- **IPsec**, **ESP** i Tunnel mode, med **IKEv2** (Internet Key Exchange) med **RSA/DSS**.

2.4.2 Krav på krypteringsalgoritmer och nyckellängder

Asymmetriska nycklar:

- **RSA** - Nyckellängd 3072 bitar eller mer (RSA-OAEP)
- **ECDSA** - För elliptiska kurvor rekommenderar NIST ECDSA Curve P-256 alternativt P-384 dvs. 256 eller 384 bitars kryptografiska elliptiska kurvor.

Symmetriska nycklar och hashfunktioner:

- **AES** - Nyckellängd 128 bitar eller mer (AES-128-GCM, AES-256-GCM)
- **SHA-2** - 256 bitar eller mer (SHA-256)

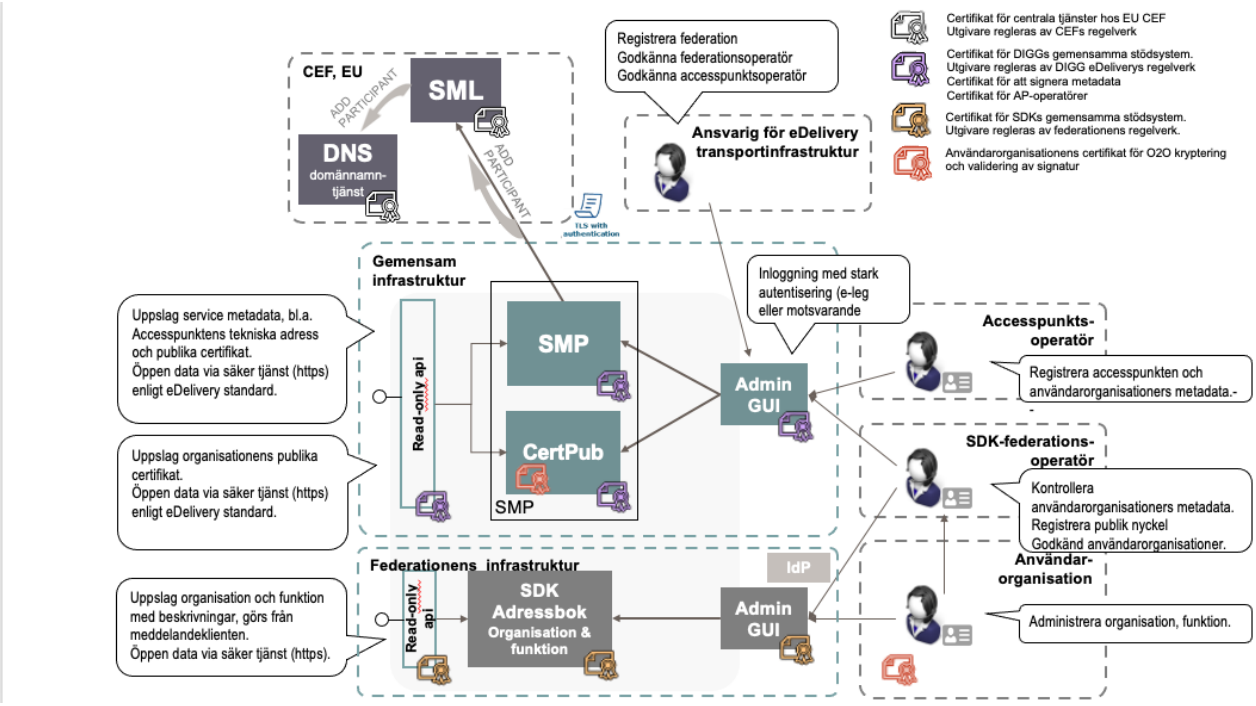
2.4.3 Krav på certifikat för TLS och IPSec

Certifikaten ska vara enligt standarden X.509[2]

[2] https://en.wikipedia.org/wiki/X.509

3. Krav på skydd vid kommunikation med gemensamma komponenter

Kapitlet beskriver den säkerhet som krävs avseende konfidentialitet och riktighet vid administration och sökning av deltagande organisationer och metadata i gemensamma komponenter.



Figur 3 - Säkerhet vid administration och sökning av deltagande organisationer och metadata

3.1 eDelivery transportinfrastrukturs gemensamma komponenter

Säkerställer konfidentialitet och riktighet vid administration och sökning av deltagande organisationer och metadata i gemensamma komponenter hos DIGG (se Figur 3).

Detta omfattar:

- Skydd mellan administratör och SMP-tjänsten
- Skydd mellan accesspunkt och SMP-tjänsten
- Skydd mellan SMP- och SML-tjänsten
- Skydd mellan administratör och Certifikatspubliceringstjänsten

- Skydd mellan anslutet system och Certifikatspubliceringstjänsten

För närmare beskrivning av krav, se DIGGs Tjänstebeskrivningar för respektive komponent[10].

3.2 SDKs gemensamma komponenter

3.2.1 Skydd mellan administratör och SDK Adressbok

Säkerställer konfidentialitet och riktighet mellan användarorganisations administratör och SDK Adressbok (se Figur 3), genom att:

- Administratör ska autentiseras enligt de metoder som godkänns enligt kvalitetsmärket Svensk e-legitimation hos DIGG[11]

3.2.2 Skydd mellan anslutande system och SDK Adressbok

Säkerställer konfidentialitet och riktighet mellan anslutande system och SDK Adressbok (se Figur 3).

Om anslutande system använder SDK Adressboks API för direktsökning eller skapar en lokal läskopia av SDK Adressbok ska:

- Transportkryptering tillämpas enligt generella krav på protokoll och krypteringsalgoritmer, se kapitel 2.1.
- För att vidmakthålla hög aktualitet i lokal läskopia behöver denna uppdateras flera gånger per dygn. Detta innebär att lokal läskopia ska uppdateras minst var 12:e timme men inte oftare än var 4:e timme.

3.2.3 Rekommendation vid ändring av funktionsadress

En funktionsadress bör inte återanvändas för ett annat syfte. Detta för att undvika risk för felaktig adressering.

4. Teknisk säkerhet

Kapitlet beskriver den säkerhet som krävs avseende loggning för felsökning samt tidssynkronisering i lokala komponenter.

4.1 Felsökning

Loggning i eDelivery transportinfrastruktur regleras av DIGGs Accesspunktsoperatör - Gemensamma Regler och Rutiner[12] som anger krav på loggning i avsändande respektive mottagande AP-funktioner.

Därutöver ska loggar för meddelandeöverföring via SDK innefatta:

- SDK Dokumenttyp
- Kommunicerande parters nätverksadresser
- Meddelandets identitet (meddelande-id)
- Meddelande-id i eDelivery transportinfrastruktur (AS4 Message ID)

En användarorganisation ska logga vilken SDK Adressbok (gemensam alt. lokal läskopia) samt vilken AP-operatör/Accesspunkt som används vid meddelandeöverföring samt när meddelande lämnas respektive hämtas i Accesspunkt.

En användarorganisation ska tillse att dess AP-operatör loggar tidpunkt för när meddelande lämnas respektive hämtas i Accesspunkt av användarorganisation.

4.2 Tid

Samtliga datorklockor ska synkroniseras mot tillförlitliga källor, spårbara till världstiden UTC(SP) men minimum UTC. Tidssynkroniseringen ska övervakas kontinuerligt.

5. Referenser

[1] DIGG eDelivery Plattform - Informationssäkerhet och tillitsmodell
Kontakta info@digg.se

[2] DIGG eDelivery definitionslista
Kontakta info@digg.se

[3] DIGG eDelivery – Transportmodell Utökad BAS
Kontakta info@digg.se

[4] DIGG eDelivery Kuverteringsprofil XHE
Kontakta info@digg.se

[5] Inera tjänsten Säker digital kommunikations öppna informationsyta
https://inera.atlassian.net/wiki/spaces/OISDK/pages/2710601964/Informationss+kerhet

[6] DIGG eDelivery – Certifikatspublicering – REST-bindning till SMP
Kontakta info@digg.se

[7] Inera Identifieringstjänster SITHS
https://www.inera.se/tjanster/identifieringstjanst-siths/

[8] E-identitet för offentlig sektor – Efos
https://www.forsakringskassan.se/

[9] ExpiTrust EID CA V4 [10] (tidigare Steria AB e-Tjänstelegitimationer Kort CA v2 hos Expisoft AB) https://www.expisoft.se

[10] DIGG eDelivery Tjänstebeskrivningar
Kontakta info@digg.se

[11] DIGG Svensk e-legitimation
https://www.digg.se/digital-identitet/e-legitimering

[12] DIGG Accesspunktsoperatör - Gemensamma Regler och Rutiner
Kontakta info@digg.se