

Riktlinjer för elektronisk signering och validering

Publicerad: 2026-10-19

Beslutsfattare: Anders Fällström, rektor.

Ansvarig funktion: Avdelningen för digitalisering och service, diarium och arkiv (DIA)

Handläggare: Cecilia Johnsson

Beslutsdatum: 2026-10-19

Giltighetstid: Tillsvidare

Senaste översyn: 2026-10-19

Sammanfattning: Detta dokument beskriver Mittuniversitetets krav, rekommendationer och tillämpning för elektroniska underskrifter, validering samt bevarande och arkivering av elektroniskt signerade handlingar.

Tidigare versioner: Första version

Innehållsförteckning

Riktlinjer för elektronisk signering och validering	3
Rättslig grund och begrepp	3
Riksarkivets krav	3
DIGG:s och PTS:s vägledningar	4
SUHF:s vägledning	5
Mittuniversitetets tillämpning av elektronisk signering	6
När signering ska användas (behov och kriterier)	6
Handlingar som enligt lag eller förordning kräver underskrift	7
Mittuniversitetets e-signeringstjänster	7
Godkända tjänster och användningsområden	8
Ej godkända signeringstjänster	9
Tekniska krav och format	10
Validering	11
Bevarande och arkivering	12
Ansvar och uppföljning	12

Riktlinjer för elektronisk signering och validering

Detta dokument beskriver hur Mittuniversitetet tillämpar gällande krav och rekommendationer för elektroniska underskrifter, e-signering, validering och bevarande av elektroniskt underskrivna handlingar.

Syftet är att säkerställa att universitetets hantering av elektroniska underskrifter är rättssäker, enhetlig och i överensstämmelse med Riksarkivets föreskrifter (RA-FS 2009:2), Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster (eIDAS-förordningen) samt de vägledningar som ges av Myndigheten för digital förvaltning (DIGG), Post- och telestyrelsen (PTS) och Sveriges universitets- och högskoleförbund (SUHF).

Rättslig grund och begrepp

Elektroniska underskrifter regleras på EU-nivå genom Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster (eIDAS-förordningen). Förordningen anger rättsverkan och nivåer för elektroniska underskrifter inom EU.

För svenska myndigheter gäller dessutom arkivlagen, förvaltningslagen och Riksarkivets föreskrifter (RA-FS 2009:2). Dessa kompletteras av nationella vägledningar från Myndigheten för digital förvaltning (DIGG) och Post- och telestyrelsen (PTS) samt rekommendationer från Sveriges universitets- och högskoleförbund (SUHF).

Det är viktigt att skilja mellan bindande krav, som följer av lag eller föreskrift, och rekommendationer, som beskriver hur myndigheter praktiskt kan uppfylla dessa krav.

Riksarkivets krav

Riksarkivets föreskrift RA-FS 2009:2 gäller för alla statliga myndigheter, inklusive universitet och högskolor, och är obligatorisk att följa.

Enligt 3 kap. 5 § ska elektroniskt underskrivna handlingar som tillkommer inom ramen för e-tjänster följa IETF RFC 2315 PKCS #7 (Cryptographic Message Syntax Version 1.5) eller XML-signatures för strukturerade dokument i XML. I praktiken innebär detta att underskrift ska ske med vedertagna tekniska standarder, såsom PAdES, CAdES eller XAdES, beroende på dokumenttyp.

Handlingar ska framställas i öppna och dokumenterade format. Myndigheten ska kunna säkerställa autenticitet (vem som har undertecknat), integritet (att innehållet inte har ändrats) och verifierbarhet (att underskriften kan kontrolleras även över tid).

Verifiering får inte förutsätta fortsatt tillgång till den ursprungliga signeringstjänsten. Om långsiktig teknisk verifiering inte kan garanteras ska resultatet av en genomförd verifiering, exempelvis ett valideringsintyg eller en valideringsrapport, bevaras tillsammans med handlingen.

Riksarkivets förtydliganden och rekommendationer

I rapporten *Framställning och bevarande av elektroniska signaturer* (Arkiv E, Delprojekt 3) beskriver Riksarkivet hur myndigheter praktiskt kan uppfylla föreskriftens krav. Rapporten betonar vikten av att bevara tillräcklig information för långsiktig verifierbarhet. Detta kan ske genom att bevara signaturinformation i sin helhet eller genom att skapa ett valideringsintyg i samband med mottagandet av en handling.

Riksarkivet rekommenderar användning av etablerade standarder för långtidsverifiering, såsom PAdES-LTV, CAdES-A eller XAdES-A, samt att bevarande sker i öppna format, exempelvis PDF eller XML.

DIGG:s och PTS:s vägledningar

DIGG och PTS ger vägledning om tillämpningen av eIDAS-förordningen. De beskriver tre nivåer av elektroniska underskrifter:

1. Enkel elektronisk underskrift (SES)¹ – exempelvis en klicksignatur eller namn i e-post. Den är juridiskt giltig men har lågt bevisvärde.
2. Avancerad elektronisk underskrift (AES)² – unikt knuten till undertecknaren, skapad under dennes kontroll och skyddad mot ändringar. Den uppfyller normalt myndigheters behov.
3. Kvalificerad elektronisk underskrift (QES)³ – en avancerad signatur som bygger på ett kvalificerat certifikat från en kvalificerad betrodd tjänsteleverantör (QTSP). Den har enligt eIDAS samma rättsverkan som en handskriven signatur.

Avancerad nivå är i normalfallet tillräcklig för myndighetsprocesser.

Kvalificerad nivå bör användas endast när det krävs enligt lag eller särskilt avtal.

DIGG och PTS rekommenderar att elektroniska underskrifter valideras i samband med mottagande eller skapande av en handling och att resultatet bevaras. Det avgörande är att myndigheten i efterhand kan visa att underskriften var giltig vid kontrolltillfället.

SUHF:s vägledning

Vägledningen från SUHF:s expertgrupp för arkiv- och informationshantering (dnr 0032–16) från 2020, ger rekommendationer för hur lärosäten bör hantera val av signeringsmetod, validering och arkivering. Vägledningen betonar att behov och syfte ska analyseras innan metod väljs, att e-signeringstjänster bör följa nationella ramverk, samt att alternativa lösningar såsom attestering och systemloggning kan vara tillräckliga för interna beslut.

SUHF framhåller att bevarande och verifierbarhet ska beaktas redan vid planering av digitala processer och att tydliga rutiner för ansvar och dokumentation bör fastställas.

¹ Artikel 3, punkt 10.

² Artikel 3, punkt 11 samt artikel 26.

³ Artikel 3, punkt 12 samt kapitel III.

Mittuniversitetets tillämpning av elektronisk signering

Mittuniversitetet tillämpar elektronisk signering i enlighet med eIDAS-förordningen (EU nr 910/2014), Riksarkivets föreskrifter (RA-FS 2009:2) samt nationella rekommendationer från Myndigheten för digital förvaltning (DIGG), Post- och telestyrelsen (PTS) och Sveriges universitets- och högskoleförbund (SUHF).

I detta och följande avsnitt anges när signering ska användas, vilka tjänster som är godkända samt krav på validering, format och bevarande.

När signering ska användas (behov och kriterier)

Mittuniversitetet ska använda elektronisk signering endast när det finns juridiska krav, avtalskrav eller ett tydligt verksamhetsmässigt behov av formell signering. Bedömningen ska alltid göras proportionerligt. Signering ska inte användas slentrianmässigt eller av tradition, utan endast när den tillför rättsligt eller bevismässigt värde.

Kriterier

Signering ska användas när minst ett av följande kriterier är uppfyllt:

- det finns ett uttryckligt krav på underskrift i lag eller förordning,
- annan myndighet eller extern organisation ställer krav på underskrift,
- handlingen ingår i en avtalsprocess med extern part, eller
- det finns ett tydligt verksamhetsmässigt behov av formell signering (t.ex. för att säkerställa spårbarhet, ansvar eller bevisvärde).

När underskrift inte krävs

Om inget av ovanstående kriterier är uppfyllt ska handlingar som huvudregel inte signeras. Beslut, godkännanden och ställningstaganden kan i sådana fall i stället dokumenteras genom digitala arbetsflöden och systemstöd som säkerställer spårbarhet, identifiering av beslutsfattare och dokumentation av beslutstidpunkt.

Det finns dock inget hinder mot att verksamheten i särskilda fall väljer att använda underskrift även när formellt krav saknas. I sådana fall gäller dock inte krav på särskild kontroll av underskriftens fullständighet vid registrering eller arkivering.

Handlingar som enligt lag eller förordning kräver underskrift

Vid tidpunkten för detta dokumentets fastställande har Mittuniversitetet identifierat följande handlingar som enligt lag eller förordning **måste** undertecknas:

- **Årsredovisning** enligt 2 kap. 8 § förordning (2000:605) om årsredovisning och budgetunderlag.
(Krav på egenhändig underskrift på papper.)
- **Miljöredovisning** som lämnas in i samband med årsredovisning enligt 20 § förordning (2009:907) om miljöledning i statliga myndigheter.
(Krav på egenhändig underskrift på papper.)
- **Inventeringsprotokoll** enligt Ekonomistyrningsverkets föreskrifter till 22 § förordning (2000:606).
- **Dokumentation rörande strålkällor** enligt Strålsäkerhetsmyndighetens föreskrifter (2018:1), 6 kap. 19 § andra stycket.
- **Ansökan om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning** enligt 7 § förordning (2024:664).

Denna lista avser handlingar med uttryckligt lagkrav på underskrift som är identifierade vid Mittuniversitetet vid tidpunkten för fastställandet. Listan kan behöva uppdateras vid förändringar i lagstiftning eller verksamhet.

Mittuniversitetets e-signeringstjänster

Mittuniversitetet tillhandahåller ett begränsat antal tjänster för elektronisk signering. Endast de tjänster som anges som **godkända** nedan får användas för att signera handlingar inom universitetets verksamhet. Tjänster som

anges som **ej godkända** får användas för att läsa och kontrollera signaturer, men inte för att skapa elektroniska underskrifter.

Godkända tjänster och användningsområden

Elektroniska underskrifter som används vid Mittuniversitetet ska minst uppfylla kraven för avancerad elektronisk underskrift (AES) enligt eIDAS-förordningen och följa Riksarkivets föreskrifter (RA-FS 2009:2).

Vid införande eller granskning av signeringstjänster ska bilagan *Checklista för bedömning av e-signeringstjänster* tillämpas. Bedömningen ska säkerställa att tjänsten uppfyller krav på identitetskontroll, tekniskt format, verifierbarhet och bevarande.

Följande tjänster är, vid tillfället för detta dokumentets upprättande, godkända enligt genomförda bedömningar⁴:

EduSign

Godkänd för i första hand interna beslut och processer. Tjänsten tillhandahålls av Sunet (Swedish University Computer Network) och bygger på SWAMID-identitet, vilket innebär att alla medarbetare kan använda EduSign. EduSign uppfyller kraven för avancerad elektronisk underskrift (AES) och är godkänd för användning utan individuell validering när samtliga undertecknare är interna parter vid Mittuniversitetet, eftersom identiteten redan är säkerställd genom universitetets federerade inloggning. EduSign ska användas för digitala dokument som också lagras digitalt och ska inte användas för handlingar som hanteras och lagras i fysisk form. Se dnr MIUN 2026/1766.

Scrive

Godkänd för användning i externa och formbundna sammanhang. Tjänsten är en onlinetjänst från leverantören Scrive AB och kan användas när bevisvärdet behöver kunna styrkas externt, till exempel vid avtal och andra handlingar där extern part undertecknar. Scrive erbjuder både

⁴ Fler godkända tjänster kan förekomma, se diariet för eventuellt ytterligare bedömningar.

avancerad och kvalificerad nivå och ska användas när kvalificerad elektronisk underskrift (QES) krävs enligt lag eller avtal. Mittuniversitetet har ett begränsat antal licenser (för närvarande 10), vilket innebär att åtkomst kan vara begränsad till särskilt utsedda funktioner. Scrive ska användas för digitala dokument som också lagras digitalt och ska inte användas för handlingar som hanteras och lagras i fysisk form. Se dnr MIUN 2026/1767.

e-Avrop (e-Avtal)

Godkänd för upphandlings- och avtalsprocesser i e-Avrop där avancerad elektronisk underskrift är tillräcklig. e-Avrop är ett upphandlingssystem och avtalsdatabas från leverantören Antirio AB och inkluderar signeringsverktyget Egreement/E-avtal. Identifiering sker via BankID och andra nordiska e-legitimationer. Kvalificerad elektronisk underskrift kan tillhandahållas via extern kvalificerad betrodd tjänsteleverantör när det krävs enligt lag eller avtal; e-Avrop är inte själv en kvalificerad betrodd tjänsteleverantör (QTSP). Se dnr MIUN 2026/1768.

Ej godkända signeringstjänster

Adobe Acrobat Pro

Adobe Acrobat Pro är inte godkänd som signeringstjänst vid Mittuniversitetet. Programvaran stödjer certifikatbaserade signaturer i PDF-format och följer etablerade tekniska standarder, men uppfyller inte universitetets krav på identitetskontroll, valideringsbevis och långsiktig verifierbarhet enligt eIDAS-förordningen och Riksarkivets föreskrifter.

Mittuniversitetet har licenser för Adobe Acrobat Pro för samtliga medarbetare, men saknar licenser för molntjänsten Adobe Acrobat Sign (Acrobat Sign), som är Adobes tjänst för elektronisk signering med spårning och juridiskt bevis. Acrobat Pro får därför inte användas för elektronisk signering av handlingar inom universitetets verksamhet.

Programmet kan däremot användas för att läsa och kontrollera digitala signaturer i PDF-dokument. Sådan verifiering kan även göras i kostnadsfria Adobe Acrobat Reader. Se dnr MIUN 2026/1769.

Tekniska krav och format

Elektroniskt underskrivna handlingar ska framställas i öppna och dokumenterade format i enlighet med Riksarkivets föreskrifter (RA-FS 2009:2). Godtagbara signaturformat är PKCS#7 samt dess moderna tillämpningar CAdES, PAdES och XAdES.

En inskannad namnteckning eller en infogad bild av en signatur räknas inte som en elektronisk underskrift enligt eIDAS-förordningen. En sådan markering saknar tekniskt skydd mot ändringar och ger ingen möjlighet att verifiera vem som har undertecknat handlingen. Handlingar som endast innehåller en inskannad signatur ska därför betraktas som handlingar utan underskrift.

Handlingar som ska signeras elektroniskt ska sparas i formatet PDF/A-2b. PDF/A-1 bör inte användas för dokument som ska signeras, eftersom signeringen kan påverka formatets giltighet. Om framtida leverans till Riksarkivet kräver formatet PDF/A-1 får konvertering ske vid leveranstillfället.

En handling får inte ändras efter att den har signerats elektroniskt. Ändringar, till exempel redigering av innehåll eller konvertering till annat filformat, bryter signaturen och gör att den inte längre kan verifieras. Om en handling behöver konverteras till ett visst format, till exempel PDF/A, ska detta därför göras innan dokumentet signeras. En signerad handling får inte heller skrivas ut och därefter skannas in igen som ersättning för originalet, eftersom den elektroniska signaturen då går förlorad.

Signerade handlingar ska kunna verifieras utan beroende av leverantörens plattform. Den tekniska lösningen ska därför möjliggöra oberoende verifiering av signaturens giltighet och dokumentets integritet.

För EduSign och Scrive finns möjlighet att spara särskild bevisdata, såsom valideringsintyg, bevispaket eller inbäddade verifieringsuppgifter i den signerade PDF-handlingen, när det behövs för att styrka signaturens giltighet. För e-Avrop innehåller den signerade PDF-handlingen inbäddad

signaturinformation och verifieringsdata. När krav på standardiserad långtidsvalidering föreligger ska tilläggstjänst för PAdES-försegling användas.

Validering

Elektroniska signaturer ska kontrolleras i samband med att en handling tas emot eller upprättas i en signeringsprocess där externa parter deltar eller där extern signeringsstjänst används.

Valideringen ska säkerställa att signaturen var giltig vid kontrolltillfället och att handlingens integritet inte har förändrats.

Resultatet av valideringen ska bevaras tillsammans med handlingen. Detta kan ske genom att ett valideringsintyg eller en valideringsrapport sparas, eller genom att den signerade PDF-handlingen med inbäddad verifieringsinformation bevaras i oförändrat skick.

Om verifieringsinformation är inbäddad i PDF-filen, till exempel i form av signaturdata eller bilagor som ingår i signeringen, ska dessa bevaras tillsammans med dokumentet och får inte tas bort eller ändras.

För handlingar som signerats i EduSign av interna användare, och där samtliga undertecknare är interna parter vid Mittuniversitetet, krävs ingen individuell validering. Dessa signaturer betraktas som betrodda eftersom identiteten är säkerställd genom universitetets SWAMID-inloggning och tjänsten uppfyller de tekniska krav som anges i detta dokument.

Om en EduSign-handling tas emot från extern part, exempelvis en annan myndighet, ska underskriften kontrolleras vid mottagandet.

Mittuniversitetet tillämpar principen att signaturer valideras en gång och att resultatet därefter bevaras. Upprepad teknisk revalidering ska inte genomföras, under förutsättning att bevis om genomförd validering finns bevarat.

Bevarande och arkivering

Signerade handlingar och tillhörande bevisdata, såsom valideringsintyg, rapporter, bevispaket eller inbäddad verifieringsinformation, ska hanteras och bevaras i enlighet med Mittuniversitetets informationshanteringsplan.

Bevarandet ska säkerställa att det i efterhand går att visa:

- vem som har undertecknat handlingen,
- att handlingens innehåll inte har förändrats efter signeringen,
- att signaturen var giltig vid kontrolltillfället.

Den signerade handlingen ska bevaras i öppet och långsiktigt hållbart format i enlighet med detta dokument. Bevis om genomförd validering ska bevaras tillsammans med handlingen när sådan validering krävs enligt fastställda principer.

Om teknisk verifiering inte längre är möjlig, exempelvis på grund av att certifikat har upphört att gälla, ska bevarad valideringsinformation eller rapport användas som bevis för att signaturen var giltig vid kontrolltillfället. Detta är förenligt med Riksarkivets krav på autenticitet och verifierbarhet.

Ansvar och uppföljning

Den som initierar eller ansvarar för en elektronisk signering ansvarar för att:

- rätt signeringstjänst används för aktuell handlingstyp i enlighet med detta dokument,
- underskriften kontrolleras när handlingar signeras eller tas emot i en signeringsprocess där externa parter deltar eller där extern signeringstjänst används,
- den signerade handlingen sparas i oförändrat skick tillsammans med den verifieringsinformation som ingår i signeringen.

Den centrala arkivfunktionen ansvarar för att elektroniskt underskrivna handlingar kan tas emot och bevaras i universitetets e-arkiv.

Bedömningar av signeringstjänster ska dokumenteras enligt bilagan *Checklista för bedömning av e-signeringstjänster*. Bedömningar ska uppdateras vid behov, exempelvis vid förändringar i tjänstens funktion, regelverk eller tekniska standarder. Systemansvarig för respektive e-signeringstjänst ansvarar för att sådan bedömning genomförs och dokumenteras.