Sveriges Kommuner och Regioner

VÄGLEDNING

Vårt dnr:
…

2025-12-10

Kenneth Zetterberg

Stöd vid upphandling av e-underskrifter

Sammanfattning

Denna vägledning har tagits fram inom ramen för Handslaget – SKR:s och kommunernas gemensamma arbete för välfärdens digitalisering, som en del av initiativet Identitet och behörighetshantering.

Syftet är att ge kommuner och regioner stöd vid upphandling och införande av e-underskriftstjänster. Vägledningen samlar grundläggande information, praktiska råd och krav som hjälper verksamheter att välja rätt nivå av säkerhet och funktionalitet.

Dokumentet ger:

- rekommendationer om när e-underskrifter behövs och när digitala godkännanden kan räcka,
- beskrivning av vilka standarder och format (t.ex. PAdES och PDF/A) som rekommenderas att användas,
- förslag på vilka krav på tillit, loggning, arkivering och bevisvärde som bör ställas vid upphandling,
- samt hur kommuner kan arbeta enhetligt med lagring och långtidsvalidering av digitalt signerade handlingar.

Vägledningen kompletterar befintliga underlag från Digg, eSam, Kammarkollegiet, Sambruk och Riksarkivet och erbjuder ett praktiskt stöd för att minska dubbelarbete och skapa likvärdiga förutsättningar i hela kommunsektorn.

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Innehåll

1 Inledning 4
1.1 Syfte och målgrupp 4
1.2 Avgränsningar 4
1.3 Om kravnivåer och marknadens mognad 4
1.4 Begrepp 5
2 Bakgrund och behov 9
2.1 Varför e-underskrifter är viktiga 9
2.2 Lagstiftning och regelverk 9
2.3 Problem och utmaningar 9
3 Om e-underskrifter 10
3.1 Grundläggande om e-underskrifter 10
3.2 Liknelsen med pass eller körkort 10
3.3 Kedjan av förtroende 11
3.4 Bevisvärde över tid 11
3.4.1 Tjänster för LTV 11
3.4.2 Valideringsintyg (Validation Evidence) 12
3.4.3 Bedömning av långtidsvalidering och bevarandeperioder .. 13
4 Tre nivåer av elektroniska underskrifter enligt eIDAS 14
4.1 Enkel elektronisk underskrift (EES) 14
4.2 Avancerad elektronisk underskrift (AdES) 15
4.2.1 Fördjupning: Avancerad elektronisk underskrift (AdES) ... 15
4.3 Kvalificerad elektronisk underskrift (QES) 16
4.3.1 Fördjupning: Kvalificerad elektronisk underskrift (QES) .. 17
4.4 Begränsningar i Sverige för kvalificerade underskrifter (QES) . 19
4.5 Beslutsmatris 19
4.6 E-stämpel (elektronisk stämpel) 19
4.6.1 Skillnaden mellan e-underskrift och e-stämpel 19
4.6.2 Nivåer enligt eIDAS 20
4.6.3 Användning i kommunal verksamhet 20
5 Standarder och format 21

5.1 Dokumentformat 21
5.1.1 Val av PDF/A-version för långtidsbevarande 21
5.2 Standarder för e-underskrifter 22
5.2.1 EU:s vägledning och krav 22
5.3 Digg:s syn 23
5.3.1 ETSI-standarderna 23
6 Oberoende validering av e-underskrifter 23
6.1 Syfte med oberoende validering 24
6.2 Validering av avancerade underskrifter (AdES) 24
6.3 Validering av kvalificerade underskrifter (QES) 25
7 Dokument som kräver underskrift 25
8 Sekretessbelagda handlingar och informationsskydd 27
8.1 Två huvudsakliga angreppssätt 27
8.2 Implikationer för upphandling och kravställning 28
8.3 Rekommendation 28
9 Inkomna elektroniskt undertecknade handlingar från privatpersoner 28
9.1 Utmaningen 28
9.2 Varför detta är en utmaning för kommunen 29
9.3 När gäller eIDAS-ramverket? 29
9.4 Problem vid vägran med hänvisning till form- eller formatkrav 29
9.5 Rekommendation för kommunen 30
9.5.1 Konsekvensbedömning 31
10 Upphandlingskrav på e-underskrifter 32
11 Digitala godkännanden – syfte och utformning 39
11.1 Begreppsförtydligande 39
11.2 Varför digitala godkännanden 40
11.2.1 Rättssäkerhet uppnås även med godkännande 40
11.2.2 Minskad komplexitet och kostnad 40
11.2.3 Bättre användarupplevelse 40
11.2.4 Framtidssäkring och bevarande 40
11.3 Krav på hur digitala godkännanden utformas 41
12 Upphandlingskrav för digitala godkännanden 41
Bilaga 1, Olika vägledningar 47

1 Inledning

Denna vägledning har tagits fram inom Handslaget – SKR:s och kommunernas gemensamma arbete för välfärdens digitalisering. Arbetet är en del av initiativet Identitet och behörighetshantering och utgör ett utökat leveransobjekt i samarbetet.

1.1 Syfte och målgrupp

Syftet med det här dokumentet är att ge kommuner och regioner stöd vid upphandling av e-underskriftstjänster. Vägledningen ska underlätta arbetet med att ställa krav på lösningar som är rättssäkra, effektiva och långsiktigt hållbara.

Dokumentet innehåller:

- Grundläggande information om vad e-underskrifter är och hur de fungerar i en kommunal kontext.
- Tips och rekommendationer kring hur olika typer av handlingar och beslut kan hanteras – när e-underskrift behövs och när digitalt godkännande kan räcka.
- Krav på digitala godkännanden när e-underskrifter inte behövs
- Länkar till fördjupande vägledningar från andra aktörer.
- Rekommendation för hantering av inkomna handlingar med e-underskrifter
- Exempel på upphandlingskrav, utformade för att vara generella och återanvändbara.

Den här vägledningen vänder sig i första hand till upphandlare och IT-teknisk personal inom kommuner och regioner som ansvarar för att kravställa, upphandla eller införa e-underskriftstjänster.

1.2 Avgränsningar

Dokumentet ger inte en komplett lista på kommunala dokument som ska undertecknas.

Dokumentet tar inte ställning till frågan om långtidbevarade, Riksarkivet bör hantera den frågan.

1.3 Om kravnivåer och marknadens mognad

Denna vägledning utgår från best practice. Den samlade kravbilden kan därför vara utmanande för marknaden att fullt ut möta i ett tidigt skede. För

att undvika att upphandlingar faller på enskilda krav rekommenderas att noga balansera SKA- och BÖR-krav. Genom att göra vissa krav till BÖR-krav signaleras inriktningen och målnivån, samtidigt som leverantörer med pågående utveckling kan lämna anbud. Vissa centrala krav kan även ställas som SKA-krav med tidsatt uppfyllelse (t.ex. ”ska uppfyllas senast X månader efter avtalsstart”), kombinerat med genomförandeplan/roadmap och avtalsuppföljning. På så sätt bibehålls ambitionsnivån, marknaden får tydlig riktning och upphandlingen ges förutsättningar att lyckas.

1.4 Begrepp

BEGREPP	FÖRKLARING	KÄLLA OCH KOMMENTAR
e-underskrift (elektronisk underskrift)	En elektronisk underskrift enligt EU:s eIDAS-förordning (nr 910/2014), vilket innebär att den är en digitalt skapad underskrift som används för att bekräfta en persons identitet och vilja att godkänna innehållet i en handling. Begreppet e-underskrift används i Sverige som det officiella och rekommenderade uttrycket inom offentlig sektor, för att undvika förväxling med den tekniska termen *digital signatur*. En e-underskrift är alltså både en juridisk handling och en tekniskt verifierbar säkerhetsmekanism. Den utgör bevis på att en identifierad person har godkänt ett dokument, och att dokumentet därefter inte har ändrats.	eSam (2018): *Vägledning e-legitimation och e-underskrift* Digg (2024): *E-underskrift* Sambruk (2025): *Praktiska erfarenheter av e-underskrifter* eIDAS-förordningen (EU 910/2014), art. 3 p. 10 och 26
Digital underskrift	Används ofta som synonym till e-underskrift, men tekniskt sett är det felaktigt. Begreppet ”digital” syftar på den matematiska, kryptografiska funktion (hash-signatur) som ligger bakom den elektroniska underskriften. I offentlig sektor används termen e-underskrift för att betona det juridiska momentet snarare än den tekniska mekanismen.	Digg; eSam (2018); och Sambruk (2025).

Digital signatur	Kryptografiskt begrepp inom IT-säkerhet som avser den tekniska metod (PKI, hashning, kryptering) som används för att skapa en elektronisk underskrift. En digital signatur är alltså en teknisk komponent, inte ett juridiskt begrepp.	ETSI EN 319 102; eSam (2018) kap. 7. Digg förklarar att digital signatur används för att säkerställa att innehållet inte har ändrats.
Skillnaden mellan signatur och underskrift	”Signatur” beskriver den tekniska funktionen som används för att säkra ett dokument (digital signatur), medan ”underskrift” beskriver den juridiska handlingen att bekräfta eller godkänna innehållet (e-underskrift).	eIDAS och eSam (2018).
e-legitimation	Ett elektroniskt bevis på en persons identitet.	DIGG – ”E-legitimation” (2024); eSam (2018) kap. 12
e-tjänstelegitimation	En e-legitimation som inte representerar en fysisk person som privatperson, utan en person i en yrkesroll eller funktion i en organisation.	SKR (2025) *Rekommendationer för identitets- och behörighetshantering* ; Digg:s definition av ”organisationslegitimation”.
Identitetsintyg (Attribute Assertion)	Elektroniskt intyg som styrker användarens identitet vid e-legitimering eller e-underskrift. Utfärdas av leverantör av identitetsintyg och används av den förlitande parten (t.ex. kommunen).	eSam (2018) kap. 7.10–7.13 .
Förlitande part	Organisation (t.ex. kommun, myndighet eller region) som använder och litar på en e-legitimation eller e-underskrift för att utföra rättshandlingar.	eSam (2018) kap. 7.13–7.20 .
Tillitsnivå (LoA – Level of Assurance)	Mått på säkerhetsnivån i en e-legitimation. Svensk tillitsram har nivå 2–4. LoA 3 motsvarar ”väsentlig” och LoA 4 ”hög”.	Digg:s tillitsramverk
AdES (Avancerad elektronisk underskrift)	En underskrift som är unikt kopplad till undertecknaren, möjliggör identifiering och upptäcker ändringar. Kräver inte kvalificerat certifikat.	eIDAS art. 26
QES (Kvalificerad	En avancerad underskrift skapad med ett kvalificerat certifikat och kvalificerad signeringsenhet (QSCD).	eIDAS art. 3 p. 12, art. 25

elektronisk underskrift)	Har samma juridiska status som handskriven signatur inom EU.	
EES (Enkel elektronisk underskrift)	Grundläggande form av elektronisk underskrift, t.ex. kryssrutor, e-post eller knapptryckning, utan stark identitetssäkring.	eIDAS art. 3 p. 10
E-stämpel (elektronisk stämpel)	Elektronisk signatur som används av en juridisk person (organisation) för att bevisa att dokumentet kommer från rätt källa och inte ändrats.	eIDAS art. 35–36
PKI (Public Key Infrastructure)	Teknisk infrastruktur för hantering av digitala certifikat och nycklar som används för e-underskrifter.	ETSI EN 319 411
Certifikatutfärdare (CA – Certificate Authority)	En betrodd part som utfärdar och administrerar digitala certifikat som kopplar en identitet till en publik nyckel.	ETSI EN 319 411
Betrodd tjänst / Betrodd leverantör (Trust Service Provider)	En aktör som erbjuder tjänster som e-underskrifter, tidsstämpling, certifikat eller arkivering enligt eIDAS.	eIDAS art. 3 p. 16
Kvalificerad betrodd tjänst (QTSP)	En betrodd leverantör som är godkänd av en nationell tillsynsmyndighet och upptagen i EU:s Trusted List (EUTL).	eIDAS art. 20
EU Trusted List (EUTL)	Officiell lista över kvalificerade betrodda tjänsteleverantörer inom EU, administrerad av medlemsstaternas tillsynsmyndigheter.	EU-kommissionen
LTV (Long-Term Validation)	Standardiserad metod för att bevara bevisvärdet av e-underskrifter över tid genom att spara all valideringsdata.	ETSI EN 319 142
Valideringsintyg (Validation Evidence)	Ett bevisdokument som skapas vid signering och bekräftar att certifikat och signatur var giltiga vid tillfället. Kan lagras separat eller inbäddas i PDF.	ETSI EN 319 102-1, EN 319 142-1
PAdES / XAdES / CAdES	EU-standarder för lagring av e-underskrifter i PDF (PAdES), XML (XAdES) och binärt CMS-format (CAdES).	ETSI EN 319 142 / 132 / 122
PDF/A	ISO-standard för arkivbeständiga PDF-filer. PDF/A-1 rekommenderas för långsiktigt bevarande i offentlig sektor.	ISO 19005

Hash / Hashvärde	En unik kontrollkod som används för att representera ett dokuments innehåll. Om dokumentet ändras, ändras även hashvärdet.	Kryptografisk term
Tidsstämpel (TSA – Time Stamping Authority)	Bevis på att en digital händelse inträffade vid en viss tidpunkt.	ETSI EN 319 421
LTV-resignering	Process där ett dokument förses med ny signatur eller tidsstämpel för att förlänga giltigheten av en tidigare signatur.	ETSI EN 319 142
Digitalt godkännande	Elektroniskt samtycke eller beslut utan kryptografisk underskrift, men med stark autentisering och loggning.	eSam, SKR
Hashsignering	Signeringsmodell där endast dokumentets hashvärde skickas till signeringstjänsten – inte själva dokumentet – för att skydda sekretess.	Digg:s säkerhetsrekommendationer
QSCD (Qualified Signature Creation Device)	Certifierad teknisk utrustning (hårdvara eller fjärrtjänst) som skyddar signeringsnycklar vid skapande av kvalificerade underskrifter.	eIDAS art. 29
OCSP / CRL	OCSP (Online Certificate Status Protocol) och CRL (Certificate Revocation List) används för att kontrollera om ett certifikat är giltigt eller spärrat.	ETSI EN 319 411
Beviskedja (Evidence Chain)	Samlad uppsättning data som krävs för att verifiera en e-underskrifts giltighet: signatur, certifikat, OCSP/CRL, tidsstämplar och eventuell valideringsrapport.	ETSI EN 319 102-1
Preskriptionstid (rättslig prövningsperiod)	Den tidsperiod under vilken en rättslig tvist om ett dokument kan väckas – relevant för hur länge valideringsdata behöver bevaras.	Juridisk term, SKR:s tillämpning

2 Bakgrund och behov

2.1 Varför e-underskrifter är viktiga

E-underskrifter är en grundläggande komponent i den digitala förvaltningen. De skapar rättssäkerhet genom att styrka vem som har godkänt ett beslut, spårbarhet genom att varje signering kan verifieras, och effektivitet genom att handlingar kan hanteras helt digitalt.
De bidrar också till interoperabilitet, eftersom e-underskrifter följer gemensamma europeiska standarder (eIDAS), vilket möjliggör utbyte av elektroniska handlingar mellan organisationer och länder.

2.2 Lagstiftning och regelverk

E-underskrifter omfattas av flera lagar och regelverk som tillsammans skapar ramen för hur kommuner och regioner får och bör använda dem:

- *eIDAS-förordningen (EU 910/2014)* reglerar elektronisk identifiering, e-legitimation och e-underskrifter inom hela EU.
- *Förvaltningslagen (2017:900)* anger att beslut ska dokumenteras skriftligt och att identiteten på beslutsfattare ska kunna fastställas.
- *Kommunallagen (2017:725)* ställer krav på korrekt beslutsfattande och delegering, vilket förutsätter att underskrifter eller godkännanden kan knytas till rätt person.
- *Arkivlagen (1990:782)* kräver att handlingar ska kunna bevaras i autentiskt skick, vilket påverkar val av format och bevarandemetod för e-underskrifter.
- *Dataskyddsförordningen (GDPR)* reglerar hur personuppgifter i samband med signering (t.ex. identitetsuppgifter, tidsstämplar, IP-adresser) ska behandlas och skyddas.

2.3 Problem och utmaningar

Trots att tekniken för e-underskrifter är etablerad finns flera olösta frågor som påverkar kommunernas möjligheter att fullt ut digitalisera beslutsprocesser:

- *Arkiv och långtidsbevarande* – Det finns standarder som syftar till att säkerställa bevisvärde över tid, såsom LTV (Long-Term Validation) och standarden för valideringsintyg. Dessa anger hur signaturer och deras beviskedjor kan lagras för att möjliggöra framtida verifiering. Däremot saknas ännu en tillförlitlig och praktiskt utvärderad metod som garanterar att validering verkligen kan genomföras efter lång tid, exempelvis efter flera decennier. Forskning, myndighetsanalyser och praktiska erfarenheter visar att kryptografiska algoritmer,

certifikatkedjor och lagringsformat riskerar att bli föråldrade innan bevarandeperioden är över. Detta innebär att ingen enhetlig och långsiktigt säker lösning ännu finns för hur e-underskrifter ska bevaras med intakt bevisvärde över tid, något som även framgår i SOU 2021:9, Digg:s vägledningar och i flera myndigheters pågående bedömningar..

- *Tillitsnivåer och krav på underskriftens styrka* – otydlighet råder kring när avancerad respektive kvalificerad underskrift behövs.
- *Standardisering och interoperabilitet* – flera standarder (PAdES, XAdES, CAdES) används parallellt, vilket kan försvåra utbyte mellan olika system.
- *Behov av gemensamma riktlinjer* – flera vägledningar (Digg, eSam, Kammarkollegiet, Sambruk) pekar på att kommuner behöver praktiska stöd för att göra rätt avvägningar i kravställning och upphandling.

3 Om e-underskrifter

3.1 Grundläggande om e-underskrifter

I samband med e-underskrifter används ofta begreppet PKI – Public Key Infrastructure. Det är i grunden är ett sätt att skapa förtroende och tillit i den digitala världen, ungefär som vi gör med pass eller ID-kort i det fysiska livet.

Grundläggande krav att ställa vid upphandling av underskriftstjänst:

- *PKI-baserad signering används* (d.v.s. underskriften kan kopplas till en verifierbar identitet).
- *Hela signaturkedjan lagras* tillsammans med dokumentet.
- *Långtidsvalidering* stöds, så att bevisvärdet finns kvar även efter många år.

3.2 Liknelsen med pass eller körkort

När du legitimerar dig visar du ett pass som är utfärdat av en myndighet. Den myndigheten garanterar att uppgifterna stämmer – ditt namn, foto och personnummer.

På samma sätt fungerar PKI:

- I stället för ett pass finns ett digitalt certifikat.

- I stället för ett foto finns en digital nyckel som bara du har kontroll över.
- I stället för myndigheten som utfärdat passet finns en certifikatutfärdare (CA) som garanterar att certifikatet verkligen tillhör dig.

3.3 Kedjan av förtroende

När någon kontrollerar din digitala underskrift tittar systemet på hela kedjan:

1. *Din underskrift* – skapas med din privata nyckel, som bara du kan använda.
2. *Ditt certifikat* – visar att underskriften tillhör just dig.
3. *Certifikatutfärdaren* – en betrodd part som har kontrollerat din identitet innan certifikatet skapades.
4. *Rotutfärdaren* – en nationellt eller internationellt erkänd part som alla litar på.

Om alla länkar i kedjan är giltiga vet mottagaren att underskriften är äkta och att dokumentet inte har ändrats.

3.4 Bevisvärde över tid

Precis som ett pass har ett utgångsdatum har digitala certifikat en begränsad livslängd. För att kunna verifiera om 10, 20 eller 30 år att ett dokument verkligen var underskrivet måste man spara hela kedjan – även beviset att certifikatet var giltigt när signeringen gjordes.

Detta kallas långtidsvalidering (LTV). En bra e-underskriftstjänst ser till att spara dessa bevis automatiskt, så att kommunen kan visa äktheten långt efter att certifikaten har gått ut.

3.4.1 Tjänster för LTV

För att säkerställa långtidsvalidering (LTV) används särskilda valideringsoch arkiveringstjänster. De kan fungera både som en del av en underskriftstjänst och som fristående komponenter. Syftet är att:

- Samla in och spara valideringsdata (OCSP-respons[1] eller CRL-listor[2]) som visar att certifikatet var giltigt vid tidpunkten för underskriften.
- Utföra återkommande "resigneringar" eller tidsstämplingar för att förlänga bevisvärdet när gamla certifikat eller algoritmer upphör att gälla.
- Automatiskt uppdatera beviskedjan så att dokumentet alltid kan valideras enligt aktuella standarder.
- Möjliggöra oberoende kontroll – det ska gå att kontrollera dokumentets giltighet i standardverktyg, inte bara i leverantörens system.

Exempel på sådana lösningar är tjänster från leverantörer av betrodda tjänster inom EU, som ofta är certifierade enligt eIDAS som *Qualified Validation Service* eller *Qualified Preservation Service*.

3.4.2 Valideringsintyg (Validation Evidence)

Valideringsintyg är ett alternativ eller komplement till långtidsvalidering (LTV) för att bevara bevisvärdet av en e-underskrift över tid. I stället för att framtida validering ska bygga på att hela certifikatkedjan och spärrinformation finns tillgänglig, skapas ett separat intyg vid signeringstillfället.

Detta valideringsintyg är en teknisk bekräftelse på att underskriften kontrollerades medan certifikatet fortfarande var giltigt och att kontrollen gav ett godkänt resultat. Intyget innehåller uppgifter om bland annat:

- identiteten på certifikatutfärdaren (CA) och dess giltighetsstatus,
- resultatet av kontrollen mot spärrinformation (OCSP/CRL),
- tidsstämpel för när valideringen utfördes, och
- referens till det dokument och den underskrift som validerats.

Vid senare granskning, exempelvis flera år efter signeringen, behöver kommunen då inte längre återskapa hela valideringskedjan. Det räcker att kunna visa att valideringsintyget är äkta och oförändrat, vilket förenklar bevisföringen och minskar beroendet av långsiktiga certifikattjänster.

För bästa rättssäkerhet kan valideringsintyg och LTV användas tillsammans, så att båda metoderna finns som bevis. I upphandlingar av e-underskriftstjänster bör kommunen därför ställa krav på att:

---

[1] OCSP (Online Certificate Status Protocol) innebär att systemet frågar en betrodd tjänst i realtid om certifikatet är giltigt.
[2] CRL (Certificate Revocation List) är en lista som publiceras regelbundet och innehåller alla certifikat som återkallats.

- valideringsintyg kan skapas automatiskt vid signering,
- intyget kan lagras som en integrerad del av PDF-dokumentet (inbäddat enligt ETSI-standard), och
- intyget kan exporteras separat för arkivering vid behov.

Denna metod rekommenderas av flera europeiska standardiseringsorgan (*ETSI EN 319 102-1 och EN 319 142*) och kompletterar befintliga LTV-lösningar genom att stärka spårbarheten och minska framtida valideringsberoenden.

Tekniks fördjupning

I PAdES-standarden (*ETSI EN 319 142-1*) kan ett valideringsintyg lagras direkt i PDF-filen som en del av underskriftens beviskedja. Detta görs i en särskild datasektion (Document Security Store) där valideringsinformationen bäddas in tillsammans med tidsstämplar och certifikatdata. När detta sker enligt PAdES-LT- eller LTA-profilen blir valideringsintyget en integrerad del av dokumentet och behöver inte hanteras som en separat fil. Det innebär att både dokument och bevisdata kan arkiveras och flyttas som en helhet, utan risk för att kopplingen mellan underskrift och intyg förloras.

3.4.3 Bedömning av långtidsvalidering och bevarandeperioder

Långtidsvalidering (LTV) säkerställer att en e-underskrift kan verifieras även efter att de tekniska certifikaten upphört att gälla. Syftet är att bevara handlingens rättsliga bevisvärde under den tid då en rättslig prövning kan bli aktuell. Det är dock inte alltid nödvändigt att bevara full valideringsmöjlighet under hela dokumentets livscykel. När den rättsliga prövningsperioden har passerat – till exempel efter preskriptionstid eller annan tidsfrist – kan handlingen fortfarande ha arkivmässigt värde, men behovet av teknisk verifiering av underskriften upphör.

Rekommendation:
Kommuner bör överväga att låta kravet på långtidsvalidering (LTV) gälla endast under den period då dokumentet kan ha rättslig betydelse. Efter den tiden kan det vara tillräckligt att bevara själva dokumentet som arkivhandling, även om möjligheten att tekniskt verifiera underskriften inte längre finns.

En sådan ordning kan betraktas som en kontrollerad gallring av valideringsdata och är förenlig med arkivlagens principer, under förutsättning att dokumentets informationsinnehåll och autenticitet i övrigt bevaras.

Respektive kommun behöver göra en egen bedömning av hur länge valideringsdata ska bevaras, med hänsyn till dokumentets funktion, rättsliga relevans och lokala dokumenthanteringsplan.

4 Tre nivåer av elektroniska underskrifter enligt eIDAS

Rekommendation

Kommuner bör som huvudregel välja avancerad elektronisk underskrift.

Enkel underskrift kan räcka för lågriskflöden där det inte finns juridiska krav. Kvalificerad underskrift bör reserveras för särskilda högriskärenden eller där det krävs för internationellt erkännande

EU:s eIDAS-förordning (EU 910/2014) definierar tre nivåer av elektroniska underskrifter: enkel, avancerad och kvalificerad. Nivåerna skiljer sig åt i hur säkra de är och vilken juridisk tyngd de har.

4.1 Enkel elektronisk underskrift (EES)

Exempel:

- Skriva sitt namn i ett e-postmeddelande
- Kryssa i en ruta “Jag godkänner” i en e-tjänst
- Ladda upp en bild på sin handskrivna signatur

Kännetecken:

- Låg säkerhetsnivå – ingen säker garanti för vem som egentligen undertecknat.
- Ingen krav på identitetskontroll eller skydd mot att dokumentet ändras i efterhand.

Användning:

- Kan duga i enkla sammanhang där det inte är avgörande att bevisa exakt vem som godkänt (t.ex. interna noteringar, låg risk), eller där det finns kompletterande bevisning.

4.2 Avancerad elektronisk underskrift (AdES)

Exempel:

- Signering via e-legitimation (e-tjänstelegitimation i tjänsten eller privat e-legitimation för invånare) där signaturen skapas kryptografiskt
- Digital signatur i PDF med spårbar identitet

Kännetecken:

- Är entydigt kopplad till undertecknaren
- Gör det möjligt att identifiera undertecknaren.[3]
- Skapas med signeringsdata som undertecknaren har under egen kontroll
- Är kopplad till dokumentet så att ändringar kan upptäckas
- Automatisk validering mot EU:s tillitsförteckningar (EUTL) gäller endast QES. För AdES sker oberoende validering genom beviskedjan (certifikat, spärrinformation, tidsstämplar) utan stöd av en officiell lista över betrodda utfärdare.

Användning:

- Passar de flesta kommunala beslut, avtal och protokoll där beviskedjan kan styrkas (certifikat, spärrinfo, tidsstämplar) och där verksamheten bedömer att AdES ger tillräckligt bevisvärde.
- Ger juridiskt starkt bevisvärde inom Sverige och EU[4]

4.2.1 Fördjupning: Avancerad elektronisk underskrift (AdES)

Teknisk grundprincip:

- Bygger på PKI (Public Key Infrastructure) och skapas med undertecknarens privata nyckel.[5]
- Underskriften knyts kryptografiskt till dokumentet genom en hashfunktion – ändras dokumentet blir signaturen ogiltig.

---

[3] I vissa verksamheter kan det vara önskvärt att dölja undertecknarens verkliga identitet, till exempel personnummer, för allmänheten. I sådana fall kan man i stället använda ett annat identitetsbärande attribut, såsom ett unikt GUID, som gör det möjligt att spåra och verifiera personen utan att avslöja dennes personuppgifter.

[4] Flera EU länder kräver kvalificeras underskrift

[5] Det finns inget uttryckligt krav i eIDAS-förordningen att en avancerad elektronisk underskrift (AdES) måste bygga på PKI (Public Key Infrastructure). PKI är den vanligaste och mest etablerade tekniska lösningen för att uppfylla kraven på integritet, autenticitet och icke-förnekbarhet, men andra tekniska lösningar som kan uppnå samma säkerhetsnivå är också tillåtna enligt eIDAS.

- Innehåller ett certifikat som identifierar undertecknaren.

Certifikatkrav:

- Behöver inte vara kvalificerat, men bör vara utfärdat av en certifikatutfärdare (CA) som följer kraven för betrodda tjänster enligt eIDAS. Efterlevnaden bedöms normalt genom etablerade rutiner, revisioner eller i efterhand vid juridisk prövning – det finns ingen formell godkännandeprocess för icke-kvalificerade CA:er.
- Kan använda befintliga e-legitimationer som godkänns av Digg.

Standarder:

- Ofta används PAdES (för PDF) eller XAdES (för XML) för att lagra signaturen.
- Stöd för LTV (Long Term Validation) bör finnas så att signaturen kan verifieras även efter certifikatets utgång.

Teknisk kontroll:

- Validering sker genom att kontrollera signaturkedjan, certifikatets status och tidsstämplar.
- Kan göras automatiskt i signeringstjänst eller med valideringsverktyg som stödjer eIDAS-profiler.

4.3 Kvalificerad elektronisk underskrift (QES)

Exempel:

- Signering med ett kvalificerat certifikat på ett smartkort eller i en HSM[6] som är godkänd enligt eIDAS
- Kvalificerad underskrift via tjänst som är certifierad som "kvalificerad betrodd tjänst"

Kännetecken:

- Är en avancerad underskrift plus extra krav:
  - Måste använda ett kvalificerat certifikat utfärdat av en kvalificerad leverantör
  - Måste skapas med en kvalificerad signeringsenhet (t.ex. certifierad hårdvara)

[6] HSM - Hardware security module, en fysisk datorenhet som skyddar och hanterar hemligheter (framför allt digitala nycklar) och utför krypterings- och dekrypteringsfunktioner för digitala signaturer, stark autentisering och andra kryptografiska funktioner.

- Identiteten för certifikatinnehavaren ska vara verifierad med säkerhetsnivå hög. Om verifieringen sker med e-legitimation ska den vara på LoA 4 (Hög).[7]
- Validering sker mot EU Trusted List (EUTL) för att säkerställa att utfärdaren är kvalificerad
- Har samma juridiska status som en handskriven signatur i hela EU[8]

Användning:

Rekommenderas när högsta möjliga säkerhet krävs, t.ex.:

- Dokument som måste accepteras i andra EU-länder
- Mycket känsliga beslut eller avtal där felaktig signatur kan få stora konsekvenser
- Domstolsärenden eller rättsakter där starkt bevisvärde är nödvändigt

4.3.1 Fördjupning: Kvalificerad elektronisk underskrift (QES)

Teknisk grundprincip:

- Bygger på samma PKI-struktur som en avancerad underskrift men med högre krav på säkerhet och kontroll.
- Skapas med en kvalificerad signeringsenhet (QSCD – Qualified Signature Creation Device) som skyddar den privata nyckeln från obehörig åtkomst.
- Underskriften innehåller ett kvalificerat certifikat som utfärdats av en kvalificerad betrodd tjänsteleverantör (QTSP) godkänd enligt eIDAS.

---

[7] I dagsläget (hösten 2025) finns ingen svensk e-legitimation som uppfyller tillitsnivå 4 (LoA High) enligt eIDAS. De e-legitimationer som används inom offentlig sektor som e-tjänstelegitimationer, är godkända på tillitsnivå 3 (väsentlig).
Det innebär att svenska kommuner i praktiken inte kan utfärda kvalificerade e-underskrifter (QES) förrän en LoA 4-baserad e-legitimation finns tillgänglig.

[8] Även om kvalificerade elektroniska underskrifter (QES) enligt eIDAS-förordningen har samma juridiska status som en handskriven signatur inom hela EU, finns två viktiga undantag:

1. *Slutna system* – Om parter i förväg har avtalat om ett visst förfarande inom ett avgränsat system (t.ex. mellan kommunen och en leverantör), kan ingen part kräva att kvalificerad underskrift används i stället för den metod som avtalats.
2. *Nationella formkrav* – I svensk rättstillämpning tolkas vissa bestämmelser med krav på "underskrift" eller "namnteckning" som att underskriften måste ske på papper, såvida inte lagen uttryckligen medger elektronisk form. Detta innebär att elektroniska underskrifter ännu inte accepteras i alla typer av kommunala beslut eller handlingar, trots eIDAS-förordningens huvudregel.

- Dokumentet kopplas kryptografiskt till signaturen med hashfunktion, och valideras mot en betrodd rotutfärdare som finns i EU Trusted List (EUTL)**.**

Certifikatkrav:

- Certifikatet ska vara kvalificerat och utfärdas av en kvalificerad tillhandahållare av betrodda tjänster (QTSP), listad i EU:s Trusted List (EUTL) enligt eIDAS.
- Certifikatet ska utfärdas till en fysisk person efter säker identifiering.
- Om identiteten kontrolleras med hjälp av en e-legitimation ska denna ha tillitsnivå Hög (LoA 4) enligt tillitsramverket för e-legitimationer.
- CA (Certificate Authority) ansvarar för att säkerställa att identiteten är korrekt verifierad och att certifikatet kopplas entydigt till rätt individ..

Standarder:

- Vanligen används PAdES (för PDF) eller XAdES (för XML), men i kvalificerad kontext krävs att dessa följer de ETSI-standarder som gäller för kvalificerade profiler, t.ex. ETSI EN 319 142-2 (PAdES Baseline – B-LTA-nivå).
- QES använder samma formatfamiljer (PAdES/XAdES/CAdES) men enligt kvalificerade profiler. Tidsstämpling krävs i flera profiler; LTV/LTA rekommenderas starkt för långtidsbevisvärde och kan vara krav i vissa profiler/kontexter. Validering sker mot EUTL.
- Signaturen ska kunna valideras mot EUTL och visa status ”kvalificerad”.

Teknisk kontroll:

- Validering sker genom att kontrollera hela kedjan: signatur, QSCD-attribut, certifikatets giltighet och att utfärdaren finns på EUTL.
- Systemet ska verifiera att både certifikat och signeringsenhet är kvalificerade enligt aktuell eIDAS-version.
- Validering kan göras automatiskt via eIDAS-kompatibla valideringstjänster eller manuellt i EU:s DSS-verktyg.
- Vid långtidsvalidering ska lösningen spara OCSP-respons, CRL-data och kvalificerade tidsstämplar för att kunna bevisa giltighet även efter certifikatets utgång.

4.4 Begränsningar i Sverige för kvalificerade underskrifter (QES)

En kvalificerad elektronisk underskrift (QES) kräver enligt eIDAS-förordningen att undertecknaren identifieras med en e-legitimation som uppfyller tillitsnivå 4 (LoA4) – den högsta säkerhetsnivån för elektronisk identifiering.

I dagsläget finns ingen svensk utfärdare av e-legitimation på LoA4-nivå som är tillgänglig för bred användning inom offentlig sektor. De svenska e-legitimationer som godkänts av ligger på tillitsnivå 3 (LoA3).

Detta innebär att kommuner och regioner i praktiken inte kan skapa kvalificerade elektroniska underskrifter (QES) i dagsläget, eftersom det saknas en infrastruktur och godkända identitetslösningar på LoA4-nivå.

4.5 Beslutsmatris

Risk/konsekvens	Rekommenderad metod	Exempel	Minimikrav
Låg (intern rutin, ingen extern rättsverkan)	Digitalt godkännande	Intern attest, mottagningskvitto	Stark autentisering, logg, tidsstämpel, export till e-arkiv
Medel (nationell rättsverkan)	AdES (PAdES)	Avtal, betyg, protokolljustering	PAdES-LTV, PDF/A vid bevarande, tillitsnivå ≥ 3
Hög (domstolsbevisning/ internationellt)	QES	EU-erkännande, högriskbeslut	Kvalificerat certifikat/QSCD, EUTL-leverantör, identitetsstyrka ‘hög’ (vid e-legitimation: LoA4).

4.6 E-stämpel (elektronisk stämpel)

En e-stämpel (elektronisk stämpel) används för att säkerställa dokumentets ursprung och integritet – inte för att uttrycka en fysisk persons avsikt att godkänna innehållet, som vid en e-underskrift. E-stämpeln används alltså av organisationer, inte individer, och fungerar som ett ”digitalt sigill” som visar att en handling kommer från rätt källa och inte har ändrats sedan den stämplades.

4.6.1 Skillnaden mellan e-underskrift och e-stämpel

Egenskap	E-underskrift	E-stämpel

Vem som stämplar/signerar	En fysisk person	En juridisk person (t.ex. kommun, myndighet eller bolag)
Syfte	Visar en persons vilja att godkänna eller besluta	Visar att dokumentet kommer från rätt organisation och är oförändrat
Certifikat	Personligt certifikat kopplat till individ	Organisationscertifikat (utställt till organisationen)
Rättsverkan	Juridiskt bindande viljeyttring	Tekniskt och juridiskt bevis på ursprung och autenticitet

4.6.2 Nivåer enligt eIDAS

Precis som e-underskrifter kan e-stämplar förekomma på tre nivåer:

- *Enkel e-stämpel* – grundläggande variant utan krav på stark identitetskontroll.
- *Avancerad e-stämpel (AdES-seal)* – entydigt kopplad till den stämplande organisationen och gör det möjligt att upptäcka ändringar i dokumentet.
- *Kvalificerad e-stämpel (QES-seal)* – använder ett kvalificerat certifikat utfärdat av en kvalificerad betrodd tjänsteleverantör (QTSP) och ger högsta juridiska bevisvärde inom hela EU.

4.6.3 Användning i kommunal verksamhet

E-stämplar kan användas när dokument behöver utfärdas automatiskt eller utan en fysisk undertecknare, exempelvis:

- beslut som genereras maskinellt i verksamhetssystem,
- intyg, registerutdrag eller aviseringar från kommunen,
- kvittenser och kontrollrapporter,
- notifieringar mellan system inom kommunen eller till andra myndigheter.

Genom att använda e-stämplar kan kommunen garantera autenticitet och spårbarhet även i helt automatiserade flöden.

5 Standarder och format

5.1 Dokumentformat

Rekommendation

Använd PDF/A som dokument format på dokument som har e-underskrifter. PDF/A är det rekommenderade arkivformatet för kommunala handlingar som ska undertecknas och bevaras.

För att säkerställa att kommunala handlingar kan bevaras och läsas i många decennier framåt krävs ett långsiktigt hållbart filformat. PDF/A är en internationell standard för arkivering av elektroniska handlingar (ISO 19005), framtagen just för långtidsbevarande.

Riksarkivet anger att PDF/A är ett av de godkända arkivformaten för handlingar som ska bevaras elektroniskt. Myndigheten har dock inte pekat ut ett enskilt obligatoriskt format för långtidsbevarande av elektroniska handlingar. PDF/A rekommenderas som ett av de godtagbara formaten för dokument som ska diarieföras, signeras eller arkiveras, eftersom det säkerställer läsbarhet över tid och är oberoende av specifika programvaror.

Samtidigt behöver formatvalet göras utifrån användningsområdet. För dokument vars informationsinnehåll ska bearbetas vidare i verksamhetssystem – till exempel där data ska kunna tolkas eller återanvändas maskinellt – bör andra format som bättre stödjer strukturerad datahantering övervägas, till exempel XML eller JSON.

Valet av format ska därför motiveras utifrån både bevarande-, användbarhets- och informationskrav, och kan variera mellan olika typer av handlingar och processer.

5.1.1 Val av PDF/A-version för långtidsbevarande

PDF/A är den ISO-standard som används för arkivbeständiga PDF-filer. Standarden har flera versioner (PDF/A-1, /A-2, /A-3) som tillkommit över tid för att stödja nya funktioner i PDF-formatet, till exempel inbäddade filer och förbättrat färghanteringsstöd.

Det råder delade meningar om vilken version som är mest lämplig för offentlig sektor:

- *PDF/A-1 (ISO 19005-1:2005)* betraktas som den mest öppna och långsiktigt stabila versionen. Den stöds brett av olika leverantörer och är inte beroende av proprietära tillägg.
- *PDF/A-2 och /A-3* erbjuder fler funktioner (t.ex. stöd för JPEG 2000, transparens och inbäddade filer), men dessa funktioner innebär samtidigt ökad komplexitet och risk för leverantörslåsning eftersom full funktionalitet ofta kräver Adobe-specifika lösningar.

Rekommendation

För att främja öppenhet, interoperabilitet och oberoende från specifika leverantörer rekommenderar SKR att PDF/A-1 används som primärt format för långtidsbevarande av e-underskrivna dokument.

PDF/A-1[9] är fullt tillräckligt för majoriteten av kommunala handlingar, särskilt textbaserade beslut och protokoll. Om särskilda behov finns (t.ex. komplex grafik, CAD-ritningar eller inbäddade bilagor) kan senare versioner övervägas, men då bör kommunen särskilt dokumentera beslutet och säkerställa att både e-arkiv och valideringstjänster stödjer den aktuella versionen.

5.2 Standarder för e-underskrifter

5.2.1 EU:s vägledning och krav

EU har genom *Kommissionens genomförandebeslut (EU) 2015/1506*[10] pekat ut vilka tekniska profiler för elektroniska underskrifter som ska erkännas inom unionen. Dessa profiler kallas ofta för *baseline-profiler* och syftar till att skapa interoperabilitet över gränser.
De tre standardformaten är:

- *PAdES* (PDF Advanced Electronic Signatures) – för underskrift av PDF-dokument
- *XAdES* (XML Advanced Electronic Signatures) – för XML-baserade dokument
- *CAdES* (CMS Advanced Electronic Signatures) – för binära data i CMS-format

[9] Riksarkivet anger i sina föreskrifter (RA-FS 2009:1, RA-FS 2020:2) att PDF/A-1 är godkänt för långtidsbevarande av statliga och kommunala handlingar. Andra versioner kan användas om myndigheten kan visa att de inte äventyrar långsiktig läsbarhet och interoperabilitet.
[10] KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2015/1506

Kommuner och myndigheter inom EU ska därför kunna ta emot och validera underskrifter i dessa format, oavsett i vilket medlemsland de skapats.

5.3 Digg:s syn

Digg anger i sin vägledning[11] att e-underskrifter i offentlig förvaltning ska följa eIDAS och därmed de standarder och profiler som EU pekat ut. Digg har inte uttryckligen sagt att *en viss standard* ska användas exklusivt (t.ex. PAdES), utan betonar att det är upp till verksamhetens behov att avgöra format.
I praktiken innebär det att svenska kommuner kan möta både PAdES, XAdES och CAdES, men att PAdES är det vanligaste formatet i administrativa sammanhang där PDF används som dokumentstandard.

5.3.1 ETSI-standarderna

De tekniska detaljerna för dessa profiler tas fram av den europeiska standardiseringsorganisationen ETSI (European Telecommunications Standards Institute)[12].

- **ETSI EN 319 142** definierar PAdES
- **ETSI EN 319 132** definierar XAdES
- **ETSI EN 319 122** definierar CAdES

Standarderna säkerställer att underskrifter kan:

- valideras tekniskt
- bevaras över tid (med stöd för långtidsvalidering, LTV)
- användas oberoende av leverantör

6 Oberoende validering av e-underskrifter

För att säkerställa att en e-underskrift kan verifieras oberoende av leverantören, behöver kommunen förstå hur valideringen fungerar både tekniskt och praktiskt. Det gäller oavsett om underskriften är avancerad (AdES) eller kvalificerad (QES).

[11] Digg, E-underskrifter
[12] ETSI

6.1 Syfte med oberoende validering

Oberoende validering innebär att kommunen själv – utan att använda leverantörens egna verktyg – kan visa att:

- dokumentet inte har ändrats sedan det signerades,
- underskriften verkligen skapades av den som är angiven som undertecknare, och
- certifikatet var giltigt vid signeringstillfället.

Detta är avgörande för rättssäkerhet, arkivering och långsiktigt bevisvärde.

6.2 Validering av avancerade underskrifter (AdES)

Avancerade underskrifter bygger på betrodda certifikat och standarden ETSI EN 319 142 (PAdES). För att en AdES ska kunna valideras oberoende krävs att dokumentet innehåller en komplett beviskedja:

KOMPONENT	BESKRIVNING
Signaturdata	Den kryptografiska underskriften som knyter undertecknarens privata nyckel till dokumentet.
Certifikatkedja (CA)	Visar vem som utfärdade certifikatet och hur det kopplas till en betrodd rot-CA.
OCSP-svar eller CRL-lista	Visar att certifikatet var giltigt vid tidpunkten för signeringen.
Tidsstämpel (TSA)	Garanterar att underskriften gjordes vid en viss tidpunkt.

Denna information lagras enligt de s.k. ETSI-basprofilerna:

- **B** – grundläggande signatur,
- **T** – inkluderar tidsstämpel,
- **LT** – inkluderar valideringsdata (OCSP/CRL),
- **LTA** – inkluderar långtidsbevarande (resignering och ny tidsstämpling).

För oberoende verifiering rekommenderas minst PAdES-LT eller PAdES-LTA. Validering kan göras med standardverktyg som:

- EU DSS Validation Tool (ec.europa.eu/digital-building-blocks/DSS)
- Adobe Acrobat Reader (med eIDAS-validering aktiverad)
- eller andra eIDAS-kompatibla verktyg.

6.3 Validering av kvalificerade underskrifter (QES)

Kvalificerade underskrifter följer samma principer som AdES men använder kvalificerade certifikat och certifierad signeringsutrustning (QSCD). Det innebär att beviskedjan automatiskt innehåller all nödvändig information för att uppfylla eIDAS art. 28–31.

KOMPONENT	BESKRIVNING
Kvalificerat certifikat	Utfärdat av en leverantör som finns på **EU Trusted List (EUTL)**.
QSCD-enhet	Säker hårdvarumodul eller fjärrtjänst som garanterar att nyckeln inte kan kopieras eller manipuleras.
Tidsstämpel (TSA)	Utfärdas av en kvalificerad tidsstämplingstjänst (Q-TSA).
Valideringsmöjlighet	Alla verktyg som är eIDAS-kompatibla kan validera QES automatiskt via EUTL-listorna.

För kommuner innebär detta att ingen särskild licens eller leverantörsverktyg behövs för att verifiera en QES – valideringen kan ske direkt i standardverktyg så länge leverantören är registrerad på EUTL.

7 Dokument som kräver underskrift

Rekommendation

Kommunen behöver göra en egen behovsinventering över vilka dokument som behöver undertecknas.

Varje kommun har ett eget ansvar att bedöma och beslut om vilka dokument som behöver e-underskrifter. Nedan lista ska ses som rekommendationer.

Rekommendation

När lag eller föreskrift inte kräver en formell underskrift bör kommunen välja digitala godkännanden framför e-underskrifter.

Digitala godkännande ger rättssäkerhet och spårbarhet, minskar kostnad och teknisk komplexitet, och underlättar långsiktigt bevarande och

automation av processer. Läs mer i kapitel 11 Digitala godkännanden – syfte och utformning.

Nedan lista exempel på dokument som behöver underskrifter.

Politiska handlingar

- *Protokoll från kommunfullmäktige, nämnder och styrelser*
  Kommunallagen (KL 5 kap. 61–63 §§) kräver att protokoll justeras och undertecknas av ordförande samt justerare.
- *Protokoll från kommunala bolagsstämmor*
  Aktiebolagslagen kräver underskrift av ordförande och justerare[13].

Myndighetsbeslut och rättsakter

- *Beslut som enligt lag ska undertecknas*
  – t.ex. beslut enligt Socialtjänstlagen (SoL) eller LSS som ska expedieras skriftligt och undertecknat av behörig tjänsteman.[14]
- *Rättsligt bindande avtal*
- *Kommersiella avtal*
  – hyresavtal, entreprenadavtal, köpeavtal, arrende, samverkansavtal, upphandlingskontrakt.
- *Anställningsavtal*
  – LAS och kollektivavtal förutsätter skriftlighet och underskrift.
- *Kollektivavtal eller lokala överenskommelser*
  – ska signeras av behörig part.

Intyg och bevis som utfärdas med rättsverkan

- *Skolbetyg*
  – Skollagen 3 kap. 16 § och Skolverkets föreskrifter kräver att betygsdokument undertecknas.[15]
- *Examensbevis och intyg inom vuxenutbildningen*
  – samma krav som för betyg.
- *Faderskapsbekräftelser och adoptionshandlingar*
  – kräver skriftlig, bevittnad underskrift enligt Föräldrabalken.

Ekonomiska handlingar med krav på signatur

---

[13] Bolagsverket, Skriva protokoll på bolagsstämma
[14] Enligt **SOSFS 2014:5, §§ 14–15**, ska beslut som avser insatser enligt SoL eller LSS dokumenteras skriftligt och inkludera namn eller befattning på beslutsfattaren. Detta implicerar att besluten ska ha en form av undertecknande eller identifierbar signering för att uppfylla dokumentationskravet
[15] Digg har utrett e-underskrifter av betyg, med slutsatsen att skollagen föreslås ändras för att möjliggöra detta

- *Årsredovisning och delårsrapporter*
  – ska undertecknas av samtliga ledamöter i styrelsen/nämnden enligt kommunal redovisningslag.
- *Budget och bokslutsprotokoll*
  – beslutas av fullmäktige och justeras enligt KL.

Övriga handlingar med uttryckliga formkrav

- *Handlingar som ska bevaras som original och har bevisvärde*
  – t.ex. kommunala beslut som expedieras i original till annan myndighet.
- *Handlingar som regleras i speciallagstiftning*
  – t.ex. beslut enligt Alkohollagen, Vapenlagen, Lokala ordningsföreskrifter där föreskrifter kräver underskrift.

8 Sekretessbelagda handlingar och informationsskydd

Vid användning av e-underskrifter eller valideringstjänster måste kommunen särskilt beakta hur sekretessbelagda handlingar hanteras i underskriftsprocessen. Vissa underskriftstjänster kräver att hela dokumentet överförs i klartext till leverantörens system för signering eller validering. Detta kan innebära risker ur både sekretess- och informationssäkerhetsperspektiv.

8.1 Två huvudsakliga angreppssätt

1. **Tjänster där dokumentet överförs till leverantören**
   I dessa fall skickas handlingen till leverantörens miljö, där signering eller validering sker. För att detta ska vara tillåtet när handlingen innehåller sekretessbelagd information krävs att leverantören är godkänd för att hantera sådan information enligt tillämplig säkerhetsklassning och kommunens informationssäkerhetspolicy. Kommunen behöver säkerställa att avtalet och personuppgiftsbiträdesavtalet (PUBA) omfattar denna hantering och att leverantörens säkerhetsnivå motsvarar de krav som gäller för aktuell informationstyp.

2. **Tjänster där endast hashsumma överförs**
   Ett alternativ är att låta dokumentet stanna kvar i kommunens egen miljö och i stället skicka en hashsumma (en unik digital kontrollkod) till underskriftstjänsten. Själva dokumentet lämnar då aldrig kommunens kontroll.
   Denna modell ger högre informationssäkerhet men ställer krav på att vissa delar av underskriftsprocessen — exempelvis hashning,

förberedelse av signeringsdata och eventuell validering — kan utföras av komponenter som driftas i kommunens egen IT-miljö.

8.2 Implikationer för upphandling och kravställning

Vid upphandling av underskrifts- eller valideringstjänster bör kommunen:

- analysera om tjänsten kräver att handlingar överförs i klartext till leverantören,
- ställa krav på att leverantören är godkänd för hantering av sekretessbelagd information, eller
- välja en lösning där endast hashsumman överförs till betrodd part.

Upphandlingsunderlaget bör tydligt beskriva vilket av dessa angreppssätt som ska användas och vilka säkerhets- och driftsmässiga krav som gäller för respektive modell.

8.3 Rekommendation

För handlingar som omfattas av sekretess eller skyddsklass bör kommunen i första hand välja lösningar där själva dokumentet aldrig lämnar kommunens miljö, utan endast en hashsumma överförs för signering eller validering.
Detta minskar riskerna vid hantering, stärker informationsägarskapet och förenklar säkerhetsgranskning av leverantörens miljö.

9 Inkomna elektroniskt undertecknade handlingar från privatpersoner

9.1 Utmaningen

En privatperson skickar in en handling till kommunen som är elektroniskt undertecknad – till exempel ett avtal, en fullmakt eller ett beslut som ska bifogas ansökan. Personen förväntar sig att kommunen ska ta emot och hantera handlingen elektroniskt utan att denne behöver skriva på för hand. Kommunen ställs inför två möjliga vägar: acceptera handlingen eller begära en pappersvariant.

Denna situation är kanske inte så vanlig men sannolikt kommer den bli vanligare. Det finns exempel på hur kommuner inte accepterar elektroniskt undertecknade handlingar motiveringen att de saknar teknisk förmåga att validera underskriften eller att arkivlösningen inte stödjer det elektroniska formatet.

9.2 Varför detta är en utmaning för kommunen

- Om handlingen är elektroniskt undertecknad men kommunen inte kan validera underskriften eller kontrollera certifikatkedjan, saknas kopplingen mellan undertecknare, tidpunkt och dokumentets integritet. Detta innebär osäkerhet för kommunen både i beslutsprocess och arkivering.
- Om handlingen tas emot men inte arkiveras i ett format eller med metadata som säkerställer fortsatt bevisvärde, riskerar kommunen att förlora möjligheten att senare verifiera dokumentet – särskilt vid tvist eller utredning.
- Om kommunen generellt vägrar ta emot elektroniskt undertecknade handlingar riskerar det att bli praxis som inte är förenlig med rättsliga krav på icke-diskriminering eller tillgänglighet.

9.3 När gäller eIDAS-ramverket?

Enligt eIDAS-förordningen (Regulation (EU) No 910/2014) får elektroniska underskrifter inte vägras sin rättsliga giltighet eller bevisbarhet endast därför att de föreligger i elektronisk form[16]. Vidare pekas det i EU-kommissionens vägledning ut att medlemsstaterna måste tekniskt möjliggöra mottagande och behandling av elektroniskt undertecknade handlingar[17]. Detta betyder att kommunen bör ha stöd för att ta emot och hantera sådana handlingar, eller åtminstone tydligt ange vilka krav som gäller för mottagandet.
Om handlingen uppfyller kraven för en e-underskrift eller stämpel enligt standarderna brukar den inte kunna vägras enbart för att den är elektronisk.

9.4 Problem vid vägran med hänvisning till form- eller formatkrav

Att vägra ett elektroniskt undertecknat dokument med motiveringen att “vi har inte system för att verifiera det” eller “vi kan inte arkivera det i formatet” kan vara en svag juridisk position.

Eftersom eIDAS kräver att elektroniska handlingar inte får ha sämre rättslig status enbart för att de är digitala, kan kommunen – vid överklagan eller domstolsprövning – behöva visa att mottagandet och hanteringen har rimliga tekniska villkor och att denna verksamhetsgräns är kommunicerad.

Det finns en paradox: en privatperson kan hävda att kommunens vägran har medfört skada – till exempel om han eller hon tvingades skicka in en

[16] EU, What is the legislation - eSignature
[17] EU, What is the legislation - eSignature

kostsam pappershandling, eller att ett beslut fördröjdes. Sådan skada kan i princip leda till ansvar eller redovisningskrav.

9.5 Rekommendation för kommunen

Rekommendation

Kommunen bör tillhandahålla en e-underskriftstjänst för invånare vid ärenden som riktas till kommunen.

Innan kommunen analyserar mottagning och validering av inkomna e-underskrifter bör det övervägas att själv tillhandahålla en säker e-underskriftstjänst för invånare, när detta rör kommunens egna ärenden eller processer. Syftet är att ge invånaren ett enkelt och rättssäkert sätt att signera handlingar på ett sätt som direkt uppfyller kommunens krav på format, spårbarhet, tillit och arkivering.

Denna möjlighet bör dock endast erbjudas när handlingen har ett direkt samband med ett kommunalt ärende, exempelvis en ansökan, ett yttrande eller ett avtal mellan invånare och kommunen.

För handlingar som inte avser kommunens verksamhet – till exempel avtal mellan två privatpersoner, föreningar eller företag – bör kommunen inte erbjuda sin e-underskriftstjänst. Sådana behov bör i stället mötas av marknadens kommersiella tjänster. Detta följer principen om att offentlig sektor ska tillhandahålla förvaltningsstöd, inte marknadstjänster, och att kommunen ska undvika att konkurrera med privata aktörer inom kommersiella e-signeringslösningar.

En tydlig avgränsning bör därför framgå i kommunens e-tjänstekatalog eller mottagningspolicy:

- när kommunen erbjuder invånaren en e-underskriftstjänst som del av ett ärendeflöde, och
- när invånaren själv ansvarar för att tillhandahålla en giltig e-underskrift med godkänd tjänst.

Att kommunen erbjuder en egen underskriftstjänst i relevanta flöden stärker rättssäkerheten, ökar servicen, minskar tekniska avvisningar och ökar likvärdigheten i invånarnas möjligheter att kommunicera digitalt med kommunen.

Vidare rekommenderas följande steg:

Steg 1: Kartlägg mottagnings- och arkivförmåga

- Identifiera vilka elektroniska undertecknade format kommunen kan ta emot – och verifiera vilka e-underskriftsnivåer (EES, AdES, QES) som kan kontrolleras av kommunens system eller via extern validering.
- Klarlägga hur handlingar ska arkiveras: format (t.ex. PDF/A), metadata, signaturkedja och eventuell valideringsintyg.
- Dokumentera villkor för mottagande: om krav finns på viss signeringsnivå eller format ska dessa vara tydliga och kommunen ska kommunicera dem till medborgare/ärenden.

Steg 2: Formulera mottagningspolicy

- Kommunen bör besluta: Vilka elektroniskt undertecknade handlingar accepteras utan vidare kontroll? Vilka kräver ytterligare verifiering?
- Policyn bör innehålla:
  - Vilken typ av underskriftnivå som krävs (t.ex. AdES eller kvalificerad)
  - Vilket filformat och arkivkrav som gäller
  - Hur validering sker och vad som händer om validering misslyckas
  - Tydlig information till privatpersoner/leverantörer om kraven innan inlämning

Steg 3: Kommunicera krav och rättigheter

- Informera medborgare och leverantörer tydligt om vilka elektroniska signeringsformer och format kommunen accepterar – och varför.
- Gör det möjligt för privatpersoner att få vägledning innan inlämning, t.ex. via webbplats eller e-tjänst.
- Om kommunen vägrar mottagande av en elektroniskt undertecknad handling, ska vägran vara sakligt motiverad och hänvisa till policyns krav – inte en generell “vi accepterar inte elektroniska underskrifter”.

9.5.1 Konsekvensbedömning

När kommunen gör bedömningen, enligt mottagningspolicyn, att en elektroniskt undertecknad handling inte kan tas emot, bör en konsekvensanalys göras. Följande frågeställningar bör besvaras:

- Om kommunen mottar handlingen trots begränsad spårbarhet – vilka risker tar kommunen (t.ex. ökad bevisbörda senare, arkivproblem)?

- Om kommunen vägrar – vilka konsekvenser får det för invånaren? Kan vägran medföra merkostnad, försening eller rättslig skada?

Utifrån denna bedömning gör kommunen ett motiverat beslut:

- Om riskerna för kommunen är *låg* och konsekvenserna för invånaren *stora*, bör mottagande övervägas – och eventuellt kompletteringskrav ställas (t.ex. ytterligare verifiering).
- Om riskerna är *höga* för kommunen och konsekvenserna för invånaren *små*, kan kommunen motiverat vägra inlämningen – men då bör tydlig information och riktlinjer finnas.

10 Upphandlingskrav på e-underskrifter

Nedan listas krav som kan ställas vi upphandling av e-underskriftstjänster. Här beskrivna som SKA-krav, men det behöver värderas separat vid varje upphandling.

De krav som beskrivs i detta kapitel avser främst själva e-underskriften – det vill säga hur signaturen ska skapas, verifieras, lagras och bevaras på ett rättssäkert och tekniskt hållbart sätt.

I praktisk tillämpning behöver kommunen även beakta krav kopplade till processflöden och informationssäkerhet. Exempelvis kan det handla om att:

- känsliga handlingar, som beslut enligt LVU eller socialtjänstlagen, endast får vara åtkomliga för avsedda mottagare,
- åtkomst och distribution av dokument måste kunna styras systemövergripande,
- och att systemet ska kunna hantera säkra kommunikationskanaler vid utskick och signering.

Dessa processrelaterade krav är viktiga att hantera i kommunens egen informationssäkerhets- och verksamhetsarkitektur, men de omfattas inte av denna vägledning, som fokuserar på de tekniska och juridiska krav som gäller e-underskriften i sig.

Krav 1. Efterlevnad av eIDAS

Beskrivning:
Tjänsten **SKA** följa EU-förordning 910/2014 (eIDAS) och uppfylla kraven för avancerade elektroniska underskrifter (AdES).

Tekniska krav:

- Signaturer ska kunna verifieras enligt eIDAS artikel 26.
- Leverantören ska redovisa vilka nivåer och standarder som stöds (EES, AdES, QES).

Acceptanskriterium:
Leverantören visar dokumentation som beskriver hur tjänsten uppfyller eIDAS-kraven och anger tillämplig signeringsnivå.

Krav 2. Tillitsnivå och identitetssäkring

Beskrivning:
Användare som genomför en e-underskrift **SKA** identifieras med en e-legitimation som uppfyller minst tillitsnivå 3 enligt Digg:s tillitsramverk för Svensk e-legitimation. Det innebär att identiteten styrks med stark autentisering, baserad på en av Digg godkänd[18] eller EU-notifierad e-legitimation.
Tekniska krav:

- Tjänsten ska stödja e-legitimationer på minst tillitsnivå 3, enligt Digg:s ramverk.
- Stöd ska finnas för svenska e-legitimationer godkända av Digg.
- Tjänsten ska även stödja signering med alla e-legitimationer som är anslutna till Auktorisationssystemet för e-legitimering och till Digg:s förbetalda avtal, förutsatt att dessa är anslutna till Sweden Connect.

Acceptanskriterium:
Kommunen kan genomföra en testsignering med e-legitimation på tillitsnivå 3 eller högre.

Krav 3. Format och standarder (PAdES)

Beskrivning:
E-underskrifter **SKA** baseras på erkända EU-standarder som säkerställer interoperabilitet.

Tekniska krav:

- Signaturer ska följa ETSI EN 319 142 (PAdES) och EU:s Baseline Profile.
- Dokumentet ska kunna valideras i standardverktyg utan proprietär programvara.

Acceptanskriterium:

[18] Digg, Godkända e-legitimationer och intygsfunktioner

Testsignerat PDF-dokument kan valideras korrekt.

Krav 4. Format, arkivering och bevarande

Beskrivning:
Underskrivna dokument **SKA** kunna bevaras långsiktigt med bibehållet bevisvärde och i format som uppfyller Riksarkivets krav.

Tekniska krav:
- Tjänsten ska kunna producera och hantera PDF/A-1 eller senare version enligt Riksarkivets föreskrifter (RA-FS 2009:1 eller senare).
- Signaturen får inte brytas vid export eller bevarande, och all signaturinformation (tidsstämplar, certifikat, OCSP/CRL) ska följa PAdES-LTA-profilen för långtidsvalidering.
- Export till kommunens e-arkiv ska inkludera hela signaturkedjan samt metadata (t.ex. diarienummer, dokument-ID, signerande användare och tidpunkt).
- Leverantören ska kunna redovisa hur långtidsbevarande säkerställs, inklusive hur algoritmer och certifikat förnyas när de upphör att gälla.

Acceptanskriterium:
Ett signerat dokument kan exporteras i PDF/A-format till kommunens e-arkiv, där det kan öppnas och valideras utan fel, med fullständig signaturkedja och bevarad juridisk giltighet.

Krav 5. Långtidsvalidering (LTV)

Beskrivning:
E-underskrifter **SKA** innehålla nödvändig valideringsdata för att säkerställa bevisvärde under hela dokumentets livscykel.

Tekniska krav:
- Långtidsvalidering ska uppfylla kraven enligt ETSI:s baseline-profiler:
  - Minimikrav: LT-nivå (ETS 319 142-1, PAdES-LT) för handlingar som ska bevaras.
  - Rekommenderad nivå: LTA för långtidsbevarande och arkivändamål.
- Signaturer ska innehålla tidsstämpel, certifikatkedja och spärrinformation (OCSP/CRL).
- Resignering ska kunna ske automatiskt för att förlänga giltigheten enligt LTA-profilen.

Acceptanskriterium:
Kommunen kan validera ett signerat dokument enligt PAdES-LT eller -LTA utan beroende av leverantörens system.

Krav 6. Validering och beviskedja

Beskrivning:
Kommunen **SKA** kunna verifiera e-underskrifter oberoende av leverantörens infrastruktur. För QES ska validering ske automatiskt via EUTL. För AdES **SKA** integritet, tidsstämpling och certifikatstatus kunna verifieras genom dokumentets beviskedja även utan EUTL.

Tekniska krav:
- Systemet ska tillhandahålla hela signaturkedjan: signaturcertifikat, CA-kedja, tidsstämplar samt OCSP/CRL-data.
- Signaturer ska följa ETSI:s Baseline-profiler (minst PAdES-LT, gärna PAdES-LTA).
- Validering ska kunna utföras i oberoende standardverktyg som följer eIDAS-profil (t.ex. EU DSS, OpenSignature eller Adobe Reader).
- För kvalificerade underskrifter ska certifikaten kunna verifieras mot EU Trusted List (EUTL).
- För avancerade underskrifter (AdES) ska tjänsten säkerställa att signaturens integritet, tidsstämpling och certifikatstatus kan verifieras, även om utfärdaren inte finns upptagen i EUTL

Acceptanskriterium:
Kommunen kan verifiera ett signerat dokument i ett oberoende verktyg (utan leverantörens plattform).

- *QES:* Giltig signatur i EUTL-baserat verktyg (t.ex. EU DSS) enligt PAdES-LT/LTA.
- *AdES:* Verktyget visar intakt signatur, giltig tidsstämpling och verifierad certifikatstatus (OCSP/CRL), även om utfärdaren inte finns i EUTL.

Krav 7. Spårbarhet och loggning

Beskrivning:
Alla signeringshändelser **SKA** vara spårbara för att möjliggöra revision och incidentutredning.

Tekniska krav:
- Loggar ska visa tid, identitet, dokumentversion och tekniskt resultat.

- Loggar ska kunna exporteras i öppet format.

Acceptanskriterium:
Kommunen kan granska och exportera loggar för en vald tidsperiod.

Krav 8. Integritet och dataskydd (GDPR)

Beskrivning:
Personuppgifter som behandlas vid signering **SKA** skyddas i enlighet med GDPR.

Tekniska krav:
- Leverantören ska redovisa hur personuppgifter (namn, ID, IP-adress m.m.) hanteras och lagras.
- Dataminimering och säkerhetskontroller ska vara implementerade.

Acceptanskriterium:
Leverantören lämnar en dataskyddsbeskrivning (DPIA eller likvärdig) som kommunen godkänner.

Krav 9. Interoperabilitet och öppna gränssnitt

Beskrivning:
Tjänsten **SKA** kunna integreras med kommunens övriga system.

Tekniska krav:
- Öppna API:er (REST, SAML, OpenID Connect eller likvärdigt) ska erbjudas.
- Dokumentation och testmiljö ska tillhandahållas.

Acceptanskriterium:
Kommunen kan anropa API och genomföra en provintegration mot ett verksamhetssystem

Krav 10. Tillgänglighet och användbarhet

Beskrivning:
Tjänsten **SKA** vara användbar för alla och följa gällande tillgänglighetsstandarder.

Tekniska krav:

- Gränssnitt ska uppfylla WCAG 2.1 nivå AA.
- Stöd för svenska och engelska, samt användning på dator, surfplatta och mobil.

Acceptanskriterium:
Leverantören redovisar tillgänglighetsutlåtande och kommunen verifierar i användartest.

Krav 11. Inbäddning av valideringsintyg i dokumentet (validation evidence)

Beskrivning:
Tjänsten **BÖR** kunna lagra valideringsintyg (validation evidence) direkt i det signerade dokumentet för att bevara kopplingen mellan intyg och originalhandling. Syftet är att säkerställa långsiktigt bevisvärde och förenkla arkivering.

Tekniska krav:

- Valideringsintyg ska kunna bäddas in i PDF-filen enligt ETSI EN 319 102-2 och ETSI EN 319 142-1 (PAdES).
- Den inbäddade filen ska innehålla uppgifter om:
  – datum och tid för validering,
  – resultat av valideringen,
  – uppgifter om certifikat och tidsstämplar som verifierats,
  – samt referens till den ursprungliga signaturen.
- Tjänsten ska kunna hantera både LTV-data och valideringsintyg parallellt.

Acceptanskriterium:
Kommunen kan öppna ett signerat dokument och visa att valideringsintyget finns inbakat i PDF-filen och att dokumentet kan valideras som en helhet utan separata filer.

Krav 12. Stöd för e-stämpel

Beskrivning:
Tjänsten **BÖR** stödja användning av e-stämplar (elektroniska stämplar) som gör det möjligt för kommunen att signera eller autentisera dokument på organisationsnivå – till exempel beslut som genereras automatiskt eller skickas utan personlig underskrift.

Tekniska krav:

- Tjänsten bör kunna skapa och hantera e-stämplar baserade på organisationscertifikat enligt eIDAS för avancerad nivå (AdES-seal).

- E-stämplar ska kunna användas för att säkerställa dokumentets ursprung och integritet.
- Det ska gå att särskilja e-stämplar från personliga e-underskrifter i metadata och loggar.
- Tjänsten bör möjliggöra att stämpeln appliceras automatiskt i systemgenererade flöden.

Acceptanskriterium:
Kommunen kan genomföra ett test där ett dokument stämplas med en organisationsstämpel, och validering visar att stämpeln är giltig och knuten till kommunen som juridisk person.

Krav13. Hantering av sekretessbelagda handlingar

Beskrivning:
Tjänsten **BÖR** stödja signering och validering av sekretessbelagda handlingar utan att själva dokumentet behöver lämna kommunens IT-miljö. Syftet är att skydda känslig information och säkerställa att sekretesskrav enligt offentlighets- och sekretesslagen (2009:400) kan upprätthållas även vid elektronisk underskrift.

Tekniska krav:
- Tjänsten bör kunna genomföra signering eller validering genom att endast överföra hashvärden (kontrollsummor) till leverantörens underskriftstjänst.
- Hashning ska ske med SHA-256 eller starkare och dokumenteras i logg tillsammans med tidsstämplar och versions-ID.
- Om hela dokumentet behöver överföras ska leverantören kunna visa att dess miljö är godkänd för hantering av sekretessbelagd information enligt tillämpliga säkerhetsnivåer.
- Tjänsten bör möjliggöra att kommunens egna komponenter för hashning och signeringsförberedelser kan driftas lokalt.

Acceptanskriterium:
Kommunen kan verifiera att en sekretessbelagd handling kan signeras utan att dokumentet lämnar kommunens IT-miljö, alternativt att leverantören kan uppvisa giltig säkerhetsgranskning och godkänd hantering för aktuell informationsklass.

11 Digitala godkännanden – syfte och utformning

11.1 Begreppsförtydligande

I praktiken används flera olika begrepp för att beskriva handlingar som inte signeras med ett personligt underskriftscertifikat men där avsikten ändå är att godkänna eller fastställa ett beslut. För att minska begreppsförvirringen används i denna vägledning följande avgränsningar:

Digitalt godkännande

Ett elektroniskt samtycke eller beslut, ofta utfört genom ett klick i ett system, markerat val eller motsvarande handling.

- Bygger normalt på autentisering med e-legitimation (privat e-legitimation eller e-tjänstelegitimation).
- Ingen kryptografisk signatur skapas, men systemets loggar ger spårbarhet, identitet och tidpunkt.
- Används där ingen formell underskrift krävs enligt lag, men ett juridiskt bindande godkännande behövs.
- Motsvarar det som ibland kallas *”enkel elektronisk underskrift”* i eIDAS-förordningen.

E-stämpel

En organisationens digitala underskrift – inte kopplad till en fysisk person utan till en juridisk person (t.ex. en kommun, nämnd eller myndighet).

- Kan vara icke kvalificerad stämpel[19] eller kvalificerad (QES) beroende på vilket certifikat som används.
- Används för att ”signera” automatiskt genererade handlingar, beslut eller intyg utan personlig handläggning.
- Beskrivs i eIDAS-förordningen som *”electronic seal”*.
- Digg rekommenderar begreppet e-stämpel framför termer som ”systemsignatur” eller ”automatisk underskrift”.[20]

Enkel elektronisk underskrift

En bred term enligt eIDAS som omfattar alla elektroniska metoder för att visa samtycke — från ett e-postmeddelande till ett klick i ett formulär.

[19] Standarderna talar om “advanced electronic seal”, men i svensk praxis används oftast begreppet “icke kvalificerad stämpel”.
[20] Digg, Vägledning för e-underskrifter och e-stämplar i offentlig sektor

- Kan alltså omfatta både digitala godkännanden och enklare e-stämpelflöden.
- Saknar krav på kryptografiskt skydd men kan ändå ha rättslig giltighet beroende på kontext och bevisvärde.

11.2 Varför digitala godkännanden

Digitala godkännanden ger rättssäkerhet, spårbarhet och effektivitet i processer där lagen inte kräver en formell e-underskrift. De är ett naturligt komplement till e-underskrifter och bidrar till att minska komplexitet, kostnader och beroende av särskilda signeringstjänster.

11.2.1 Rättssäkerhet uppnås även med godkännande

Digitalt godkännande är fullt tillräckligt när det inte finns lagkrav på underskrift.

- **Identitetssäkring:** Med e-legitimation eller säker kommunal inloggning (IAM/IGA) kan kommunen uppnå samma styrka i identitet som vid en avancerad underskrift.
- **Spårbarhet:** Systemloggar visar vem som godkände, när och vilken version som gällde. Det ger juridiskt bevisvärde.
- **Avsikt:** En tydlig knapp eller kryssruta med text som *”Jag godkänner”* eller *”Jag beslutar”* visar intentionen på ett rättssäkert sätt.

11.2.2 Minskad komplexitet och kostnad

- **Enklare implementation:** Godkännandeflöden kan byggas direkt i verksamhetssystem eller e-tjänst utan extern signeringstjänst.
- **Lägre kostnader:** Inga licenser per signatur – godkännandefunktioner utnyttjar befintliga system.

11.2.3 Bättre användarupplevelse

- Färre steg och snabbare processer.[21]
- Fungerar i webb och mobil utan särskilda filformat.
- Mindre risk för tekniska fel eller avbrutna flöden.

11.2.4 Framtidssäkring och bevarande

- **Stabil beviskedja:** Systemloggar är enklare att bevara än certifikatkedjor.

[21] För invånare kan upplevelsen ibland vara den motsatta. När digitala godkännanden ersätter e-underskrifter kan processen upplevas som mindre tydlig, särskilt om flödet sker i flera steg, via olika system eller utan en visuellt igenkännbar ”signering”. En genomtänkt design och tydlig bekräftelse till användaren är därför avgörande för att skapa förtroende även i enklare godkännandeflöden.

- **Enklare arkivering:** Handlingar kan lagras i öppna format utan behov av signaturvalidering 20 – 30 år framåt.

11.3 Krav på hur digitala godkännanden utformas

Ett digitalt godkännande bör vila på fyra grundpelare: identitet, koppling, spårbarhet och integritet.

Kravområde	Krav på utformning
Identitet	Den som godkänner ska identifieras på ett tillräckligt säkert sätt – exempelvis med e-legitimation, e-tjänstelegitimation eller autentisering via kommunens identitetshantering (IAM/SSO).
Koppling mellan person och handling	Systemet ska tydligt binda godkännandet till rätt dokument, ärende eller beslut. Det ska framgå *vad* som godkänts, *av vem* och *när*.
Spårbarhet	Godkännandet ska loggas automatiskt. Loggen ska visa användarens identitet, tidpunkt, händelsetyp och versionsinformation.
Integritet och oåterkallelighet	Ett godkännande får inte kunna ändras eller tas bort utan att det upptäcks. Systemet ska skydda mot manipulation och obehörig åtkomst.

12 Upphandlingskrav för digitala godkännanden

Nedan listat krav som kan ställas på digitala godkännanden vid upphandling av system. I detta dokument är alla markerade som SKA-krav, men det behöver värderas vid varje upphandling.

Krav 1: Identitetssäkring

Beskrivning:
Den som genomför ett digitalt godkännande ska kunna identifieras på ett tillräckligt säkert sätt för att bevisa vem som gjort godkännandet.

Tekniska krav:
- Systemet ska stödja autentisering via e-legitimation, e-tjänstelegitimation eller kommunens IAM-lösning (SSO).
- Identiteten ska loggas tillsammans med godkännandet.

- Systemet ska hantera både interna användare (anställda) och externa (invånare/leverantörer).

Acceptanskriterium:
Kommunen kan visa en testlogg där användarens identitet, tidpunkt och ärende-ID framgår efter ett godkännande.

Krav 2: Koppling mellan person och handling

Beskrivning:
Godkännandet ska vara entydigt kopplat till den handling, det ärende eller beslut som avses.

Tekniska krav:
- Systemet ska knyta godkännandet till rätt dokumentversion via unikt dokument-ID eller hashvärde.
- Det ska framgå vad som godkänts, av vem, när och i vilket sammanhang.
- Godkännandet ska sparas i direkt anslutning till ärendet eller dokumentet.

Acceptanskriterium:
Kommunen kan spåra från dokument till godkännande och vice versa, och visa att rätt version godkänts.

Krav 3: Spårbarhet

Beskrivning:
Alla godkännanden ska loggas så att de kan granskas och verifieras i efterhand.

Tekniska krav:
- Varje godkännande ska loggas med identitet, tidpunkt, händelsetyp och dokumentversion.
- Loggen ska vara sökbar och kunna exporteras i öppet format (JSON eller XML).
- Loggar ska bevaras lika länge som den handling de avser.

Acceptanskriterium:
Kommunen kan exportera en loggpost i öppet format som innehåller alla ovanstående fält.

Krav 4: Integritet och oåterkallelighet

Beskrivning:
Ett digitalt godkännande får inte kunna ändras eller tas bort utan att detta upptäcks.

Tekniska krav:
- Systemet ska skydda loggar mot manipulation (t.ex. genom hashkedja, WORM-lagring eller TSA-stämpling).
- Varje förändring eller försök till radering ska loggas som en separat händelse.
- Godkännanden ska kunna verifieras även om det bakomliggande systemet byts ut.

Acceptanskriterium:
Kommunen kan genomföra ett integritetstest där ändringar i loggar upptäcks vid verifiering.

Krav 5: Export i öppet format

Beskrivning:
Godkännanden och loggar ska kunna exporteras till e-arkiv eller andra system i öppna, standardiserade format.

Tekniska krav:
- Export ska stödja minst JSON eller XML.
- Exporten ska inkludera metadata: godkännande-ID, användar-ID, ärende-ID, dokumenthash, tidsstämpel, roll och autentiseringsmetod.
- Paketstrukturen ska kunna valideras i kommunens e-arkiv utan proprietär programvara.

Acceptanskriterium:
Kommunen kan exportera en provmängd (minst 10 poster) i JSON och importera den i e-arkiv med bibehållen information.

Krav 6: Bevarande och retention

Beskrivning:
Godkännanden ska bevaras så länge som de handlingar de tillhör och kunna kopplas till dessa över tid.

Tekniska krav:
- Loggar ska lagras minst lika länge som tillhörande handlingar enligt dokumenthanteringsplan.

- Systemet ska kunna skapa en arkivexport som innehåller både handling och tillhörande godkännande-metadata.
- Godkännanden ska kunna återsökas på ärende-ID eller dokument-hash.

Acceptanskriterium:
Leverantören visar ett exempel på arkivexport där godkännande och dokument är kopplade och kan verifieras.

Krav 7: Revisionssäker logg

Beskrivning:
Systemets loggfunktion ska vara revisionssäker och möjliggöra extern verifiering.

Tekniska krav:
- Loggar ska vara append-only och skyddade mot ändring.
- Dagliga loggkedjor eller TSA[22]-stämplar ska användas för att säkra integriteten.
- Systemet ska stödja oberoende verifiering av loggintegritet.

Acceptanskriterium:
Kommunen kan verifiera loggars integritet med extern verifiering (hash- eller TSA-kontroll) utan leverantörens system.

Krav 8: Dataskydd och åtkomstkontroll

Beskrivning:
Personuppgifter i samband med godkännanden ska hanteras enligt GDPR och åtkomst till loggar ska vara behörighetsstyrd.

Tekniska krav:
- Endast nödvändiga personuppgifter får lagras (dataminimering).
- Loggar över åtkomst till godkännandedata ska sparas.
- Systemet ska stödja maskning av IP-adress och sessionsinformation.

Acceptanskriterium:

[22] TSA (Time Stamping Authority) är en betrodd tjänst som skapar en elektronisk tidsstämpel. Den visar att en viss information existerade vid en specifik tidpunkt och inte har ändrats sedan dess. En TSA-stämpel används för att stärka bevisvärdet i loggar och digitala handlingar över tid

Leverantören visar dataskyddsbeskrivning (DPIA) och kommunen kan verifiera att loggdata kan maskas eller begränsas.

Krav 9: Användarupplevelse och bekräftelse

Beskrivning:
Användaren ska tydligt förstå vad som godkänns och få bekräftelse när godkännandet är genomfört.

Tekniska krav:
- Gränssnittet ska innehålla tydlig text som ”Jag godkänner” eller motsvarande.
- Systemet ska visa visuell bekräftelse efter genomfört godkännande.
- För riskfyllda moment bör dubbel bekräftelse användas (t.ex. tvåstegs-godkännande).

Acceptanskriterium:
Kommunen genomför ett test där godkännandeflödet tydligt visar avsikt och bekräftelse.

Krav 10: Integration och systemoberoende

Beskrivning:
Funktionen för digitala godkännanden ska kunna användas i flera system utan att vara beroende av en specifik leverantör.

Tekniska krav:
- Tjänsten ska exponera API:er för godkännande, loggning och export.
- Autentisering ska kunna hanteras via kommunens centrala IAM.
- Systemet ska kunna särskilja e-underskrift och digitalt godkännande.

Acceptanskriterium:
Kommunen kan integrera ett verksamhetssystem med godkännandefunktionen via API och utföra testgodkännande.

Krav 11: Bevisvärde och verifierbarhet

Beskrivning:
Det ska vara möjligt att långt senare visa att ett godkännande verkligen skett och att det inte har ändrats.

Tekniska krav:

- Varje godkännande ska kunna verifieras med lagrad hash, tidsstämpel och identitet.
- Beviskedjan ska kunna exporteras oberoende av leverantör.
- Tjänsten ska stödja kontroll av integritet via standardverktyg.

Acceptanskriterium:
Kommunen kan verifiera ett äldre godkännande och styrka dess giltighet med logg- och hashdata.

Krav 12: Tillgänglighet och användbarhet

Beskrivning:
Digitala godkännanden ska vara tillgängliga för alla användare oavsett enhet.

Tekniska krav:
- Systemet ska följa WCAG 2.1 nivå AA.
- Gränssnittet ska vara responsivt och fungera på dator, surfplatta och mobil.

Acceptanskriterium:
Kommunen testar gränssnittet och bekräftar att godkännandeflödet fungerar på alla enheter.

Bilaga 1, Olika vägledningar

Nedan listas vägledningar från olika aktörer som på olika sätt vägleder inom området e-underskrifter.

- PTS, Elektroniska underskrifter
- Digital hantering av betyg kräver ändring i skollagen
- Kammarkollegiets vägledning för avrop e-ID-tjänster
- eSam:s vägledning e-legitimation och e-underskrift
- Sambruks PM om praktiska erfarenheter
- Boråsregionens vägledning elektroniska underskrifter
- SKR:s rekommendationer för identitets- och behörighetshantering