IT-säkerhetsbilaga

Version 1.3

Till regelverk för anslutning till Säker digital kommunikation - Informationssäkerhet

inera
Ett företag inom SKR

Innehåll

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	2022-02-25	Malin Domeij	Beslutad version 1.0
1.1	2022-06-06	Marco de Luca	- kap.1.3.2, Översiktsbild uppdaterad - kap. 2.4, Transportkryptering refererar ej till kap. 2.1
1.2	2022-11-08	Marco de Luca	- kap. 2.2, Omarbetning, SDK-anslutning förutsätter en plattformsgodkänd accesspunktsoperatör - kap. 2.3.1, Förtydligande gällande krav på certifikat och nyckellängder
1.3	2023-03-22	Marco de Luca	- kap. 1.2, Ordlista utgår med hänvisning till tjänstens informationssida - kap. 2.2, Förtydligat att AP-operatörs AP ska vara plattformsgodkänd och federationsgodkänd - kap. 2.1.1, Krav på krypteringsalgoritmer och nyckellängder, flyttat från 2.2 samt tillåten nivå 128AES utgår - kap. 2.1.2, Tillåtna säkerhetsprotokoll för transportkryptering, flyttat från 2.2 - kap. 2.1.3, Nytt Övergripande krav på certifikat. - kap. 2.2.1, TLS regelverk specificeras i detta dokument (tidigare referens till tjänstens informationssida) - kap. 2.3, O2O-kryptering och signering av meddelanden, omstrukturering och språklig förenkling - kap. 2.4, Inre säkerhet, språklig förenkling - kap. 3.2.1, Skydd mellan administratör och SDK Adressbok, krav regleras i ny version av regelverket, v1.4. - kap. 3.2.3, Rekommendation vid ändring av funktionsadress utgår och flyttas till regelverket - kap. 2.4.2, Krav på certifikat för IPSec utgår och ersätts av krav 2.1.3 generella krav på certifikat. - kap. 4.1, Referens till Diggs specifikation ändrad (Händelselogg)

1. Inledning

1.1 Syfte

Detta är en bilaga till Regelverk för anslutning till Säker digital kommunikation – Informationssäkerhet (hädanefter benämnt Regelverket). Bilagan anger samtliga it-säkerhetskrav för kommunikation inom Säker digital kommunikation (SDK) och syftar till att upprätthålla en lämplig nivå på konfidentialitet och riktighet vid meddelandeöverföring inom SDK.

Eftersom SDK är en tillämpning av eDelivery transportinfrastruktur hos Myndigheten för digital förvaltning (Digg), innehåller bilagan också referenser till säkerhetsmekanismer och krav inom eDelivery transportinfrastruktur (Plattform för eDelivery).

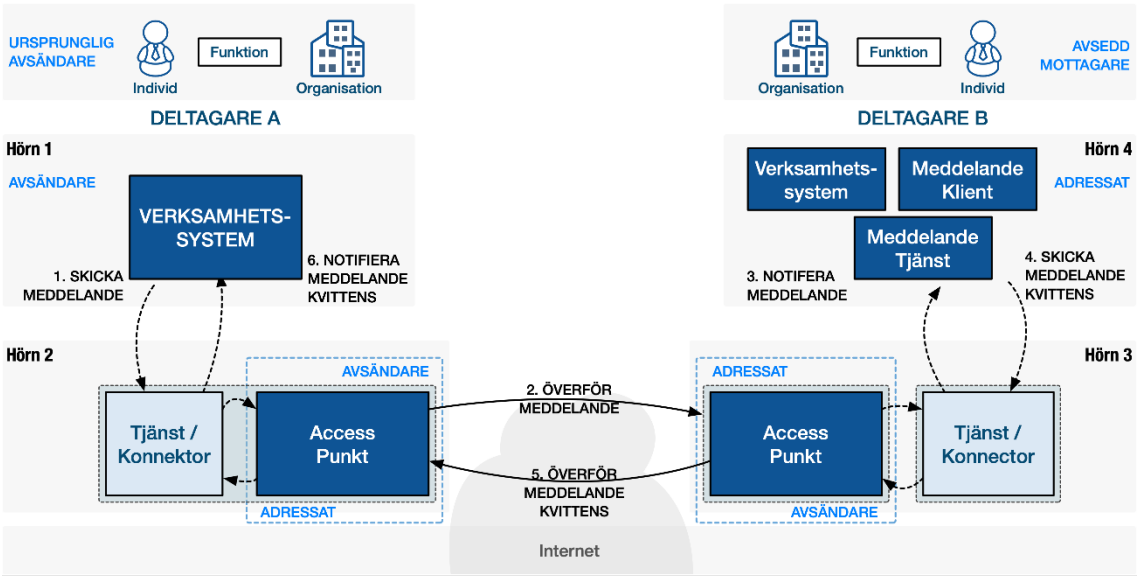
För information om eDelivery transportinfrastrukturs säkerhetsmekanismer hänvisas till ’Diggs Plattform - Informationssäkerhet och tillitsmodell’[1]. Övriga referenser anges löpande i bilagan, för mer information, se ’Diggs Ramverk för Plattform för eDelivery’[2].

1.2 Definitioner

För definitioner, se Ordlista[14] på SDKs öppna informationsyta.

1.3 Bakgrund

SDK 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 användarorganisationers (deltagares) anslutande system, där:

- Hörn 1 är avsändande användarorganisations Meddelandetjänst och Meddelandeklient
- Hörn 4 är mottagande användarorganisations Meddelandetjänst och Meddelandeklient

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

- Hörn 2 (C2) är avsändande användarorganisations Accesspunkt
- Hörn 3 (C3) är mottagande användarorganisations Accesspunkt

För mer information, se ’Diggs Ramverk för Plattform för eDelivery’[2] – 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 samt av SDK-federationsoperatör. För information om eDelivery transport-infrastrukturs säkerhetsmekanismer och skydd mellan accesspunkter, se 'Diggs Informationssäkerhet och tillitsmodell'[1] samt 'Diggs Transportmodell – Utökad Bas'[3]. Se avsnitt 2.2 för tilläggskrav avseende SDK.
O2O-kryptering och signering inom SDK	C1 - C4	Fokuserar på säkerheten vid meddelandeöverföring mellan avsändande användarorganisations anslutna system (C1) och mottagande användarorganisations anslutna system (C4). Se närmare beskrivning i definitioner. Detta område regleras av SDK-federationsoperatör. Se avsnitt 2.3.
Inre säkerhet i lokala komponenter	C1 - C2 samt C3 - C4	Fokuserar på säkerheten vid meddelandeöverföring mellan anslutande system och Accesspunkt hos avsändande och mottagande användarorganisation. Detta område regleras av SDK-federationsoperatör. Se avsnitt 2.4.

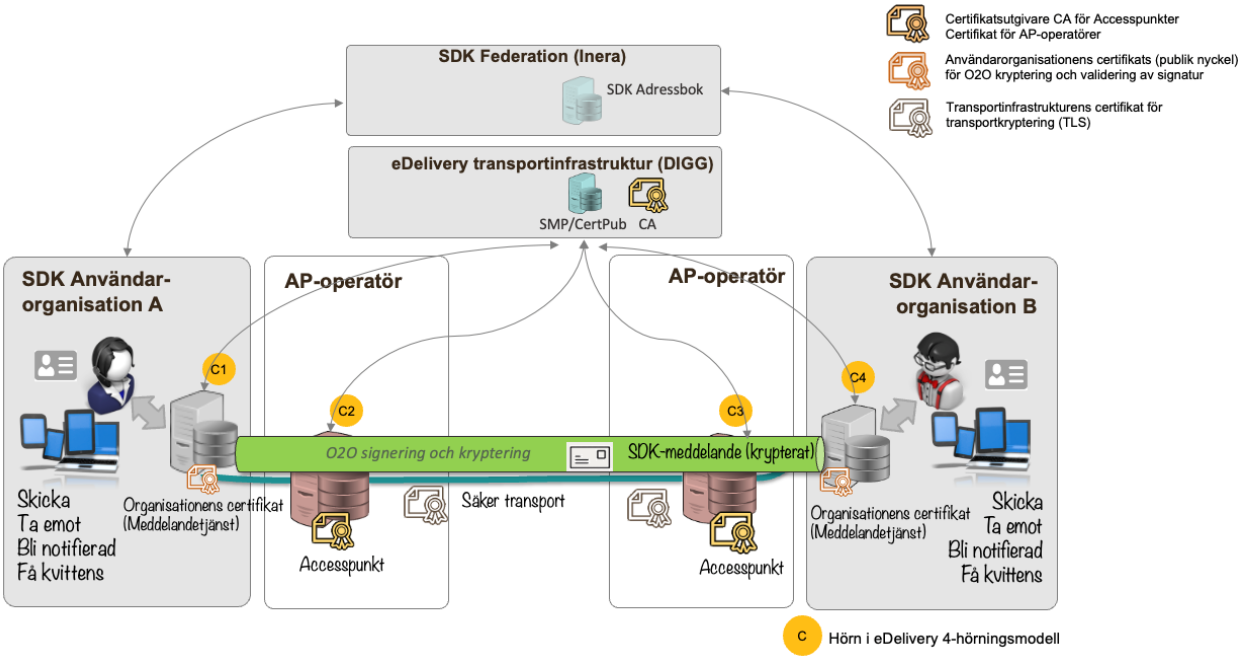
Tabell 1 – Förklaring av säkerhetsområden

1.3.2 O2O-kryptering och signering

SDK tillämpar kryptering och signering för säker meddelandeöverföring mellan användarorganisationer så kallad Organisation-till-Organisation-kryptering (O2O-kryptering).

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 'Diggs 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 krav på krypteringsalgoritmer, säkerhetsprotokoll och certifikat

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 algoritmer, nyckellängder och säkerhetsprotokoll ska följa ”best practice guidelines” [1]. Äldre säkerhetsprotokoll och algoritmer ska **INTE** användas.

I praktiken innebär detta att för skydd av information vid meddelandeöverföring gäller nedanstående algoritmer, nyckellängder, säkerhetsprotokoll och certifikat.

2.1.1 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 256 bitar eller mer (AES-256-GCM)
- **SHA-2** - 256 bitar eller mer (SHA-256)

2.1.2 Tillåtna säkerhetsprotokoll för transportkryptering

- **TLS** version **1.2** eller nyare
- TLS-konfigurationen ska vara åtminstone av ”grade A” enligt SSL Labs gradering

2.1.3 Krav på certifikat

- Samtliga certifikat ska följa standarden X.509[2]

[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”

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

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 i SDK-federationen. Både offentliga aktörer och privata tjänsteleverantörer kan bli godkända som Accesspunktsoperatörer.

För att ansluta till SDK-federationen **ska** användarorganisationen använda en Accesspunktsoperatör som är plattformsgodkänd och federationsgodkänd av Digg. För mer information, se 'Diggs Ramverk för Plattform för eDelivery'[2].

Utöver Diggs godkännande av Accesspunktsoperatör gäller följande anpassningar till de grundregler som specificeras i 'Diggs Transportprofil AS4'[4]', avsnitt 2.4.

2.2.1 Godkända certifikatsutgivare för TLS-trafik, A1

TLS ska användas och endast utgivaren SITHS ska användas.

- Rotcertifikat: SITHS e-id Root CA v2 (2019-05-15 till 2049-09-15)
- Certifikatsutgivare: SITHS e-id Function CA v1

2.2.2 Godkänd autentiseringsmetod, A2

Accesspunktsfunktioner som agerar i eDelivery transportinfrastruktur ska använda "Two-way TLS" baserad på trust till "SITHS e-id Funktion CA v1" (ej enskilda certifikat).

2.3 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 ’Diggs Transportmodell Utökad BAS’[3]

2.3.1 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)

2.3.2 Krav på certifikatshantering

Anskaffande och förnyelsehantering:

- Användarorganisationen ansvarar för att vid var tid ha ett giltigt certifikat.
- Användarorganisationen ansvarar för att 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 ’Diggs Certifikatspublicering – REST-bindning till SMP’[6]
    - Spärrhantering / revokeringskontroll ska göras enligt ’Digg Kuverteringsprofil XHE’[4]

2.3.3 Konfigurering av tillit till godkända certifikatsutgivare (CA)

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

2.4 Inre säkerhet

Säkerställer konfidentialitet och riktighet i användarorganisations inre säkerhet, dvs. inom anslutande system (meddelandetjänst och meddelandeklient) och mellan anslutande system och accesspunkt.

Här gäller följande krav:

- Transportkryptering och flerfaktorsautentisering av anslutande system.
- Information kan hanteras och transporteras 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.
    - Inom dedikerade switchar i en väl skyddad miljö

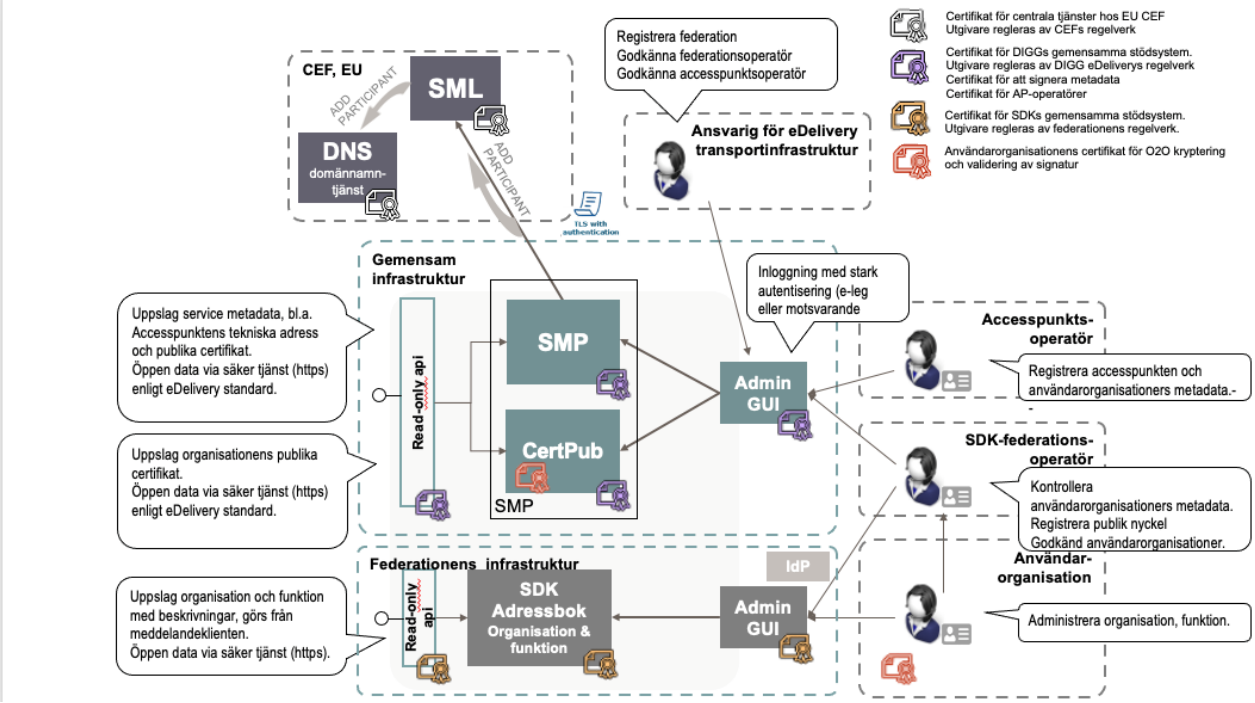
2.4.1 Tillåtna säkerhetsprotokoll för transportkryptering

Utöver TLS enligt avsnitt 2.1.2, tillåts även följande protokoll:

- **IPsec**, **ESP** i Tunnel mode, med **IKEv2** (Internet Key Exchange) med **RSA/DSS**.

3. Krav på skydd vid kommunikation med gemensamma komponenter

Säkerställer 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

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

Detta omfattar:

- Skydd mellan administratör och SDK Adressbok, som regleras i Regelverk för anslutning till SDK - Informationssäkerhet[5]
- Skydd mellan anslutande system och SDK Adressbok (se 3.2.1)

3.2.1 Skydd mellan anslutande system och SDK Adressbok

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

Här gäller följande krav:

- Transportkryptering tillämpas enligt generella krav på protokoll och krypteringsalgoritmer, se kapitel 2.1.

Om anslutande system skapar en lokal läskopia av SDK Adressbok gäller även:

- 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.

4. Teknisk säkerhet

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

4.1 Felsökning

Kraven på loggning i eDelivery transportinfrastruktur (både i avsändande respektive mottagande AP-funktioner) framgår av 'Diggs Accesspunkt – Komponentspecifikation' [13].

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)
- Vilken AP-operatör/Accesspunkt som används
- Tidpunkt när meddelande lämnas respektive hämtas i Accesspunkt

Vid adressering via SDK ska loggar innefatta:

- Vilken SDK Adressbok som används (gemensam alternativt lokal läskopia)

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] Diggs Plattform - Informationssäkerhet och tillitsmodell, info@digg.se

[2] Diggs Ramverk för Plattform för eDelivery, info@digg.se

[3] Diggs Transportmodell Utökad BAS, info@digg.se

[4] Diggs Kuverteringsprofil XHE, info@digg.se

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

[6] Diggs Certifikatspublicering – REST-bindning till SMP, info@digg.se

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

[8] Försäkringskassans 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] Diggs Tjänstebeskrivningar för respektive komponent
Kontakta info@digg.se

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

[12] Diggs Accesspunktsoperatör - Gemensamma Regler och Rutiner, info@digg.se

[13] Diggs Accesspunkt – Komponentspecifikation, info@digg.se

[14] Ineras ordlista med beskrivning av begrepp som används inom eller har beröringspunkter med Säker digital kommunikation. Länk till ordlistan