Referensarkitektur för elektronisk underskrift och stämpel

Utformning av IT-lösningar för att skapa och validera elektroniska underskrifter och stämplar.

Rev A

Innehåll

1 Dokumentinformation

1.1 Revisionsinformation

Version	Datum	Beskrivning	Författare
PA1	2019-05-01	Första utkast	Per Mützell
PA2	2019-06-02	Utkast för intern granskning i arbetsgruppen.	Per Mützell
PA3	2019-08-15	Revidering efter inkomna kommentarer arbetsgrupp.	Per Mützell
RC1	2019-09-12	Revidering efter inkomna synpunkter från bland annat arbetsgruppen, SKL, DIGG, och genomgångar med Arkitekturrådsrepresentanter. Version för utskick, slutliga synpunkter och formellt godkännande.	Per Mützell
Rev A	2020-05-12	Fastställd utgåva efter hantering av synpunkter från Inera Arkitekturråd för regioner. Se separat sammanställning av synpunkter och dess hantering.	Per Mützell

1.2 Referenser[1]

Id	Referens/dokument
RIVTA	Regelverk för interoperabilitet, Tekniska anvisningar, förvaltat av Inera AB. https://rivta.se
T-boken	VIT(S)-bokens tekniska arkitektur. Styrande principer, vägledande exempel och teknisk referensarkitektur för vård och omsorg. https://rivta.se/documents/ARK_0019/
IAM-RA	Referensarkitektur för Identitet och åtkomst https://rivta.se/documents/ARK_0046/
RIV-Kryptering	RIV Tekniska anvisningar - Anvisning för kryptering (ARK_0036) https://rivta.se/documents/ARK_0036/

[1] Se även källförteckning för begrepp och termer. Övriga referenser anges i löpande text.

eIDAS	eIDAS-förordningen (910/2014). EU:s förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG Se även https://swedenconnect.se/eidas.html
Lag 2016:561	Lag 2016:561 med kompletterande bestämmelser i Sverige till EU:s förordning om elektronisk identifiering, samt förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2016561-med-kompletterande-bestammelser_sfs-2016-561 https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2016576-med-kompletterande_sfs-2016-576
Sweden Connect	DIGG:s funktioner för elektronisk identifiering och underskrift samt anslutningspunkt för eIDAS i Sverige. https://swedenconnect.se https://digg.se
Juridisk vägledning e-legitimering och e-underskrifter	Juridisk vägledning e-legitimering och e-underskrifter. (eSam, Myndigheten för samhällsskydd och beredskap, E-legitimationsnämnden) http://www.esamverka.se/stod-och-vagledning/aktuella-vagledningar-a---o/juridisk-vagledning-for-e-legitimering-och-e-underskrifter.html
Vägledning betrodda tjänster	Vägledning för betrodda tjänster i Sverige enligt eIDAS-förordningen (PTS). https://www.pts.se/sv/bransch/internet/betrodda-tjanster-eidas/
Vägledning e-underskrifter	Vägledning för e-underskrifter (DIGG). https://elegnamnden.se/eunderskrift/anpassaetjanstforeunderskrift/vagledningdetharbehoverduveta.4.4498694515fe27cdbcf249.html
RA-FS 2009:1-2	Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar, RA-FS 2009:1, samt tekniska krav, RA-FS 2009:2. https://riksarkivet.se/rafs
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1
Lag (2018:218)	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

1.3 Målgrupp

Detta dokument riktar sig i första hand till IT-arkitekter, IT-strateger, IT-beslutsfattare samt beställare/utvecklare av såväl e-tjänster för slutanvändare som IT-infrastruktur för elektronisk underskrift och stämpel.

1.4 Bakgrund och syfte

Referensarkitektur för elektronisk underskrift och stämpel syftar till att ge stöd till utformning av IT-stöd för att skapa och validera e-underskrifter och e-stämplar. Referensarkitekturen kan i tillämpliga delar appliceras både inom en organisation, och vid samverkan mellan organisationer, t.ex. vid delning av tjänster för elektronisk underskrift och hantering av interna och externa undertecknare.
Användaren av tjänsterna kan vara såväl en medarbetare tillhörande en organisation, som en invånare som agerar i sin privata roll.

Referensarkitekturen är tänkt att användas som referensunderlag vid anskaffning och vidareutveckling av lösningar för elektronisk underskrift och stämpel samt tillhörande stödtjänster, vilket kan omfatta såväl upphandling av leverantörsprodukter, anpassning av befintlig IT-infrastruktur och kravställning på e-tjänster/IT-system för följsamhet till arkitekturen.

Valen av öppna standarder inom området är gjorda för att ge goda möjligheter att välja standardprodukter på marknaden för den IT-infrastruktur som behövs för att realisera arkitekturen, samtidigt som leverantörer av e-tjänster kan implementera allmänt användbara funktioner för elektronisk underskrift och stämpel med standardgränssnitt som kan appliceras på flera marknadssegment.

Referensarkitekturen kan även fungera som en ”normerande mall” inom området elektroniska underskrifter och stämplar, och på så sätt göra olika lösningarna enklare att kommunicera kring och jämföra med varandra. Leverantörer inom området uppmanas att beskriva sina produkter och lösningar relativt referensarkitekturen för att underlätta sådan jämförelse.

Dokumentet är indelat i följande huvudavsnitt:

- **Översiktlig orientering** över området elektronisk underskrift och stämpel.
- **Styrande principer** - Vad är styrande för utformningen av referensarkitekturen och varför?
- **Verksamhetsvy** – Vilka behov hos verksamheter och enskilda individer inom området syftar referensarkitekturen till att möta? Vilka förmågor inom området behövs för att stödja behovet?

- **Informationssystemvy** - Vilka infrastrukturtjänster behöver vi för att realisera/besitta beskrivna förmågor? Vad behöver e-tjänsterna ansvara för och förhålla sig till? Vilka principiella flöden och krav behöver stödjas?
- **Juridik och informationssäkerhet** - Vilka rättsregler gäller vid användning av elektroniska underskrifter och stämplar? Vad behöver beaktas när det gäller skydd av känsliga uppgifter i dokument och underskrifter? Avsnittet syftar till en orientering kring området och en utgångspunkt för vidare informationssökning.
- **Teknisk vy** - Hur ska tjänsterna utformas tekniskt, vilka tekniska krav, protokoll och regelverk ska följas vid realisering av tjänsterna?

För använda förkortningar i texten och symboler i bildmaterialet, se *Bilaga: Förkortningar* samt *Bilaga: Symboler*.

1.5 Grundläggande begrepp och termer

Attribut (attribute)
(här) Egenskap för användare, organisationer och IT-systemresurser. T.ex. yrkeslegitimation för personal eller privatpersons namn.

Autentisering (authentication)
Kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan system och/eller fysiska personer. Kontrollen sker mot något slags ”äkthetsbevis” som styrker identitetens riktighet. För autentisering av användare används även termen *legitimering*.

Auktorisation (authorization)
Process för att avgöra om en aktör (användare eller system) har rättighet till viss information och/eller funktion. Även *behörighetskontroll*.

Brokertjänst för underskrift
En serverbaserad tjänst som förmedlar begäran om e-underskrift från en e-tjänst till undertecknaren, för underskrift med hjälp av undertecknarens e-ID.

Dataintegritet/riktighet (data integrity)
Förhindrande av obehörig eller oavsiktlig förändring av elektronisk information.

Digital signatur (digital signature)
Information i elektronisk form som är kryptografiskt kopplad till ett annat elektroniskt material, i syfte att säkerställa det elektroniska materialets dataintegritet och ursprung.

Elektroniskt dokument (electronic document)
Information lagrad i elektronisk form, t.ex. text, bild eller ljud. I texten även förkortat till enbart ”dokument”, där elektronisk form framgår av kontexten.

Elektronisk identifiering (electronic identification)
Process där en aktörs identitet fastställs genom användandet av en elektronisk identitetshandling, typiskt med krav på *autentisering*.

Elektronisk stämpel (electronic seal)
Information i elektronisk form som är kryptografiskt kopplad till ett annat elektroniskt material, i syfte att säkerställa det elektroniska materialets dataintegritet och identiteten för den juridiska person som stämplade materialet.
Elektronisk stämpel utgör för en juridisk person (typiskt organisation) motsvarigheten till en elektronisk underskrift för en fysisk person.
Elektroniska stämplar kan utgöra bevis för att ett elektroniskt dokument har utfärdats av en viss juridisk person och säkerställa dokumentets dataintegritet.

Elektronisk tidsstämpel (electronic time seal / assertion / timestamp)
Information i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt, och därmed kan styrka att de senare uppgifterna existerade vid den angivna tidpunkten. Processen att åstadkomma en tidsstämpel kallas ***elektronisk tidsstämpling*** (***electronic timestamping***).

Elektronisk underskrift (electronic signature)
Information i elektronisk form som är kryptografiskt kopplad till ett annat elektroniskt material, i syfte att säkerställa det elektroniska materialets dataintegritet och undertecknarens (avsändarens) identitet.
Elektronisk underskrift är en tillämpning av digital signatur där materialet är elektroniskt underskrivet av en fysisk person.

> ***Avancerad elektronisk underskrift (Advanced Electronic Signature, AdES)***
> Elektronisk underskrift som uppfyller kraven i eIDAS-förordningen artikel 26.
>
> ***Kvalificerad elektronisk underskrift (Qualified Electronic Signature, QES)***
> En avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftsframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

E-legitimering för underskrift (authentication for signature)
I samband med att en användare bekräftar (godkänner) att en underskrift ska skapas, autentiseras (*e-legitimeras*) användaren via en elektronisk identitetshandling för att säkerställa användarens identitet.

e-ID / e-legitimation (eID)
Identitetshandling i elektronisk form, som vid elektronisk kommunikation används för legitimering, underskrift eller bådadera.

e-tjänst
IT-tillämpning/applikation med användargränssnitt.

Identitets- och åtkomsthantering (Identity and Access Management, IAM)
Sammanfattande benämning på det område som hanterar användares e-identiteter och behörighetsstyrande egenskaper, åtkomst till information i IT-system och regelverken som styr åtkomsten.

Identitetsfederation (identity federation)
Inom identitets- och åtkomsthantering en reglerad samverkan mellan parter med överenskomna regler, där samma elektroniska identiteter godtas av parternas datorsystem. Även kallad ***samordnad identitetshantering***.

Kontrollsumma / kondensat (document digest, hash)
Ett unikt kryptografiskt kondensat av ett dokument, framställt genom användande av en s.k. envägs *hashalgoritm* (t.ex. SHA2). Önskvärda egenskaper hos en hashalgoritm är att kontrollsumman förändras på ett slumpartat sätt vid varje ändring av dokumentet, samt att det inte går att få fram informationen i dokumentet utgående från enbart kontrollsumman.

Kvalificerad anordning för underskriftsframställning
En anordning för skapande av elektroniska underskrifter som uppfyller kraven i bilaga II enligt eIDAS-förordningen.

Lokal säker enhet (secure local device)
(här) Teknisk bärare för en elektronisk identitetshandling.

Oavvislighet/oförnekbarhet (non-repudiation)
Avsändaren av en viss information kan inte förneka att denne är avsändaren. Omvänt kan det även gälla för mottagaren av information. Oavvislighet kan vara ett medel för säkerställande av informationens ursprung.

Signeringscertifikat (signing certificate)
Ett elektroniskt intyg som kopplar valideringsuppgifter för en digital signatur till aktören som står bakom signaturen.

Spärr (revokering) av certifikat (certificate revocation)
Certifikatet görs ogiltigt genom att sätta en spärr. Information om spärrade certifikat tillhandahålls av certifikatutfärdaren.
Även kallat revokering av certifikat.

Stämpelcertifikat (sealing certificate)
Ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk stämpel till en juridisk person. Även *elektroniskt certifikat för e-stämpel*.

Säkerhetskod (PIN)
(här) Samlingsterm för personlig kod för legitimering, ***legitimeringskod***, respektive för underskrift, ***underskriftskod***, kopplade till de certifikat som används. Säkerhetskoden krävs för att kunna använda certifikatets tillhörande privata nyckelmaterial. Ofta kallad PIN.

Singelinloggning (Single sign-on, SSO)
Funktion som medför att användare bara behöver logga in (autentiseras) en gång för en tidsbegränsad session mot en eller flera e-tjänster som utnyttjar SSO. Även kallad ***samlad inloggning***.

Tillitsnivå (assurance level)
En klassificering som anger den tekniska och operationella säkerhetsnivån hos e-legitimationsutfärdaren och olika grader av identitetskontroll av att en person som använder en e-legitimation verkligen är den han eller hon utger sig för att vara.
Kan bl.a. användas i e-tjänst för att sätta kravnivån för giltigt e-ID för åtkomst till e-tjänsten.

Underskriftsbegäran
Det tekniska anropet från en e-tjänst till en underskriftstjänst i syfte att underteckna ett dokument.

Underskriftscertifikat (signing certificate)
Ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person. Vid underskrift via fristående underskrifttjänst används även termen *särskilt underskriftscertifikat*.

Jämför *Legitimeringscertifikat*, även kallat *Autentiseringscertifikat (authentication certificate)*, som används för autentisering av en användare.

Underskriftstjänst / fristående underskriftstjänst (signature service)
En serverbaserad underskriftstjänst som tillhandahåller funktion för elektroniska underskrifter och stämplar. Underskriftstjänsten skapar ett för varje underskrift unikt underskriftscertifikat inklusive ett kryptografiskt nyckelpar.

Undertecknare (signer)
Fysisk person som skapar en elektronisk underskrift. Även: fysisk person som behörigen innehar en anordning för signaturframställning.

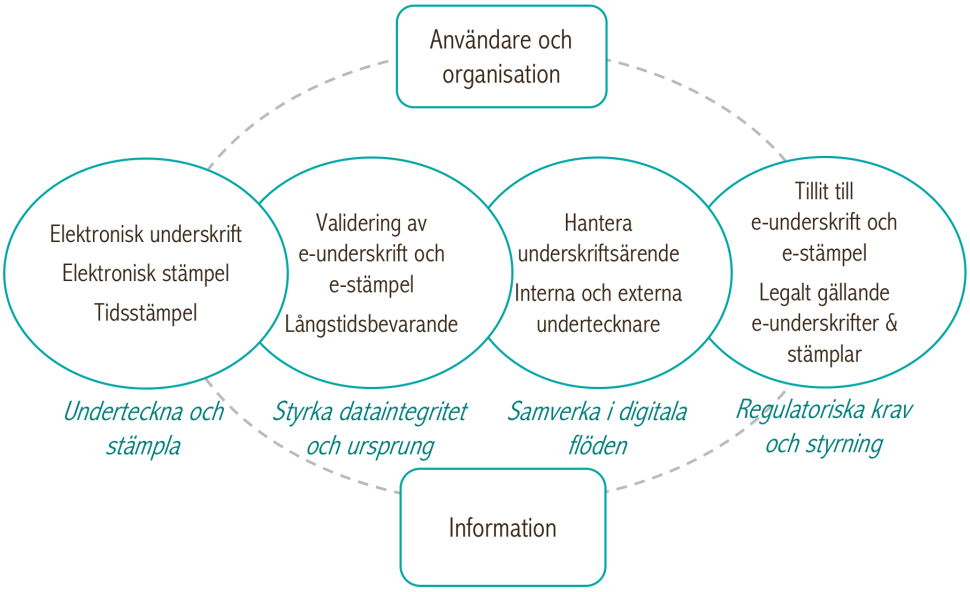
Validering av underskrift och stämpel (signature and seal validation)
Kontroll att underskriften/stämpeln är giltig, och därmed att dokumentet som undertecknats/stämplats är oförvanskat och att dess angivna ursprung är korrekt.

Källförteckning

1. Rikstermbanken, https://www.rikstermbanken.se
2. Svenska datatermgruppen, http://dataterm.termado.net
3. Myndigheten för digital förvaltning, ordlista för e-legitimering och e-underskrift, https://elegnamnden.se
4. PTS, Vägledning för betrodda tjänster i Sverige enligt eIDAS, [Vägledning betrodda tjänster] https://pts.se/sv/bransch/internet/betrodda-tjanster-eidas/
5. SIS-TR 50:2015 Terminologi för informationssäkerhet, https://www.sis.se
6. Referensarkitektur för Identitet och åtkomst [IAM RA]

2 Området elektroniska underskrifter och stämplar

2.1 Översikt



Figur 1. Området elektroniska underskrifter och stämplar - översikt

Området elektroniska underskrifter och stämplar handlar i grunden om

- Bevarande av elektronisk informations ursprung och uppnå oavvislighet, dvs. att det går att i efterhand säkerställa att förmedlad information hade en viss avsändare.
- Bevarande av elektronisk informations dataintegritet, dvs. att det går att över tid säkerställa att informationen är oförvanskad.

Elektroniska underskrifter och stämplar bygger på den bakomliggande tekniken med digitala signaturer. En digital signatur är baserad på en kryptografisk teknik som gör att varje förändring av dokumentet som låg till grund för signaturen kan upptäckas genom att i efterhand kontrollera dokument mot signatur. På motsvarande sätt skyddas själva signaturen mot förändring.

Digitala signaturer har mycket brett användningsområde i olika digitala sammanhang där skydd mot förvanskning och säkerställande av ursprung och autenticitet är viktigt, t.ex. vid säker meddelandeöverföring, överföring av uppgifter från betrodd part till förlitande part i federativa sammanhang, integritetsskydd av publika registeruppgifter, samt inte minst elektroniska underskrifter och stämplar.

Sammanfattat omfattar området förmågor för verksamheter och enskilda att elektroniskt

- Underteckna respektive stämpla elektroniska dokument.
- Validera giltigheten för ett elektroniskt dokuments underskrift resp. stämpel.
- Skapa förutsättningar för att över tid bevara integriteten för innehåll i elektroniska dokument och andra digitala tillgångar.

Referensarkitekturen syftar i stort till att beskriva en modell för hur dessa förmågor kan realiseras i digitala lösningar, hur samverkan kan etableras mellan olika organisationers lösningar, och vilka krav som därmed ställs på e-tjänster och IT-infrastruktur.

2.2 Relation till annan referensarkitektur

Området har en tydlig relation till området *Identitets- och åtkomsthantering*, *IAM*. En förutsättning för att skapa e-underskrifter som mottagare kan lita på är att det finns en tillit till de elektroniska identitetshandlingar som används vid undertecknandet. Referensarkitekturen för elektronisk underskrift och stämpel bygger också vidare på referensarkitekturen för identitet och åtkomst [IAM-RA], genom att nyttja dess förmågor för att utfärda tillförlitliga elektroniska identitetshandlingar samt säkra användarens identitet i samband med elektronisk underskrift.

3 Styrande principer

Vad är styrande för utformning av referensarkitekturen och varför?

3.1 Generella styrande principer

Från *Teknisk referensarkitektur för vård och omsorg* [T-boken] har hämtats ett antal generella styrande principer med syfte att säkerställa spårbarhet, skalbarhet, flexibilitet och interoperabilitet i IT-system. Flertalet av dessa applicerar även direkt på området elektroniska underskrifter och stämplar.

3.1.1 IT2 - Informationssäkerhet

Tillgänglighet, konfidentialitet , riktighet och spårbarhet ska säkerställas vid all samverkan.

Specifikt för området:

- **Konfidentialitet**

  Konfidentialitet[2] behöver beaktas avseende den information som skall undertecknas, samt information som ingår i själva underskriften/stämpeln. Uppgifter som behöver lämnas ut till externa parter bör alltid minimeras.

- **Riktighet**

  En underskrifts/stämpels riktighet är en fundamental egenskap. Underskriften/stämpeln måste skyddas ifrån otillbörlig manipulation, och varje förändring av det undertecknade materialet ska resultera i att den underliggande digitala signaturen inte längre validerar korrekt.

- **Spårbarhet**

  Det ska finnas en spårbarhet till vem som undertecknat/stämplat, vid vilken tidpunkt det skett, och vad som undertecknats/stämplats. Det ska även finnas spårbarhet till utgivaren av certifikat som är kopplade till den digitala signaturen.
  Det bör vidare finnas en spårbarhet till tillitsnivån som uppnåddes för autentiseringen av undertecknaren vid tillfället för undertecknandet.

[2] i [T-boken] IT2 benämnd ”Sekretess”

- **Tillgänglighet**

  Lösningar för elektroniska underskrifter och stämplar ska utformas så att lösningens tillgänglighet kan anpassas efter verksamhetsbehovet. Hänsyn behöver tas till vilka systemberoenden som skapas, samt vilken information och vilka tjänster som behöver vara tillgängliga, vid såväl skapande som validering av digitala signaturer.

3.1.2 IT3 - Skalbarhet

Avser skalbarhet från lokalt till nationellt och vice versa. Lösningarna behöver kunna appliceras såväl på det lokala planet som det nationella. Arkitekturen ska inte begränsa dess användning i detta avseende.

Specifikt för området:

- Underskrifter och stämplar bör kunna användas i samverkan även över landsgränserna. Arkitekturen behöver ta hänsyn till de regulatoriska krav som ställs inom området, inte minst genom eIDAS-förordningen [eIDAS].

3.1.3 IT4 - Lös koppling & interoperabilitet

Principen innebär bl.a. att en komponent i en lösning kan bytas ut oberoende av andra. Detta uppnås genom en tjänstebaserad arkitektur med kommunikation genom gemensamma, standardiserade gränsytor mellan komponenter.

Interoperabla, internationellt beprövade och för leverantörer tillgängliga (öppna) standarder tillämpas för meddelandeutbyte mellan system.

Specifikt för området:

- Arkitekturen bör skapa förutsättningar för att kunna byta ut (del av) lösning för e-underskrifter/e-stämplar mot en annan, genom användande av standardiserade gränsytor.
- Informationsöverföring och validering av elektroniska underskrifter och stämplar över organisations- och landsgränser förutsätter att gemensamma standarder används för att möjliggöra interoperabilitet.

3.1.4 IT6 - Samverkan i federation

Samverkan över organisationsgränser sker genom federation, såsom exempelvis identitetsfederering. Federation bygger på gemensamma överenskomna regelverk, t.ex. kring krav på autentisering av användare i IT-system, tekniska regelverk osv.

Specifikt för området:

- Principerna kring användande av identitets- och behörighetsfederering, se [IAM-RA], bör även kunna tillämpas för lösningar som skapar elektroniska underskrifter och stämplar.

3.2 Styrande principer för elektroniska underskrifter och stämplar

Inom området elektroniska underskrifter och stämplar definierar referensarkitekturen följande kompletterande och fördjupande styrande principer.

3.2.1 ES1 - Standardiserade gränssnitt

E-tjänsterna respektive IT-infrastrukturen för elektroniska underskrifter och stämplar separeras genom standardiserade gränssnitt.

Motiv: Ger en lös och standardiserad koppling mellan e-tjänsterna och de generella funktionerna för elektroniska underskrifter och stämplar. Produktanpassningar blir applicerbara på en global marknad, och bättre förutsättningar för att marknadens produkter kommer anslutningsklara från början. Skapar även grundförutsättningar för utbytbarhet, federativa lösningar och återanvändning av teknikinvesteringar. Minskar inlåsningseffekterna mot viss hårdvara och mjukvara.

3.2.2 ES2 - E-legitimering för underskrift

Lösningar för e-underskrift bör möjliggöra att använda s.k. *e-legitimering för underskrift*, vilket innebär att den elektroniska identitetshandlingen som används för att identifiera och autentisera användaren i e-tjänsten, även används vid e-underskriften.

Motiv: Det blir möjligt att använda etablerade elektroniska identitetshandlingar även för e-underskrifter. Detta är även i linje med reglering inom EU [eIDAS], vilket skapar förutsättningar för interoperabla underskrifter både nationellt och internationellt.

3.2.3 ES3 - Uppgiftsminimering

Lösningar för elektronisk underskrift och stämpel bör möjliggöra att minimera de uppgifter som behöver lämnas ut till tredje part.
Det bör vara möjligt att behålla skyddet för känslig information, även vid användande av extern, och eventuellt delad, underskriftstjänst. T.ex. bör dokument som undertecknas eller valideras inte behöva lämnas ut till externa tjänster.

Motiv: Minskar risken för exponering av känsliga uppgifter och därmed behovet av kompenserande skyddsåtgärder. Principen underlättar att använda på marknaden tillgängliga tjänster för e-underskrifter, samt att samverka med andra parter kring gemensamma, delade, lösningar för e-underskrift.

3.2.4 ES4 - ”Det du ser är vad du undertecknar” - *WYSIWYS*[3].

Lösningar för elektroniska underskrifter ska utformas så att det semantiska innehållet i det dokument som undertecknas, vilket undertecknaren ges möjlighet att granska, alltid bevaras genom den elektroniska underskriften.

Motiv: Att undertecknaren kan känna full trygghet i att det som undertecknas elektroniskt också semantiskt fullt ut överensstämmer med vad undertecknaren visuellt kan ta del av som underlag, är en grundbult för att uppnå tilltro till ett system för elektroniska underskrifter. Det är viktigt att poängtera att det är innebörden av det som undertecknaren visuellt kan ta del av som säkerställs, eftersom den fulla digitala representationen (t.ex. en binärfil i PDF-format eller en transaktion), inte kan visas för undertecknaren.

3.2.5 ES5 - Linjera med Referensarkitektur IAM

Utformning av lösningar för elektroniska underskrifter och stämplar ska linjera med Referensarkitektur för Identitets- och åtkomst [IAM-RA]. För tillämpliga delar innebär det bl.a. att tjänsterna ska kunna samverka, och att de styrande principer för området identitet och åtkomst även gäller inom detta område.

Motiv: En förutsättning för elektroniska underskrifter är tillgång till tillförlitliga elektroniska identitetshandlingar och tjänster för att säkra undertecknarens identitet och behörighet i samband med undertecknade. Genom samverkande tjänster undviks att behöva bygga upp parallella strukturer för dessa förmågor.

3.2.6 ES6 - Plattformsneutralitet

IT-infrastruktur för elektroniska underskrifter och stämplar byggs i grunden plattformsneutral. Eventuella plattformsspecifika delar läggs till som anpassningar ovanpå grundstrukturen.

Motiv: IT-infrastruktur för elektronisk underskrift och stämpel behöver kunna nyttjas för alla de olika typer av e-tjänster och klienter som ingår i verksamhetens IT-stöd: webb, tunna och feta klienter, mobila plattformar osv. Alternativet är att bygga, förvalta och administrera parallell IT-infrastruktur, vilket är resurs- och kostnadsdrivande.

3.2.7 ES7 - Säkerställ bevarande av dokument och signatur

Utformning av lösningar och val av format för elektroniska underskrifter och stämplar ska säkerställa att krav kring bevarande av digitalt signerade dokument (handlingar) kan

[3] *What You See Is What You Sign*

uppfyllas. Principen omfattar bevarande av det signerade dokumentet, signaturen självt samt förmågan att i efterhand validera signaturen.

Motiv: Det är viktigt att lösningar för elektroniska underskrifter och stämplar som följer referensarkitekturen möjliggör att hantera Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar och tekniska krav [RA-FS 2009:1-2].

4 Verksamhetsvy – behov och förmågor

Verksamhetsvyn beskriver referensarkitekturen utifrån verksamhetens behov, och lyfter fram de förmågor inom området elektroniska underskrifter och stämplar som behövs för att stödja behovet.

4.1 Verksamhetsbehov och drivkrafter

Referensarkitekturen syftar bland annat till att möta följande behov hos verksamheter och enskilda individer:

- **Digitalt först**
  - Digitala underskrifter skapar bättre förutsättningar för ett helt pappersfritt informationsflöde, t.ex. i processer där det ingår undertecknande av dokument, t.ex. protokoll, avtal osv. I en del processer behövs även legalt gällande e-underskrifter.
  - För att stödja pappersfria informationsflöden ska man kunna hantera underskriftsärenden, där det kan förekomma såväl interna som till organisationen externa undertecknare.
- **Mobila arbetssätt**
  - Användare ska kunna utföra underskrift på mobila plattformar såväl som stationära och/eller med mobila e-ID.
- **Underlätta anskaffning av digitala underskriftstjänster**
  - Med en gemensam referensmodell och gemensamma krav, underlättas anskaffning och etablering av digitala lösningar för e-underskrifter.
- **Minska inlåsning och kostnader**
  - Genom att standardisera integrationsgränssnitt mellan underskriftstjänster och andra delar av IT-miljön, ges bättre förutsättningar för byte av leverantör/lösning, och även för att organisationer ska kunna dela lösning för e-underskrift.
  - Verksamhet och invånare bör kunna arbeta med elektroniska underskrifter på de tekniska verktyg som bäst är anpassade för deras behov (datorer, läsplattor, tryckkänsliga tavlor, mobiler, osv.), med så liten teknisk inlåsning som möjligt.
- **Samverkan över organisationsgränser**
  - Med ett gemensamt ramverk för att validera och lita på e-underskrifter och e-stämplar från andra organisationer, kan digital samverkan över organisationsgränserna underlättas.

- Genom stöd för e-underskrifter enligt eIDAS-förordningen, underlättas samverkan inom såväl Sverige som EU:s inre marknad.

- **Undvik stuprörslösningar och möjliggör återanvändning**
  - Verksamheter och invånare ska kunna nyttja befintliga och kommande elektroniska id-handlingar (e-ID) och tillhörande infrastrukturtjänster även för elektroniska underskrifter. De infrastrukturella digitala tjänster som byggs upp för e-ID och dess användning i e-tjänster, ska kunna samverka med och utnyttjas av underskriftstjänster.

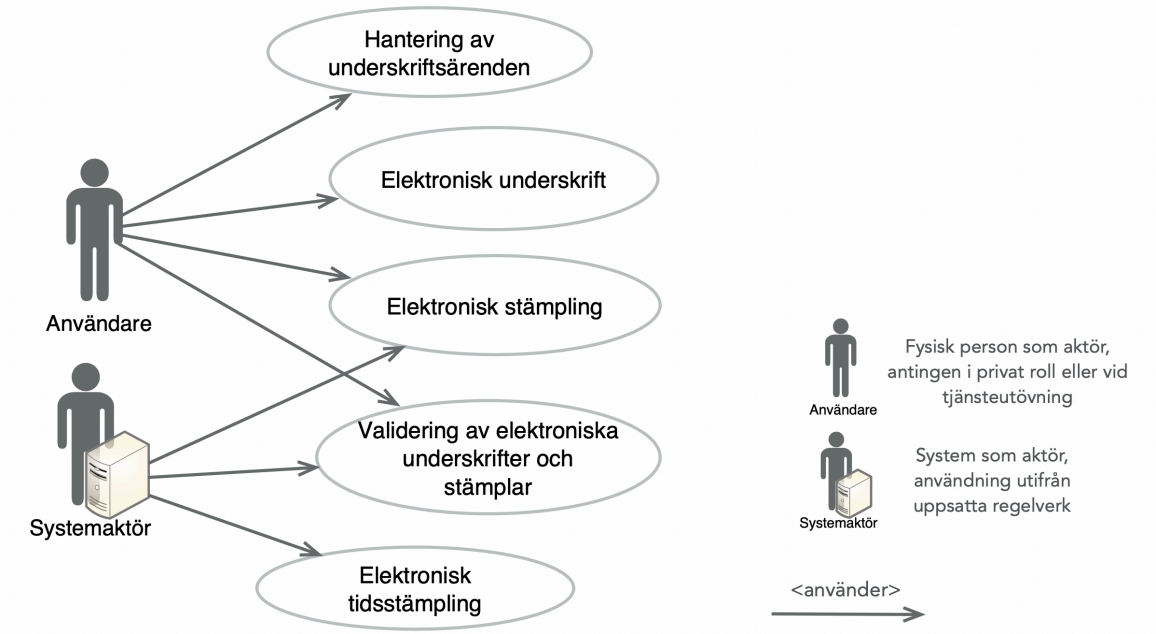
Behoven styr referensarkitekturen i en riktning mot

- Standardisering av säkerhetstekniken och gränsytorna mot övrigt IT-stöd.
- Separation av förmågor där respektive delsystem fokuserar på det den är ämnad för, t.ex. att tydligt skilja på att hantera säker inloggning respektive hantera verksamhetsinformation.
- Plattformsneutrala lösningar som medger flexibilitet i teknikval.

I de följande kapitlen kommer några huvudsakliga flöden gås igenom inom området elektroniska underskrifter och stämplar. I informationssystemvyn kommer dessa flöden och förmågor sedan omsättas i samverkande tjänster.

4.2 Användningsfall

4.2.1 Översikt



Figur 2. Användningsfall - översikt.

Ovan bild beskriver schematiskt de huvudsakliga användningsfallen inom området elektroniska underskrifter och stämplar, och hur de övergripande relaterar till användare och systemaktörer.

4.2.2 Elektronisk underskrift av dokument

Elektronisk underskrift av dokument kan typiskt användas för att påvisa att en fysisk person (ev. i en viss roll) står bakom, godkänner eller intygar att innehållet i dokumentet är korrekt.

I pappersbaserade processer där undertecknande av individer krävs, kan elektronisk underskrift vara ett sätt att helt digitalisera processen. Noteras kan dock att elektronisk underskrift framförallt gör nytta när

- Det behövs ett sätt för alla ingående parter att säkert verifiera underskrifter, som inte är beroende av ett viss IT-system. T.ex. kan detta gälla när undertecknade dokument överförs mellan flera parter med egna IT-lösningar.
- Det finns behov av legalt eller i visst sammanhang gällande e-underskrifter, t.ex. i avtalshantering, protokollföring, granskning- och godkännandeprocesser.

Att underteckna i tjänstemanna- resp. privat roll

Ur ett tillämpningsperspektiv bör man skilja på underskrift som görs av en handläggare i sin tjänstemannaroll, och underskrift i egenskap av privatperson.
I det senare fallet är det centralt att kunna knyta underskriften till individen, typiskt baserat på dennes personnummer.
I tjänsteutövning är det ofta minst lika viktigt att knyta underskriften till undertecknaren i viss roll i en organisation. Detta kan styra behovet av vilken typ av uppgifter som behöver säkras och kopplas till e-underskriften.

Elektroniska underskrifter med utländska e-legitimationer enligt eIDAS

EU-förordningen om elektronisk identifiering och betrodda tjänster [eIDAS], ställer krav på svenska offentliga organ att erkänna de e-legitimationer som andra eIDAS-länder har anmält. Detta innebär att en offentlig svensk e-tjänst baserat på vissa regler skall kunna acceptera en inloggning som utförs med en e-legitimation utställd i ett annat land. Det omvända förhållandet kan också gälla, dvs. att svenska anmälda e-legitimationer ska kunna accepteras i utländska e-tjänster.

Behovet att stödja utländska e-legitimationer kan appliceras på såväl elektronisk identifiering som underskrift i e-tjänsterna.

4.2.3 Elektronisk stämpling av dokument

En elektronisk stämpel visar att organisationen står bakom en elektronisk handling, och ger samtidigt handlingen ett integritetsskydd. Skillnaden mellan en elektronisk stämpel och en elektronisk underskrift är primärt att det med stämpeln är den *juridiska personens identitet* som framgår istället för den enskilda personens.

Elektroniska stämplar röjer inga uppgifter om fysiska personer (tjänstemän, privatperson osv.). En e-stämpel kan t.ex. vara lämpligt att använda för att visa att det är myndigheten som fattat beslutet och inte en enskild tjänsteman.

Elektroniska stämplar kan användas för att säkerställa att ett dokument utfärdats av en viss juridisk person, men även för att påvisa autenticitet för en juridisk persons digitala tillgångar, t.ex. programvarukoder eller servrar, genom att digitalt knyta tillgångarna till den juridiska personen.

4.2.4 Elektronisk tidsstämpling av dokument

En elektronisk tidsstämpel visar att en elektronisk handling hade ett visst innehåll vid en viss tidpunkt.
Genom att använda en betrodd tidsstämplingstjänst kan alla förlitande parter verifiera att den tidsstämplade informationen existerade före dess tidsstämpel.

Digital signatur med tidsstämpel *(Signature with timestamp)*

En viktig användning av tidsstämpling är att bevara möjlighet att vid senare tidpunkt validera underskrifter och stämplar, oavsett om det använda certifikatet för signaturen senare skulle återkallas eller ha passerat sin giltighetstid. Tidsstämpeln påvisar att både informationen och dess signatur existerade vid tidpunkten för tidsstämplingen, dvs. det går att påvisa att signaturen skapades vid en tidpunkt då underskriftscertifikatet fortfarande var giltigt.

Långtidsbevarande med valideringsmöjlighet (*Long-Term Archiving and Validation*)

Tidsstämpling kan även användas för att säkerställa bevarande av dokument och tillhörande underskrifter och stämplar över mycket lång tid, trots att teknikutveckling kan ha gjort tidigare teknik för e-underskrift och e-stämpel osäker eller otillgänglig.

4.2.5 Validering av elektroniska underskrifter och stämplar

Validering av elektronisk underskrift och stämpel omfattar att kontrollera att underskriften resp. stämpeln är giltig, och därmed att dokumentet är oförvanskat sedan tidpunkten för underskriften/stämplingen.
Det kan avse validering som den egna organisationen gör för undertecknade och stämplade handlingar som organisationen hanterar, men även validering hos en extern part som mottar ett undertecknat/stämplat dokument.

Man kan skilja på tre fall av validering som ställer delvis olika krav:

1) Validering **i nära anslutning till** skapandet av e-underskrift eller e-stämpel, t.ex. omedelbart efter att en undertecknad handling inkommer till en organisation. I detta fall kan antagas att förutsättningarna för valideringen är de samma som vid skapandet av e-underskriften eller e-stämpeln.
2) Validering **efter lång tid**, dvs. en lång tid efter skapandet av e-underskrift eller e-stämpel.
   I detta fall kan det behövas ytterligare valideringsinformation för att avgöra om e-underskriften eller e-stämpeln är korrekt utförd.
   Det förutsätts dock här att den använda tekniken som använts vid framställning av den digitala signaturen fortfarande är aktuell och giltig.
3) Validering **efter mycket lång tid**, där teknikutvecklingen kan ha förändrat de tekniska förutsättningarna för framställning och validering av digitala signaturer. De ändrade förutsättningarna ställer ytterligare krav på tillgänglig valideringsinformation för att avgöra om e-underskriften eller e-stämpeln är korrekt utförd.

Hur dessa fall kan realiseras i arkitekturen och vilka krav det ställer på valideringsinformationen beskrivs vidare i *Arkitekturella mönster*.

4.2.6 Hantering av underskriftsärenden

Vid praktisk tillämpning av elektroniska underskrifter kan man behöva stöd för att hantera underskriftsärenden, där handläggare kan förbereda och genom hela processen hantera ett ärende för att underteckna ett eller flera dokument, eventuellt i flera steg.

Ett systemstöd för underskriftsärenden bör typiskt kunna hantera följande:

- Ange vilket/vilka dokument som behöver undertecknas.
- Ange vilken eller vilka personer som bör underteckna, ev. i vilka respektive roller de ska underteckna, samt ev. i vilken ordning de ska underteckna (för kontrasignering).
- Ange vilket syfte undertecknandet har, t.ex. godkänna att innehållet överensstämmer med vad som sades på mötet, undertecknade för beslut/fastställande av dokumentet osv.
- Utskick av notifiering av underskriftsärende till berörda undertecknare, typiskt med länk för att kunna logga in till ärendet.
- Möjlighet för undertecknare att logga in i systemstödet för att slutföra processen att underteckna ett eller flera dokument.
- Möjlighet att granska dokument i underskriftsärende och ändra status till godkänd för undertecknande eller motsvarande.
- Styrning av behörigheter, dels för att skapa och administrera underskriftsärenden, dels för att endast tilldelade undertecknare kommer åt ärendet och dessa dokument.
- Säker elektronisk identifiering och autentisering av användare (handläggare/undertecknare).
- Loggning av spårbarhetsinformation, såsom vem/vilka som undertecknat/stämplat, vid vilken tidpunkt det skett, vad som undertecknats/stämplats.

Vidare kan ett sådant systemstöd innehålla funktioner för

- Lagring/arkivering av undertecknade dokument.
- Konvertering av dokument till lämpligt format för undertecknande och arkivering.
- Hantera både för organisationen interna och externa användare.

Mer om hur sådant systemstöd kan realiseras baserat på referensarkitekturen i *Hantering av ärendeflöden för underskrift och stämpel*.

5 Informationssystemvy

Informationssystemvyn beskriver en referensarkitektur för hur samverkan och funktion uppstår via tjänster i IT-stödet. Vilka infrastrukturtjänster behövs för att realisera beskrivna förmågor?

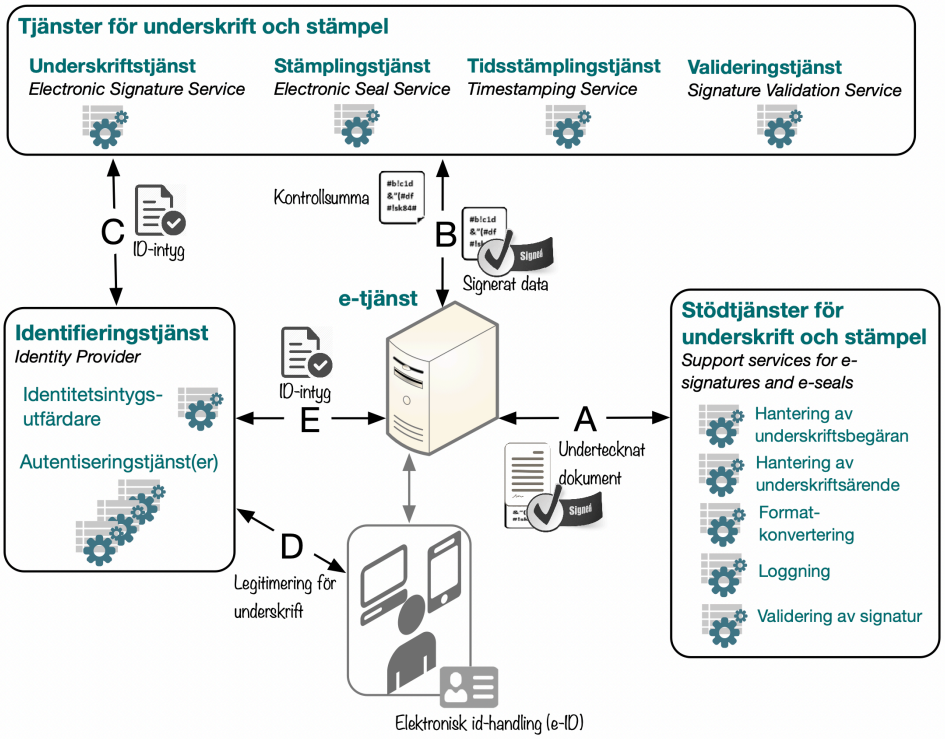
5.1 Referensmodell för elektroniska underskrifter och stämplar

5.1.1 Översikt

Referensarkitekturen för elektroniska underskrifter och stämplar innehåller ett antal IT-infrastrukturtjänster som ger de grundläggande förutsättningarna för att realisera

- Elektronisk underskrift.
- Elektronisk stämpling.
- Elektronisk tidsstämpling.
- Validering av elektroniska underskrifter och stämplar.
- Hantering av underskriftsärenden.

Arkitekturen kan översiktligt visualiseras i följande referensmodell:



Figur 3. Referensmodell för elektroniska underskrifter och stämplar – översikt

Följande egenskaper är utmärkande för referensarkitekturen:

- ✓ Stöd för att realisera e-tjänster som hanterar processer där elektroniska underskrifter och stämplar ingår.
- ✓ Stödjer återanvändning och delning av tjänster för underskrift och stämpel.
- ✓ Följsam till riktlinjer och normativa specifikationer för fristående underskriftstjänster i Sverige [Sweden Connect]
- ✓ Stödjer användning av e-underskrifter och e-stämplar enligt eIDAS-förordningen [eIDAS].
- ✓ Linjerar med Referensarkitektur för Identitet och åtkomst [IAM-RA] - möjliggör att bygga vidare på infrastrukturtjänster inom IAM-området för elektroniska underskrifter.

5.1.2 Referensarkitekturens ingående tjänster

Referensarkitekturen omfattar ett antal betrodda tjänster som utgör grunden i en arkitektur för elektroniska underskrifter och stämplar:

- Underskriftstjänst
- Stämplingstjänst
- Tidsstämplingstjänst
- Valideringstjänst
- Identifieringstjänst

5.1.2.1 Funktionaliteten realiseras i e-tjänster

Referensarkitekturen utgår från en behörig och autentiserad användare som via *e-tjänster* får tillgång till att underteckna dokument, validera elektroniska underskrifter, använda organisationens e-stämpel, hantera underskriftsärende osv.
Arkitekturen stödjer även att ett system (e-tjänsten själv), utan inblandning av användare, använder tjänsterna för elektronisk stämpel, tidsstämpling och validering av signatur.

5.1.2.2 Stödjande tjänster

Användare loggar in i e-tjänst och autentiseras med stöd av en *Identifieringstjänst (IdP)*, enligt [IAM-RA].
När användaren önskar underteckna/stämpla ett dokument, kan e-tjänsten ta hjälp av *stödtjänster* för att

- Vid behov konvertera dokumentet till format lämpligt för digital signatur samt ev. arkiveringskrav.

- Utgående från dokumentet som ska undertecknas/stämplas, skapa en underskriftsbegäran och skicka denna till *Underskriftstjänst.* I begäran ingår en för dokumentet unik kontrollsumma.
- Hantera den resulterande elektroniska underskriften från *Underskriftstjänst* och sammanfoga till ett undertecknat/stämplat dokument enligt standardformat för digitala signaturer.
- Logga spårbarhetsinformation avseende underskriften/stämpeln.

5.1.2.3 Betrodda tjänster för underskrift och stämpel

Underskriftstjänsten ansvarar för att utgående från en begäran om undertecknande samt verifiering/godkännande av undertecknaren skapa en digital signatur. Beroende på användningsfallet kan den digitala signaturen motsvara en elektronisk underskrift eller stämpel[4].
Den digitala signaturen baseras på ett underlag i begäran som genererats utifrån det dokument som ska undertecknas/stämplas.
Tjänsten är fristående i avseendet att den genererar den digitala signaturen utgående från nyckelmaterial och certifikat som tjänsten själv tillhandahåller och står som garant för.

Underskriftstjänsten delegerar autentisering av undertecknaren vid tillfället för undertecknandet till *Identifieringstjänsten*. Beroende på vilken typ av elektronisk identitetshandling användaren innehar, använder identifieringstjänsten motsvarande *Autentiseringstjänst* för själva autentiseringen, här kallad *legitimering för underskrift*. I samband med undertecknandet visas även för användaren vad som undertecknas.

Stämplingstjänst ansvarar för att på begäran elektroniskt stämpla en viss informationsmängd. Den elektroniska stämpeln kan användas för att i efterhand verifiera dataintegritet och/eller avsändare för informationen, t.ex. vid utlämnande av ett dokument från en part till en annan.
Till skillnad mot *Underskriftstjänsten* ställer inte stämplingstjänsten krav på att en fysisk person undertecknar varje enskilt dokument: stämplingstjänsten autentiserar och auktoriserar istället det anropande systemet. Därmed kan stämplingstjänst användas för elektronisk stämpling inom automatiserade processer.

[4] Se vidare

Användningsfall

Med hjälp av *Tidsstämplingstjänst*[5] kan viss informationsmängd knytas till en säkerställd tidpunkt. Tidsstämpeln ger spårbarhet till att informationen såg ut på visst sätt vid en bestämd tidpunkt. Tidsstämpling kan användas upprepat på en viss informationsmängd, och även i kombination med organisationens stämpel, för att kunna bevara och påvisa dataintegritet för information över lång tid.

Undertecknade/stämplade dokument kan i efterhand valideras, antingen lokalt med hjälp av en stödtjänst, eller genom nyttjande av en betrodd *Valideringstjänst*.

5.1.3 Relation till Referensarkitektur för Identitet och åtkomst

Genom att referensarkitekturen nyttjar identifieringstjänst (IdP) från Referensarkitektur för Identitet och åtkomst [IAM-RA] för användarautentisering, kan uppbyggd infrastruktur för elektronisk identifiering återanvändas för e-underskrifter. Dock ställer arkitekturen kompletterande krav på de identifieringstjänster som ska kunna användas för elektronisk underskrift.

Följsamheten till Referensarkitektur för Identitet och åtkomst ger också mönster för att federera tjänster inom elektroniska underskrifter och stämplar.

Dessa kopplingar beskrivs mer utförligt i följande kapitel.

[5] *Timestamping Service* även kallad *Timestamping Authority, TSA*

5.2 Elektronisk underskrift och stämpel

5.2.1 Arkitekturella mönster

Arkitekturellt kan man skilja på två principiella mönster för att skapa elektroniska underskrifter och stämplar:

- Digital signatur via lokalt e-ID
- Digital signatur via (fristående) underskriftstjänst

5.2.1.1 Digital signatur via lokalt e-ID

Vid *digital signatur via lokalt e-ID* används ett underskriftscertifikat och tillhörande hemligt nyckelmaterial, som e-identitetsutfärdaren försett användaren med. Processen hanteras normalt av en klientprogramvara och den digitala signaturen genereras i en s.k. *lokal säker enhet* (*secure local device*) innehållande det hemliga nyckelmaterialet. Processen kan också understödjas av en *brokertjänst* som kan ge e-tjänster ett tekniskt gränssnitt för att begära underskrift/stämpel som är oberoende av klientprogramvaran.

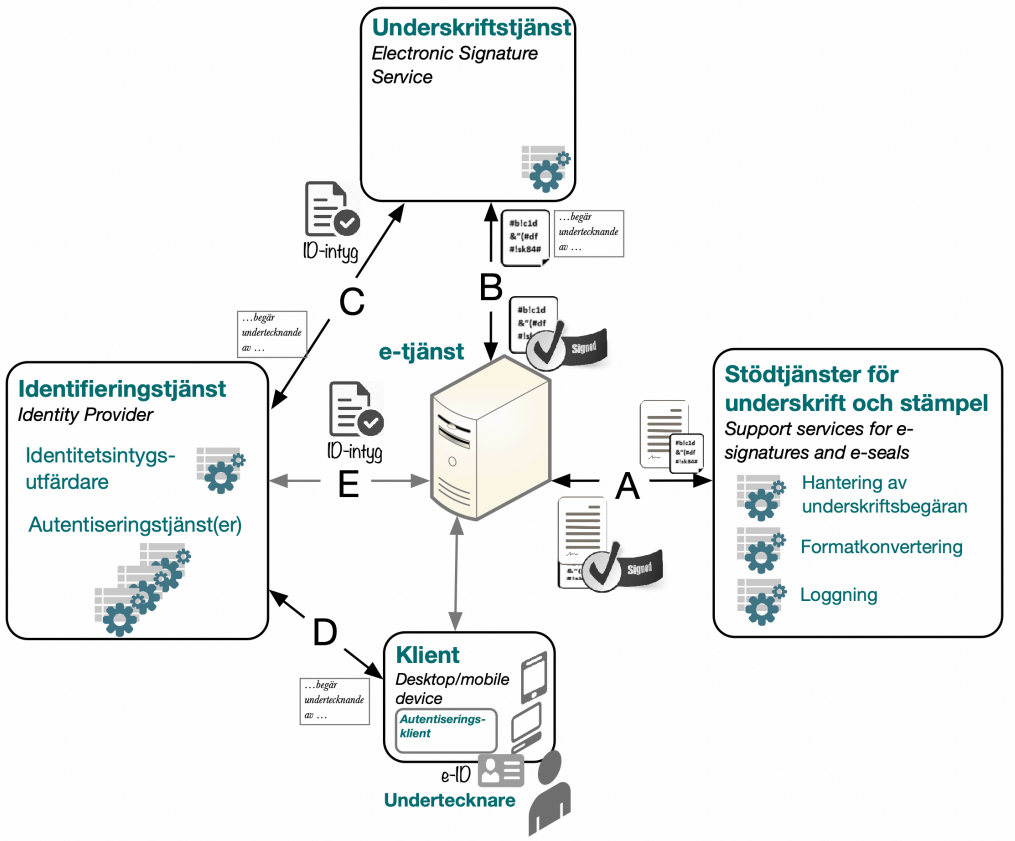
5.2.1.2 Digital signatur via underskriftstjänst

Vid *digital signatur via underskriftstjänst* används istället en fristående underskriftstjänst som ansvarar för att framställa den digitala signaturen. Underskriftstjänsten tillhandahåller (i realtid) ett för den specifika underskriften unikt underskriftscertifikat och tillhörande hemligt nyckelmaterial. Underskriftscertifikatet knyts till undertecknaren genom valideringsdata, baserat på autentiseringen i samband med att undertecknaren godkänner underskriften.

Referensarkitekturens principer ES1 - separation i löst kopplade tjänster med standardiserade gränssnitt - och ES2 - användande av e-legitimering för underskrift - styr mot att använda mönstret *digital signatur via underskriftstjänst*.
Digital signatur via lokalt e-ID och brokertjänst beskrivs dock också nedan för jämförelsens skull.

5.2.2 Digital signatur via fristående underskriftstjänst

5.2.2.1 Översikt



Figur 4. Digital signatur via fristående underskriftstjänst – översikt.

(A) E-tjänsten kan ta hjälp av lokala stödtjänster för att skapa en underskriftsbegäran, ta emot och hantera den resulterande underskriften/stämpeln, och slutligen sammanfoga till ett undertecknat dokument.

(B) E-tjänsten begär och erhåller underskriften/stämpeln från en fristående *Underskriftstjänst*.

(C) Underskriftstjänsten delegerar autentisering av användaren (*undertecknaren*) i samband med underskriften till betrodd *Identifieringstjänst (IdP)*. Identifieringstjänsten returnerar ett *identitetsintyg* som resultat av en utförd e-legitimering för underskrift.

(D) Identifieringstjänsten ansvarar för att autentisera användaren som ett godkännande av underskriften, även kallat *e-legitimering för underskrift.*

(E) E-tjänsten delegerar autentisering av användaren i e-tjänsten till identifieringstjänsten enligt [IAM-RA].

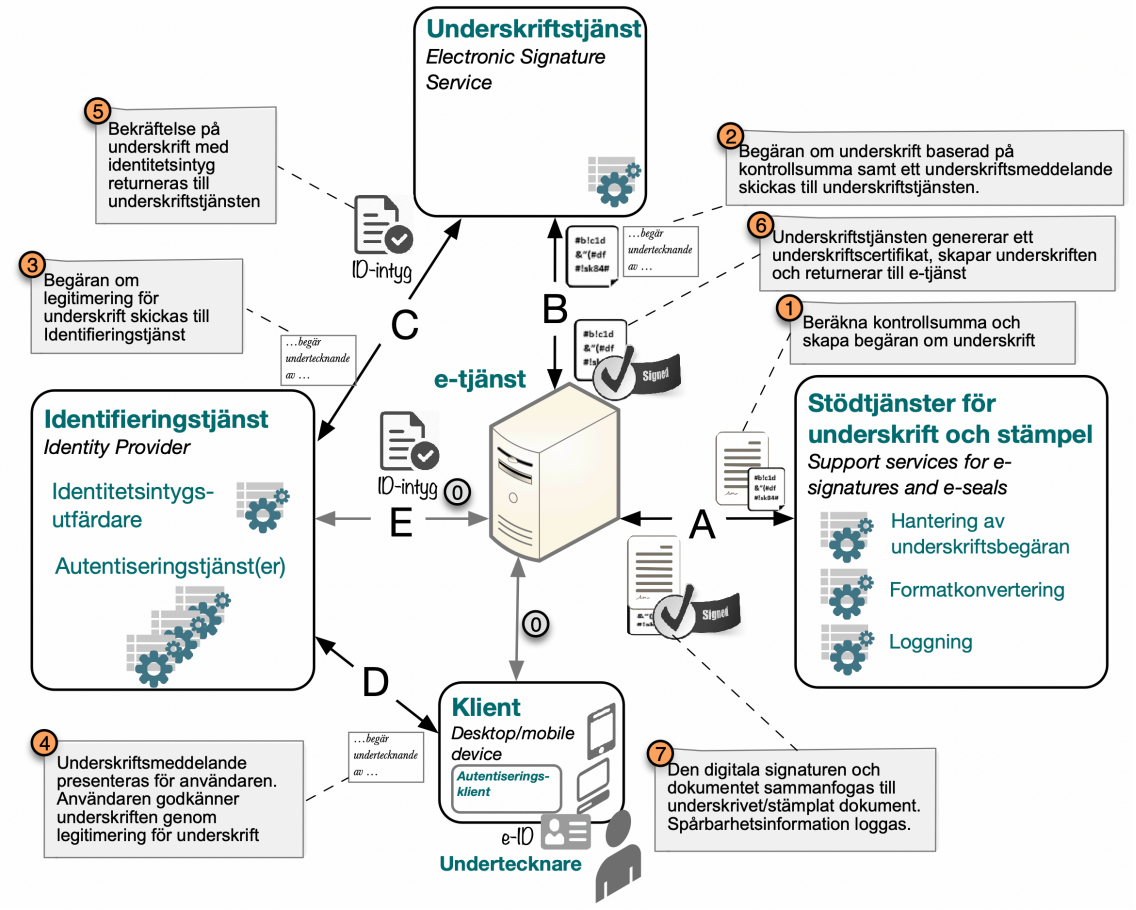
5.2.2.2 Utmärkande för digital signatur via underskriftstjänst

Följande är värt att notera vid digital signatur via fristående underskriftstjänst:

- Principerna för mönstret är följsamma till riktlinjer och normativa specifikationer för fristående underskriftstjänster [Sweden Connect], och stödjer användning av elektroniska underskrifter och stämplar enligt eIDAS-förordningen [eIDAS].
- Mönstret gör det tekniskt möjligt att använda olika typer av elektroniska identitetshandlingar (e-ID), förutsatt att dessa erbjuder tillräcklig grad av tillit, även sådana som inte är certifikatbaserade, utan att speciella anpassningar i e-tjänsten behövs. Resultatet av en e-legitimering för underskrift är alltid ett elektroniskt utställt identitetsintyg med samma format oavsett vilken typ av e-legitimation som användaren använder.
  Det medför också att underskrifter kan nyttja legitimeringscertifikatet i de e-ID som används, och dessa behöver således inte ha stöd för speciella underskriftscertifikat (även om dessa också stöds i mönstret).
- Genom att användarorganisationens Identifieringstjänst kan användas för att autentisera användaren i samband med underskriften, ges möjlighet att återanvända organisationens befintliga infrastruktur för elektronisk identifiering för e-underskrifter och -stämplar. Dock ställs kompletterande krav på Identifieringstjänsten, bl.a. att kunna hantera underskriftsmeddelande, se vidare det detaljerade flödet nedan.
- Tilliten till underskriften styrs av tilliten till använt e-ID samt till Underskriftstjänsten och dess mekanismer för framställande av underskriftscertifikat. Tillitsnivå kan förmedlas både i begäran och i det resulterande svaret.
- Mönstret stödjer en federativ samverkan kring elektroniska underskrifter och stämplar, se vidare *Arkitekturella mönster för federativ samverkan*.
- Vid digital signatur via underskriftstjänst abstraheras tekniken för själva framställan av digital signatur bort från e-tjänsterna. Framställan av digital signatur hanteras av underskriftstjänsten, och användarautentiseringen kan göras *out-of-band*, dvs. i en annan teknisk kanal separerad från e-tjänstens kanal. Detta skapar en lösare teknisk koppling (minskar teknikberoendet) till klientdatorn, klientprogramvaran samt den eventuella hårdvara som används som bärare av e-ID.
- Den resulterande underskriften/stämpeln kan anpassas efter det aktuella användningsfallet, genom att styra detta i Underskriftstjänsten. T.ex. kan en underskrift som görs av en handläggare i sin tjänstemannaroll utformas på ett annat sätt än om samma person undertecknar som privatperson.

- Det rekommenderas att etablera för organisationen lokala stödtjänster för e-underskrifter och stämplar, för att förenkla användningen i e-tjänster. Det är dock även möjligt att låta e-tjänsten realisera dessa funktioner själv.
- Tillgängligheten för en lösning med digital signatur via underskriftstjänst är beroende av underskriftstjänsten, identifieringstjänsten samt stödtjänsterna. Alla dessa komponenter kan utifrån verksamhetens behov utformas för hög tillgänglighet (typiskt multipla instanser), samt kan skalas horisontellt (fler instanser) och vertikalt (mer resurser till varje instans).

5.2.2.3 Principiellt flöde för digital signatur via underskriftstjänst



Figur 5. Digital signatur via fristående underskriftstjänst – principflöde.

Det principiella flödet vid digital signatur via fristående underskriftstjänst kan beskrivas enligt följande:

0. (Försteg) Användaren, här även kallad *undertecknare (signer)*, loggar in i e-tjänst[6] som erbjuder funktion för undertecknande/stämpling av dokument.
    a. Användaren autentiseras med stöd av en *Identifieringstjänst (IdP)*, samt auktoriseras för användning av e-tjänsten **(E)**.
    b. Användaren väljer att underteckna/stämpla ett dokument.
    c. E-tjänsten ansvarar för visa upp (det semantiska) innehållet i dokumentet för påseende/granskning av användaren, enligt styrande princip ES4 ”*Det du ser är vad du undertecknar*”[7].
1. **(A)** E-tjänsten tar hjälp av lokal stödtjänst för att ev. konvertera dokumentet till lämpligt format för digitala signaturer, samt skapa en *underskriftsbegäran* inkluderande
    a. En *kontrollsumma* av dokumentet som ska undertecknas (*document digest*).
    b. *Identifieringstjänst*[8] att använda för autentisering av användaren i samband med underskriften (*identity provider, IdP*).
    c. *Personidentifierare* för användaren, vilken erhållits från Identifieringstjänsten (*signer*).[9]
    d. *Underskriftsmeddelande* (*sign message*) - ett textmeddelande att visa upp för användaren i samband med underskriften.
    e. Den *tillitsnivå* som e-tjänsten begär att underskriften utförs på (*signature assurance level)*.[10]
    f. Namn/identifierare på den *e-tjänst* som är avsändare av underskriftsbegäran (*service provider*).
    g. Det underskriftsformat (*signature format*) som önskas (om valbart hos underskriftstjänsten).
2. **(B)** E-tjänsten tar hjälp av stödtjänst för att skicka underskriftsbegäran till *Underskriftstjänst*. Underskriftstjänsten verifierar att begäran är korrekt ställd,

[6] E-tjänst som erbjuder elektronisk underskrift/stämpling kan även kallas ”*Signature Requestor*”

[7] Se *Specifika krav* för mer information.

[8] Kan vara samma IdP som användes vid inloggningen i e-tjänsten, men är inte ett krav.

[9] Kan utelämnas varvid identifieringstjänsten ansvarar för att säkerställa personidentifieraren.

[10] Eventuellt är denna underförstådd genom att den valda ingången till underskriftstjänsten är knuten till en specifik tillitsnivå.

bl.a. att angiven identifieringstjänst är en betrodd tjänst för ändamålet, och returnerar annars ett fel.

3. **(C)** Underskriftstjänsten skickar en digitalt signerad ”*begäran om e-legitimering för underskrift*” till angiven *Identifieringstjänst*, inkluderande
    a. *Personidentifierare* för användaren (*signer*).
    b. *Underskriftsmeddelande* (*sign message*) - ett textmeddelande att visa upp för användaren i samband med underskriften.
    c. *Tillitsnivå* för begärd legitimering (*assurance level)*.
    d. En markering om att ev. tidigare autentisering ska förnyas, dvs. ev. SSO-session ska inte användas (*forced authentication*).[11]
4. **(D)** Identifieringstjänsten kontrollerar att begäran är korrekt, och ansvarar sedan för att autentisera användaren som ett aktivt godkännande av underskriften, även kallat *e-legitimering för underskrift*.
    a. Identifieringstjänsten delegerar autentiseringen till lämplig *Autentiseringstjänst* beroende på vilken typ av e-ID användaren väljer att autentisera sig med, samt vilken tillitsnivå som är begärd.
    b. För användaren visas underskriftsmeddelandet och vilken e-tjänst som begär underskriften.
    c. Användaren godkänner underskriften genom att legitimera sig med hjälp av valt e-ID (alternativt avbryter eller avstår).
5. **(C)** Identifieringstjänsten returnerar resultatet till underskriftstjänsten. Vid godkänt resultat skickas ett *identitetsintyg* för undertecknaren tillbaka till underskriftstjänsten.
6. **(B)** Efter kontroll av giltigt identitetsintyg skapar underskriftstjänsten ett särskilt *underskriftscertifikat* med tillhörande privat nyckel, vilken används för att skapa en digital signatur på kontrollsumman. Den digitala signaturen, underskriftscertifikatet samt en *signerad kvittens*[12] returneras till e-tjänsten. Använd privat nyckel raderas efter användning.
7. **(A)** E-tjänsten, ev. med hjälp av stödtjänst, fogar samman dokument och digital signatur och skapar *undertecknat/stämplat dokument*.

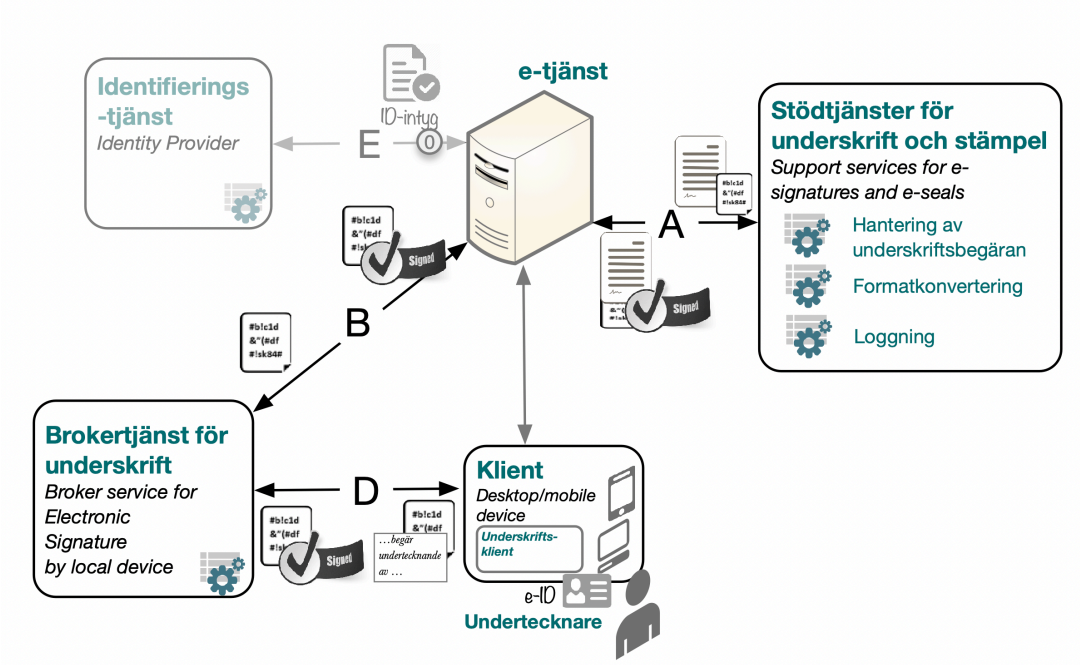
[11] Notera att ev. SSO-session inte får utnyttjas vid underskrift; identifieringstjänsten ska kräva ny autentisering av användaren. Detta kallas även *forced authentication*.

[12] I kvittensen ingår ID-intyg från identifieringstjänsten samt aktuellt underskriftsmeddelande

E-tjänsten, ev. med hjälp av stödtjänst, loggar spårbarhetsinformation enligt *Spårbarhet.*

5.2.3 Digital signatur med lokalt e-ID via brokertjänst

5.2.3.1 Översikt



Figur 6. Digital signatur med lokalt e-ID via brokertjänst – översikt.

(A) E-tjänsten kan ta hjälp av lokala stödtjänster för att skapa en underskriftsbegäran, ta emot och hantera den resulterande underskriften/stämpeln, och slutligen sammanfoga till ett undertecknat dokument.

(B) E-tjänsten begär och erhåller underskriften/stämpeln från en s.k. *Brokertjänst för underskrift*.

(D) Brokertjänsten ansvarar för att hantera underskriftsbegäran i samverkan med en klientprogramvara. Den digitala signaturen skapas i en *lokal säker enhet (secure local device)* ansluten till användarens klient, t.ex. ett smart kort.

(E) E-tjänsten delegerar autentisering av användaren i e-tjänsten till betrodd Identifieringstjänst (IdP*)* enligt [IAM-RA].

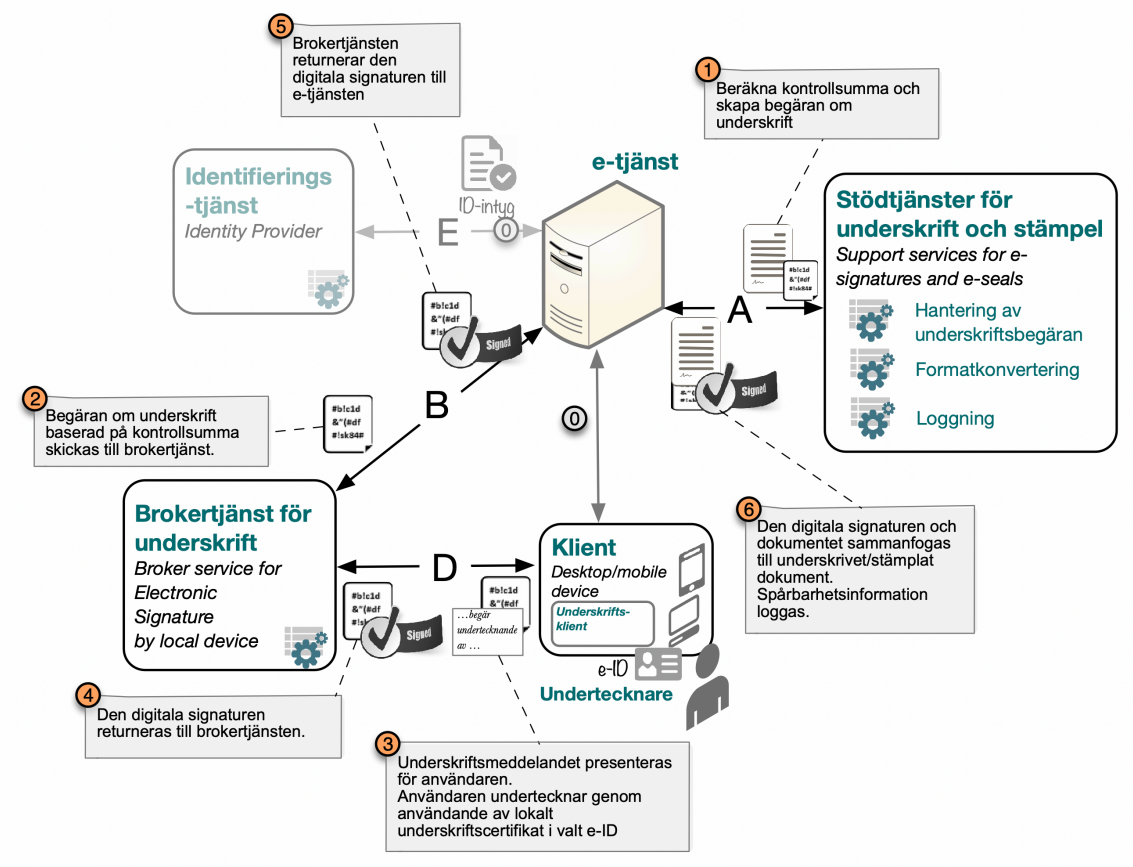
Observera att endast delar av referensmodellen används i detta mönster; C-gränssnittet används inte, och brokertjänsten tar över ansvaret för att hantera underskriften i D-gränssnittet.

5.2.3.2 Utmärkande för digital signatur med lokalt e-ID

Följande är värt att notera vid digital signatur med lokalt e-ID:

- Digital signatur med lokalt e-ID utan brokertjänst ger ett hårt beroende till den använda tekniken och de klientprogram som används och bör undvikas.
- Användande av brokertjänst abstraherar bort tekniken för själva framställan av digital signatur från e-tjänsterna. Framställan av digital signatur kan göras *out-of-band*, dvs. i en separat teknisk kanal. Detta skapar en lösare teknisk koppling till e-tjänsten. E-underskriften som sådan har dock kvar ett tekniskt beroende till aktuell klientprogramvara för underskrift, samt till den använda lokala säkra enheten, t.ex. ett smart kort.
- Den elektroniska identitetshandling (e-ID) som används i samband med undertecknandet måste tillhandahålla ett *underskriftscertifikat* (med tillhörande hemligt nyckelmaterial) för att skapa den digitala signaturen. Detta ställer särskilda krav på använt e-ID, och hänsyn kan behöva tas till hur säkerhetskoder för både legitimering och underskrift hanteras för användaren.
- Användande av digital signatur med lokalt e-ID försvårar utbytet och användning av utländska e-underskrifter enligt eIDAS-förordningen [eIDAS]. En samverkan bygger på att alla parter kan hantera alla de e-ID för underskrift och tillhörande underliggande teknik som förekommer, vilket med många parter kan vara mycket svårt att åstadkomma.
- Tillgängligheten för en lösning med digital signatur via brokertjänst är beroende av brokertjänsten i sig samt stödtjänsterna. Dessa komponenter kan utifrån verksamhetens behov utformas för hög tillgänglighet (typiskt multipla instanser), samt kan skalas horisontellt (fler instanser) och vertikalt (mer resurser till varje instans). Notera dock att tillgängligheten vid samverkan och validering av digitala signaturer skapade med lokala e-ID kan vara utmanande att uppnå (se resonemang i föregående punkt).

5.2.3.3 Principiellt flöde för digital signatur via brokertjänst



Figur 7. Digital signatur med lokalt e-ID via brokertjänst - principflöde

Det principiella flödet vid underskrift med lokalt e-ID via brokertjänst kan beskrivas enligt följande:

0. (Försteg) Användaren, här även kallad *undertecknare (signer)*, loggar in i e-tjänst som erbjuder funktion för undertecknande/stämpling av dokument.
    a. Användaren autentiseras med stöd av en *Identifieringstjänst (IdP)*, samt auktoriseras för användning av e-tjänsten.
    b. Användaren väljer att underteckna/stämpla ett dokument.

c. E-tjänsten ansvarar för visa upp (det semantiska) innehållet i dokumentet för påseende/granskning av användaren, enligt styrande princip ES4 ”*Det du ser är vad du undertecknar*”[13].

1. **(A)** E-tjänsten tar hjälp av lokal stödtjänst för att ev. konvertera dokumentet till lämpligt format för digitala signaturer, samt skapa en *underskriftsbegäran* inkluderande
    a. En *kontrollsumma* av dokumentet som ska undertecknas (*document digest*).
    b. *Personidentifierare* för användaren, vilken erhållits från Identifieringstjänsten (*signer*).
    c. *Underskriftsmeddelande* (*sign message*) - ett textmeddelande att visa upp för användaren i samband med underskriften.
    d. Den *tillitsnivå* som e-tjänsten begär att underskriften (minst) utförs på (*signature assurance level)*.[14]
    e. Namn/identifierare på den *e-tjänst* som är avsändare av underskriftsbegäran (*service provider*).
2. **(B)** E-tjänsten tar ev. hjälp av stödtjänst för att skicka underskriftsbegäran till *Brokertjänst för underskrift*. Brokertjänsten verifierar att begäran är korrekt ställd, och returnerar annars ett fel.
3. **(D)** Brokertjänsten ansvarar för att underskriftssteget hanteras i samverkan med en *underskriftsklient* på användarens klientdator.
    a. För användaren visas underskriftsmeddelandet och vilken e-tjänst som begär underskriften.
    b. Användaren undertecknar genom användande av lokalt underskriftscertifikat i dennes valda e-ID, matchande den tillitsnivå som brokertjänsten kräver. Den digitala signaturen baseras på dokumentets kontrollsumma.
4. **(D)** Resultatet av underskriften, digital signatur samt använt underskriftscertifikat (publik del), returneras till brokertjänsten.
5. **(B)** Brokertjänsten returnerar resultatet av underskriften tillbaka till e-tjänsten.

---

[13] Se *Specifika krav* för mer information.

[14] Eventuellt är denna underförstådd genom att den valda ingången till brokertjänsten är knuten till en specifik tillitsnivå.

6. **(A)** E-tjänsten tar hjälp av stödtjänst för att foga samman handling och digital signatur och skapa *undertecknat/stämplat dokument*.
   E-tjänsten, ev. med hjälp av stödtjänst, loggar spårbarhetsinformation enligt *Spårbarhet.*

5.2.4 Specifika krav

- Arkitekturmönstret *digital signatur via fristående underskriftstjänst* ska i första hand användas för framställan av elektroniska underskrifter och stämplar, med följande delkrav:
  - Lösningar för underskrift och stämpel bör följa specifikationerna för fristående underskriftstjänst enligt [Sweden Connect].
  - E-tjänsten skickar begäran om underskrift till underskriftstjänst. Begäran ska vara digitalt signerad av e-tjänsten.
  - Underskriftstjänsten ansvarar för att delegera identifiering och autentisering av användaren till Identifieringstjänst, genom begäran om e-legitimering för underskrift. Begäran ska vara digitalt signerad av underskriftstjänsten.
  - Underskriftstjänsten ska alltid begära att en ny autentisering av användaren utförs vid undertecknandet (*forced authentication*). Ev. SSO-session hos identifieringstjänsten får inte användas.
  - Underskriftstjänstens svar tillbaka till den e-tjänst som begär underskriften ska vara digitalt signerad av underskriftstjänsten.
- Autentisering av användare i samband med underskrift bör utföras *out-of-band*, dvs. i en separat teknisk kanal oberoende av informationskanalen, för att minska de tekniska kraven på användarens klient. Se mer utförliga motiv i [IAM-RA].
- Allt informationsutbyte över nätverk i samband med e-underskrift ska förmedlas över krypterad förbindelse.
  Se vidare [RIV-Kryptering] för specifika krav och rekommendationer.

5.2.4.1 Krav på underskriftscertifikat i underskriftstjänst

Det underskriftscertifikat som underskriftstjänsten tillhandahåller för att skapa den digitala signaturen är en central del i lösningen. Certifikatet innehåller typiskt information om undertecknaren och till denne kopplade attribut, men kan också ge information om autentiseringen av undertecknaren, bland annat dess tillitsnivå.

Följande krav applicerar på underskriftscertifikat vid underskrift via fristående underskriftstjänst:

- Underskriftscertifikatet ska vara digitalt signerad av underskriftstjänstens privata nyckel.

- Underskriftscertifikatet ska innehålla ett eller flera attribut kopplade till undertecknaren och/eller dennes organisation (för stämplar). För att uppfylla *avancerad elektronisk underskrift*, ska det finnas minst ett attribut genom vilket undertecknaren säkert kan identifieras.
  För mer information om klassificering av elektroniska underskrifter se *Avancerad respektive kvalificerad elektronisk underskrift och stämpel*.
- Underskriftscertifikatet ska innehålla säkrad tidpunkt utifrån tillförlitlig tidskälla för skapandet av den digitala signaturen.

  Notera att detta krav minskar behovet av att tidsstämpla elektroniskt undertecknade dokument, åtminstone på kort och medellång sikt: den digitala signaturen är från start knuten till en viss tidpunkt. För mer information om tidsstämpling och tillförlitliga tidskällor se *Elektronisk tidsstämpling* och *Krav på valideringsdata.*
- Underskriftscertifikatet bör innehålla information om tillitsnivån för den e-ID som användes vid e-legitimering för underskrift.
- Exakt vilka attribut kopplade till undertecknaren som ska ingå i underskriftscertifikatet ska kunna anpassas efter det aktuella behovet.
  Detta kan avgöras på flera olika sätt:
  - E-tjänsten specificerar krav på ingående attribut i begäran till underskriftstjänst. Stöd för detta finns i specifikationerna för fristående underskriftstjänst enligt [Sweden Connect].
  - Attributsprofiler konfigureras i underskriftstjänsten, vilka t.ex. kan kopplas till vilken e-tjänst som anropar underskriftstjänsten.

5.3 Elektronisk stämpling i automatiserade processer

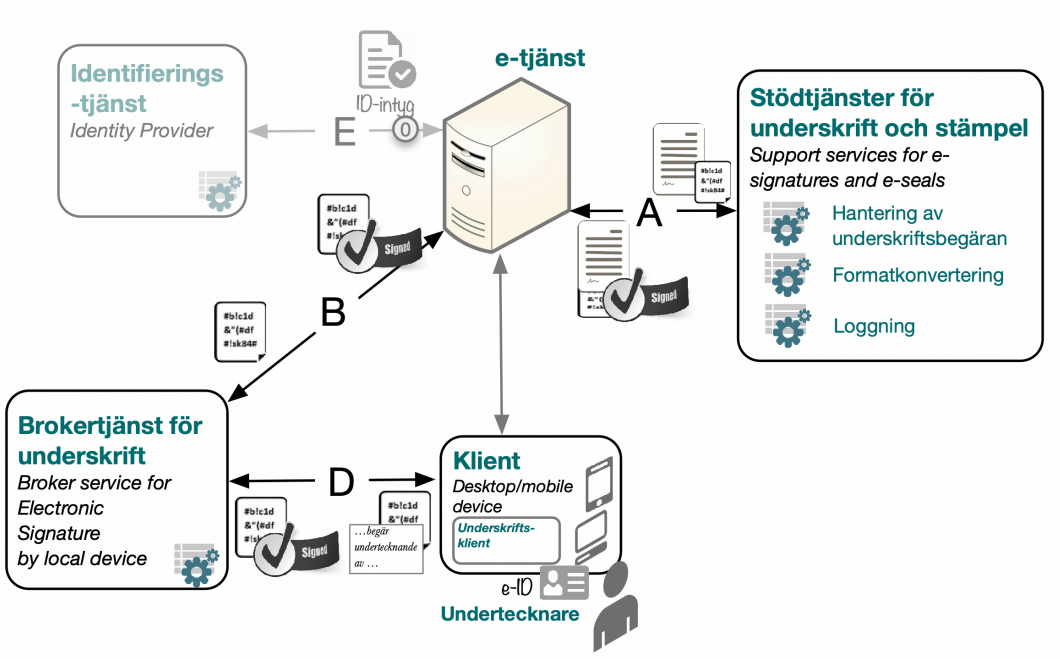
5.3.1 Arkitekturella mönster

Elektronisk stämpling kan vara en aktiv handling av en behörig användare i en organisation, t.ex. när en handläggare stämplar ett dokument inför delning med andra parter.

Men e-stämpling kräver inte nödvändigtvis en användarinteraktion; även automatiserade systemprocesser kan utnyttja e-stämpling. Exempelvis kan en myndighet låta e-stämpla alla inkomna handlingar automatiskt, eller att information som lämnas ut digitalt per automatik förses med organisationens stämpel.

Dokumentkonvertering kan behöva göras som ett försteg innan stämpling, beroende på dokumentets ursprungliga format, beroende på de format som tjänsterna kring stämpling stödjer, men också för att möta arkiveringskrav.

5.3.1.1 Översikt



Figur 8. Elektronisk stämpling av dokument – översikt. Stämplingen initieras eventuellt av en användare, men kan även vara en automatiserad process.

(A) E-tjänsten kan ta hjälp av lokala stödtjänster för e-stämpel, för att skapa en stämpelbegäran, ta emot och hantera den resulterande stämpeln, och slutligen sammanfoga till ett stämplat dokument.

(B) E-tjänsten begär och erhåller stämpel från en fristående *Stämplingstjänst*, på initiativ av behörig användare, alternativt i en automatiserad process utan användarinteraktion.

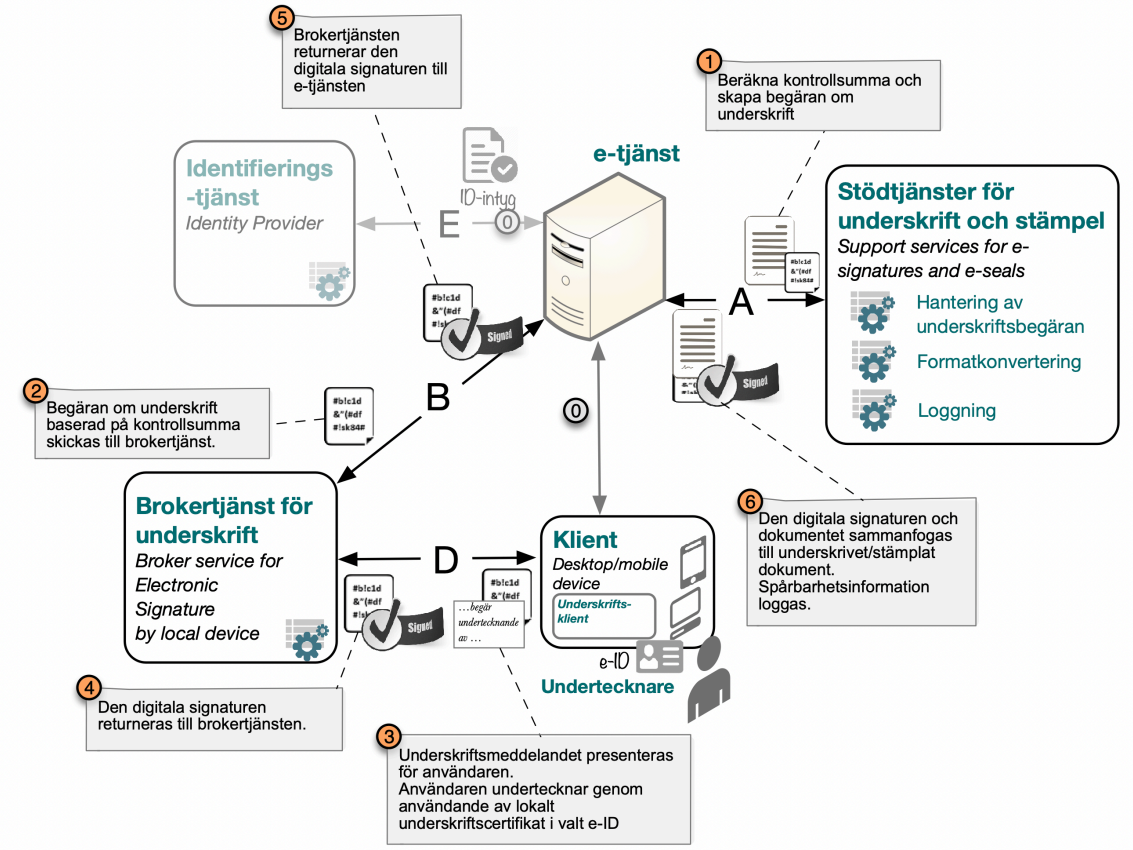
(E) E-tjänsten delegerar i förekommande fall autentisering av användaren i e-tjänsten till identifieringstjänsten enligt [IAM-RA].

5.3.1.2 Utmärkande för elektronisk stämpel i automatiserade processer

Följande är värt att notera vid elektronisk stämpling med stöd för automatiserade processer:

- Ett stämpelcertifikat är associerat med en viss organisation (juridisk person). Organisationen avgör vilka medarbetare och/eller vilka e-tjänster (system) som är behöriga att använda organisationens elektroniska stämpel.
- Elektronisk stämpling kan vara en automatiserad systemprocess, alternativt initierad av en behörig användare.
- Den underliggande tekniken för elektronisk stämpel, dvs. en digital signatur, är i princip den samma som för elektronisk underskrift; samma tekniska format och principer för validering av stämpel och underskrift kan tillämpas.
- Det rekommenderas att etablera för organisationen lokala stödtjänster för e-stämplar, för att förenkla för e-tjänster. Det är dock även möjligt att låta e-tjänsten realisera dessa funktioner själv.

5.3.1.3 Principiellt flöde för e-stämpling i automatiserade processer



Figur 9. Elektronisk stämpling av dokument med stöd för automatiserade processer – principflöde.

Det principiella flödet vid elektronisk stämpling med stöd för automatiserade processer kan beskrivas enligt följande:

0. (Försteg) Användaren loggar in i e-tjänst som erbjuder funktion för e-stämpling av dokument. Notera att detta steg hoppas över om det är e-tjänsten som utan användarinteraktion använder elektronisk stämpling.
    a. Användaren autentiseras med stöd av en *Identifieringstjänst (IdP)*, samt auktoriseras för användning av e-tjänsten **(E)**.
    b. Användaren väljer att stämpla ett (eller flera) dokument å sin organisations vägnar. E-tjänsten kontrollerar att användaren är behörig att använda organisationens e-stämpel.
1. **(A)** E-tjänsten tar hjälp av lokal stödtjänst för att ev. konvertera dokumentet till lämpligt format för e-stämpling, samt skapa en *begäran om e-stämpling* inkluderande

a. En *kontrollsumma* av dokumentet som ska stämplas (*document digest*).
b. Namn/identifierare på den *e-tjänst* som är avsändare av begäran (*service provider, seal requester*).
c. Eventuellt anges vilket specifikt stämpelcertifikat som ska användas (om flera stämpelcertifikat är knutna till organisationen och det inte är underförstått vilket som avses för aktuell e-tjänst.

2. **(B)** E-tjänsten tar ev. hjälp av stödtjänst för att skicka begäran om stämpling till *Stämplingstjänsten*. Stämplingstjänsten autentiserar e-tjänsten och kontrollerar att e-tjänsten har behörighet att använda e-stämpel för associerad organisations räkning, och returnerar annars ett fel.
3. **(B)** Stämplingstjänsten skapar e-stämpel utgående från begäran och användande av angiven organisations stämpelcertifikat, och returnerar e-stämpeln till e-tjänsten.
4. **(A)** E-tjänsten tar ev. hjälp av stödtjänst för att foga samman dokument och stämpel och skapa *stämplat dokument*.
   E-tjänsten loggar tillämpbar spårbarhetsinformation, se vidare avsnitt *Spårbarhet.*

   Not: Steg 1–4 upprepas vid behov att stämpla flera elektroniska dokument.

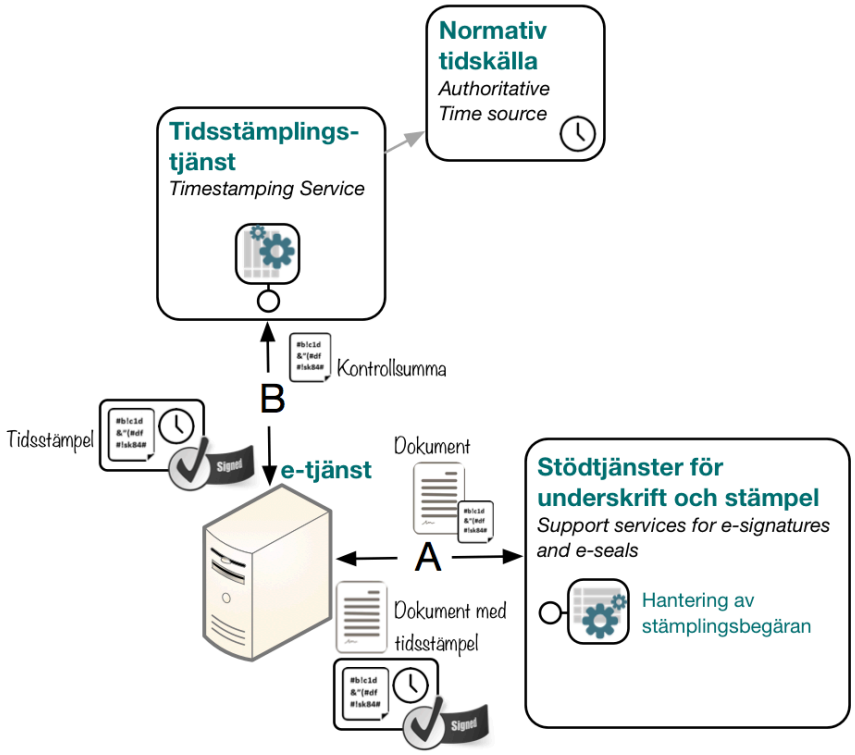
5.3.2 Specifika krav

- Stämplingstjänsten ansvarar för att skydda stämpelcertifikat och tillhörande nyckelmaterial.
- Om stämplingstjänst delas mellan flera organisationer ska stämplingstjänsten ha mekanismer som säkert kopplar respektive stämpelcertifikat till respektive organisations godkända e-tjänst.
- Stämplingstjänsten ska autentisera anropande e-tjänst och kontrollera att e-tjänsten har behörighet att använda e-stämpel för kopplad organisations räkning, och returnera annars ett fel.
- Allt informationsutbyte över nätverk i samband med e-stämpling ska förmedlas över krypterad förbindelse.
  Se vidare [RIV-Kryptering] för specifika krav och rekommendationer.

5.4 Elektronisk tidsstämpling

5.4.1 Arkitekturella mönster

5.4.1.1 Översikt



Figur 10. Elektronisk tidsstämpling via Tidsstämplingstjänst - översikt.

(A) E-tjänsten kan ta hjälp av lokala stödtjänster för att skapa tidsstämplingsbegäran.

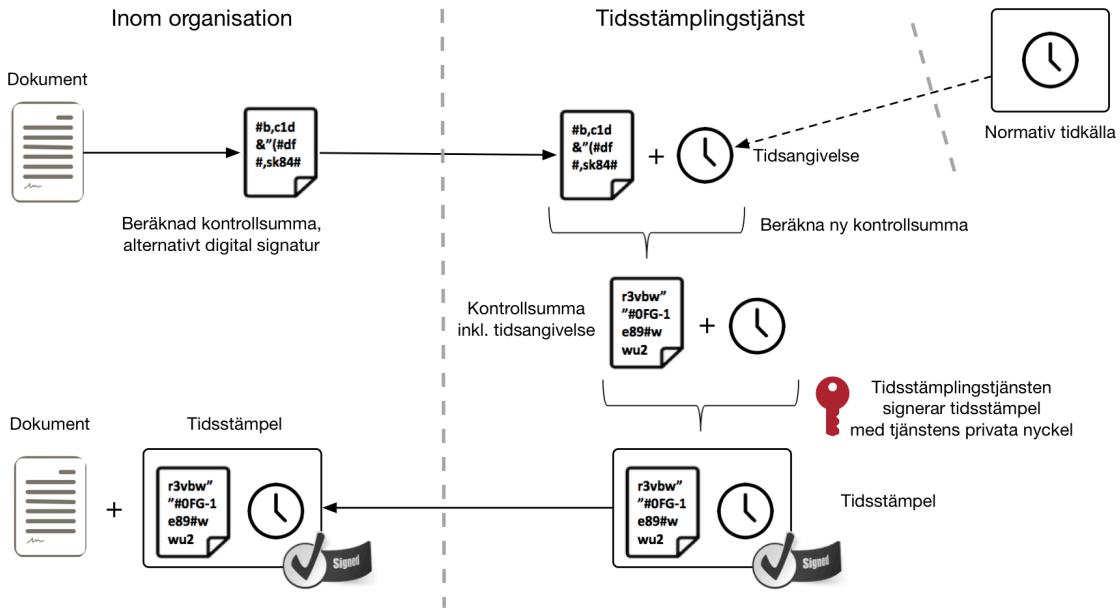
(B) E-tjänsten begär och erhåller tidsstämpel från en *Tidsstämplingstjänst*.

Tidsstämpeln lagras kopplat till dokumentet som stämpeln avser, vilket möjliggör validering av tidsstämpeln vid senare tidpunkt.

5.4.1.2 Principiella flöden för tidsstämpling

Elektronisk tidsstämpling ger möjlighet att påvisa att en viss information existerade i viss form vid en viss tidpunkt.

Nedan bild illustrerar principen för standardbaserad tidsstämpling via en betrodd tidsstämplingstjänst.



Figur 11. Princip för standardbaserad elektronisk tidsstämpling av dokument via tidsstämplingstjänst.

För information som ska tidsstämplas skapas först en kontrollsumma, vilken sedan skickas till tidsstämplingstjänsten. För digitalt signerade dokument skickas istället den digitala signaturen till tidsstämplingstjänsten.

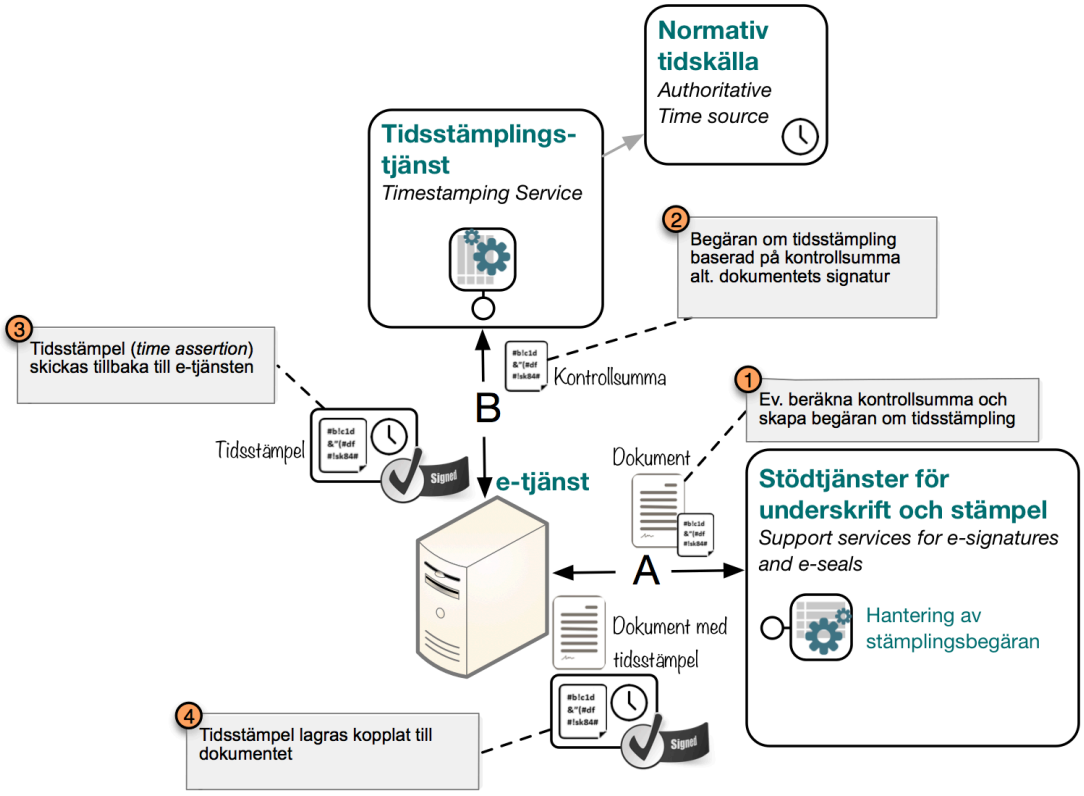
Tidsstämplingstjänsten genererar en tidsangivelse baserat på en tillförlitlig tidskälla, normalt spårbar till världstiden *UTC* (*Coordinated Universal Time*[15]) med en viss garanterad noggrannhet.

Tidsstämplingstjänsten sätter samman inkommen kontrollsumma med tidsstämpeln och beräknar en ny kontrollsumma.

Slutligen signerar tidsstämplingstjänsten kontrollsumman och tidsstämpeln tillsammans till en *tidsstämpel* (*time assertion*), vilket returneras till anropande system. Tidsstämpeln förvaras kopplat till det dokument som stämplades.

Relativt referensmodellen kan detta principflöde sammanfattas enligt nedan bild:

[15] https://en.wikipedia.org/wiki/Coordinated_Universal_Time

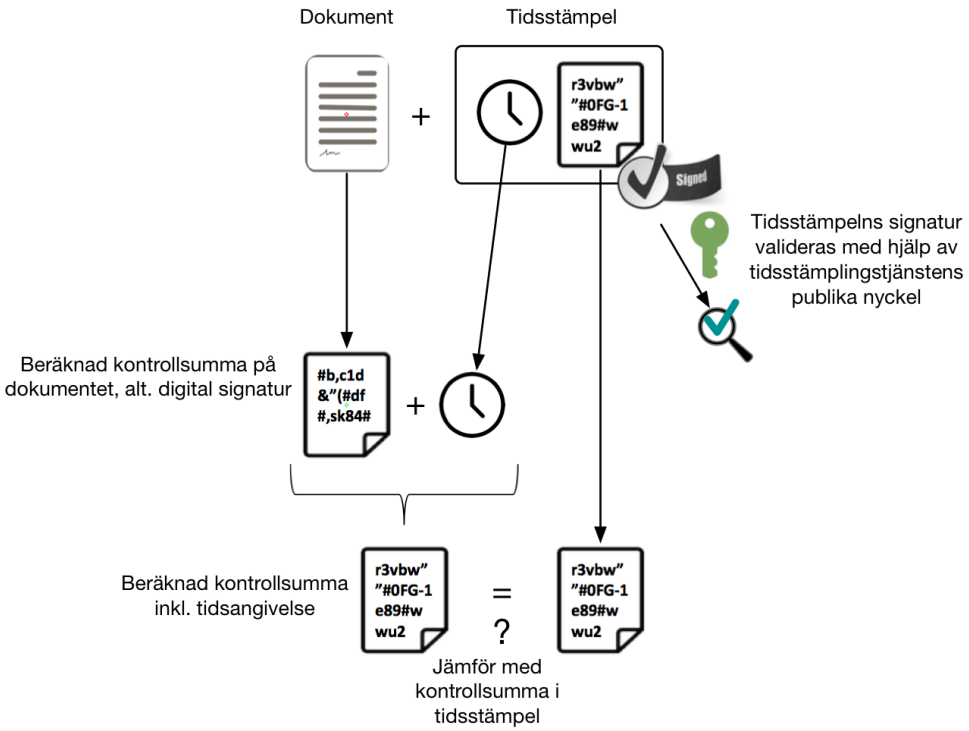


Figur 12. Elektronisk tidsstämpling av dokument - principflöde.

För att validera ett dokuments tidsstämpel behövs dokumentet självt (dess digitala signatur vid signerat dokument), tidsstämpeln samt tidsstämplingstjänstens publika nyckel, vilket kan hämtas från tjänstens publika certifikat.

Med hjälp av tidsstämplingstjänstens publika nyckel valideras först tidsstämpelns signatur.

Processen att räkna fram en kontrollsumma baserat på dokumentets kontrollsumma och tidsangivelsen upprepas. Denna kontrollsumma jämförs med kontrollsumman i tidsstämpeln, och om de är lika är tidsstämpeln valid och dokumentet har inte ändrats sedan stämplingen genomfördes.



Figur 13. Principiellt flöde för att validera en elektronisk tidsstämpel.

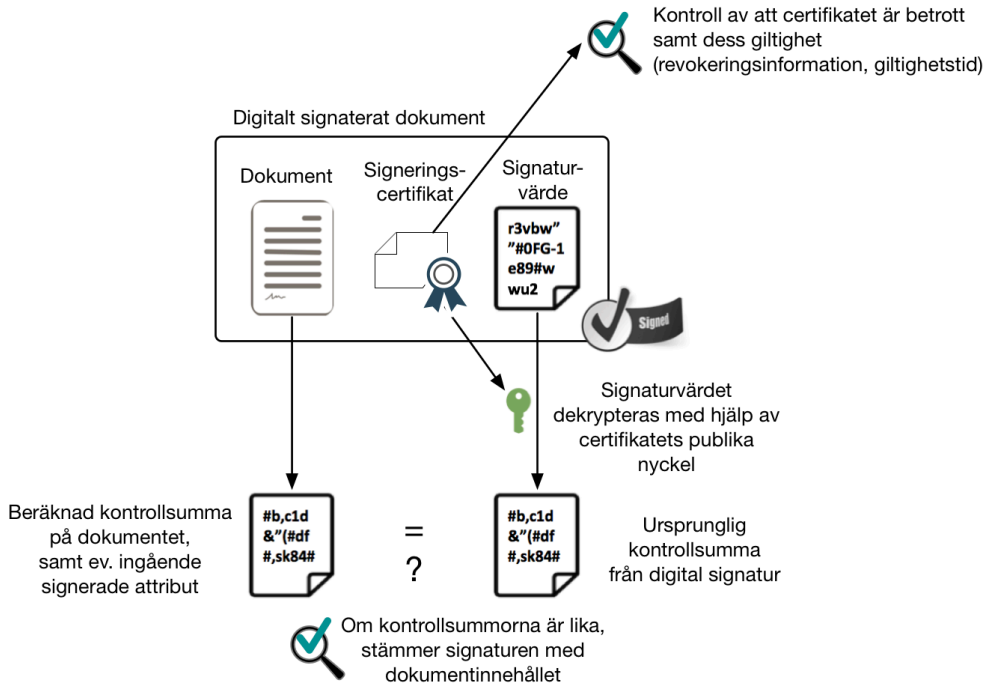
5.5 Validering av underskrift och stämpel

5.5.1 Valideringsmekanismer

Validering av elektronisk underskrift resp. stämpel består principiellt av tre typer av kontroller:

1) att underskriften resp. stämpeln framställts från ett signeringscertifikat[16] utfärdat av en trovärdig organisation (certifikatutfärdaren).
2) att certifikatet var giltigt vid tidpunkten för underskriftens resp. stämpelns skapande, såväl avseende dess giltighetstid som att certifikatet inte var spärrat.
3) att dokumentet inte har förändrats sedan underskriftens resp. stämpelns skapande.

Nedan bild visar schematiskt flöde för de olika momenten i valideringen.



Figur 14. Validering av elektroniska underskrifter och stämplar - principiellt flöde

[16] Underskriftscertifikat resp. stämpelcertifikat, i kapitlet refererat som *signeringscertifikat* eller endast *certifikat*.

Kontroll av betrodd certifikatutfärdare

Att signeringscertifikatet är betrott kontrolleras mot en lista över de certifikatutfärdare som den förlitande parten anser är betrodda (även kallad *trusted list*).
Listan kan vara lokal hos organisationen (validering kan ske med lokal stödtjänst), eller externt hanterad. I det senare fallet kan även en extern valideringstjänst användas.
Kontrollen kan behöva följa förekommande certifikatskedjor för att kunna konstatera om utfärdaren är betrodd.

Ifall elektroniskt undertecknade eller stämplade dokument skickas till externa parter (t.ex. leverantörer, privatpersoner osv.), behöver man tänka på om och hur kontrollen mot betrodda utfärdare kan hanteras av dokumentmottagarna. Använder de externa parterna enbart standardprogramvara för att läsa och validera dokumentet (t.ex. PDF-läsare), kommer kontrollen normalt ske mot mjukvaruleverantörernas inbyggda stöd, såsom *Microsoft Trusted Root Certificate List*, *Apple Trust Store*, *Adobe Approved Trust List* osv. För att den externa parten automatiskt ska få ”grön bock” i sin programvara som kvittens på att underskriften är validerad, behöver således den använda certifikatutfärdaren finnas med i dessa listor. Respektive certifikatsprogram har rutiner för att ansöka om att få en certifikatutfärdare inkluderad i programmet.

Som en följd av eIDAS tillhandahåller respektive medlemsland en publik lista över godkända betrodda kvalificerade certifikatutfärdare. EU tillhandahåller dessutom en konsoliderad lista över listorna – *List of Trusted Lists* (*LOTL*). Syftet med listorna är att kunna bygga in automatiska certifikatskontroller utan att ha djupare kännedom om andra EU-medlemmars interna strukturer.

Kontroll av giltigt certifikat

Kontroll av signeringscertifikatets giltighet omfattar två delmoment. Dels kontrolleras certifikatets giltighetstid, och dels görs kontroll mot källa för certifikatsspärr, normalt en certifikatrevokeringslista (*CRL*) eller via uppslag mot en tjänst för certifikatstatus (OCSP-tjänst). Uppgifter om var certifikatsspärrinformation kan erhållas finns normalt i signeringscertifikatet självt.
Notera att kontrollerna som princip ska göras relativt tidpunkten för underskriftens resp. stämpelns skapande.

Kontroll att dokumentet inte har förändrats

Kontroll att dokumentet inte har förändrats sedan underskriftens resp. stämpelns skapande, sker genom att beräkna dokumentets kontrollsumma igen och jämföra med kontrollsumma hämtat från den digitala signaturen för e-underskriften resp. e-stämpeln. Beroende på vilket signaturformat och vilken policy som använts kan det ingå kompletterande attribut i underlaget för den digitala signaturen, och dessa ska i så fall ingå i underlaget för beräkning av kontrollsumma.

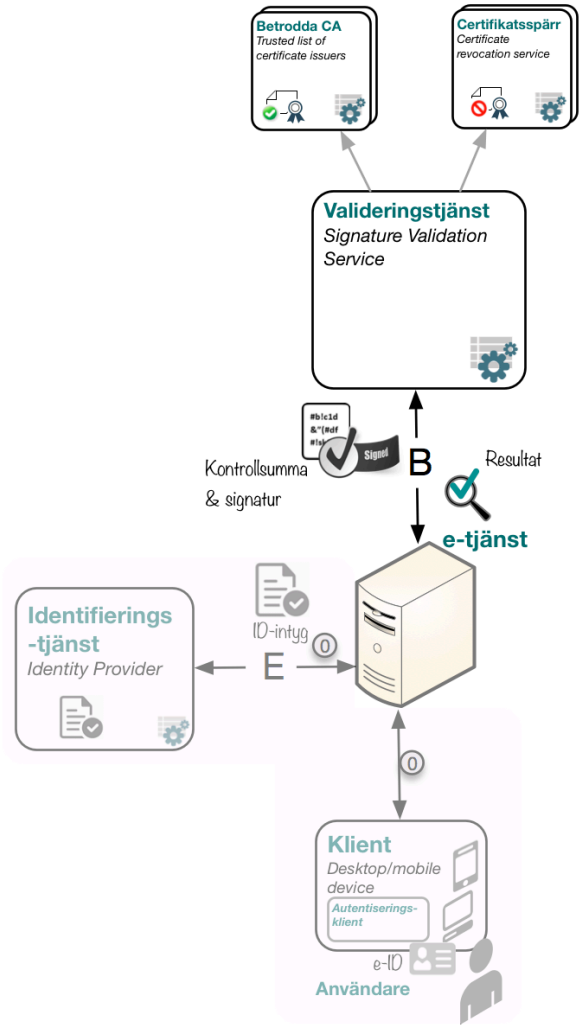
5.5.2 Arkitekturella mönster

På motsvarande sätt som för elektronisk stämpel, kan validering av elektronisk underskrift och stämpel vara en aktiv handling av en person (t.ex. i samband med dokumentgranskning), men realiseras ofta i en automatiserad systemprocess. Exempelvis kan en myndighet tänkas välja att automatiskt validera inkomna e-undertecknade och e-stämplade dokument.

Värt att notera är att de arkitekturella mönstren nedan gäller för både elektroniska underskrifter och stämplar.

5.5.2.1 Översikt

Nedan bild visar översiktligt validering via extern valideringstjänst.



Figur 15. Validering av elektroniska underskrifter och stämplar – översikt. Validering initieras eventuellt av en användare, men kan även vara en automatiserad process.

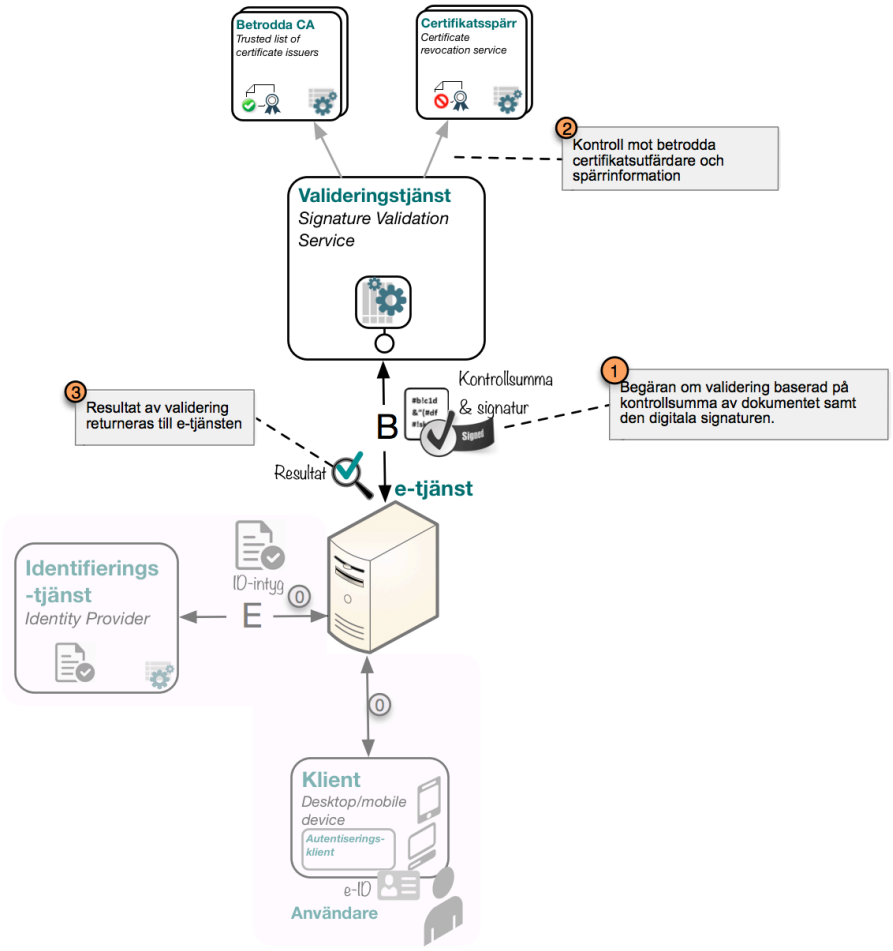
(B) E-tjänsten begär validering av elektronisk underskrift resp. stämpel från en fristående *Valideringstjänst*. Valideringstjänst använder efter behov externa tjänster för att erhålla information om betrodda certifikatutfärdare (CA) och spärrade certifikat.

(E) E-tjänsten delegerar i förekommande fall autentisering av användaren i e-tjänsten till identifieringstjänsten enligt [IAM-RA].

5.5.2.2 Utmärkande för validering

- Validering av elektroniska underskrifter och stämplar kan baseras på tillgång till det ursprungliga dokumentet, alternativt på dokumentets kontrollsumma. I det senare fallet behöver inte dokumentinnehållet exponeras för valideringstjänsten.
- Validering av elektroniska underskrifter och stämplar kan vara en automatiserad systemprocess, alternativt initierad av en behörig användare.
- Den digitala signaturen kan inkludera mer eller mindre valideringsdata. Som minst måste ingå det signeringscertifikat (eller referens till) som använts vid framställning av signaturen. För att möjliggöra validering efter längre tid, kan den digitala signaturen behöva vara kompletterad med ytterligare valideringsdata. Mer om detta i *Krav på valideringsdata*.

5.5.2.3 Principiellt flöde för validering



Figur 16. Validering av elektroniska underskrifter och stämplar – principflöde.

Det principiella flödet vid validering av elektronisk underskrift resp. stämpel kan beskrivas enligt följande:

0. (Försteg) Användaren loggar in i e-tjänst som erbjuder funktion validering av dokument. Notera att detta steg hoppas över vid automatiserad process.
    a. Användaren autentiseras med stöd av en *Identifieringstjänst (IdP)*, samt auktoriseras för användning av e-tjänsten **(E)**.
    b. Användaren väljer att validera ett dokument.
1. **(B)** E-tjänsten skickar *begäran om validering* till *Valideringstjänsten* inkluderande

a. En *kontrollsumma* av dokumentet som ska valideras[17].

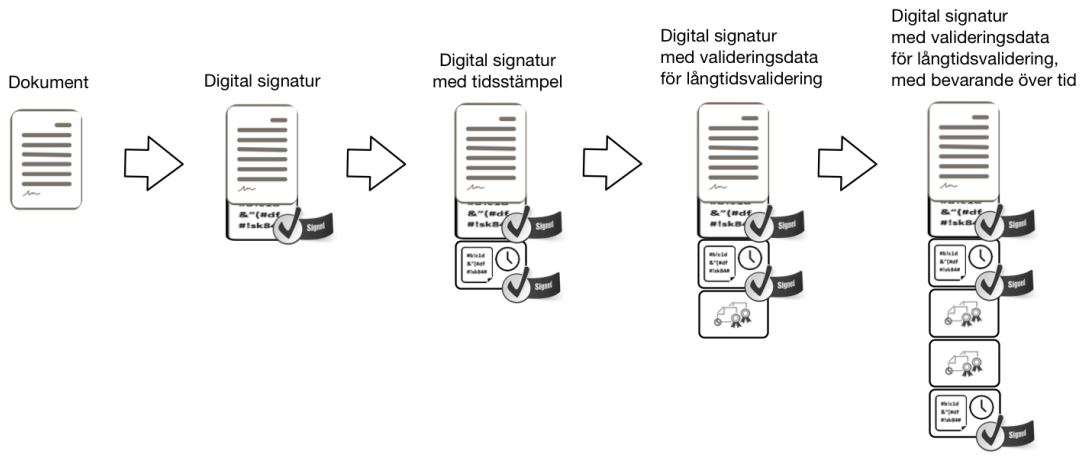
b. Dokumentets digitala signatur, inkluderande signeringscertifikatet alt. en referens till certifikatet.
Signaturen kan även inkludera ytterligare valideringsdata beroende på signaturformat och signaturpolicy.

2. Valideringstjänsten utför kontroll av signeringscertifikatet mot betrodda certifikatutfärdare och spärrinformation, samt kontrollerar att dokumentets signatur är korrekt (baserat på dokumentets kontrollsumma).
3. Valideringstjänsten returnerar resultat av validering till e-tjänsten.

5.5.2.4 Krav på valideringsdata

En digital signatur i en elektronisk underskrift eller stämpel kan kompletteras med valideringsdata, typiskt de certifikatkedjor som behövs för kontroll samt certifikatsspärrinformation. På så vis kan validering göras även om valideringsinformationen inte längre är tillgänglig online (relaterar till styrande princip IT2). Genom att dessutom tidsstämpla en digital signatur kan det påvisas att signaturen och dess valideringsdata existerade före en viss tidpunkt.

Nedan bild beskriver en tänkt digital signaturs ”livscykel”, där signaturen succesivt byggs på med mer valideringsdata:

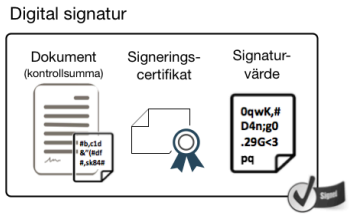


Figur 17. En digital signaturs ”livscykel” med avseende på dess valideringsmöjligheter.

[17] Notera att tjänsten även kan stödja att skicka själva dokumentet istället. I principflödet används dock kontrollsumman för att inte behöva exponera dokumentets innehåll till den externa valideringstjänsten.

Kapitlet *Validering av elektroniska underskrifter och stämplar* skilde på tre fall av validering, vilka ställer delvis olika krav på den valideringsinformation som behöver finnas tillgänglig kopplat till den digital signaturen:

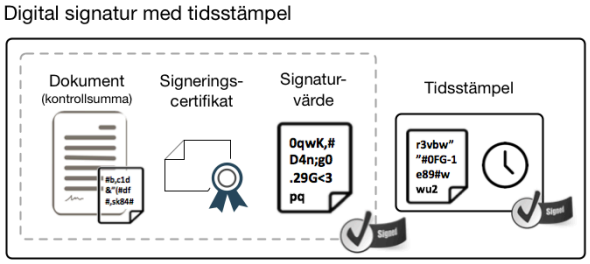
1) **Validering i nära anslutning till skapandet** av e-underskrift eller e-stämpel.
I detta fall kan antagas att förutsättningarna för valideringen är de samma som vid skapandet av e-underskriften eller e-stämpeln. Valideringen kan baseras på enbart en grundläggande digital signatur samt tillgängliga källor online med certifikatstatus.



Figur 18. En grundläggande digital signatur (Basic Digital Signature).

2) **Validering efter lång tid**, dvs. en relativt lång tid efter skapandet av e-underskrift eller e-stämpel.
Det certifikat som en alldeles giltig digital signatur baserades på, kan en tid senare ha passerat sin giltighetstid eller blivit återkallat. Att basera kontrollen på aktuell tidpunkt kan därmed ge ett missvisande resultat – istället behöver valideringen baseras på tidpunkten för skapandet av den digitala signaturen.
Det förutsätts dock att den använda tekniken i den digitala signaturen fortfarande är aktuell och möter säkerhetskraven.
I detta fall behövs en digital signatur med tidsstämpel för att kunna ”frysa” skapandet av signaturen till före en viss tidpunkt.

   a) Förutsatt att källor för kontroll av certifikaten är tillgängliga online räcker det att den digitala signaturen kompletterats med en tidsstämpel:

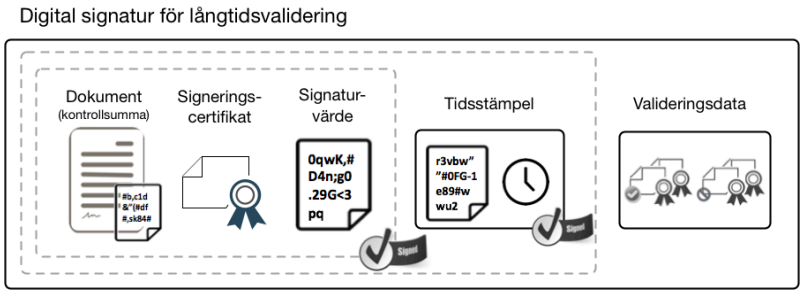


Figur 19. Digital signatur med tidsstämpel (Digital Signature with Time)

.

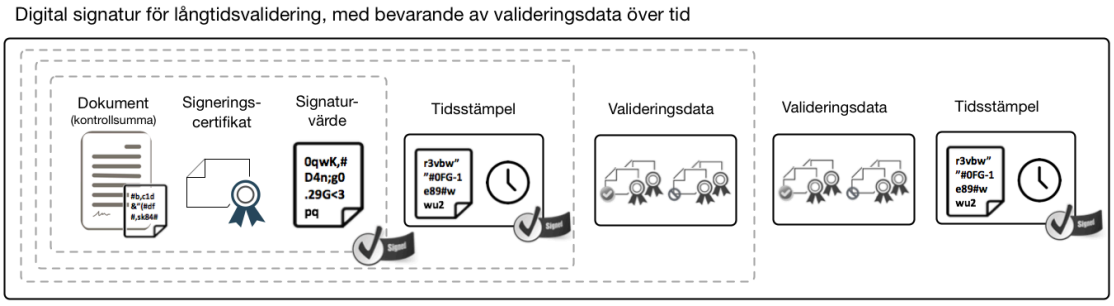
   b) För att säkerställa validering även efter att källor för kontroll av certifikaten inte längre kan förutsättas vara tillgängliga online, behöver signaturen även

kompletteras med all nödvändig valideringsdata:



Figur 20. Digital signatur med tidsstämpel och komplett valideringsdata (Long-Term Validation Material).

3) **Validering efter mycket lång tid**, där med tiden tekniken för den ursprungliga digitala signaturen blivit utdaterad, använda algoritmer numera räknas som osäkra, eller någon annan förutsättning i omgivningen saknas för validering av den ursprungliga digitala signaturen.
För att hantera detta kan de digitalt signerade dokumenten upprepat tidsstämplas innan den gamla tekniken utdaterats. I varje stämpling läggs även till förnyade valideringsdata. Varje tidsstämpling använder uppdaterad teknik med algoritmer och kryptonyckellängder som anses starka.



Figur 21. Digital signatur för långtidsvalidering, med bevarande av valideringsdata över tid.

5.5.2.5 Bevarande av möjligheten att validera över tid

När behov finns att bevara möjlighet att validera elektroniska underskrifter och stämplar över tid, kan mönstret med Valideringstjänst ovan (*Översikt*) användas med en utökad funktionalitet:

- Efter utförd validering kompletterar Valideringstjänsten signaturen med en tidsstämpel och ev. kompletterande valideringsdata (certifikat- och spärrinformation), och returnerar den ”förstärkta” digitala signaturen.

- Genom upprepade tidsstämplar, som vid varje tillfälle använder nycklar och algoritmer som anses starka, kan integriteten hos dokument och signaturer kontrolleras även efter mycket lång tid.
- Tidsstämpeln kan antingen genereras av Valideringstjänsten själv (agerar i rollen tidsstämplingstjänst) eller i sin tur nyttja en extern tidsstämplingstjänst.

5.6 Elektronisk underskrift och stämpel i federativ samverkan

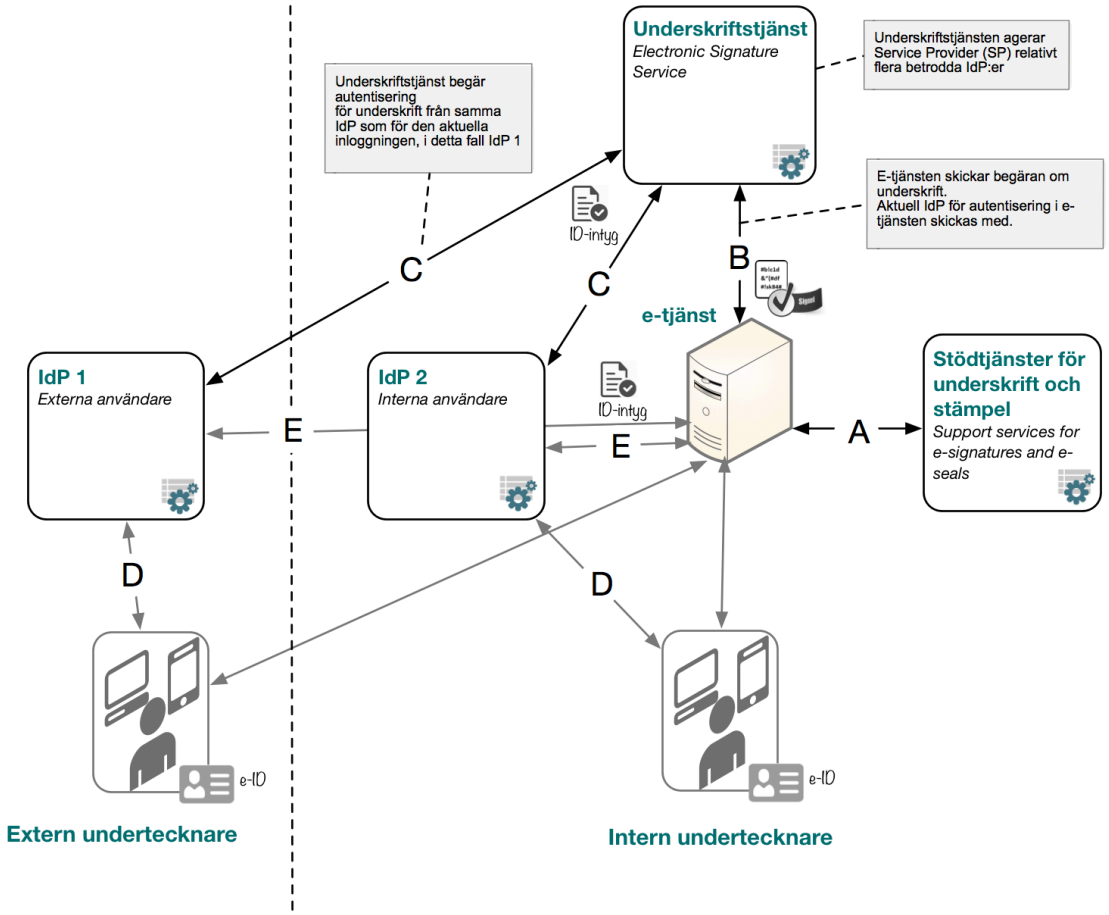
5.6.1 Arkitekturella mönster för federativ samverkan

Som framgår av det arkitekturella mönstret *digital signatur via fristående underskriftstjänst* delegerar underskriftstjänsten autentisering av undertecknaren till en *Identifieringstjänst (IdP).* Detta sker enligt ett federativt mönster mellan en IdP och en *Service Provider (SP)*, vilket beskrivs i [IAM-RA].

I ett federativt perspektiv agerar underskriftstjänst i rollen som *Service Provider*, i detta fall en tjänst som tillhandahåller elektroniska underskrifter och stämplar.
Inom ramen för en identitetsfederation kan således ingående funktioner och tekniska ramverk även tillämpas för digitala signaturer.

Detta kan t.ex. användas för att dela en underskriftstjänst mellan flera organisationer, där varje organisation kan använda sin befintliga infrastruktur för identitet och åtkomst (IdP, katalog osv.) för åtkomst till underskriftstjänsten.
Enligt samma princip kan erbjudas åtkomst till tjänsten för såväl invånare som medarbetare, för interna resp. externa medarbetare, genom att federera mot lämpliga identifieringstjänster.

Värt att notera här är att användaren behöver styras till samma identifieringstjänst som denne använder vid inloggning till e-tjänsten, varför det är viktigt att aktuell IdP kommuniceras till underskriftstjänsten. Bilden nedan visar ett exempel med interna resp. externa undertecknare som delar en underskriftstjänst.



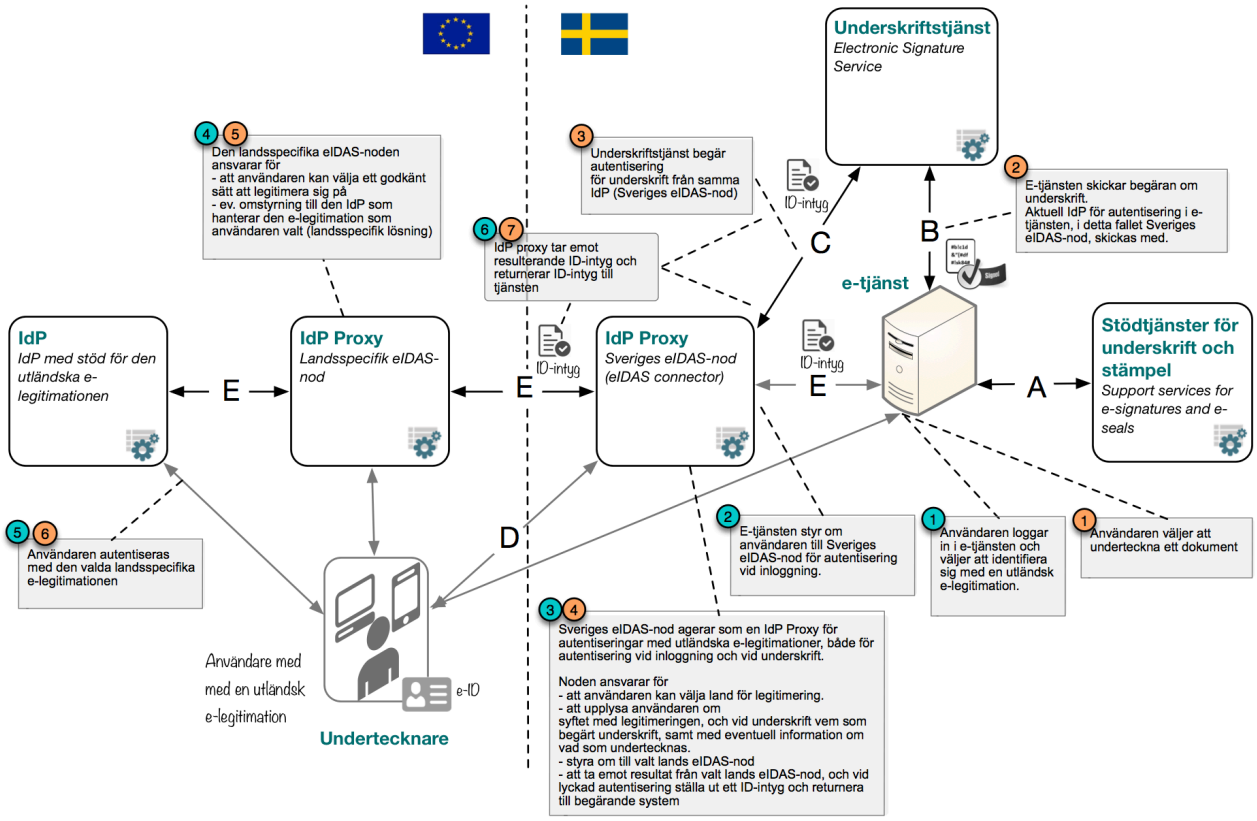
Figur 22. Delad underskriftstjänst för både organisationens interna såväl som för externa undertecknare.

5.6.2 Elektroniska underskrifter med utländska e-legitimationer enligt eIDAS

Den federativa modellen i referensarkitekturen för e-underskrifter ger även stöd för att hantera kraven enligt eIDAS, genom att autentiseringsflödet är frikopplat från skapandet av underskriften, samt att olika identifieringstjänster federativt kan kopplas samman med såväl e-tjänsten som underskriftstjänsten.
Man kan se samverkanslösningarna för att hantera eIDAS-kraven som en tillämpning av den federativa modellen beskriven i föregående kapitel.

Genom att tillämpa referensmodellen och digital signatur via fristående underskriftstjänst kan man tillhandahålla möjlighet för användare att såväl logga in och underteckna med utländsk e-legitimation i en svensk e-tjänst. Underskriftstjänsten behöver här kopplas mot den svenska eIDAS-noden, vilken agerar IdP-proxy för alla förekommande utländska identifieringstjänster.

Nedan bild illustrerar principflödet då en användare med utländsk e-legitimation loggar in i en svensk e-tjänst, för att sedan underteckna ett dokument. Både vid inloggning och undertecknande styrs användaren till den identifieringstjänst som hanterar dennes utländska e-legitimation.



Figur 23. Elektronisk identifiering och underskrift i svensk e-tjänst med utländsk e-legitimation. Grönblå resp. orangefärgade steg motsvarar identifiering resp. underskrift i e-tjänsten.

Scenariot kan även ”spegelvändas”, dvs. tillämpas för en användare med svensk e-legitimation som loggar in och undertecknar dokument i en e-tjänst i utlandet. Principiellt är det samma flöden även i detta fall.

5.6.3 Specifika krav

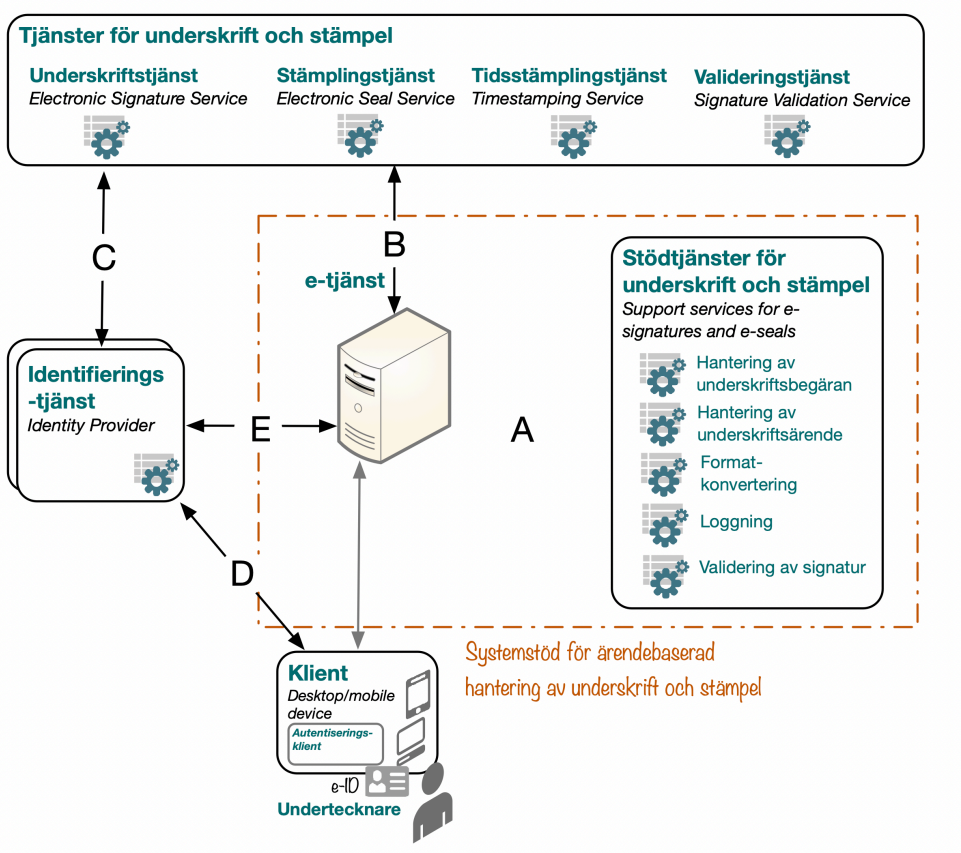
- Tjänsterna för elektroniska underskrifter och stämplar ska stödja att kunna användas i ett federativt sammanhang, vilket bl.a. omfattar
    - Underskriftstjänster ska kunna agera *Service Provider* i enlighet med Referensarkitektur för Identitet och åtkomst [IAM-RA]

- Underskriftstjänster ska efter behov kunna konfigureras för flera betrodda Identifieringstjänster.
- Hantering av vilken Identifieringstjänst som används i det aktuella fallet ska följa specifikationerna för fristående underskriftstjänst enligt [Sweden Connect].

5.7 Hantering av ärendeflöden för underskrift och stämpel

5.7.1 Arkitekturellt mönster för hantering av ärendeflöden

Ett IT-system för att hantera ärenden för underskrifter och stämplar, från beredning av ärendet till att undertecknade dokument är lagrade och/eller distribuerade, motsvarar i referensarkitekturen en *e-tjänst*. E-tjänsten kan här vara en dedikerad ”underskriftsapplikation” eller som en del av ett större system.



Figur 24. Digitalt systemstöd för att hantera underskriftsärenden och relaterad funktionalitet - översikt.

E-tjänsten kan nyttja lokala stödtjänster för att

- Hantera underskriftsärenden, vilket kan inkludera dokumentlagring, notifiering till berörda undertecknare osv.
- Hantering av underskriftsbegäran och paketering av digital signatur och dokument.
- Konvertering av dokument till lämpliga format för undertecknande och arkivering.
- Lokal validering av digitala signaturer
- Logga spårbarhetsinformation kring utförda elektroniska underskrifter och stämplar.

Beroende på vilken funktionalitet som e-tjänsten ska stödja, kan den kopplas till en eller flera tjänster för underskrift, stämpel, validering och tidsstämpling[18].

5.7.2 Specifika krav

- E-tjänsten ansvarar för att hantera styrande princip ES4 ”*Det du ser är vad du undertecknar*”.
  Detta innebär bland annat att
  - E-tjänsten ska för användaren tillgängliggöra allt underlag avseende underskriften, t.ex. samtliga förekommande bilagor
  - E-tjänsten ska tydligt visa hur många delar (om flera) som ingår i underlaget.
  - E-tjänsten bör i möjligaste mån säkerställa att användaren tagit del av hela underlaget, t.ex. genom att kontrollera att alla dokument har öppnats av användaren, innan användaren ges möjlighet att gå vidare till undertecknande.
  - E-tjänsten ska utforma underskriftsmeddelandet (det som visas i samband med legitimering för underskrift) så att innebörden av undertecknandet framgår, samt att det tydligt hör samman med det presenterade underlaget

[18] Tidsstämpling kan även kravställas som en del av Valideringstjänst.

(t.ex. genom att referera till dokumentets titel eller dylikt).
Dock bör ev. känsliga uppgifter undantas från underskriftsmeddelandet[19].

- Elektronisk identifiering och autentisering av användare, både för inloggning i e-tjänsten och för legitimering för underskrift, hanteras genom att e-tjänsten nyttjar en eller flera identifieringstjänster. Behovet att stödja t.ex. externa användare, invånare, användare i andra utländska e-legitimationer osv. styr vilka identifieringstjänster som e-tjänsten behöver federeras med.
- E-tjänsten ansvarar för att logga spårbarhetsinformation avseende utförda underskrifter och stämplar. För mer information se avsnittet *Spårbarhet*.
- E-tjänst som omfattar dokumenthantering som faller under Riksarkivets föreskrifter och allmänna råd kring bevarande av elektroniska handlingar ska omfattas av motsvarande krav på tekniska format (styrande princip ES7):
  - E-tjänsten ska hantera dokumentformat enligt PDF/A-1

[19] T.ex. kan det innebära att meddelandet refererar till ett ärende som kräver undertecknande, men att känsliga uppgifter om exakt vilken individ det berör mm. inte är med i texten.

6 Juridik och informationssäkerhet

Ett användningsområde för elektroniska underskrifter är att en säkert identifierad användare på ett juridiskt hållbart sätt ska kunna utföra rättshandlingar i digitaliserade processer. En elektronisk stämpel kan på motsvarande sätt tänkas användas för att föra i bevis att en handling inkom till en myndighet vid en viss tidpunkt.

Användning av elektroniska underskrifter och stämplar är relaterad till många frågeställningar inom juridik och informationssäkerhet, inte minst om syftet är att ersätta hantering av handlingar med rättsliga krav på underskrift eller stämpel.

Vid sådan tillämpning behöver hänsyn tas till den rättsliga regleringen som berör undertecknande och stämpling. För att underlätta tolkning av dessa har några svenska myndigheter tagit fram juridiska vägledningar för användning av elektroniska identitetshandlingar, underskrifter och stämplar.

6.1 Rättslig reglering för elektroniska underskrifter och stämplar

Detta kapitel sammanställer några av de lagar, förordningar och föreskrifter som i Sverige på olika sätt har bäring på användning av elektroniska underskrifter och stämplar. Kapitlet gör inga anspråk på att vara komplett i detta avseende.

- *Brottsbalken* (BrB).
  Brottsbalken reglerar bland annat urkundsförfalskning, förnekande av underskrift, osann försäkran mm. Brotten mot urkunder har här sträckts ut till att även gälla e-underskrivna och e-stämplade handlingar.

- *eIDAS-förordningen (910/2014)* [eIDAS], kompletterad med svenska bestämmelser enligt [Lag 2016:561] samt förordning 2016:576.
  Förordningen reglerar elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden inom EU. Bland annat definieras begreppen *avancerad* respektive *kvalificerad* elektronisk underskrift och stämpel (se även nedan)[20].
  Förordningen ger ett uttryckligt stöd för distansbaserade förfaranden för elektronisk underskrift, exempelvis då en e-legitimation används för att aktivera en fristående (central) underskriftsfunktion [Juridisk vägledning e-legitimering och e-underskrifter, kap 12.9].

[20] Även ”enkel underskrift” (*simple electronic signature*) definieras i eIDAS, vilket endast behöver vara någon elektronisk information tillagd till dokumentet. Denna typ av signatur hanteras inte inom referensarkitekturen.

- *Arkivlagen*, kompletterad med *Riksarkivets föreskrifter om elektroniska handlingar och tekniska krav* [RA-FS 2009:1-2].
  Dessa reglerar och ger föreskrifter kring hantering, arkivering och gallring av allmänna handlingar i elektronisk form hos myndigheter, vilket har påverkan på val av dokumentformat, och i viss mån använd signaturteknik i elektroniskt underskrivna dokument.
  I referensarkitekturen ges stöd för att hantera de dokument- och signaturformat som Riksarkivet föreskriver för bevarande av elektroniska handlingar, såsom dokumentformatet PDF/A-1 samt digitala signaturer enligt [XMLDSIG] och [CMS]. Se vidare *Rekommenderade protokoll per förmåga*.
- *Dataskyddsförordningen*, kompletterad med svenska bestämmelser enligt [Lag 2018:218]. Dataskyddsförordningen reglerar bl.a. persondataskydd i digitala lösningar, vilket behöver beaktas vid utformning och användning av elektroniska underskrifter.

6.2 Vägledning inom juridik och informationssäkerhet

Detta kapitel syftar till att sammanställa vägledningar som kan underlätta tillämpning av e-underskrift och e-stämpel i verksamheten på ett juridiskt hållbart sätt.

Exempel på frågeställningar som berörs:

- När får elektroniska underskrifter och stämplar användas? Vilka formkrav kan hindra dess användning och vilka kan möjliggöra?[21]
- Vilka rättsregler gäller vid användning av elektroniska underskrifter och stämplar? Gäller samma förutsättningar för en elektronisk underskrift som en egenhändig underskrift på papper?
- Vilken information om elektroniska underskrifter och stämplar behöver bevaras i syfte att styrka handlingars ursprungliga skick och äkthet, och vilken information får tas bort (gallras) från systemen?
- Vad behöver beaktas när det gäller persondataskydd vid användning av elektroniska underskrifter och stämplar?

[21] En ”tumregel” är att om det inte finns särskilda krav på s.k. ”egenhändig underskrift”, så kan elektronisk underskrift användas som alternativ till papper och bläck.

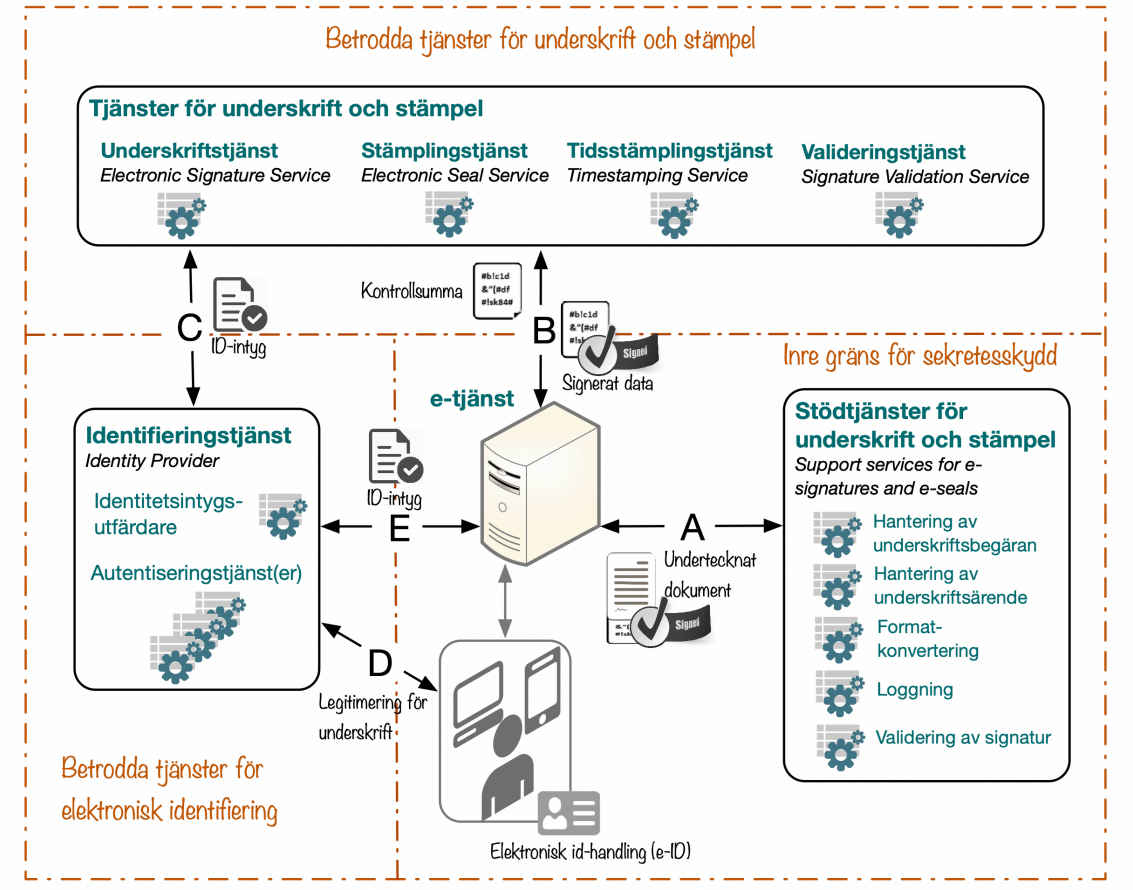
- Hur påverkas organisationerna av EU:s förordning om gränsöverskridande elektronisk legitimering [eIDAS] och dess krav på ömsesidigt erkännande av anmälda e-legitimationer?

Vägledningar:

- *Juridisk vägledning för införande av e-legitimering och e-underskrifter*, eSam [Juridisk vägledning e-legitimering och e-underskrifter].
  Vägledningen tar utgångspunkt i rättsliga förutsättningar, myndigheternas behov och Riksarkivets riktlinjer, för att beskriva juridiska aspekter på införande och användande av e-legitimering, e-underskrifter och e-stämplar.
  Exempel på aspekter som tas upp är giltigheten för e-underskrifter och e-stämplar, straffrättsliga ansvar, krav på bevarande och kontroll av dokuments äkthet, persondataskydd mm.
- *Vägledning för betrodda tjänster i Sverige enligt eIDAS*, PTS [Vägledning betrodda tjänster].
  Vägledningen beskriver krav och process för att tillhandahålla kvalificerade betrodda tjänster inom elektronisk identifiering i Sverige.
- *Vägledning för e-underskrifter*, DIGG [Vägledning e-underskrifter].
  Denna vägledning är mer praktiskt inriktad, och innehåller bland annat rekommendationer för hur tjänster för e-underskrifter kan anskaffas, checklistor för att säkerställa följsamhet mot krav enligt [eIDAS], samt rekommendationer för utformning av lösningar för e-underskrifter.

6.3 Referensarkitekturen och aspekter på informationssäkerhet

6.3.1 Översikt



Figur 25. Översikt referensmodell för e-underskrift och e-stämpel med perspektiven juridik och informationssäkerhet.

Genom att i referensarkitekturen tydliggöra uppdelning i organisationens e-tjänster respektive betrodda tjänster för elektronisk identifiering, underskrift och stämpel, underlättas reglering av ansvarsförhållanden mellan berörda parter. Detta kan vara särskilt viktigt om tjänsterna tillhandahålls av externa parter och/eller delas mellan flera organisationer i en federativ samverkan.

Nedan beskrivs aspekter på hur styrande principer inom informationssäkerhet, såsom konfidentialitet, uppgiftminimering och spårbarhet, har beaktats i referensarkitekturen.

6.3.2 Konfidentialitet och uppgiftsminimering

Referensarkitekturen bygger på en modell som ger stöd för att skydda och inte i onödan sprida känsliga uppgifter, såsom t.ex. integritetskänsliga personuppgifter, i samband med skapande, validering och delning av elektroniskt undertecknade och stämplade dokument (styrande princip ES3).

Referensarkitekturen ger samtidigt stöd för att kunna (åter)använda externa betrodda tjänster för elektronisk identifiering och underskrift, med möjlighet att minimera uppgiftslämnandet till externa parter.

Enligt en rekommendation i [Vägledning e-underskrifter] bör lösningarna utformas så att dokumenten som undertecknas eller stämplas inte ska behöva lämna organisationen. Referensmodellens mönster med digital signatur via fristående underskriftstjänst, samt stödtjänster som kan hållas lokalt inom organisationen, skapar förutsättningar för detta.

Vid delning av elektroniska undertecknade dokument, bör även beaktas vilka uppgifter som förmedlas i underskriftscertifikatet. Underskriftscertifikatet är nödvändigt för att mottagaren ska kunna validera underskriften, samt kunna avgöra dokumentets ursprung. Även här ger referensarkitekturens modell och arkitekturella mönster stöd för att reglera och vid behov minimera vilka uppgifter som läggs i underskriftscertifikatet, vilket beskrivs i följande avsnitt.

6.3.2.1 Underteckna och stämpla elektroniska dokument

Vid skapande av e-underskrift och e-stämpel med stöd av fristående tjänster överförs dokumentets kontrollsumma (i stället för dokumentet självt) till tjänsterna för underskrift och stämpel. Kontrollsumman skapas genom en envägskryptering (*hashalgoritm*), som med rätt val av algoritm och nyckellängder, praktiskt sett omöjliggör att återskapa dokumentet utifrån kontrollsumman.
Det överförs även en text (underskriftsmeddelandet) som sammanfattat beskriver vad man som användare skriver under. Texten skyddas under transport med hjälp av kryptering[22] och kan efter undertecknandet gallras. Vid utformning av underskriftsmeddelandet bör inte känsliga uppgifter ingå i texten.

Vid validering av e-underskrift och e-stämpel behöver endast dokumentets kontrollsumma samt dess digitala signatur inklusive signeringscertifikatet överföras till valideringstjänsten. Validering kan även i många fall göras helt lokalt via lokal stödtjänst.

[22] Det finns även en möjlighet att kryptera underskriftsmeddelandet i sig. Meddelandet måste i så fall dekrypteras hos identifieringstjänsten för att kunna visas upp för användaren.

6.3.2.2 Dela elektroniskt undertecknade dokument

Vid delning av elektroniskt undertecknade dokument enligt referensmodellen, är det möjligt att styra innehållet i underskriftscertifikatet. T.ex. kan undertecknarens roll eller befattning i organisationen ingå, men inte nödvändigtvis dennes personnummer. Eftersom underskriftscertifikatet vid underskrift skapas i realtid av den betrodda underskriftstjänsten, är det möjligt att styra innehållet genom att välja vilka attribut kopplade till undertecknaren som ska ingå.
Kraven på vilken information som ska ingå i den digitala signaturen kan därmed styras av de aktuella kraven på spårbarhet till vem som undertecknade och i vilken roll.

6.3.3 Spårbarhet

Enligt styrande princip IT2, ska det i processen att skapa elektroniska underskrifter och stämplar finnas en spårbarhet till

- **Vem** som undertecknat/stämplat
- **Tidpunkt** då den digitala signaturen skapades
- **Vad** som undertecknats/stämplats
- **Utgivaren** av underskriftscertifikatet
- **Autentiseringsinformation** såsom tillitsnivån som uppnåddes för autentiseringen av undertecknaren vid tillfället för undertecknandet

Enligt de rekommenderade arkitekturella mönstren för *Elektronisk underskrift och stämpel* ges stöd för att implementera denna spårbarhet genom att

- Underskriftstjänsten returnerar aktuellt underskriftscertifikat samt en signerad kvittens till e-tjänsten som bevis på utförd underskrift. Kvittensen inkluderar signerat ID-intyg med autentiseringsinformation från identifieringstjänsten, skapandetidpunkt för den digitala signaturen, samt det aktuella underskriftsmeddelandet.
- E-tjänsten (t.ex. en underskriftsapplikation) ansvarar för att spårbarhetsinformationen loggas kopplat till en viss underskrift/stämpel, företrädesvis med hjälp av en stödtjänst för loggning. E-tjänsten har förutom svaret från Underskriftstjänsten tillgång till uppgifter om vem som undertecknade och vad som undertecknades.

6.4 Avancerad respektive kvalificerad elektronisk underskrift och stämpel

6.4.1 Avancerad elektronisk underskrift och stämpel

Begreppen *avancerad elektronisk underskrift* respektive *avancerad elektronisk stämpel* är definierade i [eIDAS] i artikel 26 respektive 36.

En avancerad elektronisk underskrift ska uppfylla följande krav:

1. Underskriften ska vara unikt knuten till undertecknaren.
2. Undertecknaren ska kunna identifieras genom underskriften.
3. Underskriften 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.
4. Underskriften ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

På motsvarande sätt gäller för en avancerad elektronisk stämpel att

1. Stämpeln ska vara unikt knuten till skaparen av stämpeln.
2. Skaparen av stämpeln ska kunna identifieras genom stämpeln.
3. Stämpeln ska vara skapad på grundval av uppgifter för skapande av elektroniska stämplar som stämpelns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplar.
4. Stämpeln ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

För att realisera en avancerad elektronisk underskrift resp. stämpel krävs i praktiken användande av PKI-teknologi (*public-key infrastructure*) inkluderande certifikat och kryptografiska nycklar.

Av [eIDAS] artikel 27 följer en skyldighet för offentliga organ att ömsesidigt erkänna avancerade elektroniska underskrifter eller högre i e-tjänster i enlighet med de format som framgår av ett särskilt genomförandebeslut. Enligt [Juridisk vägledning e-legitimering och e-underskrifter] anses de svenska (förekommande) underskrifterna generellt sett uppfylla kraven för avancerade elektroniska underskrifter. För att skapa en avancerad e-underskrift enligt eIDAS behöver e-legitimeringen som kopplas till e-underskriften minst vara på tillitsnivå 2 (eIDAS ”låg”) eller högre.

En elektronisk stämpel respektive underskrift enligt eIDAS-förordningens definitioner får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller att det inte uppfyller kraven för

kvalificerade elektroniska stämplar [eIDAS, artikel 25 och 35]. Grundprincipen är att rättslig verkan av avancerad elektroniska underskrifter i ett visst land definieras i nationell rätt.

6.4.2 Kvalificerad elektronisk underskrift och stämpel

En kvalificerad elektronisk underskrift respektive stämpel definieras i [eIDAS] som en avancerad elektronisk underskrift (resp. stämpel) som skapas med hjälp av en *kvalificerad anordning* för underskriftframställning (skapande av elektroniska stämplar), och som är baserad på ett *kvalificerat certifikat* för elektroniska underskrifter (stämplar).

Kraven för kvalificerad anordning och kvalificerat certifikat är vidare specificerade i [eIDAS, bilaga I-III]. Kraven är framförallt inriktade på informationsskydd och säker hantering i processen att skapa certifikat, underskrift och stämpel.

För att skapa en kvalificerad e-underskrift behöver e-legitimeringen som kopplas till e-underskriften ligga på åtminstone tillitsnivå 3 (eIDAS ”väsentlig”).

Kvalificerade elektroniska underskrifter ska enligt eIDAS-förordningen ha samma rättsliga verkan inom EU som en handskriven underskrift [eIDAS, art 25], förutom i de fall de finns särskilda nationella formkrav på egenhändig underskrift.

Kraven för att uppfylla kvalificerad nivå är ganska svårtolkade.
Skillnaderna mellan avancerad och kvalificerad blir mer praktiskt påtaglig när en part önskar tillhandahålla en *kvalificerad betrodd tjänst* för elektronisk identifiering, underskrift eller stämpel. I Sverige är PTS tillsynsmyndighet för kvalificerade betrodda tjänster enligt [eIDAS]. Mer om kraven och processen att erhålla status kvalificerad tillhandahållare finns att läsa i [Vägledning betrodda tjänster].

6.4.3 Kvalificerad elektronisk tidsstämpel

Tidsstämpeln kan ses som en särskild form av elektronisk stämpel, och [eIDAS, avsnitt 6] har motsvarande reglering även för dessa.

Noterbart för tidsstämplar är att det inte existerar absolut tid; det finns alltid en liten (om än försumbar) avvikelse mot den referens som används. När man menar *juridiskt hållbar tid* avses här att tiden är spårbar till en källa som kan garantera att den med viss noggrannhet följer världstiden UTC (*Universal Time Coordinated*), även kallad *samordnad universaltid*.

En kvalificerad elektronisk tidsstämpling ska uppfylla följande krav:

1. Tidsstämpeln ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.
2. Tidsstämpeln ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid (UTC).

3. Tidsstämpeln ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

7 Teknisk vy – tekniska regelverk

Hur ska tjänsterna utformas, vilka tekniska krav och regelverk ska/bör vi följa när vi realiserar tjänsterna? Teknik/standard-perspektivet.

Notera att detta avsnitt normalt behöver revideras med tätare intervall än de övriga avsnitten i referensarkitekturen pga. den tekniska utvecklingen på området.

7.1 Indelning av protokoll baserat på dess användning

I referensarkitekturen görs en uppdelning av protokoll och format för elektroniska underskrifter och stämplar i följande kategorier, sorterade under respektive gränsyta inom ramen för referensmodellen:

Gränsyta A:

- Format och paketering för digital signatur (*Digital signature formats and packaging*)

Gränsyta B:

Protokoll för att

- Begära skapande av digital signatur (*Digital signature creation)*
- Begära skapande av tidsstämplar (*Digital timestamp creation)*
- Validera digital signatur (*Digital signature validation*)

Gränsyta C:

- Begära autentisering för elektronisk underskrift (*Authentication for signature*)

Gränsyta D:

- Autentisering

För autentiseringsteknik i gränsyta D hänvisas till [IAM-RA]. Referensarkitekturen för elektroniska underskrifter adderar dock krav på autentiseringstjänster och -klienter, såsom att visa upp underskriftsmeddelande för användaren vid legitimering för underskrift.

Grundläggande standarder för digital signatur

Denna kategori omfattar grundläggande standarder för att skapa och representera digitala signaturer. Dessa utgör bas för (inkluderas i) protokollen på högre nivå.

7.2 Rekommenderade protokoll per förmåga

Vid val av tekniska protokoll att använda för att implementera referensarkitekturen, ska de styrande principerna i kap. 3 vara vägledande. Principerna leder till ett urval öppna internationella standarder, med i vissa fall europeisk och/eller nationell profilering.

Styrande princip ES7 angående bevarandeperspektivet beaktas genom att inkludera tekniska format och standarder som linjerar med arkiveringskrav, såsom stöd för signerade PDF/A-dokument (se [PDF/A - ISO 19005] samt PAdES).

Notera att för transportskydd, dvs. skydd av nätbaserad kommunikation i samband med elektronisk underskrift och stämpel, samt autentiseringsteknik, hänvisas till rekommendationer i [RIV-Kryptering] respektive [IAM-RA].

Förmåga	Rekommendation
Format och paketering för digital signatur	Europeisk standard för avancerad elektronisk underskrift och stämpel[23]: Advanced Electronic Signature Baseline Profiles, ETSI. - ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES) Elektroniskt undertecknade dokument i XML-format. - ETSI EN 319 122 CMS Advanced Electronic Signatures (CAdES) Elektroniskt undertecknade dokument i textformat. - ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES) Elektroniskt undertecknade dokument i PDF-format. - ETSI EN 319 162 Associated Signature Containers (ASiC) Format för paketering av dokument och frikopplade signaturer (*detached signatures*) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards ETSI TS 119 312: ”Electronic Signatures and Infrastructures (ESI); Cryptographic Suites” Specificerar krav och rekommendationer för kryptografiska algoritmer för användning i digitala signaturer och stämplar. https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.03.01_60/ts_119312v010301p.pdf
Protokoll för skapande av digital signatur	Grundläggande standard: [OASIS-DSS] Digital Signature Service Core Protocols, Elements, and Bindings, OASIS https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss Profilering Profilering för digital signatur via underskriftstjänst enligt [Swedish eID Technical Framework]: https://docs.swedenconnect.se/technical-framework/

[23] Ingår som krav i eIDAS-förordningens implementeringsdirektiv

	- [ELN-602] “Deployment Profile for the Swedish eID Framework” Implementationsprofil inklusive autentisering för underskrift via underskriftstjänst https://docs.swedenconnect.se/technical-framework/latest/ELN-0602_-_Deployment_Profile_for_the_Swedish_eID_Framework.html - [EidDSSProfile] ”Implementation Profile for Using OASIS DSS in Central Signing Services” Implementationsprofil för underskriftsbegäran och -svar enligt OASIS-DSS https://docs.swedenconnect.se/technical-framework/latest/ELN-0607_-_Implementation_Profile_for_using_DSS_in_Central_Signing_Services.html - [EidDSSExt] ”DSS Extension for Federated Central Signing Services” Implementationsprofil som utökar OASIS-DSS med ytterligare definitioner för elektronisk underskrift via fristående underskriftstjänst. https://docs.swedenconnect.se//technical-framework/latest/ELN-0609_-_DSS_Extension_for_Federated_Signing_Services.html - [EidCertProf] ”Certificate profile for certificates issued by Central Signing services” Certifikatprofil som specificerar innehåll i signeringscertifikat. Denna profil tillämpar en certifikatextension till stöd för fristående underskriftstjänst, Authentication Context Certificate Extension [AuthContext], vilken beskriver hur ”Authentication Context” representeras i X.509 certifikat. https://docs.swedenconnect.se/technical-framework/latest/ELN-0608_-_Certificate_Profile_for_Central_Signing_Services.html
Protokoll för validering av digital signatur	Grundläggande standard: [OASIS-DSS] Digital Signature Service Core Protocols, Elements, and Bindings, OASIS https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss Profilering: ”Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services” Profilering för betrodda tjänster för validering av avancerade elektroniska underskrifter och stämplar. https://www.etsi.org/deliver/etsi_ts/119400_119499/119442/01.01.01_60/ts_119442v010101p.pdf ”Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services” Policykrav för leverantörer av för betrodda tjänster för validering av avancerade elektroniska underskrifter och stämplar. https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf
Protokoll för skapande av tidsstämplar	Grundläggande standard: [RFC 3161]: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), IETF https://www.ietf.org/rfc/rfc3161.txt

	Profilering: ETSI EN 319 422: ”Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles”. Profilering av protokoll och format för tidsstämplar enligt RC 3161. https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" Policy- och IT-säkerhetskrav för leverantörer av för betrodda tidsstämplingstjänster. https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
Begära autentisering för elektronisk underskrift	För grundläggande standarder för autentisering via Identifieringstjänst, se [IAM-RA]. Profilering Profilering för elektroniska underskrifter enligt [Swedish eID Technical Framework]: [ELN-0613] Signature Activation Protocol for Federated Signing Protokoll som används av en underskriftstjänst för att begära autentisering för underskrift av ett eller flera dokument via en Identifieringstjänst (IdP). Protokollet utökar autentiseringsbegäran [24]med autentisering för underskrift (även kallat legitimering för underskrift). https://docs.swedenconnect.se/technical-framework/latest/ELN-0613_-_Signature_Activation_Protocol.html
Grundläggande standarder för digital signatur	[XMLDSIG] XML-Signature Syntax and Processing, W3C Recommendation Grundläggande standard för att skapa och strukturerat representera digitala signaturer. Utgör bas för bl.a. XAdES-standarden. https://www.w3.org/TR/xmldsig-core/ [CMS] Cryptographic Message Syntax, RFC 5652. Grundläggande standard för att digitalt signera, skapa kontrollsumma, validera och kryptera godtyckligt meddelandeinnehåll. Utgör bas för bl.a. CAdES-standarden. Bygger på PKCS #7 enligt RFC 2315. https://tools.ietf.org/html/rfc5652 [ISO 32000-1] "Document management - Portable document format - Part 1: PDF 1.7" Formatstandard för PDF-dokument inkl. signaturer. Utgör bas för bl.a. PAdES-standarden. Källa ISO.org, publikt tillgängliggjord även på http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf [PDF/A - ISO 19005] Electronic document file format for long-term preservation. PDF-format för långtidsarkivering, med stöd för digitala signaturer enligt PAdES-standarden. https://www.pdfa.org/resource/iso-19005-pdfa/

[24] I nuvarande version stöds SAML2-protokollet. Förväntas inkludera OpenID Connect i senare versioner.

	Profilering Profilering för avancerade elektroniska underskrifter och stämplar, ETSI: ETSI TS 119 102-1: ”Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation” https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

Figur 26. Sammanställning rekommenderade tekniska protokoll och standarder per förmåga inom e-underskrifter och e-stämplar.

8 Bilaga: Förkortningar

Förteckning över ett urval använda förkortningar/beteckningar.

CMS	*Cryptographic Message Syntax*
AdES	*Advanced Electronic Signature*
QES	*Qualified Electronic Signature*
WYSIWYS	*What You See Is What You Sign* https://en.wikipedia.org/wiki/WYSIWYS
ETSI	Europeiskt standardiseringsorgan inom informations- och kommunikationsteknologi (ICT). Har en uttalad roll att stödja europeisk reglering och lagstiftning genom att skapa och förvalta harmoniserade europeiska standarder. https://www.etsi.org
PTS	Post- och Telestyrelsen i Sverige. Tillsynsmyndighet för kvalificerade betrodda tjänster enligt [eIDAS]. https://pts.se
TSA	*Timestamping Authority*
UTC	*Coordinated Universal Time,* Samordnad universaltid https://en.wikipedia.org/wiki/Coordinated_Universal_Time
CA	*Certificate Authority* Certifikatutfärdare; Betrodd part som utfärdar certifikat för användning i PKI-baserade system.
LOTL	*List of Trusted Lists.* En konsoliderad lista tillhandahållen av EU över medlemsstaternas respektive lista över kvalificerat betrodda certifikatutfärdare enligt eIDAS.
PKI	*Public-Key Infrastructure* Teknologi inkluderande certifikat och kryptografiska nycklar. https://sv.wikipedia.org/wiki/Public_key_infrastructure

PKCS	*Public Key Cryptography Standards*. https://en.wikipedia.org/wiki/PKCS
IAM	*Identity & Access Management*, Identitets- och åtkomsthantering
SSO	*Single sign-on*, Singelinloggning
IdP, OP	*Identity Provider* respektive *OpenID Provider*. Identifieringstjänster inom SAML resp. OpenID Connect.
SP, RP	*Service Provider* resp. *Relying Party*. Beteckning på e-tjänst inom SAML resp. OIDC som tar emot intygade uppgifter om vem användaren är och dennes egenskaper och i syfte att kunna logga in användaren i e-tjänsten. Även kallad *förlitande part*.
XML	*Extensible Markup Language*, ett standardiserat utbyggbart märkspråk. https://sv.wikipedia.org/wiki/XML
SAML	*Security Assertion Markup Language* https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
OIDC	*OpenID Connect*, OpenID Foundation http://openid.net

9 Bilaga: Symboler

Nedan beskrivs några ofta förekommande symboler i dokumentets bildmaterial.

	Tillhandahåller en funktionellt avgränsad systemtjänst
	E-tjänst (IT-tillämpning/applikation)
	Samverkanspil - indikerar kommunikation mellan samverkande komponenter i arkitekturen. Vilken komponent som är initierande och vilken information som överförs anges i beskrivningar av flödet.
	I flödesbeskrivningar: indikerar flödesriktning (A leder till B)
	I användningsfallsbeskrivningar: indikerar användning (A använder B)
	Användare (fysisk person)
	Elektronisk identitetshandling (e-ID)
	Elektroniskt dokument
	En läsbar text riktad mot användare
	Elektroniskt identitetsintyg som utfärdas av en Identifieringstjänst
	Kontrollsumma (kondensat) av elektroniskt dokument
	Digital signatur

	Elektroniskt undertecknat resp. stämplat dokument
	Elektronisk tidsstämpel
	Tidskälla, tidsangivelse
	Elektroniskt certifikat
	Spärrinformation för certifikat
	Lista över betrodda certifikatutfärdare
	Nyckelmaterial för kryptografiska funktioner med publik och privat nyckel.