

Digital transformation genom kommunal samverkan i Föreningen Sambruk >15 år av sambrukande

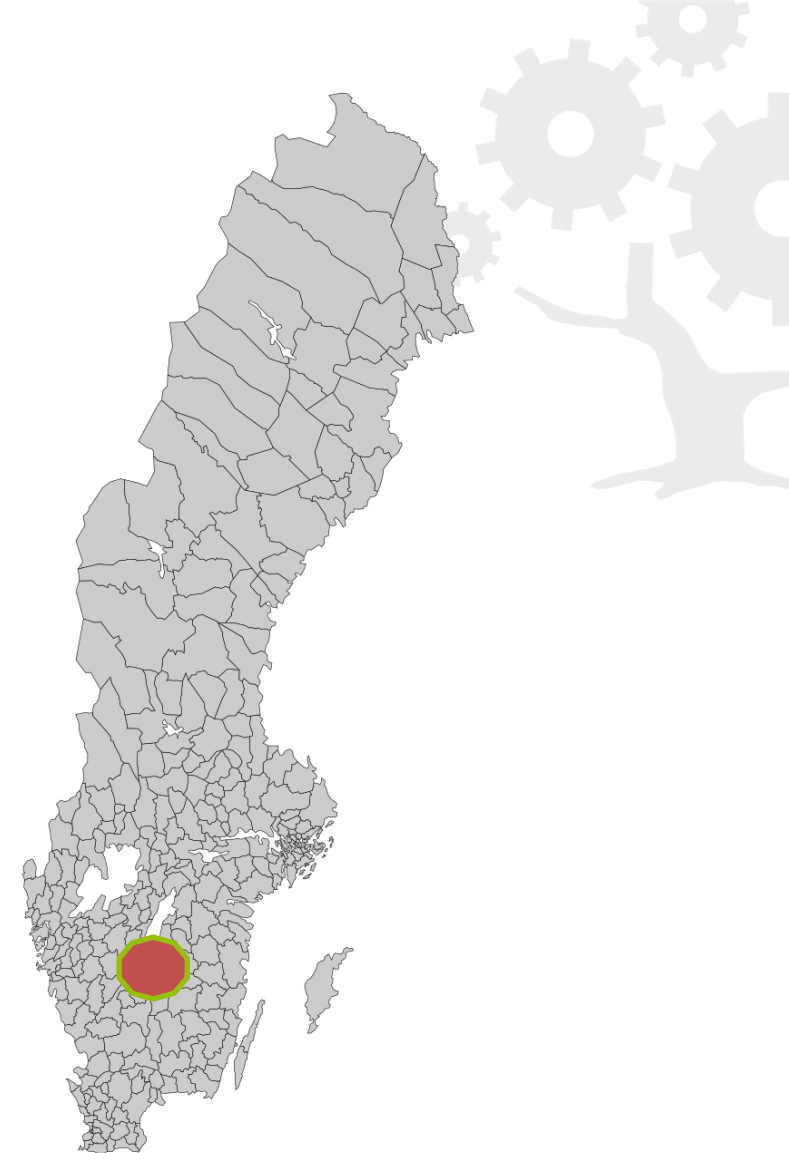


Samarbetsbehov

- 2003 - 10 IT-chefer samlas
- 2005 - Färdiga formerna organisation

Ändamål

- verka för en samverkan kring och effektivisering av de digitala processerna
- främja utvecklingen av en sambruksplattform och av digitalisering
- att ta tillvara medlemmarnas gemensamma intressen vad gäller inre och yttre effektivisering



Av Lokal_Profil, CC BY-SA 2.5, <https://commons.wikimedia.org/w/index.php?curid=1929839>

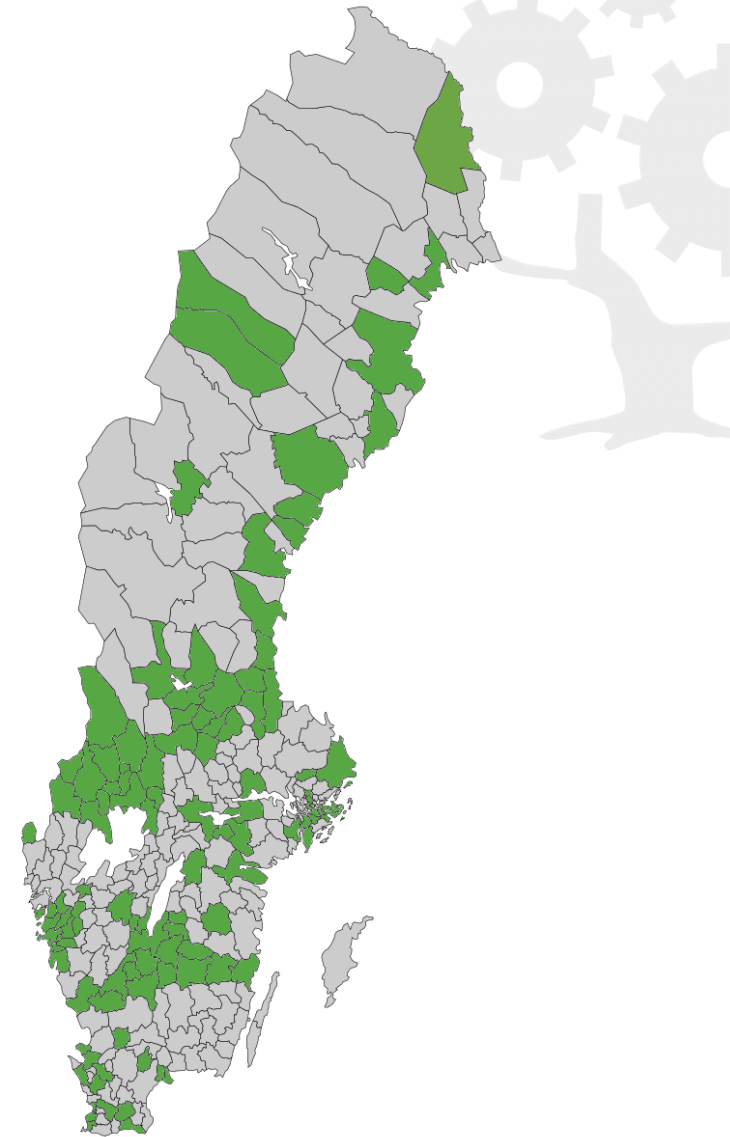
Medlemsorganisation

Ideell förening

- Av kommuner för kommuner
- En dryg tredjedel av kommunerna medlemmar
- Några regioner samt SKR medlemmar
- Mål 2021 – 125 medlemmar

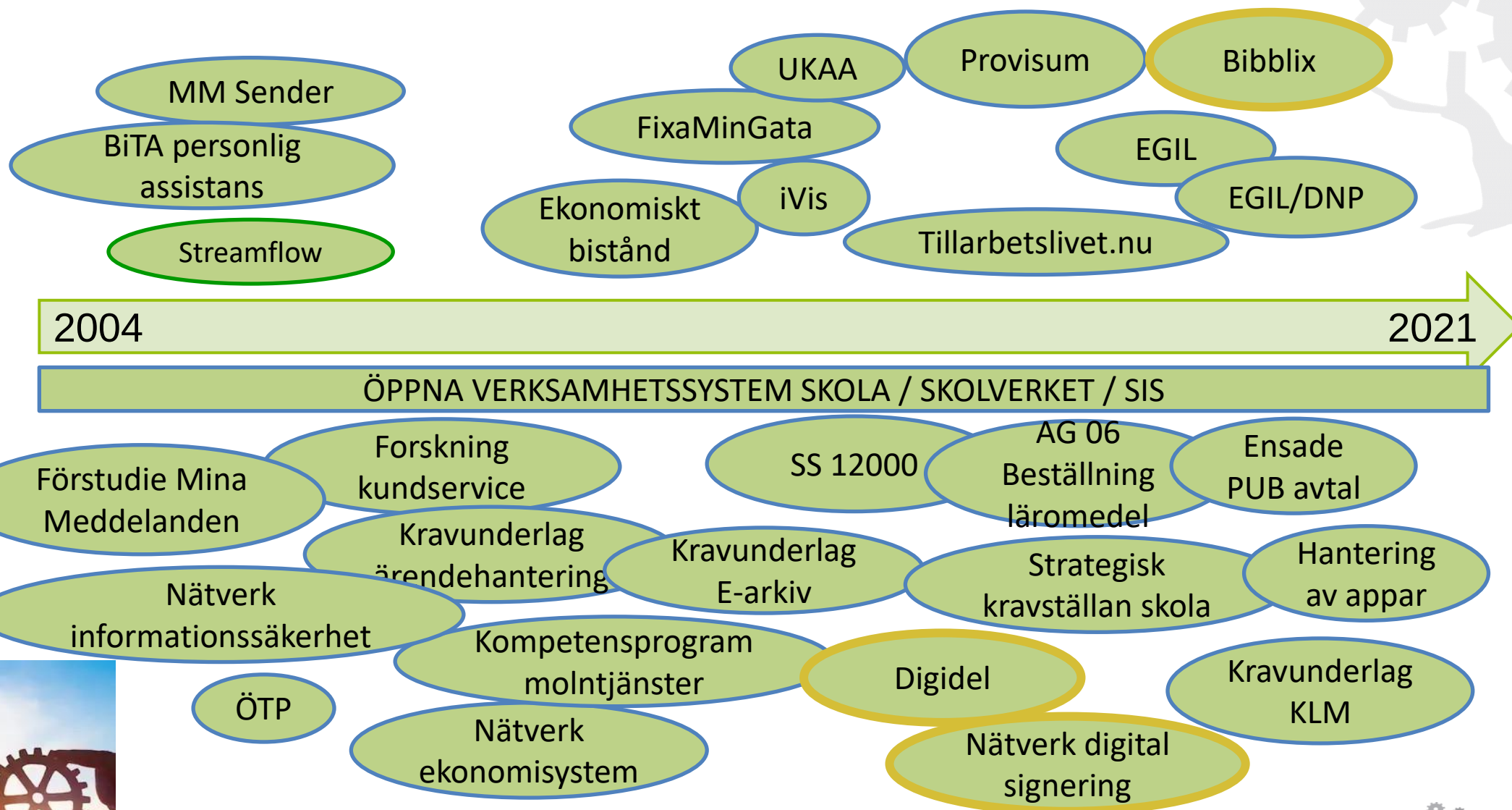
Organiseras

- Fyra egna
- Partners & konsulter
- Forskarmedverkan, UU, LIN, HIS, LLA

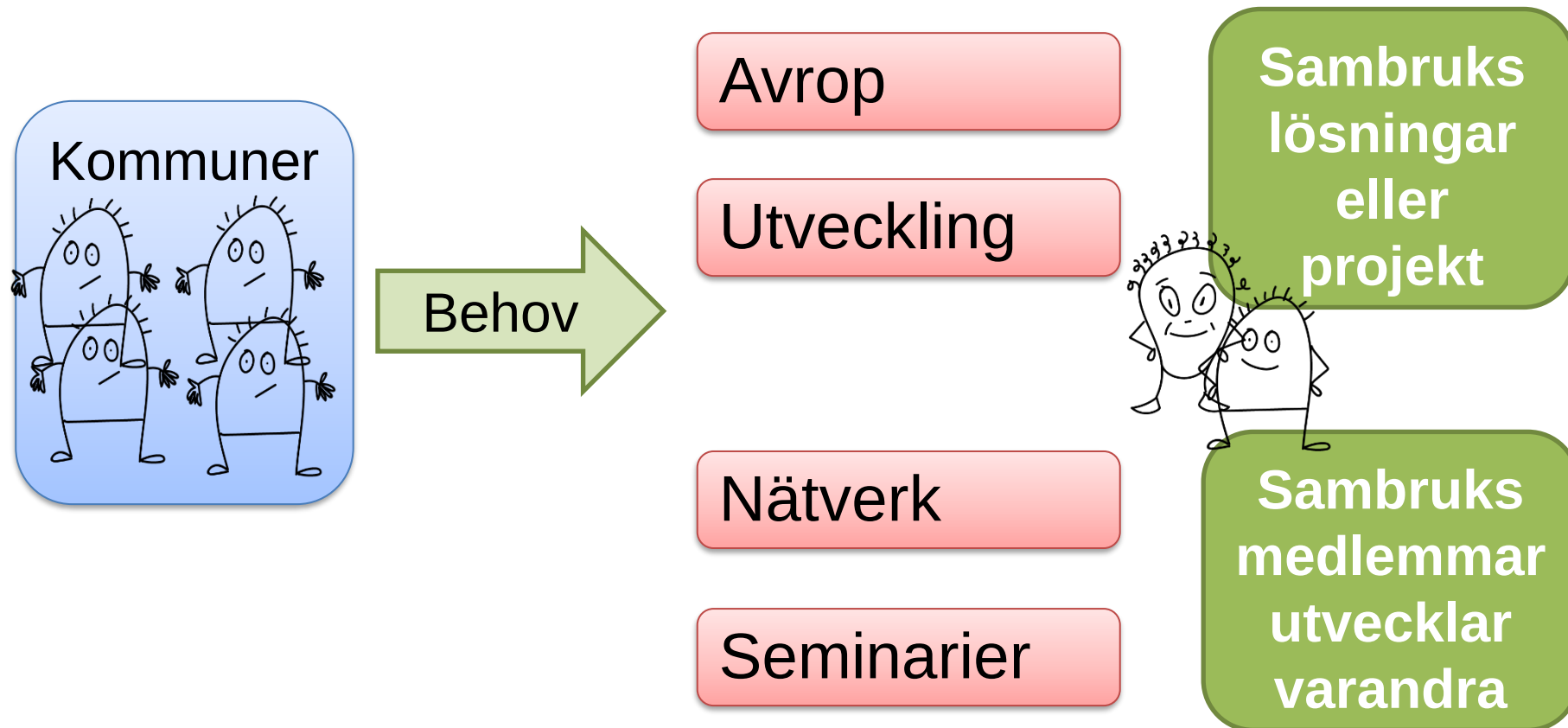


Av Lokal_Profil, CC BY-SA 2.5, <https://commons.wikimedia.org/w/index.php?curid=1929839>

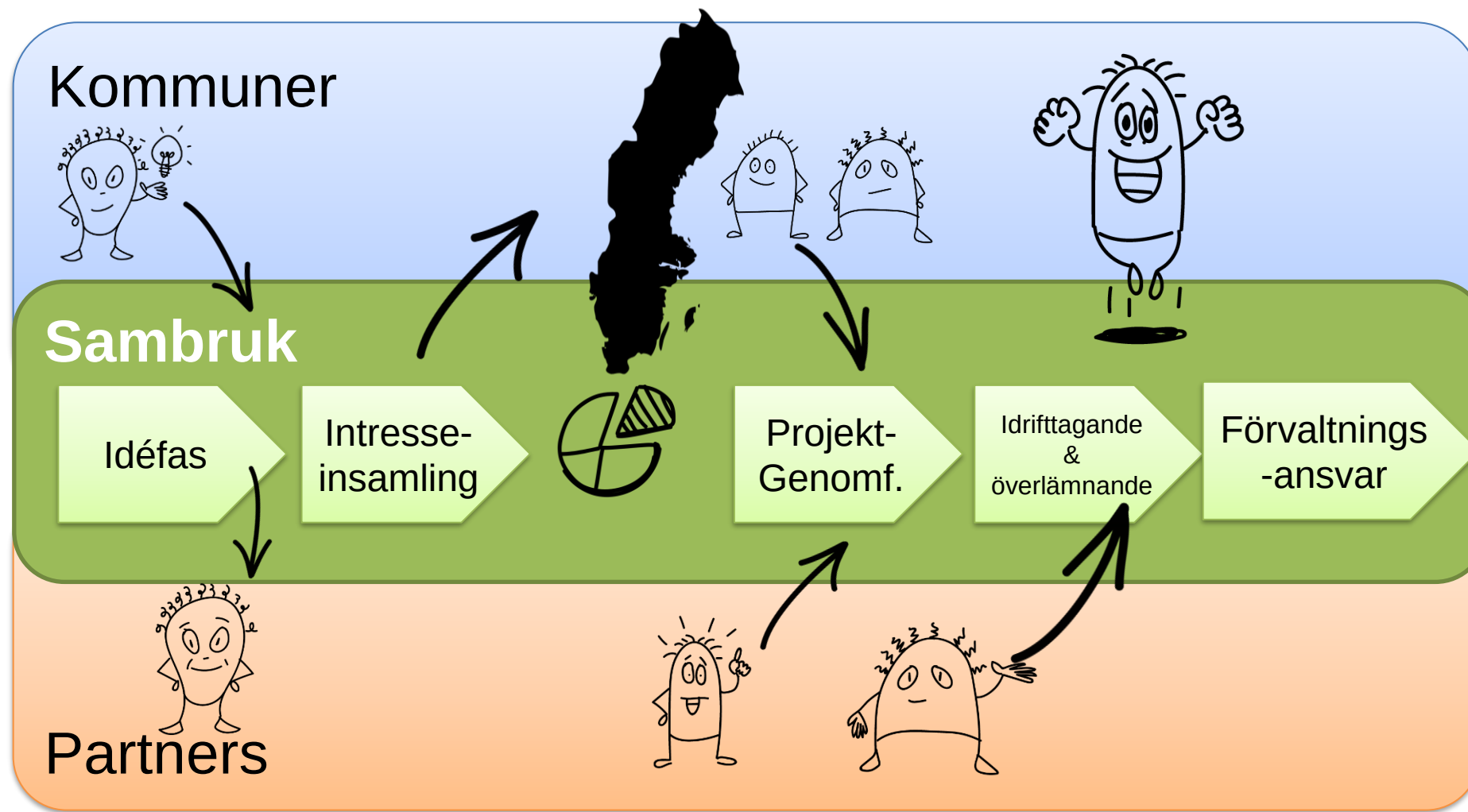
Medlemmarna och Sambruk



Föreningen Sambruk

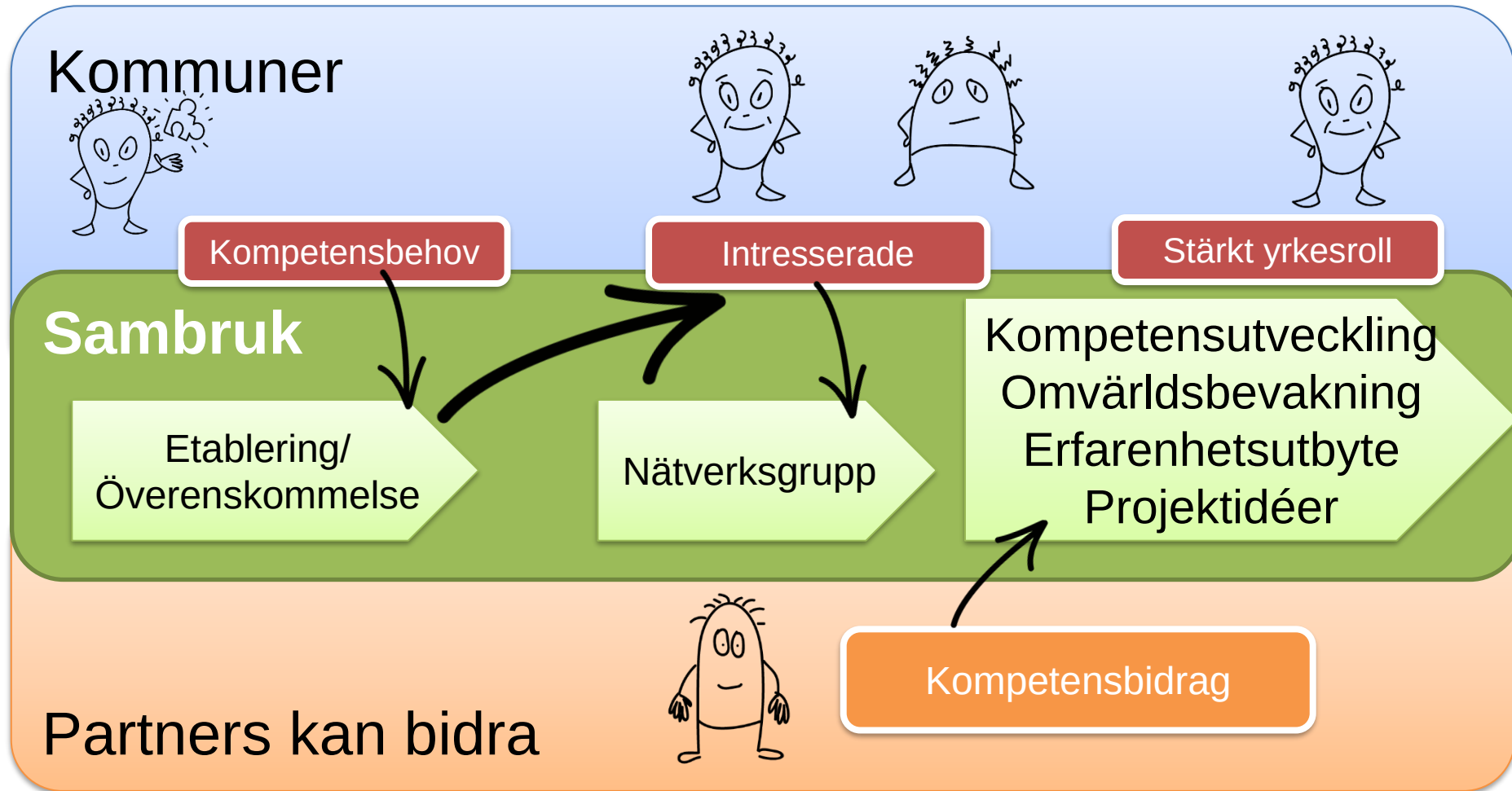


Dela utveckling med andra



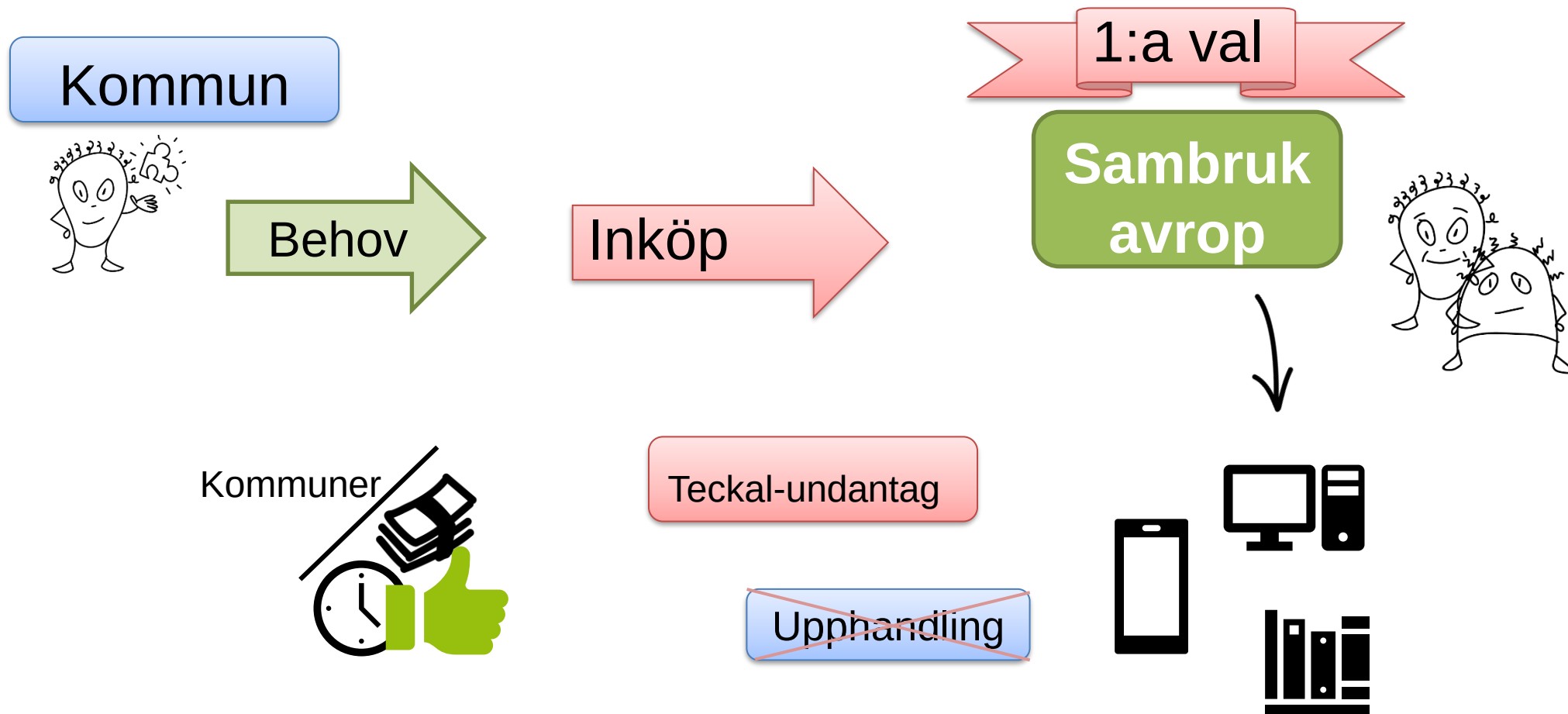
Hållbar användning av skattemedel

Erfarenhetsutbyte



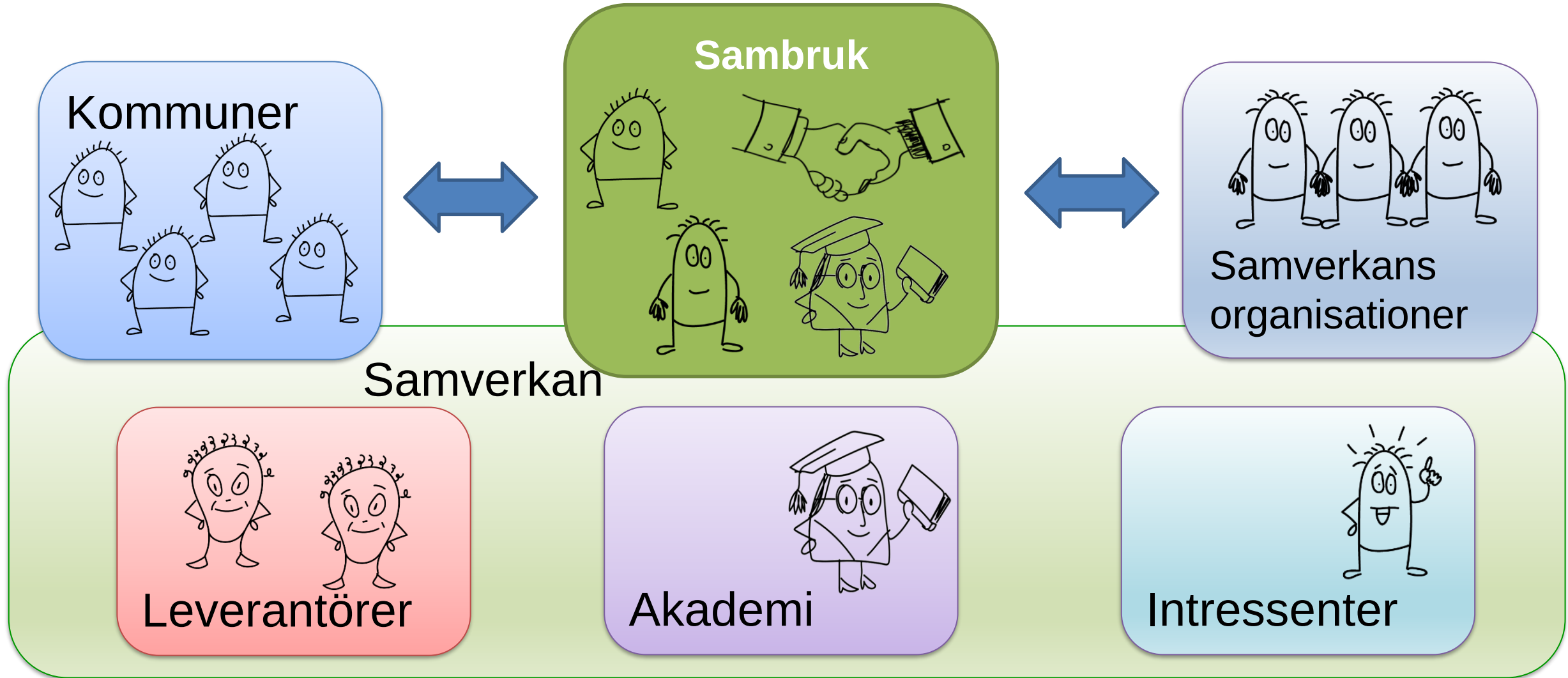
Hållbar användning av skattemedel

Anskaffningsmodell



Hållbar användning av skattemedel

Hållbart samarbete



Föreningen Sambruk tjänster och projekt



Sambruks hållbara samverkansmodell



Digitalisering – i samverkan

- ⇒ Initierar och genomför projekt *tillsammans*
- ⇒ Unik digitalisering baserade på medlemmarnas/medborgarnas *behov*



Portfölj

- Barnbiblioteksapp

→ Bibblix

Skola

- Uppföljningssystem
kommunala aktivitetsansvaret
- Praktisk arbetslivsorientering
(Prao), enkel administration
- Konton till Digitala Nationella
Prov (DNP) och
läromedelsförlag

→ UKA

→ tillarbetslivet.nu

→ EGIL



Portfölj

Stöd och bistånd

➤ Ekonomiskt bistånd

→ Multifråga &

→ eAnsökan-EkBist

➤ Överförmyndare

→ Provisum

→ Valter

Teknisk nämnd

➤ Nationell e-tjänst

→ FixaMinGata.se



Resultat i övrigt

Skola

- Öppen verksamhetsinfo, standards

- Beställningar och Leverans, BoL
- Digitala Lärresursen – SIS AG 06
- Informationsstandard
SS 12000, SIS, & AG 10

Öppen teknisk plattform

- Arkitekturstandard för upphandlingar



Nätverk och projekt

- Skola
 - Strategisk kravställan skola
 - EGIL / DNP
- Digital signering
 - Elektroniska signaturer i kommunal verksamhet
- Digidel
 - Digital inkludering
- Projekt
Kommunala
Lantmäterimyndigheter
 - Fastighetsbildning – projekt för systemstöd



Strategiskt viktigt

➤ Medlemmar

- Skapa relation - involvera och interagera
- Relevant förening
- Fler och fler medlemmar

➤ Projekt och tjänster

- Många som nyttjar befintliga tjänster
- Bra utveckling av befintliga tjänster
- Relevant inflöde av nya projekt och tjänster

➤ Nätverk

- Intressanta och aktuella problemområden
- Intressanta upplägg med talare
- Bra inflöde av nya nätverk



Teckal-undantaget

Undantaget för internupphandling

Teckal-undantag i LoU kan utnyttjas av upphandlande myndighetsenheter för en offentlig upphandling.

Två kriterier måste vara uppfyllda .

- **Kontrollkriteriet** - den upphandlande enheten har kontroll över en juridisk person eller en nämnd som även den har kontroll över sin egen förvaltning.
- **Verksamhetskriteriet** - den eventuella verksamhet som Sambruk utför tillsammans med någon annan än våra medlemmar endast får vara av marginell karaktär.



Sambrukgemensamt Material SGM



Avtalsramverk - SGM

- Forskningssamarbete Linköpings universitet
- Ramverk som reglerar
 - Upphovsrätt & Utveckling
 - Nyttjande & Förvaltning
- SGM tanken att material och digitala tjänster ska
 - vara tillgängligt för alla medlemmar
 - i möjligaste mån följa öppna standarder
- Syftet med SGM är att
 - förhindra att upphovsrätt till material som förvärvas via Sambruk blir proprietär
 - och därmed skapar inlåsnings effekter för användare

Föreningen Sambruk ekonomi



Löpande intäkter

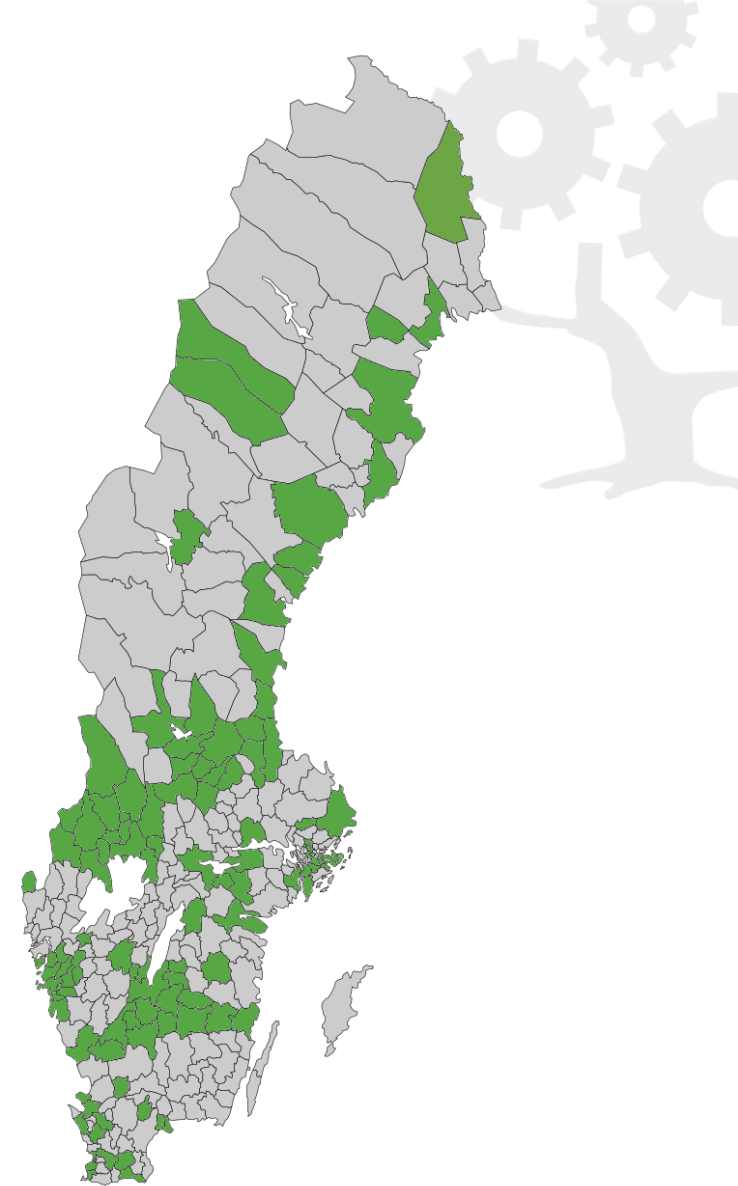
- Medlemsavgifter
- Förvaltningsavgifter
 - Tjänster bör vara självfinansierade
 - Ju fler kommuner som nyttjar en tjänst desto billigare för var och en, styrka och svaghet
- Vidareutveckling av tjänster, beslut
 - Medlemmar i förvaltningsråd, alt lagstiftning
- Projektinvesteringar för nya projekt
 - Medlemmar vänder sig till Sambruk, eller vs
- Projektbidrag
 - Sambruk ansöker tillsammans med medlemmar



Medlemsorganisation

Principer - inflytande

- Stämman beslutar övergripande
- Styrelse löpande styrning
- Löpande kontakt med medlemmar
- Förvaltningsråd beslutar om tjänsternas utveckling
- Styrgrupper beslutar om särskilda projekt



Av Lokal_Profil, CC BY-SA 2.5, <https://commons.wikimedia.org/w/index.php?curid=1929839>



www.sambruk.se

Verkställande tjänsteperson

Britta Sandblom

britta.sandblom@sambruk.se

+46 (0)733 – 415 410

Förvaltningsledare

Ulf Timerdahl

ulf.timerdahl@sambruk.se

+46 (0)

Ordförande

Monika Bubholz

monika.bubholz@karlstad.se

+46 (0)76 – 126 01 02



Alingsås kommun - e-underskrifter i samverkan



KS handlingsplan

- Digital målbild - KF
- Årlig handlingsplan - KS
- 2:a reviderade handlingsplanen
- I I områden



<https://sammantradesportal.alingsas.se/committees/kommunstyrelsen/mote-2020-05-11>

Område 9: Digitalt först

Handlingsplan Digital målbild för Alingsås kommun - öppen och smart 2020-2022

Typ av styrdokument: Handlingsplan
Beslutande instans: Kommunstyrelsen
Datum för beslut: 2020-05-11, § 77
Diarienummer: 2020.036 KS

Gäller för: Kommunövergripande
Giltighetstid: 2020-12-31
Revideras senast: 2020-12-31
Dokumentansvarig: Digitaliseringsansvarig



- På följande områden finns idag digitala underskrifter*
- Nämndsprotokoll
 - Avtal för upphandlade tjänster/varor
 - Samverkansprotokoll
 - Godkännade/underskrift i e-tjänstplattformen

Ensam är inte stark

- November 2018: På möte om e-underskrifter (Kivos & Sambruk) kläcktes **idéen** om ett GEMENSAMT KOMPETENSNÄTVERK
- Februari 2019: Uppstart av nätverk i Mölndal
- I Sambruks regi - **Låga trösklar för samverkan** - inget krav på medlemskap
- Facilitatorer - Annika Samuelsson, Mölndals stad & Göran Westerlund, Alingsås kommun



Göran Westerlund
19 december 2018 - Privat grupp

Vi noterar stark respons på nedanstående inbjudan, som gått ut till seminariedeltagarna som var med den 16:e november. På en dag har mer än tio personer som anmält sig!

"Nätverk för elektroniska underskrifter - vill du vara med?"

Detta mailet riktar sig till dig som var med på Sambruk/Kivos dag om elektroniska underskrifter i Mölndal den 16:e november. Vi bjuder nu in dig till att delta i ett nätverk för att dela erfarenheter och kompetens.

Vi avser att starta upp nätverket i slutet av januari / början av februari 2019.

Vi tror att fokus kommer att ligga på hur vi kan använda elektroniska underskrifter juridiskt och erfarenhet kring tekniska lösningar.

Vår tanke är att vi agerar som en del av Sambruk eller i samverkan med Sambruk. Eftersom vi vet att många av de kommuner som är intresserade idag inte är medlemmar i Sambruk kommer vi att lyfta frågan på Sambruks styrelsemöte den 9:e januari. Men vi vill få in er anmälan nu. Och glädjande nog kan vi konstatera att vi redan har förhandsbesked från fem kommuner som vill delta - Alingsås, Kungsbacka, Lerum, Stenungsund och Mölndal.

Vänliga hälsningar Göran Westerlund / Annika Samuelsson"

Foto: Frode Wendelbo



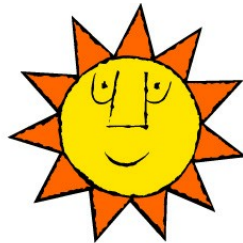
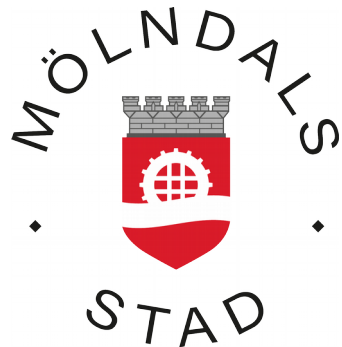
Göran Westerlund
20 februari 2019 - Privat grupp

På det gemensamma Kivos- och Sambruk-mötet i november bestämde vi att starta upp ett nätverk för e-underskrifter i Sambruks regi. Igår gick startskottet i Mölndals stadshus. 25 engagerade deltagare samlades till uppstart. Listan med närvarande kommuner blev lång: Uddevalla, Strömstad, Alingsås, Göteborg, Lerum, Mölndal, Trollhättan, Vänersborg, Kungsbacka Partille, Falköping, Tidaholm, Stenungsund, Lidköping och Tjörn var på plats. Karlskrona är också med i nätverket. Arbetet... Visa mer





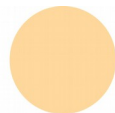
- Få kommuner hade någon praktisk erfarenhet
- Relativt lite nationell vägledning
- E-underskrifter sätter fokus på dokumentets/handlingens livscykel
- Leverantörer sitter på kunskapen



KARLSTADS KOMMUN

Nätverket e-underskrifter - idag 20 kommuner

Boråsregionen
Sjuhärad's kommunalförbund



ÖREBRO



Kungsbacka

FALKÖPING
KOMMUNEN



ALINGSÅS
KOMMUN



Kommunala kompetenser

Strateg

E-arkivarie

IT-chef

Systemutvecklare

Kommunarkivarie

IT-arkitekt

Projektledare

Digitaliseringschef

Verksamhetsutvecklare

Kommunjurist

Digitaliseringsansvarig

IT-controller

Chef IFO

Dataskyddsombud

Kvalitetsutvecklare

Leverantörer

Nexus/Stefan Runneberger

Definitivus/Sven-Håkan Olsson

Högskola



Software Systems Research Group

Alingsås erfarenheter

- Tänk efter före – inventera handlingar & kartlägg behov
- Uppdaterade dokumenthanteringsplaner underlättar
- Fokusera - välj ut några områden
- Men glöm inte dialogen med alla
- Underskrifter av sekretesshandlingar – infoklassning, risk & sårbarhetsanalys och ev. konsekvensbedömning

Alingsås erfarenheter

- Ett (1) system för e-underskrifter i kommunen eller flera system?
Hållbarhet & förvaltning vs flexibilitet
- Vilka tjänster i e-tjänstplattformen? Undertecknade eller bara godkänna?
- Verifiering av signatur
- Ett eller två bevarandeobjekt?
- Livscykel för underskriven handling

Frågor till våra förvaltningar

- Vilka handlingar skriver ni idag under på papper?
- För vilka handlingar av dessa finns legala krav på underskrift?
- Vilka bevarandekrav finns för de handlingar som skrivs under ?

- För vilka av era nuvarande e-tjänster bedömer ni som att det finns legala krav på underskrift ?
- Vilka bevarandekrav finns för dessa e-tjänster?
- För vilka framtida e-tjänster, som kan komma, finns legala krav på underskrift ?
- Och vilka bevarandekrav finns för kommande e-tjänster ?



ALINGSÅS
KOMMUN

Ett urval av svar

- ”De flesta beslut, protokoll och avtal skrivs under på papper idag”
- Delegationsbeslut, anställningsavtal, avtal i samband med bostadsuthyrning, låneavtal digitala verktyg, nämndyttrande vid överklagan, PUB-avtal, närvarolistor nämnd, beslut i elevärenden, faderskap, adoption, vårdnadsumgänge, ordförandebeslut, samtycke fotografering, nybyggnadskarta, årsräkning, anbudsöppning,

- Legala krav på underskrift för utbildningskontrakt, beslut om åtgärdsprogram, djurens hälso- och sjukvård, nämndprotokoll, MBL-protokoll, faderskap, adoption, vårdnadsumgänge, ordförandebeslut,
- Bevarandekrav för nämndprotokoll, faderskap, adoption, vårdnadsumgänge, ordförandebeslut, ...
- E-tjänster som behöver skrivas under: ansökan försörjningstöd, intresseanmälan f-hem, alkohol/tobaks-ansökningar, ...
- Bevarandekrav för e-tjänster som skrivs under: journalhandling
- Inga svar pekar på att planerade nya e-tjänster kräver underskrift
- Inga svar pekar på tydliga bevarandekrav för kommande e-tjänster

e-Arkiv och långtidbevarande

- Kravställa på format - räcker det då med leverantören säger att de klarar det?
- Verifiering av PDF/A-I
- Samarbete med Högskolan i Skövde

Format för bevarande

Elektronisk signering av digitala handlingar ...



... behöver hantera flera olika utmaningar ...

- Organisationer **använder** många **olika programvaror** och **filformat** för att hantera digitala artefakter
- **Supportkontrakt** för proprietär programvara finns att tillgå för en tidsperiod (upp till) **10 år**
- Organisationer behöver skapa, förvalta, återanvända och distribuera **digitala artefakter** samt den programvara som används över flera **decennier**
- Programvara för signering tillgängliggörs genom **lokal installation** eller **som tjänst** (SaaS-lösningar)

Format för bevarande

Filer från verksamhetssystem i fyra kommuner



*... som analyserats med **fyra** oberoende programvaror ...*

Åtta olika PDF-filer (".pdf") från fyra olika kommuner:

- Filer från Kommun A: **Fil #1**, **Fil #2**, **Fil #3**
- Filer från Kommun B: **Fil #4**
- Filer från Kommun C: **Fil #5**, **Fil #6**, **Fil #7**
- Filer från Kommun D: **Fil #8**

Fyra programvaror för analys av huruvida en fil uppfyller PDF/A-1:

- **3-HEIGHTS** (analyserar även de slutna formaten **PDF/A-2** & **PDF/A-3**)
- **callas** pdfaPilot v6.2.256 (analyserar även **PDF/A-2** & **PDF/A-3**)
- **PDFBox** preflight 2.0.19
- **veraPDF** v1.14.8 Greenfield (analyserar även **PDF/A-2** & **PDF/A-3**)

Format för bevarande

Analys av elektroniskt signerade filer

Resultat från analys med *fyra* oberoende programvaror ...



PDF-fil	Programvara ...			
	3-HEIGHTS	callas	PDFBox	veraPDF
#1	EJ PDF/A (PDF 1.5)	EJ PDF/A	EJ PDF/A	EJ PDF/A
#2	EJ PDF/A	PDF/A-1b	PDF/A-1b	PDF/A-1b
#3	EJ PDF/A	PDF/A-1b	PDF/A-1b	PDF/A-1b
#4	EJ PDF/A (PDF 1.7)	EJ PDF/A	EJ PDF/A	EJ PDF/A
#5	EJ PDF/A (PDF 1.7)	EJ PDF/A	EJ PDF/A	EJ PDF/A
#6	PDF/A-2b	PDF/A-2b	?	PDF/A-2b
#7	EJ PDF/A (felaktig PDF/A-3a)	EJ PDF/A	EJ PDF/A	EJ PDF/A
#8	EJ PDF/A (felaktig PDF/A-3a)	EJ PDF/A	EJ PDF/A	EJ PDF/A

Nätverkets erfarenhetsdokumnet

Praktiska erfarenheter kring
e-underskrifter

Sammanställt av
Lena Arvidsson Pape, Trollhättans stad
Lena Lindström, Örebro kommun
Göran Westerlund, Alingsås kommun



- Vad behöver man skriva under
- Olika former av e-underskrift?
- Underskrift av sekretessdokument
- E-arkiv & bevarande
- Vilka projekt har genomförts i kommunerna?
- Olika standarder & rekommendationer
- Summering & referenslista



Tack !



goran.westerlund@alingsas.se

Praktiska erfarenheter kring e-underskrifter

Sammanställt av
Lena Arvidsson Pape
Lena Lindström
Göran Westerlund

Version 1.0
2020.06.23

Innehållsförteckning

1. Bakgrund	5
2. Vad behöver man skriva under	6
2.1. Inventering av handlingar	6
2.2. Kartläggning av behov	6
3. Olika former av elektronisk underskrift?	7
3.1. Elektronisk, avancerad och kvalificerad enligt eIDAS	7
3.1.3. Kvalificerad	8
3.2. Inbäddad, extern eller hybrid	8
3.3. Annan form av elektronisk godkännande	9
3.4. Systemoberoende resultat	9
4. Underskrifter av sekretessdokument	9
5. Distribuera och verifiera underskrivna dokument	10
5.1. Acceptans för elektroniskt underskrivna dokument	10
5.2. Verifiera	10
6. E-arkiv och bevarande av underskrivna handlingar	11
6.1. Bevarandekrav	11
6.2. E-arkiv	11
7. Omvärldsanalys	12
7.1. Vilka projekt har genomförts i kommunerna?	12
7.2. Marknadsanalys	12
7.3. Säker kommunikation	13
7.4. Pågående utredningar	13
8. Olika standarder och rekommendationer att ta hänsyn till	14
8.1. eIDAS	14
8.2. DIGG	14
8.3. Esam	14
8.4. SKL	14
8.5. Konsekvensbedömning (GDPR)	14
9. Summering	15
10. Referenslista	16
Bilaga, uppställning av dokument med krav på signering	17
Dokument med juridiska krav på signering	17
Dokument utan juridiska krav	20

1. Bakgrund

Intresset för elektroniska underskrifter i kommunerna är stort. Därför driver Sambruk ett kompetensnätverk kring e-underskrifter. Nätverkets syfte är att skapa och sprida kunskap och kompetens samt dela erfarenheter från införandeprojekt. Begreppen e-underskrifter/digital signering/digitala underskrifter kan användas simultant men vi har valt att i huvudsak använda begreppet e-underskrifter. Våra erfarenheter har sammanställts i detta dokument som är tillgängligt enligt Creative Commons "CC-BY-SA 4.0" som stimulerar återanvändning och fortsatt öppenhet.

Nätverket som varit igång sedan februari 2019 är öppet för alla landets kommuner. I nätverket finns en mängd kompetenser, däribland kommunjurister, kommunarkivarier, verksamhetsutvecklare, digitaliseringsansvariga, IT-chefer osv. Idag deltar 20 kommuner och kommunförbund – de flesta från Västra Sverige – i nätverket. Nätverket bjuder regelbundet in branschexperter på digital signering som föreläsare och har ett samarbete med akademien, framförallt kring format för underskrivna handlingar där Högskolan i Skövde hjälper till.

Olika digitaliseringsprojekt pågår i kommunerna med fokus på att göra beslutsprocesser snabbare och säkrare. Flera av de deltagande kommunerna har infört e-underskrifter i någon del av verksamheten, i andra pågår införandeprojekt och hos några pågår omvärldsbevakning. Juridik, teknik och ekonomi är ämnesområden som belyses av nätverket. Detta dokument är ett försök att samla ihop våra erfarenheter sedan februari 2019 då nätverket startades.

Vi har sett nya aspekter kring införande av e-underskrifter i takt med fler verksamhetsområden kommer med. Det har också löpande kommit mer vägledning nationellt. Vi tror att detta dokument kan vara en hjälp för de som vill börja med digitala signaturer men vill framhålla att det är en ögonblicksbild år 2020 inom ett område som fortfarande utvecklas.

2. Vad behöver man skriva under

Det finns inget generellt krav på att handlingar som upprättas hos en myndighet ska skrivas under. Det kan däremot finnas regler i vissa lagar, förordningar eller interna styrdokument om undertecknande av handlingar för att säkerställa att upprättade handlingar inte förvanskas och vilken myndighet de härrör från. Bilagan på s. 17-22 innehåller en lista på dokument med juridiska krav på signering följt av en lista på dokument utan juridiska krav på signering men där det kan finnas andra skäl (ex. bevisskäl) till varför en myndighet vill använda sig av signering.

En inventering över vilka handlingar som idag signeras i kommunen och hur de signeras kan vara ett första steg för att komma fram till vilken/vilka lösning(ar) som stämmer överens med kommunens behov. Inventeringen är också till hjälp för att få vetskap om vilka handlingar som skrivs under i onödan.

I vissa fall är det inte aktuellt att den juridiske personen bekräftar handlingens äkthet utan det kan det räcka med en enklare lösning som ett godkännande av handlingens innehåll. I en ansökan i e-tjänst kombineras ofta identifiering med BankID med ett kryss i en bockruta för godkännande av innehållet vilket kan vara tillräckligt i de fall det inte finns lagkrav på underskrift.

2.1. Inventering av handlingar

Förslag på frågeställningar vid inventering:

- Dokumenttyp som skrivs under manuellt?
- Dokumenttyp/e-tjänst som skrivs under elektroniskt?
- Volym av handlingar/e-tjänster, antal eller uppskattning i annan form?
- Vilket lagkrav grundar sig underskriften på?
- Om ej lagkrav, varför skrivs handlingen under?
- Hur signeras handlingen/informationen idag?
- Var förvaras handlingen/informationen?

2.2. Kartläggning av behov

Nedan finns förslag på frågeställningar för en kartläggning av behov vid ett införandeprojekt av e-signeringsverktyg och som underlag för framställning av krav.

- Vilken tillitsnivå krävs/är tillräcklig?
- Vem är signatär (tjänsteman/roll/organisation)?
- Kommer sekretessuppgifter att hanteras?
- Hur ska handlingens äkthet verifieras?
- Var ska handlingen/informationen förvaras?
- Vilka bevarandekrav finns?

3. Olika former av elektronisk underskrift?

Det finns flera olika former av elektroniska underskrifter och definitionerna låter ibland snarlika. Nedan ska vi försöka förtydliga skillnaderna. Förutom definitioner av själva signaturen så finns även en skillnad i tekniken för lösningarna. Många lösningar på marknaden använder samma tjänst för identifiering och signering och detta avråder DIGG ifrån. De rekommenderar istället en fristående underskriftstjänst dvs en lösning som om BankID används för identifiering använder en annan tjänst för själva signeringen. Detta kallas en fristående tjänst.

3.1. Elektronisk, avancerad och kvalificerad enligt eIDAS

I eIDAS förordningen nämns tre olika nivåer av underskrifter nämligen elektronisk, avancerad och kvalificerad. Det finns även fler sätt att definiera, kategorisera eller beskriva elektroniska underskrifter som är bra att känna till.

I dagsläget finns det dock ingen skillnad på olika benämningar såsom e-signatur, digital signatur, elektronisk signatur m fl utan man behöver titta snäppet djupare för att veta vilken sorts signatur som avses.

3.1.1. Elektronisk underskrift

Elektronisk underskrift definieras inte i någon större utsträckning i eIDAS-förordningen utan används mer som ett samlingsbegrepp. Dock står klart och tydligt att "En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter." vilket kan tolkas att detta gäller för alla former av elektronisk underskrift oavsett om den uppfyller kraven för avancerad eller kvalificerad underskrift.

3.1.2. Avancerad

Enligt eIDAS ska en avancerad elektronisk underskrift uppfylla vissa krav nämligen; den ska vara unikt knuten till undertecknaren; undertecknaren ska kunna identifieras genom den; den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll och slutligen den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Detta lämnar dock utrymme för tolkning och många tjänster beskriver att de framställer avancerade signaturer. Det finns dock ingen lista över verifierade tjänster för avancerad signatur och heller inte tillsyn av dessa.

3.1.3. Kvalificerad

En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift enligt eIDAS. För att skapa en kvalificerad underskrift krävs en certifierad anordning samt kvalificerade certifikat. Det finns idag inga instanser i Sverige som har krav på kvalificerad underskrift och det finns bara en leverantör av kvalificerade certifikat. Dock ingen leverantör som erbjuder en e-tjänst för kvalificerade underskrifter.

3.2. Inbäddad, extern eller hybrid

Förutom eIDAS indelning av underskrifter i en form av tillitsnivåer finns det även en mer teknisk skillnad i e-underskrifter relaterad till hur signeringsinformationen sparas.

3.2.1. Inbäddad signatur

För en inbäddad signatur bäddas relevant information in i metadata för den PDF som signeras. Det innebär att även efter signeringen finns bara en fil och i denna fil finns information om vilka som signerat och när. Detta sparas i metadata för filen som skickats för signering men som vid exempelvis en utskrift ser oförändrad ut.

Även information om de certifikat som används för signering sparas och kan användas vid validering av dokumentet även långt efter skapandet om filen uppfyller de rekommendationer som finns gällande Pades och LTV som tagits fram av ETSI. Standarden stödjer eIDAS och rekommenderas av DIGG.

3.2.2. Extern signatur

För en extern signatur sparas signeringsinformationen i en separat XML-fil. Förutom information om vem som signerat finns i denna filinformation som verifierar giltigheten i själva signeringen av hashsumman dvs låsningen av filen som säkerställer att den inte ändrats eller påverkats. Denna information är inte vare sig lättläst eller lättförståelig. Det ska gå att verifiera signaturerna med hjälp av något ganska generellt kodverktyg men det är inget vi i gruppen kan och således inte heller enkelt för gemene man.

En risk vi sett med externa signaturer är också att när man skickar ut den signerade handlingen bifogar man inte XML-filen och då omöjliggörs en verifiering. I de flesta fall den en extern signatur används tillfogas en sida till originaldokumentet där en förteckning över vem som signerat och när tillsammans med någon form av referensnummer. Denna är inte juridiskt giltig och dessutom lätt att kopiera som exempelvis bild för att klistra in på ett annat dokument och ge sken av att också det är signerat. Detta i kombination med att XML-filen inte bifogas vid distribution gör att du får en signatur som ser pålitlig ut men som mycket väl kan vara förfalskad.

För oss är det också lite oklart om certifikat används vid denna form av signatur och om det då kan sparas med i dokumentet. Att signaturen ska skapas med certifikat krävs för att det ska vara en avancerad signatur enligt eIDAS.

3.2.3. Hybrid

Flera lösningar som uppges skapa en avancerad signatur enligt eIDAS använder båda lösningarna ovan för att på ett enkelt sätt åstadkomma en troligen juridiskt giltig signatur som troligen uppfyller kraven för avancerad signatur. Detta görs genom att de som ska granska och signera dokumentet gör det via exempelvis BankID eller annan tjänst som skapar en extern signatur, sedan skapas en samlings-PDF av originaldokumentet, signeringsinformation i text eller dokumentform samt XML-filen. Denna samlings-PDF signeras sedan med ett certifikat som sedan kan valideras i exempelvis Adobe Reader. Notera dock att det som då valideras av Adobe Reader är inte de individer som signerat handlingen utan det certifikat som använts för att signera samlings-PDFen.

Frågan om denna lösning verkligen uppfyller kravet för avancerad signatur med tanke på certifikat är lyft till regeringskansliets utredning om bland annat e-signering.

3.3. Annan form av elektronisk godkännande

I de fall man ur en juridisk aspekt inte behöver en signatur men verksamheten ändå upplever ett behov av en signatur kan man istället utgå ifrån vilket syfte signaturen har. Om det exempelvis ska signalera en överenskommelse mellan vårdnadshavare och skola kan detta troligen uppnås via en e-tjänst där vårdnadshavaren loggar in och kryssar i en ruta för att godkänna något. Då finns likväl en koppling till individen och ett tydligt dokumenterat ställningstagande. Detta är dock varken enkelt att distribuera eller arkivera vilket troligen heller inte är nödvändigt.

Värt att notera är också att vi idag redan bekräftar överenskommelser på flera olika sätt utifrån skiftande behov såsom muntlig överenskommelse, handslag, underskrift eller bevitnad underskrift. Vi bör därför försöka undvika att tro att vi kan ersätta alla dessa nivåer med en form av elektronisk underskrift som fyller alla behov.

3.4. Systemberoende resultat

Oavsett hur e-underskriften framställs och sparas är det också viktigt att säkerställa att den kan läsas och verifieras utan ett beroende till leverantören. Förutom verksamheten som äger dokumentet så ska även en mottagare kunna verifiera underskrifterna med den informationen som den fått.

4. Underskrifter av sekretessdokument

Det finns flera aspekter att tänka på vid e-signering av sekretessdokument. Sekretess regleras i Offentlighet och sekretesslagen (OSL), exempel på andra tillämpliga lagutrymmen kan vara Patientdatalagen (PDL), Socialtjänstlagen (SoL) och Skollagen. Hantering av personuppgifter i allmänhet och känsliga personuppgifter i synnerhet regleras i GDPR.

I samband med att signering av sekretessklassade handlingar införs bör en risk- och sårbarhetsanalys göras. Även en konsekvensbedömning enligt GDPR kan vara aktuell. Kriteriet för när man bör göra en sådan är "om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter".

Inför signering av sekretessdokument kan följande frågor vara bra att fundera på; Lämnar dokumentet myndigheten? Var kommer data att behandlas? Under vilken jurisdiktion? Värt att notera är att även om servrar står i Sverige kan tjänsten lyda under annat lands lagstiftning beroende på ägandeskap. Fundera även på vilka eventuella underleverantörer som anlitas och var har de sin verksamhet och juridiska hemvist.

Vad vi känner till så bygger många (kanske de flesta) underskriftslösningarna på att data/dokumentet skickas till leverantören av signeringstjänsten när underskrift ska göras och lagras där för kortare eller längre tid. Det är också vanligt att det underskrivna dokumentet mailas till signatärerna eller att det finns tillgängligt för nedladdning via en länk. Båda dessa alternativ innebär en risk för att sekretessklassade uppgifter kommer på villovägar.

DIGG rekommenderar en lösning där dokumentet inte lämnar den egna organisationen.

Några kommunerna i nätverket har infört e-signering av ordförandebeslut för Socialnämnden exempelvis vid LVU-beslut där e-signering förenklar den administrativa rutinen och undviker onödig fördröjning av beslutet.

5. Distribuera och verifiera underskrivna dokument

5.1. Acceptans för elektroniskt underskrivna dokument

Acceptans för e-underskrivna beslut ökar, Bolagsverket och domstolar är exempel på det. Statens institutionsstyrelse (SiS) är en myndighet som i dagsläget inte tar emot e-underskrivna beslut.

5.2. Verifiera

För dokument med inbäddad signering kan programvara användas för verifiering exempelvis Acrobat Reader. Dock stödjer Adobe en begränsad mängd certifikat initialt. Detta kan vara problematisk då utgivaren flaggas som okänd om certifikatet inte finns bland de betrodda. Man kan dock lägga till fler certifikatutgivare i listan eller välja att lita till de som Windows litar på (vilket iofs inte rekommenderas av Adobe). Acrobat Reader visar också tydligt om något förändrats i dokumentet efter signering eller om något certifikat inte är giltigt vid signeringstillfället.

DIGG rekommenderar att man har certifikat från en betrodd utgivare. De har dock inte en sammanställning över vilka dessa skulle kunna vara. För kvalificerade certifikat finns en lista kopplat till eIDAS och där finns Trustweaver som enda svensk leverantör - de är nu uppköpta av Sovos som främst fokuserar på fakturahantering men kan vara möjlig att teckna avtal med om det gäller 100 000 signaturer eller fler per år.

En variant som ofta ses är en textruta på sista sidan i det undertecknade dokumentet där det kan stå digital signatur, dag och klockslag, samt namn på undertecknare: Detta för att underskriften ska upplevas som mer lättillgänglig. Det är dock ingen juridiskt giltig underskrift utan bara information som måste verifieras.

Även här behöver aspekten med system- och leverantöroberoende verifiering tas med.

6. E-arkiv och bevarande av underskrivna handlingar

6.1. Bevarandekrav

Dokument omfattas av olika krav gällande bevarande. Detta regleras för varje kommun i arkiveringsplanen. Det kan också styras av OSL eller specifik lagstiftning som bokföringslagen. I de fall handlingar ska bevaras behöver de arkiveras. Eftersom e-underskrifter finns i elektronisk form som inte lämpar sig för utskrift betyder detta att dessa handlingar behöver arkiveras i ett e-arkiv.

6.2. E-arkiv

I nätverket e-signerar flera kommuner nämndprotokoll. Bevarandekraven på politiska protokoll är att de ska bevaras för alltid och de behöver föras över till ett e-arkiv. Vissa tjänster för e-underskrifter renderar två filer – originaldokumentet plus en fil med den digitala signaturen dvs en extern signatur. Dessa bör man fundera på hur man ska hantera, förslagsvis igenom att använda ett bevarandeobjekt för både filerna eller genom att koppla samman filerna med hjälp av ett dokumenthanteringssystem.

E-tjänstplattformar erbjuder ofta extern signatur. Men enligt vår erfarenhet är det undantagsvis att transaktioner och data i e-tjänstplattformar behöver slutarkiveras. De torde gallras i sin livscykel i ett tidigare skede eller föras över till ett verksamhetssystem. Exempel på e-tjänster där digital signatur används är ansökan om ersättning för förtroendevalda, bygglovsärenden, ansökan om VA-anslutning, registrera livsmedelsverksamhet, ansökan om plats i skola och i vissa fall används signeringen även av en extern part (inte den som har initierat ärendet) som skall intyga något och i vissa fall vill man försäkra sig om att båda vårdnadshavarna godkänner en ansökan.

Avtal mellan kommun och leverantör som resultat av en genomförd LOU-upphandling kan skrivas under elektroniskt. Gällande att ekonomiska verifikationer fastställer bokföringslagen att de ska sparas i 7 år men det är oklart vad som gäller för avtal som skulle kunna behövas bevaras längre än så. I detta sammanhanget kan framhållas att möjligheter till export av data från e-tjänstplattform och e-upphandlingstjänst bör finnas för att möjliggöra framtida byte av plattform eller för lagring i ett mellanarkiv. När det gäller hyresavtal etc som kan löpa över lång tid torde kraven på bevarande vara omfattande. Kartläggning av bevarandekrav pågår i flera kommuner.

Dokumenthanteringsplaner i kommunerna är styrande för hantering av dokumenten och arkiveringsplanen för bevarandet. Det kan vara aktuellt att se över dessa utifrån ovanstående.

6.2.1. Dokumentformat

Det är viktigt är att de undertecknade dokumenten skapas med ett arkivsäkert dokumentformat, PDF/A-1, samt att de uppfyller standard för dokument innehållande elektronisk signatur exempelvis Pades. Ska signaturen kunna valideras bör de också uppfylla standarden för långtidsvalidering LTV, (se ETSIs standard. ETSI EN 319 142-1).

Nätverket har haft hjälp av forskare från Högskolan i Skövde för att analysera om de PDF:er som signeras i kommunerna är PDF/A-1. Fyra av varandra oberoende programvaror har använts för verifikation. Av hittills åtta testade filer från olika system och olika kommuner så är resultatet relativt nedslående. Som bäst indikerade tre validatorer två av filerna som PDF/A-1. Övriga var

olika varianter av PDF som inte uppfyllde kraven för PDF/A-1. Den senaste sammanställningen återfinns i referenslistan nedan. Vill man kunna verifiera att de signerade dokumenten uppfyller Pades kan man kontrollera det med ett verktyg som tillhandahålls av ETSI, se referenslista. Detta verktyg kontrollerar dock varken giltigheten på signaturen eller certifikatkedjan.

7. Omvärldsanalys

7.1. Vilka projekt har genomförts i kommunerna?

Många av kommunerna i nätverket har börjat med e-underskrivna protokoll från de kommunala nämnderna, kommunstyrelsen och kommunfullmäktige. Protokoll från samverkansgrupper som ska undertecknas av fackliga företrädare och arbetsgivare är ofta närbesläktade och kan ofta hanteras i samma systemlösning.

Flera kommuner är också intresserade av underskrift av avtal efter upphandling av produkt eller tjänst enligt LOU. Tidsbesparing torde vara betydande i förhållande till att det är en större mängd avtal som hanteras och att en del är flerpartsignering. Här finns en del integrerade lösningar dvs upphandlingssystem som erbjuder e-signering som en del av samma system. En annan möjlighet är att integrera med en annan signeringstjänst via API:er men ingen i nätverket har någon erfarenhet av en sådan sammankoppling.

Några kommuner har också infört signering av ordförandebeslut i Socialnämnden och socialjouren (exempelvis omedelbart omhändertagande enligt LVU - Lagen om vård av unga).

Även i e-tjänstplattformar kan underskrifter förekomma men i de flesta e-tjänster räcker det med godkännande. Det kan krävas Bank-ID för ett sådant godkännande men ofta räcker det med att kryssa i en ja-ruta när man redan har loggat in med Bank-ID.

Vissa kommuner är tveksamma till om en enda underskriftstjänst i kommunen som olika system anropar är möjlig av olika integrationstekniska skäl. Det är därför inte orealistiskt att tro att kommuner kommer välja att ha flera underskriftstjänster men att det bör vara så få som möjligt för att minimera förvaltningkostnader.

Ett ökat intresse visas för underskrift av anställningsbevis. Vi har inte funnit några lagkrav kring underskriften men många arbetstagare vill troligen först ha ett undertecknat nytt anställningsavtal innan man avslutar sin pågående anställning. Huruvida underskrifter behövs för timanställda eller om det då kan räcka med ett godkännande i en e-tjänst återstår att se.

Andra utvecklingsområden som kommuner tittar på är politikerarvoden och närvaro för politiker på nämndmöten

7.2. Marknadsanalys

Under våren 2019 gjorde en arbetsgrupp i nätverket en marknadsanalys som redovisades i nätverket. Den består i dels en analys av funktioner och dels genomlysning av leverantörernas prisbild. De leverantörer som granskades var

- Signature Service CGI
- SignPort Cybercom (Chas)
- Public Document Signing Tieto

- Nexus Go PDF Signing,
- ProSale Signing Comfact
- Visma Addo.

Under 2019 upplevdes marknaden som ganska ny och delvis omogen - både sett till funktion och prisbild. En kommun som var tidigt ute beskrev att de upplevde att kostnaden blev högre än tänkt för e-underskriftsplattformen och man därför planerade att konkurrensutsätta inför fortsatt utveckling.

7.3. Säker kommunikation

Idag pågår Ineras projekt Säker Digital Kommunikation (SDK) med målet att skapa en säker infrastruktur mellan kommuner och myndigheter. Det finns även tjänster på marknaden för säker kommunikation. Möjligheter till två-faktors-autentisering, behörighetsstyrning och kvalificerad kryptering av kommunikationen bör finnas.

Säker kommunikation är en viktig fråga oavsett om man använder en extern underskriftstjänst eller om den är lokaliserad till kommunens nätverk. Digitalt underskrivna dokument innehållande sekretess kan behöva skickas mellan olika instanser och huvudmän (domstolar mfl).

7.4. Pågående utredningar

7.4.1. Regeringskansliet

Regeringen gav i den 12 mars 2020 en särskild utredare i uppdrag att utreda "Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen" och redovisa senast detta den 30 december 2020. Med betrodda tjänster avses bland annat e-underskrifter och e-legitimation. Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används. I utredarens uppdrag ingår att kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster men också lämna förslag till åtgärder. Utredaren ska tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas, hur elektroniska underskrifter ska kunna valideras och bevaras samt hur kunna använda e-legitimation i tjänsten.

7.4.2. Riksarkivet

Hos Riksarkivet pågår projektet FormatE som ska "kontextualisera grundprinciper för val av format i föreskrifter, vägledningar, och information som förbättrar förutsättningarna för val, framställning, återgivning, och kontroll av format i [ett visst tekniskt] skick, samt vid tillsyn, rådgivning och överföring till bevarande". Nätverket är referensgrupp till FormatE.

8. Olika standarder och rekommendationer att ta hänsyn till

8.1. eIDAS

Den lagstiftning som i huvudsak styr e-underskrifter är EUs eIDAS förordning dvs "Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden". I denna definieras olika nivåer av underskrifter (se punkt 3.1) och att ingen får neka en elektronisk underskrift bara för att den är elektronisk (avsnitt 4, kapitel 25). Dessutom regleras kvalificerad underskrift i detalj i en bilaga till förordningen. Länk till förordningen finns i referenslistan. I eIDAS förordningen eller snarare i frågor och svar kopplat till den finns också hänvisningar till en ETSI standard för dokumentformat och för certifikat för signering.

8.2. DIGG

Digitaliseringsmyndigheten är den svenska myndighet som har ansvar för e-legitimationer och elektroniska underskrifter av enklare form än kvalificerad. De har en mängd rekommendationer på sin webbplats, indelade efter i vilken roll du söker information om e-underskrift. Sidorna om e-underskrift är inte helt enkla att hitta via webbplatsen men länk finns i referenslistan.

8.3. Esam

Det finns också en vägledning från esam med titeln "Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1". Den är på en mer teoretisk nivå om aspekter att ta hänsyn till men är bra att ta med för att belysa att det är en fråga som bör inkludera exempelvis juridik och informationssäkerhet vid ett införande i en organisation. Bakom den stod eSam, e-legitimationsnämnden och MSB. Länk finns i referenslistan.

8.4. SKL

Redan 2011 gjorde dåvarande SKL en rapport till vägledning vid införande av e-tjänster där elektronisk underskrift finns med. Den kommer troligen uppdateras vilket behövs men den är trots sin ålder läsvärd. Länk finns i referenslistan.

8.5. Riksarkivet

Även riksarkivet har skrivit om e-underskrifter, bland annat 2014 i sin rapport "Framställning och bevarande av elektroniska signaturer". Länk finns i referenslistan.

8.6. Konsekvensbedömning (GDPR)

För stöd om när en konsekvensbedömning ska göras finns en förteckning hos datainspektionen. Länk finns i referenslistan

9. Summering

Området är i växande. Starta enkelt, börja i det lilla formatet. E-underskrifter eller digital signatur är i första hand ingen IT-fråga utan en verksamhetsfråga se därför till att ni har med er verksamheten. Undersök om det finns lagliga krav på underskrift. Betänk att när man går från pappersunderskrift till digital hantering så kanske det räcker med ett godkännande. Var medveten att det finns en kostnad för varje underskrift. Ha koll på om underskriven handling ska till e-arkiv. Fundera på hur avancerad signatur just ni behöver och granska er tänkta lösning noga!

10. Referenslista

eIDAS

<https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0910&from=SV>
https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.00.00_20/en_31914201_v010000a.pdf

DIGG

<https://www.digg.se/digital-identitet/e-underskrift>
<https://elegnamnden.se/eunderskrift/eunderskriftitjansten/valideraochbevaraeunderskrifterochstampar.4.4498694515fe27cdbc1b0.html>
<https://www.elegnamnden.se/juridikochteknik/tekniskakravdokumentochstandarder.4.4498694515fe27cdbc120b.html>

Esam

<http://esamverka.se/stod-och-vagledning/stod-och-vagledning-hos-andra-aktorer/juridisk-vagledning-for-e-legitimering-och-e-underskrifter.html>
<http://esamverka.se/download/18.9d698431645a14fcab34974/1530793977619/eSam%20-%20V%C3%A4gledning%20E-legitimation%20och%20E-underskrift%201.1.pdf>
<http://esamverka.se/stod-och-vagledning/stod-och-vagledning-hos-andra-aktorer/juridisk-vagledning-for-e-legitimering-och-e-underskrifter.html>

SKL

https://bcc-production-attachments-us-west-1.s3-us-west-1.amazonaws.com/72c73ee2-5f18-11ea-b0f6-0242ac110002?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAS5PME4CTVEEQXIYT%2F20200609%2Fus-west-1%2Fs3%2Faws4_request&X-Amz-Date=20200609T233650Z&X-Amz-Expires=3600&X-Amz-Signature=e451aeb0c4c729c185dd293bda8126e65268028d1d65eb295cbdaf0d300d5ac&X-Amz-SignedHeaders=Host&response-content-disposition=inline%3B%20filename%3D%22Rapport%20till%20v%25C3%25A4gledning%20vid%20inf%25C3%25B6randet%20av%20e-tj%25C3%25A4nster.pdf%22&response-content-type=application%2Fpdf

Riksarkivet

https://riksarkivet.se/Media/pdf-filer/doi-t/framställning-och-bevarande-av-elektroniska-signaturer_v1.3_pub-20141007.mso03-ar10.doc.a1a.pdf

GDPR

<https://www.datainspektionen.se/lagar--regler/dataskyddsförordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/>

Högskolan i Skövde

<https://www.kivos.se/bevarandeformat-for-digital-signerade-dokument-uppdatering/>

Bilaga, uppställning av dokument med krav på signering

Denna bilaga har utgått från SKR:s "Rapport till vägledning vid införandet av e-tjänster" från 2011 och Boråsregionens "Vägledning elektroniska underskrifter" från 2019.

Undersökning har gjorts huruvida användande av elektronisk rutin juridiskt tolkas idag. Enligt eIDAS-förordningen ((EU) nr 910/2014) får inte en elektronisk underskrift avvisas såvida det inte finns särskilda formkrav som förbjuder det.

Varje organisation behöver dock stämma av denna uppställning med sin egen juridiska funktion då juridik är ett område där lagar tolkas och olika jurister kan ha olika slutsatser.

Dokument med juridiska krav på signering

Upprättade handlingar (och lag som kräver signering)	Signeras av	Kan elektronisk rutin användas?	Beskrivning/förklaring av hantering av signering
Slutbetyg, grundskola/gymnasie skola SKOLFS 2011:157 14 §	Rektor	Nej, handskriven underskrift av rektor krävs.	Handskriven underskrift av rektor krävs. Med underskrift ska ett namnförtydligande ges.
Terminsbetyg grundskola/gymnasie skola SKOLFS 2014:50 18 §	Rektor el. delegerad personal	Nej, handskriven underskrift av rektor/delegerad personal krävs.	Handskriven underskrift av rektor/delegerad personal krävs. Med underskrift ska ett namnförtydligande ges.
Faderskapsbekräftelse 1 kap 4 § föräldrabalken	Medborgare Vittnen Socialnämnd	Nej, inte i dagsläget men ändring av föräldrabalken för möjlighet till elektronisk rutin och borttag av vittnen vid signering har föreslagits. I förslaget ska ändringen träda i kraft 1 januari 2021. ¹	I dagsläget: Skriftlig, bevitnas av två personer; socialnämnden och av modern eller särskilt förordnad vårdnadshavare för barnet. Utredningen <i>Nya regler om faderskap och föräldraskap</i> , SOU 2018:68 lämnar förslag som gör det möjligt att bekräfta faderskap eller föräldraskap elektroniskt inom 14 dagar från barnets födelse. Samma formkrav ska gälla som för en bekräftelse enligt huvudregeln i 1 kap. 4 § FB, med den skillnaden att en elektronisk bekräftelse inte ska godkännas av socialnämnden. En elektronisk bekräftelse ska göras i ett system som tillhandahålls och administreras av Skatteverket. I förslaget ska ändringen träda i kraft 1 januari 2021. ¹
Dokument inom ÖF Föräldrabalken 13 kap:14 §, 15 § (Redovisning av viss egendom)14 kap: 2 §	Förmyndare, god man, förvaltare	Ja	4.4.1. Kontroll av att handlingarna är undertecknade på heder och samvete I föräldrabalken ställer krav på att årsräkningar, sluträkningar och förteckningar ska avges på heder och samvete. Detta innebär att handlingarna antingen måste undertecknas egenhändigt; i original

Upprättade handlingar (och lag som kräver signering)	Signeras av	Kan elektronisk rutin användas?	Beskrivning/förklaring av hantering av signering
(Förteckningar över egendom) 15 § och 18 § (Redovisning av förvalttad egendom)			eller signerad med godkänd e-legitimation, t. ex. mobilt BankID. ²
Omedelbart omhändertagande av barn eller missbrukare	Socialnämnds ordförande	Ja	Vad gäller elektroniska underskrifter har frågan behandlats av JO i ett ärende (JO dnr 742-2018.) ³
Ansökan om fastighetsbildning 4 kap 8 § fastighetsbildningslagen	Sökande eller dennes ombud	Ja	4 kap 8 § En ansökan ska undertecknas eller skrivas under med en elektronisk signering av sökanden eller sökandens ombud.
Köpehandlingar vid köp av fast egendom Jordabalken 4 kap 1 §	Köpare och säljare	Ja	4 kap 1 §: Köp av fast egendom slutes genom upprättande av köpehandling som underskrives av säljaren och köparen. Ett av syftena med kravet på underskrift i 4 kap. 1 § jordabalken är att knyta en person till handlingen. Detta är särskilt viktigt ur bevishänseende. Lantmäteriets bedömning: Elektroniska underskrifter kan mycket väl tjäna syftet med formkravet på underskrift i 4 kap. 1 § jordabalken och är dessutom i huvudsak säkrare och mer lämpliga att använda ur bevishänseende än underskrifter på papper. ⁴
Dokument som kräver firmateckning (Anbud och avtal i upphandling) 12 kap 7 § LOU		Ja	7 § En upphandlande myndighet får kräva att elektroniska anbudsansökningar och anbud ska vara försedda med en sådan avancerad elektronisk underskrift som avses i artikel 3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, i den ursprungliga lydelsen.
Protokoll 5 kap § 61 kommunallagen	Ordförande Justerare Sekreterare	Ja, delvis	Kan enligt dom i Kamrarrätten i Göteborg 2014-09-24, justeras med avancerad elektronisk signatur.
Initiativ om folkomröstning	Medborgare	Vet ej	Initiativet ska vara skriftligt, ange den aktuella frågan samt innehålla initiativtagarnas egenhändiga namnteckningar, uppgifter om när namnteckningarna gjorts, namnförtydliganden, personnummer och uppgift

Upprättade handlingar (och lag som kräver signering)	Signeras av	Kan elektronisk rutin användas?	Beskrivning/förklaring av hantering av signering
8 kap § 2 kommunallagen			om deras adresser.
Anmälan för registrering av livsmedelsanläggning 12 § Livsmedelsverkets föreskrifter om livsmedelshygien	Medborgare	Troligtvis	En anmälan från en juridisk person ska vara undertecknad av behörig företrädare. ⁵

- (2018) *Nya regler om faderskap och föräldraskap*, SOU 2018:68, Stockholm: Elanders Sverige AB, s. 26.
<https://www.regeringen.se/4a4540/contentassets/d655bb3a85b4487196071727fd145ed7/nya-regler-om-faderskap-och-foraldraskap-sou-201868> (Hämtad 2020-03-23).
- (2019) *Nationella riktlinjer för överförmyndare – förordnade ställföreträdarens redovisning*, ISBN 978-91-7281-906-1, s. 20.
<https://www.lansstyrelsen.se/download/18.4dc15f2816a53b76de718d8a/1558360280598/Nationella%20riktlinjer%20f%C3%B6r%20%C3%B6verf%C3%B6rmyndare-f%C3%B6rordnade%20st%C3%A4llf%C3%B6r%C3%A4dare%20redovisning.pdf> (Hämtad 2020-03-23).
- (2020) *LVU Handbok för socialtjänsten*, ISBN 978-91-7555-522-5, s. 105.
<https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/handboken/2020-3-6642.pdf> (Hämtad 2020-05-20).
- (2018) *Fastighetsöverlåtelser i en digital tid*, Dnr 519–2018/565 s. 66.
<https://www.lantmateriet.se/contentassets/50c7b8feec4744e5a0fa2ffaf0ea07ec/fastighetsoverlatelser-i-en-digital-tid.pdf> (Hämtad 2020-03-27).
- (LIVSFS 2005:20) *Livsmedelsverkets föreskrifter om livsmedelshygien*
<https://www.livsmedelsverket.se/globalassets/om-oss/lagstiftning/livsmedelshygien/livsfs-2005-20-kons-2019-6.pdf> (Hämtad 2020-03-26).

Dokument utan juridiska krav

Där andra skäl för att signering eller identifiering finns.

Det bör tilläggas att varje verksamhet bör göra en egen genomlysning över vilka behov som finns för bekräftelse av handlingen och dess efterlevnad. Verksamheten bör också fundera över vilken komplexitet av e-signering som är nödvändig i varje specifikt fall.

Handlingar	Signeras av	Kan elektronisk rutin användas?	Skäl för underskrift
Överklaganden	Sökande	Vet ej	Myndighet kan välja att begära underskrift för att säkerställa vem som överklagar.
Medborgarförslag 8 kap 1 § kommunallagen	Medborgare	Ja	Krav på folkbokföring i kommunen kräver någon form av identifiering eller underskrift från förslagsställaren.
SKOLA OCH BARNOMSORG			
Ansökan om plats, barnomsorg (vid godkännande av plats)	Vårdnadshavare	Ja	Bevisskäl (pga avgiften) och båda vårdnadshavarna bör vara eniga.
Inkomststopp, barnomsorg	Vårdnadshavare	Ja	Bevisskäl (pga avgiften) och båda vårdnadshavarna bör vara eniga.
Uppsägning, barnomsorg	Vårdnadshavare	Ja	Bevisskäl då båda vårdnadshavarna bör vara eniga.
Ansökan om ledighet, grundskola	Vårdnadshavare	Ja	Lämpligt att båda vårdnadshavare är eniga vid längre ledighet
Ansökan om skolskjuts	Vårdnadshavare	Ja	Båda vårdnadshavare bör vara eniga
Inackorderingsbidrag, gymnasieskola	Sökande Vårdnadshavare	Ja	Bevisskäl
INDIVID- OCH FAMILJEOMSORG			
Ansökan om försörjningsstöd	Sökande	Ja	Sekretesskäl, bevisskäl
Ansökan om insatser för kontaktpersoner	Sökande	Ja	Integritetskänsliga uppgifter
VÅRD OCH OMSORG			
Godkännande av vårdplan/vårdplanering	Sökande eller behörig företrädare	Ja	Identifiering: Planen innehåller kända personuppgifter med sekretess. Identifiering nödvändig då ansökan endast kan ske av den som ska erhålla insatsen (eller behörig företrädare).
Ansökan om insats, ex. vid äldreomsorg	Sökande eller behörig företrädare	Ja	Identifiering: En ansökan innehåller kända personuppgifter med sekretess. Identifiering nödvändig då ansökan endast kan ske av den som ska erhålla insatsen (eller behörig företrädare).

Handlingar	Signeras av	Kan elektronisk rutin användas?	Skäl för underskrift
Ansökan om insats, LSS	Sökande eller behörig företrädare	Ja	Identifiering: En ansökan innehåller kända personuppgifter med sekretess. Av informationssäkerhetsskäl krävs EID vid inloggning och kommunikation med sökanden.
Ansökan, bostadsanpassnings bidrag	Sökande med funktionsnedsättning	Ja	Bevisskäl.
Ansökan om färdtjänst	Sökande med funktionsnedsättning	Ja	Bevisskäl.

PLAN- OCH BYGGOMRÅDET, LANTMÄTERI			
Ansökan om bygglov	Sökande	Ja	Bevisskäl. (Krav på skriftlig handling. 9 kap 21 § plan- och bygglagen.)
Ansökan om dispens från strandskydd	Sökande	Ja	Bevisskäl. (Krav på skriftlig handling 23 § (1998:1252) om områdesskydd enligt miljöbalken.)
MILJÖ- OCH HÄLSSKYDD			
Ansökan, gemensam sopbehållare	Innehavare av aktuella fastigheter	Ja	Bevisskäl
Ansökan för tillstånd, hålla vissa djur inom område med detaljplan	Innehavare av djur	Ja	Spårbarhetsskäl Ev. tillståndsplikt finns i lokala hälsoskyddsföreskrifter meddelade med stöd av 39 § förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd. Formkrav finns i 46 § men där sägs inget om underskrift.
Ansökan om dispens och om befrielse avs. sophämtning	Innehavare av fastighet	Ja	Bevisskäl. Kontroll av riktiga uppgifter
Ansökan, befrielse från sophämtning obobodd fastighet	Innehavare av fastighet	Ja	Bevisskäl. Kontroll av oriktiga uppgifter.
Ansökan respektive anmälan om spridning av kemiska bekämpningsmedel	Fastighetsägare Verksamhetsutövare	Ja	Bevisskäl
Underrättelse om driftstörning miljöfarlig verksamhet och hälsoskydd	Verksamhetsutövare	Ja	Beviskrav. Spårbarhet
Ansökan, värmepump	Fastighetsägare Verksamhetsutövare	Ja	Spårbarhetsskäl, skriftlig ansökan (Anmälningsplikt, men kommunen får föreskriva tillståndsplikt, se 17 § förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd. Se även 18 kap 5 § och 22 kap 1 § 1 stycket miljöbalken. Det finns även värmepumpsanläggningar som är anmälningspliktiga C-verksamheter enligt 21 § i förordningen samt bilagan (SNI-kod 40.110)).

Handlingar	Signeras av	Kan elektronisk rutin användas?	Skäl för underskrift
Ansökan, avloppsanordning	Fastighetsägare Verksamhets- utövare	Ja	Spårbarhetsskäl (Samma resonemang beträffande värmepumpar-, I vissa fall anmälan, men även tillståndsplikt.
ÖVRIGT			
Beslut med stöd av delegation (ordförandebeslut och liknande)	Kommundirektör Förvaltningschef Avdelningschef Anställd	Ja	Lämpligt av spårbarhetsskäl.
Beslut om vidaredelegation	Nämnd	Ja	Lämpligt av spårbarhetsskäl.
Skrivelse i revisorernas namn i granskningsarbetet	Ordförande och ytterligare en person som revisorerna utser	Vet ej	Fastlagt i reglemente att skrivelse ska hanteras på detta sätt
Anställningsavtal	Arbetsstagare och arbetsgivare	Ja	Bevisskäl.

Kommunledningskontoret
Förstudierapport

Datum:
2020-10-05

Diarienummer:
KSN-2020-00341

Handläggare:
Annelie Blanck, Robert Reineck, Mattias Prising, Johan Olofsson, Pontus
Baum, Helena Wottle, Marcus Torstensson, Karin Ajaxon och Simon Elfstadius

Version : 1.0

Säkra meddelanden och e-underskrifter

Innehållsförteckning

Sammanfattning och rekommendation	3
Sammanfattning	3
Rekommenderade förändringar	3
Förstudierrapporten	5
Mål och uppdrag	6
Identifierade behov	6
Effektmål	8
E-underskrifter	9
Översikt	9
Nuläget i Uppsala kommun	12
Förslag till lösningsarkitektur	13
Säkra meddelanden	17
Översikt	17
Nuläget i Uppsala kommun	25
Förslag till lösningsarkitektur	27
Dokumenthistorik	29
Bilaga 1 - Referenser	30
Bilaga 2 - Begrepp	31

Sammanfattning och rekommendation

Sammanfattning

Denna förstudierapport är framtagen inom ramen för projektet *Säkra meddelanden och e-underskrifter* och redovisar bland annat behov av säker kommunikation och e-underskrifter, vilka aktörer och processer som berörs samt vilka möjliga lösningar som finns.

Förstudien har lett till rekommendationer kring hur det fortsatta förändringsarbetet med säkra meddelanden och e-underskrifter bör ta form.

Utgångspunkt har varit en analys av behov och effektmål. Ett antal rekommendationer har identifierats:

Förändrat arbetssätt och nya processer.

- De verksamheter som arbetar med säkra meddelanden och e-underskrifter bör redan nu kartlägga aktuella processer, analysera vad som krävs för att processen ska bli helt digital och bedöma när och hur behoven av säkra meddelanden och e-underskrifter behöver omhändertas.
- Objektverksamheten bör skapa förmåga till samverkan mellan verksamhet, objekt och övrig expertis kring frågor inom informationsförvaltning, juridik, arkitektur och säkerhet för att möjliggöra förändrade arbetssätt.

Ny teknik

- Projektet för säkra meddelande och e-underskrifter bör fortsätta med att etablera e-underskrifter och tillhörande stöd i ett objekt.
- Nuvarande lösning för krypterad e-post, och tillhörande stöd för säkra meddelanden, bör omdefinieras och etableras i ett objekt med en eller flera tjänster. Digitaliseringsmyndighetens funktion *Digital post* bör på sikt ingå liksom de lösningar som tas fram via Inera AB via projektet Säker digital kommunikation (SDK). Objektet behöver löpande bevaka utvecklingen av betrodda tjänster för säkra meddelanden.

Viktiga förutsättningar

- Förmågan till *Identitet och åtkomst* bör omgående införlivas i objektverksamhet och ses över med avseende på innehåll och leverans.
- Det fortsatta arbetet med e-tjänsteplattform och integrationsplattform bör även omfatta en djupare analys av beroenden kring lösningar för säkra meddelanden och e-underskrifter.

Rekommenderade förändringar

Förändrat arbetssätt och nya processer

Förstudien pekar på behovet av grundläggande förmågor inom säker digital kommunikation och digitala underskrifter utifrån ett koncernperspektiv. Förmågorna kommer i huvudsak att användas i relationen mellan respektive verksamhet och tillhörande objekt i enlighet med kommunens förvaltningsmodell PM3.

Verksamheterna behöver göra en analys av befintliga processer för att identifiera krav på säkra meddelanden och e-underskrifter. I takt med att objektverksamheten utvecklar sin förmåga att hantera säkra meddelanden och e-underskrifter behöver också stödprocesser skapas för kvalificering och analys av behoven inom verksamheten.

För att medarbetare ska kunna ta till sig och tillämpa de nya arbetssätten behövs förändringsledning, utbildning och goda exempel. Flera parter behöver bidra till detta arbete där även kommunledningskontoret ger stöd i olika former.

Ny teknik

E-underskrifter - genomförande utifrån nuvarande projekt

Fortsättningen på projektet föreslås omfatta leverans av en teknisk och förvaltningsbar lösning för avancerade elektroniska underskrifter för fysiska personer. En koncernövergripande och fristående lösning som baseras på Digitaliseringsmyndighetens (DIGG) ramverk för fristående underskriftstjänst och Ineras referensarkitekturer.

Under arbetets gång har projektet varit i kontakt med flera andra projekt och verksamheter som är i stort behov av tjänst för e-underskrifter. Därför rekommenderas att införande av e-underskrifter påbörjas snarast möjligt för att minimera risken för särlösningar eller interimistiska lösningar.

Vidareutveckla Krypterad e-post till Säkra meddelanden

Krypterad e-postlösning från leverantören Deltagon bör bytas ut till förmån för tjänster och lösningar som följer nationella och internationella standarder, ramverk och rekommendationer. Projektet föreslår att lösningen på sikt byter namn från *Krypterad e-post* till *Säkra meddelanden* för att tydliggöra förmågan och området, där olika former av säkra meddelanden som SDK, Mina meddelanden etc ingår. E-post bör undvikas inom ramen för Säkra meddelanden, på grund av riskerna för felaktig hantering i befintlig lösning. Det är ett arbete som bör ta hänsyn till kommande avropsbara produkter för anslutning till SDK.

Vinsten med att föregå SKL Kommentus upphandling av ramavtal för SDK-produkter bör jämföras med den insats som skulle krävas för en egen upphandling och vad det alternativet medför. Den samverkan projektet har idag med Ineras SDK-projekt bör fortsätta i takt med Uppsala kommuns egen utveckling.

Mina meddelanden - Digital post

Den befintliga lösningen som har testats i pilotverksamhet under ungefär ett års tid inom HR och IT-supporten baseras på öppen källkodprogramvara. Ansvar för programvaran har på senare tid övergått från Skatteverket till DIGG. Lösningen har bevisat sig vara fullgod avseende behovet av att skicka meddelanden till privatpersoner, företag och organisationer. Lösningen, som idag inte är förvaltd, behöver hanteras i objektverksamheten innan användande inom kommun utvidgas. Liksom Skatteverket ger inte heller DIGG någon support på lösningen och projektet föreslår att Uppsala kommun upphandlar en produkt med support för Mina meddelanden men, om ändamålsenligt, även med andra funktioner som behöver ersättas i samband med avvecklingen av nuvarande produkt för krypterad e-post.

Detta bör dock ställas i relation till verksamheternas behov och till utvecklingen av Ineras SDK.

Säker digital kommunikation (SDK)

Projektet föreslår en anslutning till Ineras SDK och att det hanteras inom ramen av kommunens objektverksamhet när Inera sedan öppnar upp för möjligheten att ansluta. Detta behöver föregås av en upphandling eller avrop av produkt(er) som kan ansluta till SDK.

SDK-projekt har börjat arbeta med att skapa en gemensam adressbok. Verksamheternas funktionsadresser behöver anpassas till kommunens grundstruktur. Administrativa rutiner behöver skapas. Information i adressboken behöver uppdateras kontinuerligt. Arbetssätt kopplat till hantering av inkommande och utgående meddelanden behöver anpassas.

Viktiga förutsättningar

Identitet och åtkomst (e-legitimation mm)

IT-säkerhet hanterar användares e-identiteter och behörighetsstyrande egenskaper, åtkomst till information i IT-system och regelverken som styr denna åtkomst. För detta krävs lösningar som hanterar användares identiteter och behörighetsstyrande egenskaper.

För att kunna upprätthålla en god förmåga att leverera lösningar som möter verksamhetens behov föreslår projektet att nuvarande förmåga för identitet och åtkomst ses över utifrån bland annat aspekterna teknik, avtal och innehåll. Projektet rekommenderar att förmågan etableras i objektverksamhet och att en beredskap skapas för att kunna inkludera tjänster med högre tillitsnivåer och legitimationer. För att basförmågorna inom säkra meddelanden och e-underskrifter ska kunna omsättas i t ex verksamhetssystem behövs vissa kompletterande komponenter. Det kan handla om plattformar för e-tjänster, Mina sidor, integration, processtöd (attestflöden) med mera. Det är viktigt att bland annat kunna hantera integrationer med verksamhetssystem och attestflöden.

En god digital nyckelhantering och certifikathantering är av stor betydelse i detta sammanhang. Det kräver en ändamålsenlig form för såväl organisation som arbetssätt och möjliggör hantering på olika tillitsnivåer. Projektet rekommenderar att området genomlyses i samband med ovan nämnda översyn.

Förstudierapporten

Denna förstudierapport är framtagen inom ramen för projektet Säkra meddelanden och e-underskrifter och ska svara på:

- Vilka behov finns av säker kommunikation och e-underskrifter och mellan vilka aktörer?
- Vilka processer berörs?
- Vilka möjliga arkitektoniska lösningar finns?

Syftet är att adressera frågeställningar och ta fram rekommendationer för fortsatt arbete med att etablera grundläggande förmågor inom e-underskrifter och säkra meddelanden.

Kommunfullmäktige beslutade tidigare i år om en ny *Policy för digital transformation* som ersätter tidigare *Policy för IT-utveckling och digitalisering* (från 2015) och *Riktlinje för styrning av IT* (2012). Genom att anta strategiska styrprinciper för digital transformation i en ny policy tillämpar kommunen ett kommungemensamt helhetsperspektiv för nämnder, bolag och förtroendevalda. Styrprinciper anges för fyra områden:

- Sammanhållen digital service
- Ledning, styrning och organisation
- Arkitektur och säkerhet
- Informationsförsörjning och digital infrastruktur

I detta sammanhang fokuserar projektet på förmågorna att kunna kommunicera enhetligt och säkert och att skapa förutsättningar för digital hantering med e-underskrifter.

Idag sker en stor del av informationsutbytet via e-post, telefon, brev, och fax. Det tar tid, det är svårt att hitta rätt mottagare och att veta att informationen har nått fram till rätt person. Det finns också en risk att informationen blir liggande eller kommer på avvägar.

Kommunen har under en tid använt och utvärderat produkter för exempelvis krypterad e-post vid digital leverans av känslig eller sekretessreglerad information. Den förmåga som finns idag har brister med avseende på säkerställande av mottagarens identitet, lagring och överföring, användbarhet med mera.

Det ursprungliga behovet av att säkra kommunikationen med brukare inom socialförvaltningen (SCF), som låg till grund för dagens lösning *Krypterad e-post*, har med tiden förändrats. I dagsläget är merparten (90–95%) av all krypterad e-post interna meddelanden inom kommunen. Till detta kan läggas att det inom ramen för Microsoft Office 365 finns funktionalitet som kan komplettera behovet internt inom kommunen.

Krav som ställs i nationell och internationell lagstiftning måste uppfyllas vid införande av e-underskrifter. Det gäller bland annat Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen) och lagen (2016:651) med kompletterande bestämmelser till samma förordning. Samtidigt ska införandet genomföras med en hög grad av användbarhet.

Mål och uppdrag

Identifierade behov

Inom hela kommunkoncernen finns ett stort behov av enkel, säker och enhetlig hantering av information.

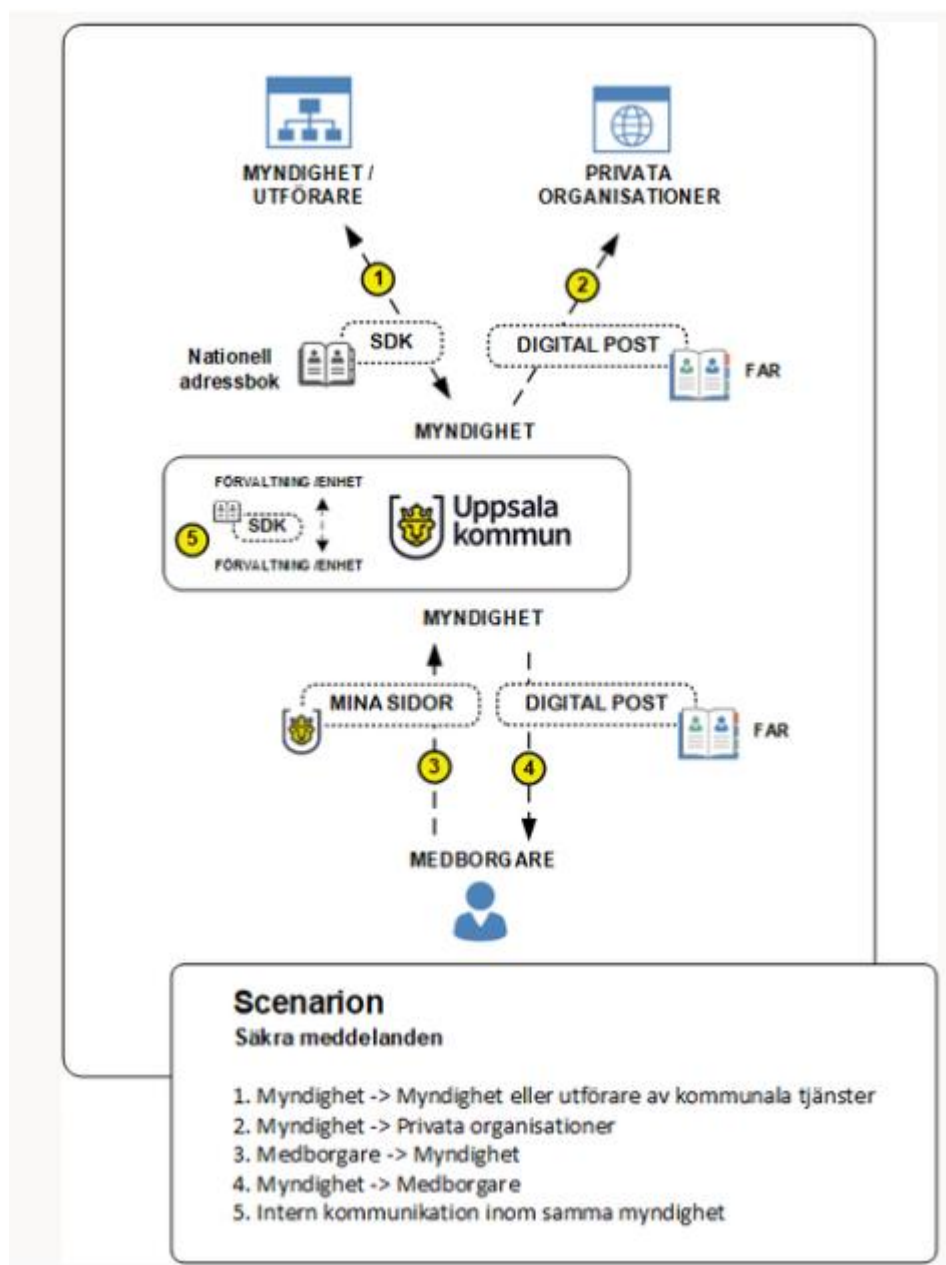
Kommunens bolag och förvaltningar har behov av säkra meddelanden i flera sammanhang. De behöver kunna dela digital information säkert och tillförlitligt med

kommuner, regioner och statliga myndigheter. Information behöver också kunna delas med medborgare och företag på ett säkert sätt. Informationen måste delas på ett tillräckligt säkert sätt för att känslig information ska kunna delges och att båda parter kan lita på att informationen är tillförlitlig och korrekt. De vanliga metoderna som används för att kommunicera (fax, brev, vanlig e-post och telefonsamtal) är i många sammanhang ineffektiva, för osäkra eller otillräckliga. Genom en eller flera digitala lösningar för säkra meddelanden kan verksamheten effektiviseras och digitaliseras samtidigt som en mer behovsanpassad lösning erhålls. Vissa ställningstaganden måste dock göras innan ett införande kan ske, framförallt gällande arkivering, kommunikation enligt förvaltningslagen och delgivning. Det är också viktigt att säkerhetskraven på kommunikationen nog kartläggs så att lösningarna i efterhand inte visar sig otillräckliga.

Underskrifter är ett sätt att verifiera att rätt person tagit ett beslut, det är också ett sätt att markera vilken version av handlingen som är slutgiltig. I dagsläget används fysiska underskrifter kommunens handlingar. På grund av det tvingas medarbetare skriva ut, posta och skanna in handlingar. Detta försvårar distansarbete, ökar risk för felhantering och leder till längre handläggningstider.

Ibland är underskrifter ett lagkrav och ibland görs underskrifter på grund av ovan nämnda skäl. I vissa fall görs underskrifter bara av tradition utan att det formellt sett finns skäl till det. Det är viktigt att behoven kartläggs för att identifiera i vilken omfattning en lösning för e-underskrifter behövs, och i vilka fall underskrifter kan ersättas av andra digitala funktioner i till exempel ärendehanteringssystem eller verksamhetssystem, alternativt tas bort. Det är av vikt att se till att e-underskrifter uppfyller de krav som ställs på diarieföring och långtidsbevarande av allmänna handlingar.

Några handlingar som kräver fördjupad analys är delegationsbeslut, avtal liksom protokoll i styrelser och kommunala bolag.



Figur 1 Scenarion för säkra meddelanden.

Ovanstående bild illustrerar de scenarion projektet ser behov av att kunna lösa med ett samlat grepp kring säkra meddelanden.

Effektmål

Säkra meddelanden och e-underskrifter bidrar till det långsiktiga effektmålet att kommunkoncernens informationshantering karaktäriseras av hög effektivitet, kvalitet och säkerhet.

De föreslagna förändringarna levererar en förmåga till ökad säkerhet i kommunikation, såväl internt som externt, av sekretessreglerad information samt hantering av elektroniskt underskrivna handlingar. Dessa förmågor är grundläggande för digitaliseringen av processer i syfte att effektivisera ärendehantering. Fler ärenden kan handläggas på kortare tid och det går att förutse färre felskickade meddelanden. Genom tydlighet i vilka lösningar som står till buds känner medarbetare trygghet i hur

de ska kommunicera digitalt. Antalet pappersbevarande aktiviteter bör minska i samband med införandet av den tänkta förmågan i verksamheten.

De föreslagna tekniska förändringarna medför att koncernen får tillgång till tjänster, produkter och stöd som gör övergången till effektiv och kvalitetssäkrad digital informationshantering möjlig och långsiktigt hållbar. Lösningar för att hantera säkra meddelanden och e-underskrifter finns efter förändringarna tillgängliga och koncernen får möjlighet att skapa nya säkra och effektiva arbetssätt för kommunikation och processer i den digitala transformationen.

För mer information om effektkedjan se **Fel! Hittar inte referensälla..**

E-underskrifter

Översikt

Elektroniska underskrifter är ett komplext ämne med stort utrymme för subjektiva tolkningar och där områden som juridik, teknik och säkerhet går i varandra. Det råder många missuppfattningar inom området och det saknas i vissa avseenden en tydlig vägledning som gör det enkelt att veta vad som gäller. Det finns också en utmaning i hur elektroniska underskrifter ska valideras över tid samt vilka produkter och tjänster som är långsiktigt hållbara.

EU:s förordning nr 910/2014, [eIDAS-förordningen](#), är styrande för hela EU och reglerar området. Inom svensk författning finns [kompletterande bestämmelser](#) med avseende på elektroniska underskrifter.

[eIDAS definierar](#) tre nivåer av elektroniska underskrifter.

- Elektronisk underskrift
Uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.
- Avancerad elektronisk underskrift (AdES, advanced electronic signature)
En elektronisk underskrift som uppfyller kraven enligt artikel 26 i eIDAS-förordningen (se nedan).
- Kvalificerad elektronisk underskrift
En AdES som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

Definitionen av elektronisk underskrift ger ett stort utrymme för val av lösningar. I svensk författning används begreppen *elektronisk underskrift* samt *avancerad elektronisk underskrift*.

Giltigheten i en elektronisk signatur är idag mer eller mindre oprövad i förhållande till svenskt rätt och eIDAS-förordningen. Under denna rådande osäkerhet gäller därför att välja lösningar som minimerar risken för problem på längre sikt i takt med att förutsättningarna klarnar.

[Artikel 26 i eIDAS-förordningen](#) reglerar kraven på en AdES. Utöver detta är även [artikel 27 Elektroniska underskrifter i offentliga tjänster](#) (krav på att erkänna AdES samt möjligheter till formkrav) och [artikel 37 Elektroniska stämplor i offentliga tjänster](#) av

vikt för offentlig verksamhet. Oberoende tolkningar av dessa artiklar saknas ännu, men projektet ser möjligheter för Uppsala kommun att med stöd av dessa artiklar begränsa format och metoder och därigenom förenkla hanteringen.

E-legitimationsnämnden (numera en del av DIGG) startade 2011 ett standardiseringsarbete och 2014 kom första standarden för en fristående underskriftstjänst. En fristående underskriftstjänst möjliggör hanteringen av en AdES utan att innehållet i sig behöver överföras till tjänsten. Därigenom blir det möjligt att på ett enklare sätt hantera floran av elektroniska identiteter inom EU som kan behöva accepteras (se artikel 27 eIDAS-förordningen). Det underlättar skydd av känslig information som då kan stanna kvar i användarens egen miljö. Det skapar inte heller ett långsiktigt beroende till underskriftstjänsten när en AdES senare ska valideras.

Det råder idag en stor osäkerhet vad som gäller för arkivering av elektroniska signaturer. Initiativ har tagits för att råda bot på denna osäkerhet. I väntan på tydlighet har organisationer löst det på eget sätt genom att till exempel spara loggar från underskriftsflödet i arkivet tillsammans med den underskrivna handlingen. Detta kan vara en utväg för att undvika svårigheter att validera en elektronisk underskrift utanför den egna miljön.

Följande utredningar av standarder är relevanta för sammanhanget.

- [SOU I 2020:01](#) gällande *Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen* redovisas senast 30 december 2020.
- Digitaliseringsmyndighetens tekniska ramverk kommer att uppdateras till version 2.0.

I väntan på att dessa utredningar är färdiga behöver osäkerheten hanteras. Att vänta med utveckling av grundläggande förmågor för elektroniska underskrifter på grund av dessa oklarheter är inte att rekommendera på grund av stora förseningar i införande. Ett fortsatt arbete handlar därför till stor del om riskminimering vid val av tekniska lösningar och att utgå från nationella betrodda tjänster, referensarkitekturer och ramverk.

EU:s arbete med standarder, öppen källkod samt politisk reglering via eIDAS-förordningen är tänkt att underlätta långsiktig och säker implementering av e-underskrifter. Det är komplext och tillämpningen skiljer sig beroende på vilket sammanhang en e-underskrift befinner sig i.

DIGG har i uppdrag att ta fram ramverk och vägledningar för hur svenska myndigheter bör tillämpa e-underskrifter. Den återkommande rekommendationen DIGG ger är att använda en fristående e-underskriftstjänst baserad på Sweden Connect:s tekniska ramverk (se DIGGs utkast till rapport [eID för medarbetare](#)). Anledningen till denna rekommendation är att myndigheten har en och samma tekniska implementering för e-underskrifter oberoende av teknisk implementering av e-identifikation (eID).

En nackdel med en fristående underskriftstjänst är att ett visst ansvar hamnar på den egna e-tjänsten då det blir den som utifrån eIDAS-förordningen utgör den betrodda tjänsten, med den fristående underskriftstjänsten som underleverantör.

En fördel är dock, som tidigare nämnts, att informationen som skrivs under inte behöver lämna kommunens kontroll, vilket förenklar i de fall där dokumenten innehåller sekretessreglerade uppgifter. En annan fördel är den förenklade tekniska implementationen när den fristående underskriftstjänsten tar hand om interaktionen med användarens elektroniska identitet (vilken kan variera stort till exempel med andra EU-medborgare).

Inera gav nyligen ut en ny referensarkitektur för elektronisk underskrift och stämpel, där beroendet till specifik leverantör gällande teknik och mjukvaror undviks och användning av en fristående underskriftstjänst istället poängteras. Inera kommer även med en ny generation av en autentiseringsklient för SITHS. Det är samma teknik som används för e-identifikationslösningarna Freja eID och BankID.

Det råder delade meningar om vilken elektronisk identitetshandling som lämpar sig bäst vid användning i tjänsten. Hos vissa finns ett motstånd till att använda exempelvis BankID då det skapar spår från aktiviteter i tjänsten som kopplas till den privata identiteten. Detta är en frågeställning som hanteras inom ramen för den statliga utredningen om betrodda tjänster samtidigt om det pågår en förstudie hos DIGG i samma fråga. Ett betänkande förväntas i slutet av året eller i början av nästa år.

Leverantörsmarknaden i Sverige är i sin linda och en utmaning är tilliten till den mångfald av e-underskriftstjänster som finns att tillgå. De är sällan baserade på ett standardiserat ramverk och de kräver en långsiktig relation till vald leverantör då valideringen är beroende av leverantörens tjänst.

I nuläget är tre leverantörer godkända av DIGG för leverans av fristående underskriftstjänst. Det är i dag den enda kvalitetsstämpeln som finns att luta sig mot i Sverige.

Områden som idag saknar vägledning och tydlighet och som behöver lösas långsiktigt är följande.

- Rekommendationer för vad som ska gälla när underskrifter ska arkiveras och på lång sikt kunna valideras.
- Ramverk för hur enhetlig validering av en e-underskrift ska ske.
- Visuellt representation av elektronisk underskrift.

Vidare är svenska författningen inte konsekvent utan pekar ibland på enkla elektroniska underskrifter som en myndighet inte kan validera och ibland på AdES utifrån artikel 26 i eIDAS-förordningen.

Utifrån ett internationellt perspektiv återstår en stor utmaning i hur ska man kunna hålla en aktuell lista med betrodda utfärdare av AdES. Detta finns idag enbart för kvalificerade underskrifter där EU har central lista.

Slutsats

Området är komplext och det krävs ett omfattande arbete med granskning och kvalitetssäkring för att minska risken för att lösningar inte blir långsiktigt hållbara. Vår rekommendation är därför att, i de fall det finns behov av e-underskrifter på nivån avancerade elektroniska underskrifter för fysiska personer, välja en fristående underskriftstjänst som godkänns av DIGG samt följa de referensarkitekturer som Inera publicerar.

E-underskrifter är beroende av e-legitimationer för EU-medborgare, representanter för företag och tjänstepersoner inom offentlig förvaltning. Lösningar för alla dessa perspektiv måste tas fram i samverkan med utvecklingen av betrodda tjänster och de initiativ som tas centralt från DIGG.

De behov av e-underskrifter som uppstår i verksamheterna bör kvalificeras och granskas med avseende på legala krav och lämplighet i varje enskilt fall. I många fall kan behovet lösas på ett enklare vis genom registrering i verksamhetssystem eller

diarium med tydlig referens till exempelvis vem som har fattat beslut. En förutsättning här är att processen är väl definierad och att handlingen uppfyller krav på bevarande.

Om e-underskrifter ändå är önskvärt föreslås att man i de enskilda fallen, i väntan på en koncerngemensam lösning, överväger följande:

- Säkerställ att man på sikt kan använda den koncerngemensamma lösningen för e-underskrift.
- Finns behov här och nu behövs en interimslösning tillsammans med möjlighet att på sikt använda vår koncerngemensamma lösning.
- Om behov ligger tillräckligt långt fram behövs ingen interimslösning

Nuläget i Uppsala kommun

Det finns statistik från användningen av kommunens nuvarande funktionstjänster (från CGI AB). Dessa används främst vid identifiering av kommuninnevärdarna mot befintliga e-tjänster som till exempel Uppsala kommuns e-tjänst för att söka förskole/grundskoleplats, [eBarnUngdom](#). Av statistiken framgår att tjänsten under 2018 användes för 948 675 e-legitimeringar samt 2260 elektroniska underskrifter. Projektet har dock inte gått vidare med analys av i vilka sammanhang dessa underskrifter sker. En översyn av förvaltningen och avtal avseende funktionstjänsten är nödvändig.

Inom ramen för DHS-projektet (införande av digitalt handläggarsöd) ingick tidigare att etablera en funktion för e-underskrifter och då kopplat till nämndhandlingar. Detta beslutades dock att hanteras utanför DHS och istället lösas av projektet för Säkra meddelanden och e-underskrifter. Den lösning som tidigare erbjöds från en underleverantör inom ramen för DHS svarade inte mot DIGG:s ramverk för fristående underskriftstjänster.

Ett annat sammanhang där handläggare i kommunen använder sig av e-underskrifter är socialjouren när kommunen bistår annan kommun i handläggningen. I detta fall har till exempel Enköpings kommun köpt in en lösning från socialjour.se. Denna bygger i sin tur på samma lösning som tidigare erbjöds via DHS. En observation är också att överföringen av det elektroniskt underskrivna beslutet till handläggare på Statens institutionsstyrelse (SIS) sker via fax. Detta gör att frågan om värdet av den elektroniska signaturen kan ifrågasättas då analoga moment fortfarande krävs. För att SIS ska acceptera ett beslut ställer de också krav på den visuella utformningen av beslutet där hänvisning till en elektronisk underskrift framgår.

Coronakrisen i sig har också medfört ett ökat tryck på e-underskrifter för medarbetare och beslutsfattare som arbetar på distans. Det kan dock sägas att det inte finns några formella krav på e-underskrift avseende i stort sett all intern handläggning där man traditionellt använt analoga underskrifter. Man kan också överväga att fortsätta med analoga underskrifter i de få sammanhang det ändå krävs. För handläggning som inbegriper externa parter kan dock kraven och behoven vara andra.

I korthet finns det ett antal funktioner inom en del av befintliga tekniska lösningar och IT-system som hanterar underskrifter och attester men som inte uppfyller de krav som ställs på avancerade elektroniska signaturer.

Förslag till lösningsarkitektur

Lösningsarkitekturen avser att beskriva, främst utifrån ett tekniskt och praktiskt fokus på översiktlig nivå, hur elektroniska underskrifter bör realiseras inom kommunen. Den beskriver även hur ett underskriftsförfarande sker och hur olika tekniska områden och förmågor behöver förhålla sig till varandra och samspela, inklusive konsumtionsaspekten mellan tjänsteproducent och -konsument.

Principer för lösning

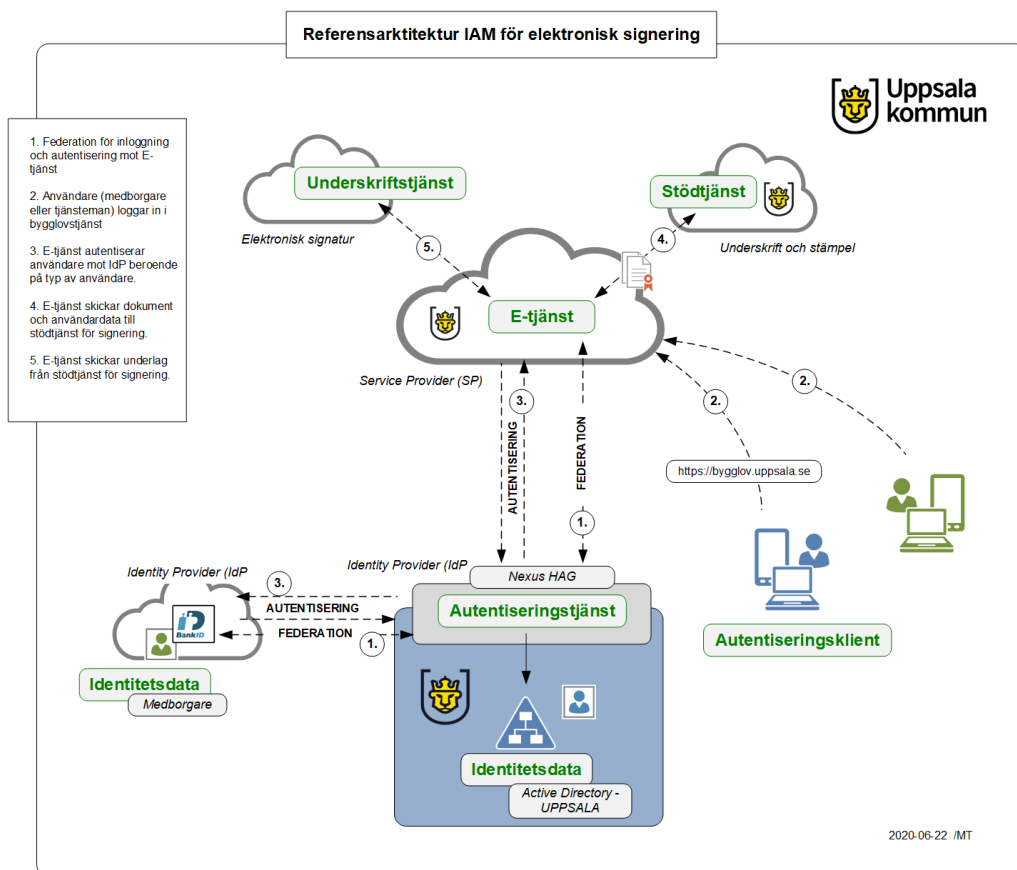
Med anledning av att området är komplext är en nödvändig och grundläggande princip att arbetet bör vila på nationella standarder och rekommendationer från normerande aktörer¹. Dessutom bör följande principer gälla.

- Lösningen bör stödja avancerade elektroniska signaturer för fysiska personer.
- Undertecknaren behöver ha full kontroll över de uppgifter som ska signeras.
- Signaturen bör vara inbäddad i PDF/A-format och baseras på PAdES (PDF Advanced Electronic Signature).
- En visuell representation av signaturen bör tillföras den signerade handlingen för att det även ska framgå av en utskriven version att den är elektroniskt signerad.
- Lösningen bör följa rekommendationer, vägledningar och standarder från DiGG för e-underskrifter.
- Lösningen bör följa Ineras referensarkitekturer för e-underskrifter och identitet och åtkomst.
- Utformningen och implementeringen av lösningen bör utgå ifrån att kunna nyttjas över hela kommunen/koncernen som en generisk tjänst och byggblock.
- Utformningen av lösningen bör ge stöd till att komponenter med enkelhet kan bytas ut över tid med låg påverkan för lösningen i sig såväl som för dess användare.
- Denna lösning bör utgöra första-hands-valet när verksamheter har behov av en elektronisk signatur baserat på en analys av författningskrav, lämplighet och risk/konsekvens.

Teknik

Det finns ett antal komponenter och funktioner involverade i ett digitalt underskriftsförfarande. Nedan följer en beskrivning inklusive förutsättningar för varje involverad del och dess interaktioner enligt kommunens föreslagna arkitektur för e-underskrifter.

¹ eIDAS förordningen och ramverk från DiGG



Figur 2 Referensarkitektur för elektronisk signering

Lösningen baseras på en fristående underskriftstjänst enligt tidigare nämnda rekommendationer och principer samt en stödtjänst för underskrifter. Underskriftstjänsten levereras av extern leverantör och stödtjänsten hanteras i vår egen miljö. Lösningen i sig består av och är beroende av andra tjänster och lösningar inom kommunen för hantering av identiteter och åtkomst, som autentiseringsstjänst och identitetsdata.

Lösningens tillgänglighetskrav baseras på de praktiska behov som finns inom verksamheterna såväl som för externa (medborgare med flera). Dessa i sin tur ställer krav på de ingående komponenterna. Tjänstens skyddskrav är höga och den fristående underskriftstjänsten behöver efterleva DIGG:s ramverk, samt att stödtjänsten behöver säkras och skyddas utifrån flera aspekter, såsom åtkomstkontroll, upptäcksförmåga, extern loggning mm.

e-tjänst

E-tjänsten består av interna och externa IT-system och tjänster, såsom verksamhetssystem eller stödsystem där användare (interna och externa) har behov av att kunna utföra underskrifter, till exempel inom en del av en process eller ärende.

Följande kriterier bör tillämpas för e-tjänster som använder en underskriftstjänst.

- System som upprättar dokument för signering bör förse upprättat dokument med unikt ID. Med hjälp av unikt ID på dokument ska det vara möjligt att spåra dokument till källan och det beslut eller underskrift som skedde.
- E-tjänsten bör ansvara för hanteringen av hur många som ska signera och dess turordning.

- E-tjänsten bör ansvara för hanteringen av handlingar med utförda underskrifter, exempelvis lagring.
- E-tjänsten bör ansvara för index av utförda underskrifter, dvs vilka handlingar som skrivits under när och av vem med mera.
- E-tjänsten bör ansvara för att säkerställa att gjorda underskrifter är korrekta vilket inkluderar att det säkerställs i alla delar att det är rätt handling som får rätt underskrift.
- E-tjänsten bör ansvara för att kontrollera att returen från underskriftstjänsten är korrekt, bland annat att det är rätt dokument som är underskrivet.

Följande tekniska förutsättningar och förmågor bör gälla.

- e-tjänsten bör kunna använda ett integrations-API (val om till exempel REST/SOAP, som anropar en server och lagrar information)
- e-tjänsten bör kunna hantera referensnummer (unikt ID) i dokument/datafil (om krav/lämpligt)
- e-tjänsten bör ha stöd för protokollen SAML eller OpenID (identifikationsloggningssystem) för federerad inloggning inklusive de attribut/claims som krävs för att knyta användaren till genomförd signatur.
- e-tjänsten bör uppfylla krav på riktighet, tillgänglighet och tillförlitlighet enligt DiGG:s tillitsramverk.

Autentiseringstjänst

Kommunens IT-infrastruktur hanterar idag olika typer av autentiseringstjänster och lösningar för åtkomst till både internt och externt placerade system och e-tjänster/IT-stöd, vilka har stöd för Ineras föreslagna referensarkitektur.

Tekniska tjänster och förutsättningar i dessa sammanhang är autentiseringsprotokollet SAML för federerad inloggning för åtkomst till e-tjänster. Detta kan vid behov kompletteras med krav på stark autentisering med hjälp av BankID, SMS eller autentiseringsapp. Dessa funktioner kan tillhandahållas av kommunens autentiseringsplattform HAG (Hybrid Access Gateway) från leverantören Nexus.

Figur 2 ovan visar hur kommunens egna IT-infrastruktur stödjer en e-tjänst som utnyttjar digital signering enligt DiGG:s föreslagna arkitektur.

Kommunen utnyttjar även Microsoft Azure som tillhandahåller stöd för inloggning och åtkomst till tjänster via SAML och tekniker som OpenID. Denna plattform bör i nuläget inte användas i sammanhang där elektronisk underskrift krävs. En orsak till rekommendationen är att det saknas stöd för autentisering via elektronisk legitimation (exempelvis BankID), samt en fortsatt oklarhet beträffande det rättsliga läget avseende nyttjandet av Microsofts molntjänster.

Autentiseringsklient

Utgörs av webbläsare eller applikation på mobil enhet eller dator för inloggning och åtkomst mot e-tjänst. Bör kunna utnyttja stark autentisering som BankID eller Freja eID (e-identifikation) för signering eller inloggning.

Identitetsdata

Katalogtjänster eller databaser där det användarkonto som används vid inloggning finns placerat. De används av Autentiseringstjänst (identifieringstjänst) för att utfärda biljett/intyg om godkänd inloggning vilken skickas till e-tjänst.

Tjänsterna bör innehålla alla användarattribut som används av användarprofilen i e-tjänsten. Dessa attribut (exempelvis personnummer) kan användas behörighetsgivande egenskaper i tjänsten eller för stark autentisering via till exempel BankID.

Underskriftstjänst

Underskriftstjänsten tar emot underlag med data om innehållet (med unika kontrollsummor) som signering sker emot. Ingen lagring av utförda underskrifter eller innehåll (handlingar) ska ske hos underskriftstjänsten. Underskriftstjänsten bör ha en kort lagringstid för loggar avseende underskrifter.

För att uppfylla [DIGG:s krav och rekommendationer](#) bör kommunen utnyttja en [fristående underskriftstjänst](#). Denna funktion levereras av de [leverantörer](#) som uppfyller både [eIDAS:s och DIGG:s krav](#). Kommunens e-tjänster anropar därefter funktionen enligt vissa givna förutsättningar och får tillbaka en giltig signering av dokumentet eller underlaget.

Stödtjänst (till underskriftstjänst)

Stödtjänsten är den komponent som ingår i underskriftsprocessen med funktioner som krävs för att förbereda underskrift och skriva under med stöd av fristående underskriftstjänst. Stödtjänsten är den komponent som tar emot innehållet (handlingarna) för undertecknande.

Bevarandeaspekter

Att validera e-underskrifter för all framtid i e-arkivet ser projektet inte som en hållbar väg framåt. Bevarande av elektroniska underskrifter bör bygga på samma principer som bevarande av analoga underskrifter idag, det vill säga genom att de uppkommer i en kontrollerad miljö och att handlingarnas autenticitet, tillförlitlighet, integritet och användbarhet kan garanteras under deras hela livscykel.

Detta innebär att en underskrift valideras i det sammanhang den uppkommer och att det är denna validering som kommunkoncernen sedan bevarar tillsammans med den underskrivna handlingen. Även regelverk för hur validering sker och rutiner för att upprätthålla autenticitet, tillförlitlighet, integritet och användbarhet behöver bevaras. Genom att underskrifter skapas inom dessa givna ramar kan de ses som tillförlitliga över tid.

Både den elektroniskt signerade handlingen och valideringen av denna bör bevaras i godkända bevarandeformat, såsom PDF/A-1 eller XML.

Samordnad hantering

Det är av vikt att förmågan med e-underskrifter hanteras samordnat där möjligheten att använda lösningen för att genomföra e-underskrifter erbjuds som en tjänst. Tjänsten innehåller såväl digitala tjänster för praktiskt och tekniskt utförande från till exempelvis verksamhetssystem som stöd och vägledning i de frågor som uppstår vid

behov av konsumtion av tjänsten. Detta innebär att vissa praktiska frågor behöver lösas, som till exempel vilka krav och skyldigheter konsumerande objekt har samt vilka juridiska och tekniska förutsättningar som råder i respektive objekt.

Säkra meddelanden

Översikt

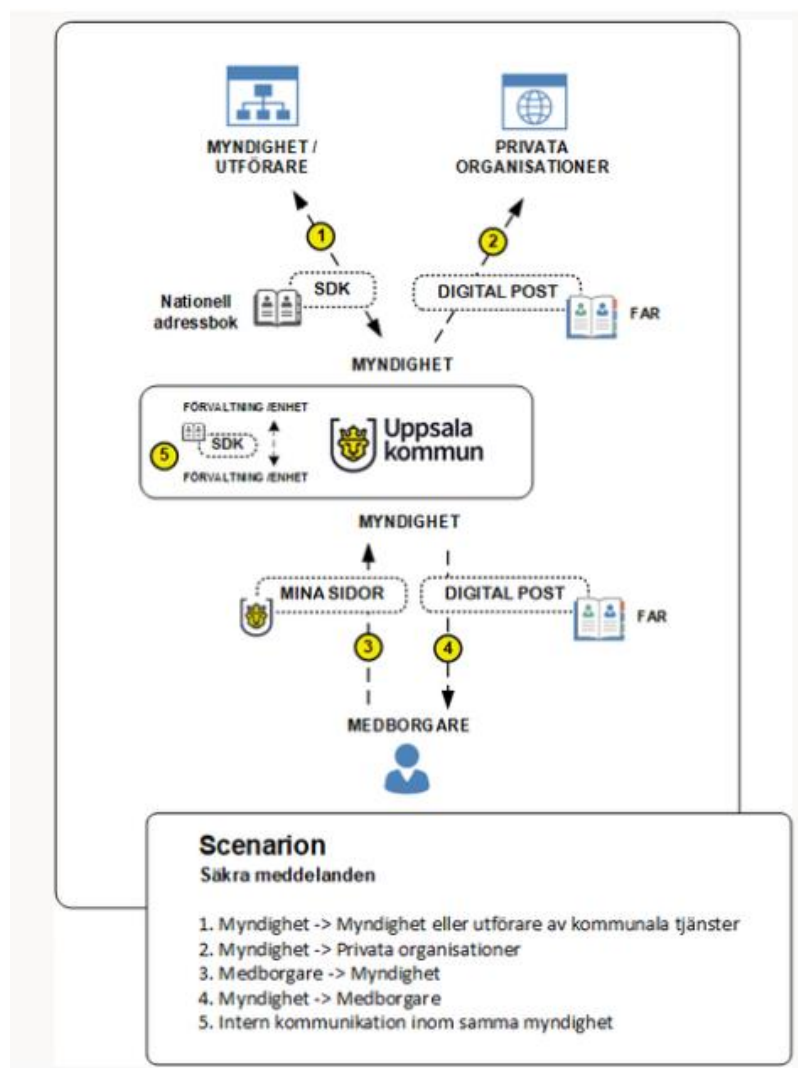
I detta arbete har projektet valt att använda Säkra meddelanden som samlingsbegrepp för de behov som löses av SDK, DIGG:s Digital post samt nuvarande tjänst för Krypterad e-post. Projektet har inte angivit en tydlig avgränsning mot andra lösningar för säker överföring av digital information från kommunen till andra parter, exempelvis lönefiler.

Offentlig sektor ha stora behov av att kommunicera säkert mellan olika funktioner i myndigheter, regioner och kommuner. Vissa av de befintliga lösningarna kan med tiden komma att ersättas med nationella lösningar i linje med det initiativ Inera tagit kring SDK, DIGG:s Digital post med mera.

Detta projekt behandlar inte förmågor för säkra digitala möten som förutom ljud och bild även kan inbegripa chatt och fildelning. Även inom detta område tas nationella initiativ i form av exempelvis Ineras tjänst för Digitala möten.

Uppsala kommun har liksom många andra offentliga aktörer identifierat begränsningar (såväl legalt som utifrån ett riskperspektiv, i nyttjandet av befintliga funktioner för ljud, bild, chatt, filöverföring, delning med mera) inom ramen för Microsoft Office 365 när informationen omfattar känsliga och sekretessreglerade uppgifter.

Såväl regeringen som DIGG och Inera har tagit initiativ till att klarlägga rättsläget, behoven och nödvändiga lösningar för att komma tillrätta med dagens situation.



Figur 1 Scenarion för säkra meddelanden (bilden finns även på sid 8)

Ovanstående bild illustrerar de scenarion som behöver hanteras med ett samlat grepp kring säkra meddelanden. Bilden visar även tänkbara lösningar såsom Ineras SDK, Mina meddelanden (Digital post) samt Mina sidor. Notera att Mina meddelanden enbart medger envägskommunikation. Mottagaren av ett sådant meddelande behöver alltså använda en annan kanal för att kontakta kommunen, till exempel genom en e-tjänst eller Mina sidor.

Mina Meddelanden (Digital post)

Myndighet till medborgare (personnummer).

Myndighet till företag (organisationsnummer).

Med digital post kan kommunen skicka post digitalt till privatpersoner och företag. Kommunikationen är envägs såtillvida att mottagaren inte kan svara i samma kanal. I dessa fall hänvisas mottagaren till en annan kanal för att kontakta kommunen exempelvis i form av Mina sidor.

Förmedlingsadressregistret (FaR) är grunden för infrastrukturen för digital post. I registret finns information om alla som på något sätt är ansluta till infrastrukturen. Det är mottagare, avsändande, offentliga aktörer, förmedlare och brevlådeoperatörer.

FaR förvaltas och tillhandahålls som en nationell tjänst av DIGG och anropas av tjänster som Mina Meddelanden i samband med utskick.

Säker digital kommunikation (SDK)

Myndighet till myndighet (utförare av offentligt uppdrag)

Om projektet

SDK-projektet är ett nationellt samverkansprojekt som handlar om att skapa förutsättningar för enkel, säker och enhetlig hantering av känslig information. Det gäller information som utbyts mellan verksamheter inom offentlig sektor, som exempelvis inom vård, socialtjänst och skola.

Inera är projektägare och i projektet ingår Sveriges kommuner och regioner (SKR), enskilda regioner och kommuner, Myndigheten för digital förvaltning, DIGG, och andra statliga myndigheter. Totalt deltar cirka 230 parter (per mars 2020) som styr- eller referensgruppsmedlemmar, pilotaktörer eller generella intressenter. Finansieringen delas av regioner, kommuner och statliga myndigheter.

Målet med projektet är att Sverige ska ha en standardiserad förmåga till säker digital kommunikation mellan offentliga aktörer, inklusive privata utförare av offentligt uppdrag. Det innebär att definiera ett gemensamt sätt att överföra känslig information på ett enhetligt, effektivt, säkert och överenskommet sätt. Genom att ta fram gemensam infrastruktur för till exempel adressuppgifter och standarder för säkert meddelandeutbyte som organisationerna kan anpassa sin egen IT-miljö och egna IT-stöd till, skapas förutsättningar för ett säkrare informationsutbyte.

Ett tydligt exempel på beroende till e-legitimationer ges av kraven för anslutning till SDK vilka uttrycks som att "[v]år organisation tillser att varje användares identitet inom användarorganisationens berörda verksamhet verifieras genom en fullgod svensk identitetshandling".

Vad som avses med fullgod svensk identitetshandling är dock oklart i nuläget. Det kan dock konstateras att det finns behov av en tjänstelegitimation.

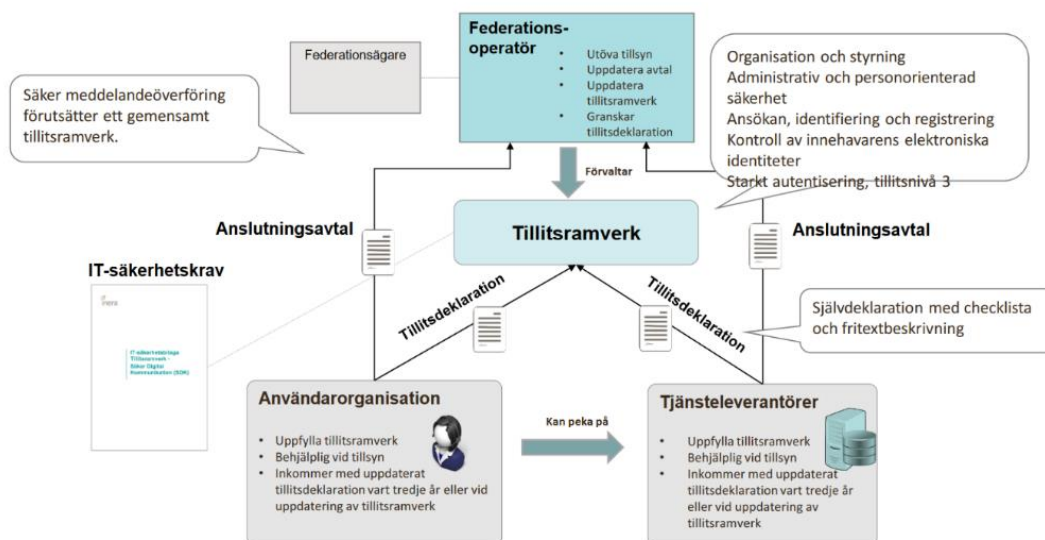
Tillitsramverk

Tillitsramverket är framtaget för organisationer som har för avsikt att ansluta till SDK och specificerar de säkerhetskrav som ställs på anslutna aktörer till SDK. Tillitsramverket har som syfte att etablera gemensamma krav för alla som är anslutna till SDK.

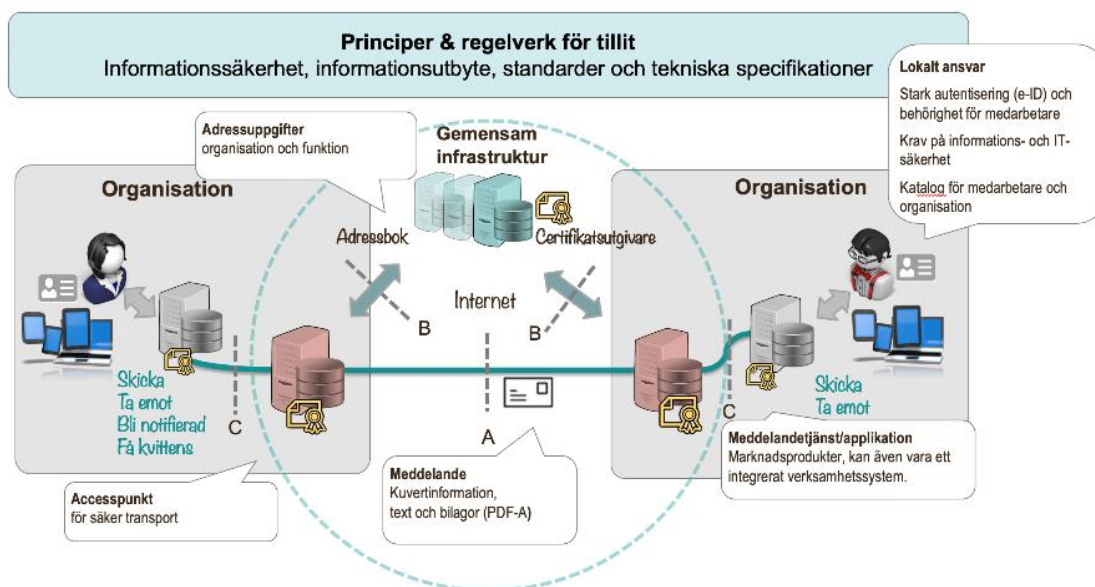
SDK har för avsikt att hantera tillräckliga gemensamma säkerhetskrav för kommunikation med information klassad med på konsekvensnivå betydande och lägre. Konsekvensnivåer definieras utifrån Myndigheten för samhällsskydd och beredskaps (MSB:s) modell för klassificering av information.

För att säkerställa efterlevnaden av tillitsramverket krävs att varje användarorganisation upprättar en tillitsdeklaration som är godkänd av federationsoperatören av SDK. I tillitsdeklarationen ska det tydligt framgå vad anslutningen ska användas till. Den får inte användas för något annat syfte.

Federation för tillit och informationsutbyte



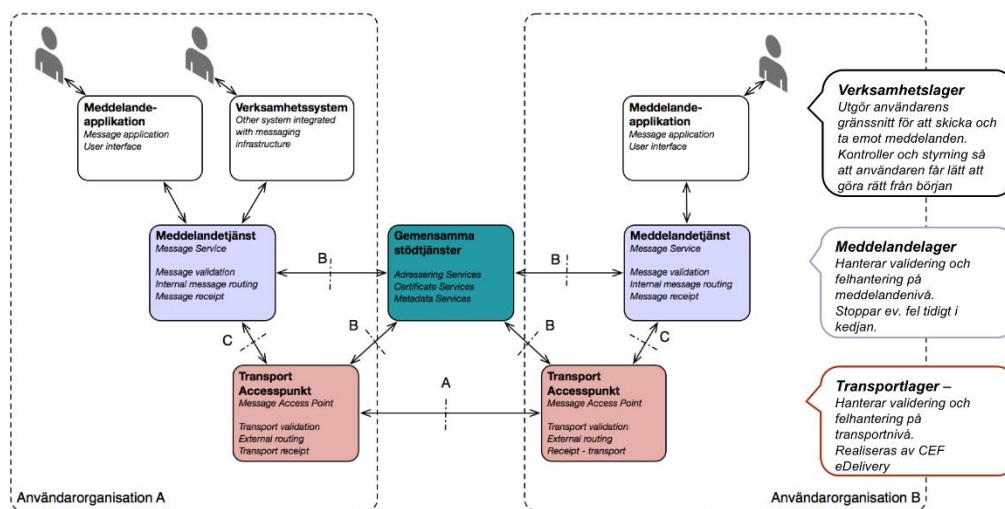
Figur 3 Federation för tillit och informationsutbyte



Figur 4 Principer och regelverk för tillit

Arkitektur

Bilden nedan visar SDK-projektets referensarkitektur för säker meddelandeöverföring, se Figur 6. Bilden visar lösningens övergripande komponenter, ansvarsfördelning samt gränssytor.



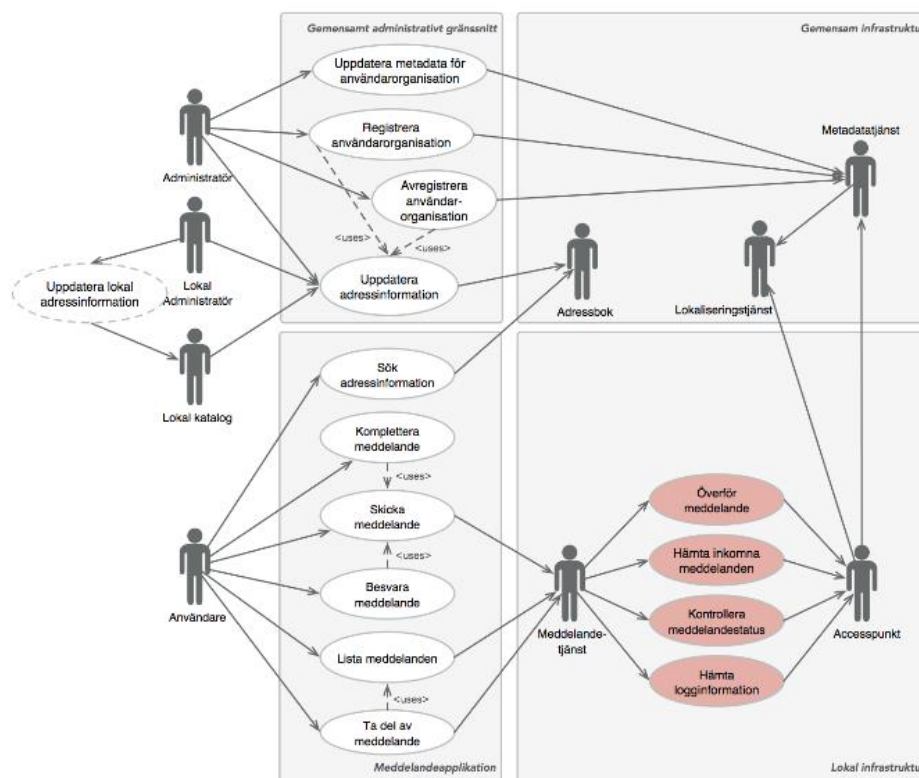
Figur 5 Referensarkitektur för säker meddelandeöverföring

Adressbok

SDK Adressbok är en gemensam tjänst som utvecklas, testas och förvaltas av Inera inom ramen för projektet SDK. I korthet är tjänsten ett gemensamt adressregister för anslutna användarorganisationer och deras adresserbara funktioner. Tjänsten syftar till:

- att vara en *källa för adressuppgifter*, genom att behöriga användare registrerar och underhåller information om en användarorganisation och dess funktioner (funktionsadresser) via adressbokens administrationsgränssnitt
- att tillhandahålla funktionalitet för att *hitta mottagare*, genom att SDK-anslutna användarorganisationer kan söka och hitta andra anslutna användarorganisationer och deras funktionsadresser

Adressboken är inte ett komplett register från början, utan fylls med uppgifter i takt med att användarorganisationer har avtalat om och godkänts för anslutning till SDK.



Figur 6 SDK Adressbok är en gemensam tjänst

Projektets uppdrag avseende adressbok

Utöver att utveckla, testa och förvalta adressboken har ett tilläggsuppdrag tilldelats SDK-projektet. Tilläggsuppdraget syftar till att underlätta för kommunala verksamheter att ansluta sig till och börja använda SDK. Fokus ligger på socialtjänst men hela kommunkoncernen ska omfattas. Uppdraget ska genomföras i samverkan mellan SKR och dess nätverk.

Tilläggsuppdraget omfattar följande.

1. Framtagning, förankring och beslut om grundstruktur för hur adressboken ska fyllas med innehåll.
 - Hur organisationer ska struktureras i adressboken och till vilken nivå (till exempel indelning inom olika verksamhetsområden, hur organisationer ska benämnas, osv) och beskrivas genom exempelvis gemensamma standardtexter.
 - Hur funktionsadresser ska struktureras inom organisationer och beskrivas (ska det till exempel finnas en standarduppsättning med funktionsadresser med enhetlig benämning och gemensamma standardtexter för hur de beskrivs?)
 - Hur sökbegrepp på funktionsadress ska struktureras och beskrivas. Detta är viktigt för att öka sökbarheten på funktionsadresser.
 - Avgränsning: Grundstruktur, funktionsadresser och sökbegrepp kommer inte att vara heltäckande men kommer att utgöra en bra start och vara vägledande avseende de kompletteringar som senare ska göras.
2. Vägledning för kommuner och andra användarorganisationers tillvägagångssätt för hur man ska fylla adressboken med innehåll.

- Hur användarorganisationer ska benämna och beskriva sin organisation och sina funktionsadresser i adressboken.
 - Hur användarorganisationer ska benämna och beskriva kategorierna
3. Fortsatt förvaltning
- Ta fram en rekommendation om fortsatt förvaltning av den kommunala innehållsdelen av adressboken

Funktionalitet i SDK Adressbok

- Adressbok 1: Grundfunktionalitet, nuläge
 - Logga in
 - Skapa organisation
 - Ta bort organisation
 - Uppdatera organisation
 - Skapa funktionsadress
 - Uppdatera funktionsadress
 - Ta bort funktionsadress
 - Söka i Adressboken - mer avancerad sökfunktionalitet
 - Skriva till och läsa auditlogg
- Adressbok 2: Kompletterande utveckling av grundfunktionalitet
 - Uppdatera organisation - stöd för kodverk
 - Uppdatera funktionsadress - stöd för kodverk
- Adressbok 3: Utveckling enligt tilläggsuppdrag
 - Skapa urval: Valbara kodverk för användarorganisationen vid kodning
 - Välja kodverk för användarorganisation
 - Kodverksadministration - Hantera kodverk - funktionalitet i roll som central administratör av kodverk
 - Kodverksadministration: Hantera kodverk - funktionalitet för roll som central administratör av kodverk
 - Grafiskt gränssnitt för adressbok och testklient
 - Söka i Adressboken - mer avancerad funktionalitet som stöd för kodverk
 - Skriva till och läsa auditlogg- mer avancerad funktionalitet som stöd för kodverk

Till ovanstående funktionalitet tillkommer anpassningar enligt fördjupad behovsanalys som genomförs inom ramen för tilläggsuppdrag kommunal grundstruktur.

Användarorganisationen i SDK Adressbok

Användarorganisationen består av kommuner, regioner och andra myndigheter i Sverige. Användarorganisationerna

- har behörighet att logga in i SDK Adressbok för att hantera den egna organisationens information (skapa organisationens egna funktionsadresser)
- är informationsägare av sin information i SDK Adressbok och ansvarar för att administrera och underhålla den
- har läsrättigheter till övriga organisationers adressinformation i SDK Adressbok

Den kommunala grundstrukturen

Som en del av uppdraget arbetar Ineras SDK-projekt med att ta fram den kommunala grundstrukturen. Denna ska underlätta för de kommunala verksamheterna att komma igång, man får, något att utgå ifrån, istället för att behöva etablera hela strukturen med funktionsadresser var och en för sig. Arbetet utgår från följande principer:

1. Utgå från Klassa 2.0 (Klassificeringsstruktur för kommunala verksamheter)
<http://www.samradsgruppen.se/index.php/rad-och-stod>
2. Organisationsstruktur ska vara enhetlig över sektorn
3. Benämning av funktionsadresser ska möta andra offentliga aktörers behov av att hitta rätt funktion inom en kommun.
4. Funktionsadresser ska vara stabila över tid
5. Funktionsadresser ska inte hindra korrekt hantering i mottagande organisation

Status för utvecklingen av SDK Adressbok

Det SDK-projektet kommit fram till hittills är att:

- det verkar räcka med två logiska nivåer i adressboken; organisation och funktion.
- begreppen i Klassa 2.0 inte räcker hela vägen.
- det behövs olika kodverk, exempelvis geografisk hemvist, sökord mm. bland annat som sök- och navigeringsstöd.

Under hösten 2020 kommer SDK-projektets pilotverksamheter att testa:

- ett första utkast av den kommunala grundstrukturen
- ett första utkast till kodverk inom socialtjänst
- HSA verksamhetskoder

Slutsats

Projektet rekommenderar att invänta SKL Kommentus upphandling av ramavtal för mjukvara eller tjänst för anslutning till SDK. Detta om det vid tid för införande inte finns någon lösning inom Uppsala kommun som redan följer ramverket eDelivery. Finns det en befintlig lösning ska den utvärderas och ställas mot det som kan avropas inom avtalet via SKL Kommentus. Under tiden rekommenderas även att dialogen mellan Uppsala kommun och Inera bibehålls och utvecklas i syfte att följa utvecklingen av SDK och dess olika faser. Det bör ske utifrån det förvaltningsobjekt som syftar till att kunna erbjuda säkra meddelanden, i samverkan med andra former som bedrivs - såsom referensgruppen för upphandling av SDK och genomförandeprojektet. Den part som erbjuder *säkra meddelanden* bör även ha en kontinuerlig dialog med intressenter av *säkra meddelanden* i syfte att informera om kommande möjligheter och erbjudanden, såsom att integrera mellan verksamhetssystem och SDK.

Inom SDK är *Adressboken* en viktig komponent, som byggs upp gemensamt av SDK:s medlemmar där det är av stor vikt att mottagare och avsändare följer en standard avseende namnsättning och id. Ett aktivt deltagande i arbetet med adressboken är högst nödvändigt för att säkerställa förståelse och möjlighet till att behov tas om hand och eventuella risker minimeras. Den redan etablerade kontakten mellan Uppsala

kommun och SDK-projektet bör bibehållas och utvecklas, där från Uppsala kommun ingående verksamheter bör involveras i de praktiska frågorna.

Avseende kommunikation mellan myndighet och medborgare är *Digital post/Mina Meddelanden* som kanal för säkra meddelanden en möjlig väg. Varje enskild verksamhet ansvarar själva för vilken (digital) kanal som är lämplig för respektive kommunikation för respektive kontakt/dialog/beslut utefter informationen. Utöver informationen i sig bör även kanalvalet präglas av hur lämpligt det är utifrån bland annat upplevelse och målgrupp.

För myndighetskommunikation som initieras av medborgaren är frågan om kanalvalet liknande ovan. Medborgare behöver kunna känna att dialog med myndigheten och till exempel bifogande av dokument sker på ett säkert och tillförlitligt sätt.

Andra offentliga aktörer skapar den här tydligheten och tilliten genom Mina sidor-funktionalitet på aktörens webbsida. Genom denna kan medborgare vägledas till säkra kanaler på ett robust sätt.

Nuläget i Uppsala kommun

Krypterad e-post

Uppsala kommun har under en tid använt och utvärderat produkter för krypterad e-post för digital leverans av känslig information eller information som omfattas av sekretess.

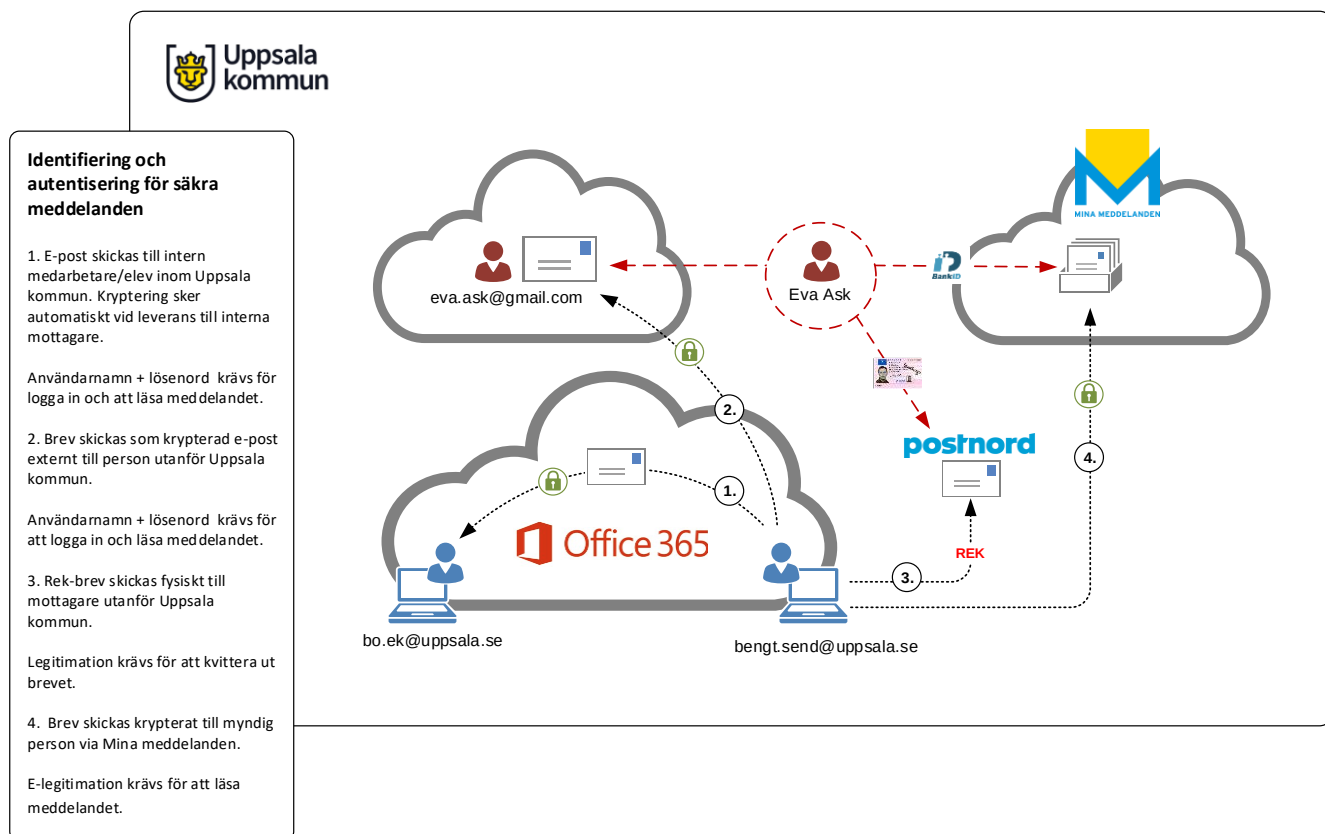
Den förmåga som finns idag, baserad på Deltagon, har brister och kan endast i begränsad omfattning säkerställa mottagarens identitet. Detta är olämpligt vid överföring av exempelvis känsliga personuppgifter. Nuvarande lösningar avser dessutom endast överföring från person till person, eller myndighet till person.

Problemen med nuvarande lösning kan sammanfattas med:

1. Krypterad e-post skickas till uppgiven e-postadress och i vissa fall tillhörande mobilnummer som säkerhetsverifiering. Ingen av dessa metoder kan garantera att mottagaren verkligen är rätt mottagare. Detta har även visat sig i de personuppgiftsincidenter som har inträffat inom Uppsala kommun.
2. Skickade meddelanden lagras i Outlook då e-postservern används för att överföra meddelanden till en säker portal
 - a. Bärbara datorer krypteras inte och synkroniserad e-post kan enkelt läsas i klartext om datorn förloras eller blir stulen.
 - b. Åtkomst och inloggning till e-postlåda innehållande krypterad e-post sker endast med användarnamn och lösenord.. Detta gäller även medarbetare inom Uppsala kommun vid åtkomst till e-post från enheter utanför kommunens interna nätverk.
 - c. Känsliga uppgifter /sekretess i e-postlådan lagras och hanteras av molntjänstleverantör utanför EU (Microsoft Office 365), vilken omfattas av CloudAct.
 - d. Det finns idag inget sätt att tydligt särskilja meddelanden som innehåller känsliga uppgifter från sådan som kan anses öppna
3. Anslutningsprocessen för tillgång till Krypterad e-post sker okontrollerat:

- a. Krypterad e-post beställs och används till exempel för att skicka känslig information internt mellan anställda inom Uppsala kommun (ca 95% av alla meddelanden via Deltagon). Detta spår på problematiken under punkt 2 ovan samt att det inte tillför något ur ett IT-säkerhetsperspektiv.
4. Det finns ingen etablerad funktion för säkert inskickande till kommunen.
5. Kostnader för förvaltning, licenser, support är oklara.
6. Säker meddelandehantering kan endast ske från myndighet till privatperson (mina meddelanden). Lösningar för säker överföring mellan myndighet eller företag saknas.

Följande bild visar hur identifiering eller autentisering sker för olika metoder av meddelanden i dagsläget.



Figur 7 Identifiering och autentisering för Säkra meddelanden

Oavsett ovanstående behöver förmodligen en förnyad upphandling genomföras. Då kan problemen ovan adresseras samt andra närbesläktade förmågor eventuellt inkluderas. Produkter eller lösningar för att skicka Säkra meddelanden mellan myndighet och myndighet eller företag saknas i Sverige idag.

Mina meddelanden

Ett steg i att etablera mer långsiktiga funktioner för förmågan att meddela privatpersoner har varit införande av Mina Meddelanden (Min myndighetspost, Kivra

m.fl.). Mina Meddelanden körs i testverksamhet av kommunens IT-support och av HR Löneservice. Lösningen bygger på en open source-licens från Skatteverket (numera från DIGG) som saknar support. Därför finns det anledning att undersöka om det går att köpa in en tjänst eller produkt som inkluderar anslutning till Mina meddelanden med support och underhåll.

Förslag till lösningsarkitektur

Lösningsarkitekturen avser att beskriva hur säkra meddelanden bör realiseras inom Uppsala kommun. Beskrivningen har tekniskt och praktiskt fokus och är på en översiktlig nivå. Beskrivningen redovisar vilka områden och förmågor som berörs och hur de påverkar sin omgivning. Då SDK fortsatt är under utveckling och etablering så kommer förslaget nedan att behöva revideras. Se även ovan i avsnittet *Slutsats* under rubriken *Översikt*.

Principer för lösning – Säker Digital Kommunikation

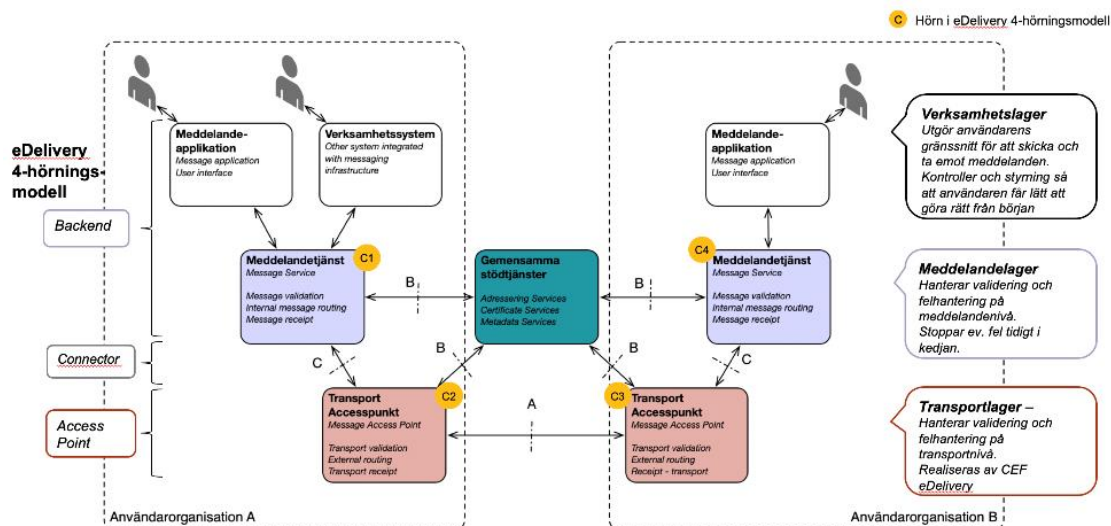
- En framtida lösning ska följa de krav som ställs för anslutning till SDK, vilket innebär ramverket CEF eDelivery. DIGG ansvarar för detta ramverk i Sverige.
- Utformning och implementering av lösning ska utgå från att kunna användas över hela kommunkoncernen.
- Utformningen av lösningen bör ge stöd till att förändringar kan ske kontinuerligt med låg påverkan för dess användare, där så är möjligt.

Teknik

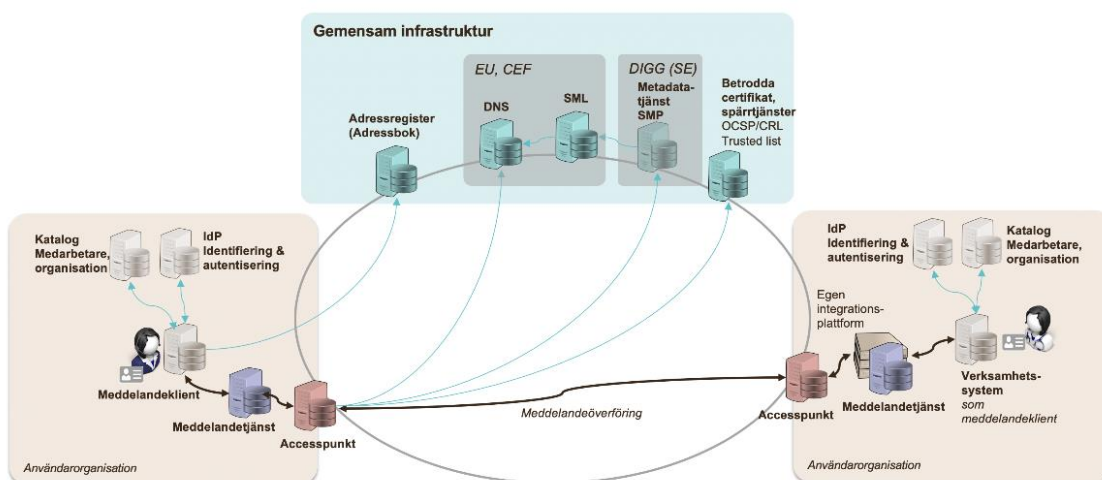
Säker Digital Kommunikation

Referensarkitektur för säker meddelandeöverföring (figur 5) avseende SDK (myndighet <-> myndighet) bör följas.

Frågan om *Meddelandetjänst* och *Transport Accesspunkt* bör drifas i egen regi eller tillgås som tjänst av leverantör, beror på utfallet av SKL Kommentus upphandling. Inom arbetet hanteras även frågan om att kunna integrera verksamhetssystem till SDK som kommer att kunna besvara vilka förutsättningar och kriterier som ställs för dessa informationsutbyten. Beroende på upphandlingen och dess kravställning kommer det tydliggöras på vilket sätt en klient respektive funktioner för integrationer med verksamhetssystem kommer att tillgängliggöras och hur det ställer krav på IT-landskapet.



Figur 8 - eDeliverys 4-hörningsmodell mappad mot referensmodellen för säker meddelandeöverföring



Figur 9 Gemensam infrastruktur

Mina meddelanden (Digital post)

Digital post/Mina meddelanden är ett möjligt alternativ för kommunikation (exempelvis delgivning av beslut) mellan myndighet och medborgare. En vidare analys för förändringar inom teknik behövs, baserad på lärdomar och erfarenheter av befintlig lösning. Förvaltningsaspekten bör även tas med i analysen.

Förvaltning

Behoven som beskrivs i avsnittet Översikt och i figur 1 är likartade även om tillämpningen av lösning kan variera. Att samla kunskap, kompetens och även praktiskt utförande till erbjödanden riktade till dem som har behoven i ett objekt är en stark rekommendation. Tjänsterna, lösningarna och behoven inom detta objekt samt dess kringliggande tjänster och förmågor kräver ett aktivt och kontinuerligt arbete för att fånga upp den ständiga förändringen och utvecklingen. Tjänsterna och lösningarna adresserar likvärdiga behov, även om syfte och ändamål skiljer sig. Detta inkluderar även interaktionen mellan konsument som använder dessa tjänster och lösningar och

producent som erbjuder dem. Viktigt är dock att stöd och vägledning ges inom dessa områden.

De olika verksamheter som använder dessa tjänster/lösningar kommer vid sin anslutning till SDK att behöva följa de roller och ansvar som gäller för SDK, som en del av åtagandet. Detta inkluderar skyldigheter och gränsdragningar för vad som ingår och utförs av producent respektive konsument. DIGG:s tillitsramverk innehåller även krav på självdeklaration som kontinuerligt ska uppfyllas och rapporteras in från SDK:s medlemmar till SDK centralt.

Dokumenthistorik

Version	Utförda förändringar	Skapat datum	Skapad av	Godkänt datum	Godkänd av
1.0		2020-10-23	Arbetsgrupp Säkra meddelanden och underskrifter	2020-11-05	Markus Bylund

Bilaga 1 - Referenser

1. [EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING \(EU\) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG \(eIDAS-förordningen\)](#)
2. [EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING \(EU\) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter](#)
3. [Kompletterande bestämmelser till EU:s förordning om elektronisk identifiering \(Trafikuskottets bet 2015/16:TU18\)](#)

Bilaga 2 - Begrepp

Begrepp/akronym	Fullständig betydelse	Förklaring
eIDAS	electronic identification and trust services	EU förordning för betrodda tjänster
AdES	Advanced Electronic Signature	Avancerade elektroniska underskrifter i enlighet med Artikel 26 i eIDAS förordningen
QES	Qualify Electronic Signature	Kvalificerade elektroniska underskrifter i enlighet med artikel 28
Pdf	Portable Document Format	Dokumentformat som elektroniskt kan skrivas under
XML	Extensible Markup Language	Dokumentformat som elektroniskt kan skrivas under.
PadES	PDF Advanced Electronic Signatures	Elektroniskt signerat format av en Pdf i enlighet med standard från ETSI
XadES	XML Advanced Electronic Signatures	Elektroniskt signerat format av en XML i enlighet med standard från ETSI
PKI	Public Key Infrastructure	Teknik, infrastruktur och policy kring digitala certifikat och dess livscykelhantering.
dSIG	Digital Signature	Standard för elektroniska underskrifter på Pdf och XML.
Elektronisk underskrift		uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.
Validering av elektronisk underskrift		Att man i efterhand kan avgöra att dokumentet inte ändrats efter underskriften samt vem som skrivit under dokumentet.
Valideringspolicy		Policy vilka tester som ska utföras då man verifierar ett elektroniskt underskrivet dokument, till exempel ETSI EN 319 102-1
SAML	Security Assertion Markup Language	Autentiseringsprotokoll för s k federerad inloggning. Bygger på äkthetsintyg som utfärdas efter godkänd inloggning, vilket sedan konsumeras av IT-stödet.

Begrepp/akronym	Fullständig betydelse	Förklaring
CEF eDelivery		Byggblock för säker meddelandehantering i Europakommissionens Connecting Europe Facility, CEF, som bygger på öppna globala standarder. eDelivery är beprövad teknik som redan används i Sverige inom andra områden. Bland annat tjänsten Digital post/Mina meddelanden.

Följande begrepp är hämtade från DIGG, Normativ specifikation Fristående Underskriftstjänst.

Begrepp	Definition
Aktör	Organisation som tillhandahåller eller använder tjänst i eIDsystemet.
Användare	Fysisk person som nyttjar e-tjänst. I samband med fristående underskriftstjänst, fysisk person med e-legitimation som nyttjar e-tjänst i syfte att skriva under elektronisk handling
Bråd tid	Tidperiod med hög och tidskritisk belastning där aktör behöver extra stöd för att säkerställa kapacitet och tillgänglighet inom systemet för elektronisk underskrift
E-tjänst	Webbtjänst som användaren besöker och där användaren begär att få underteckna en elektronisk handling, till exempel underskrift av självdeklaration i Skatteverkets e-tjänst
eID-system	Ett antal tjänster och funktioner som samverkar och kommunicerar med varandra på ett ordnat sätt. Det är tjänster och funktioner som e-tjänster, legitimeringstjänster, utfärdare av e-legitimationer, e underskriftstjänster med flera.
Elektronisk legitimering	Med hjälp av elektroniska medel bevisa sin identitet. Vid legitimering i samband med elektronisk underskrift uttrycker användaren normalt också sin avsikt att skriva under en handling
Elektronisk underskrift	Uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.
Avancerad elektronisk underskrift	En elektronisk underskrift som uppfyller kraven enligt artikel 26 eIDAS
Kvalificerad elektronisk underskrift	En avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter som uppfyller krav på kvalificerade elektroniska underskrifter enligt avsnitt 4 eIDAS.

Begrepp	Definition
Underskriftsprocess	Ett antal samverkande delar som gör att användaren kan skriva under en elektronisk handling. Processen startar med att användaren kommer in i den delen av e-tjänsten som initierar underskrift och slutar med att underskriften är genomförd och den handling som skrivits under är sammanfogad med underskriftscertifikatet på ett kontrollerat sätt.
Fristående underskriftstjänst	Fysiskt avskild del i underskriftsprocessen där användaren kan skriva under en elektronisk handling med en avancerad eller kvalificerad elektronisk underskrift. I den fristående underskriftstjänsten signeras ett kondensat av den handling som skrivs under på ett säkert sätt och ett underskriftscertifikat ställs ut. Vid underskriftstillfället sker legitimering av den fysiska personen i en fristående legitimeringstjänst. Eng: Sign Service
eIDAS	Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden
SITHS	Identifieringstjänst SITHS är en säkerhetslösning som används för att utfärda elektroniska identitetshandlingar till både personer och system. SITHS e-legitimation används för att identifiera personer och SITHS funktionscertifikat används för att identifiera system.