FAQ

Innehållsförteckning

Allmänna frågor om eduSIGN

Vad krävs för att komma igång?

- För användartjänsten räcker det med att det går att logga in till tjänsten om IdPn uppfyller kraven som tjänsterna ställer.
- För infrastrukturstjänsten - dvs om man vill köra en egen instans av edusign - behöver en hel del tekniska förberedelser göras. Se informationen under teknisk dokumentation.

Vilka får använda tjänsten?

- Alla som är kunder till eduSign och har skrivit på avtal får använda tjänsten. Avtal krävs även om din organisation vill köra en egen instans av tjänsten.
- Rent praktiskt kan alla som är med i SWAMID logga in på tjänsten och bli inbjudna att signera dokument. Det krävs dock ett avtal med Sunet att använda eduSign för att kunna ladda upp egna dokument och bjuda in andra att signera dem.
  - Under en kortare övergångsperiod kommer det fortfarande att gå att logga in med eduID och ladda upp dokument för att signera dem.

Hur fungerar detta?

- Tjänsten består av tre delar:
  - en e-tjänst (edusign.sunet.se) där användaren kan logga in, ladda upp ett dokument, få det signerat och ladda ner det signerade dokumentet.
  - en infrastrukturtjänst (signservice.edusign.sunet.se) som hanterar själva signeringen.
  - en valideringstjänst som kan verifiera att elektroniska signaturer är giltiga (eller ej).
- edusign.sunet.se "kan" PDF och XML och i framtiden ev. andra dokumentformat
- signservice.edusign.sunet.se "kan" bara signera digitala objekt och har ingen information om det som signeras

- validator.edusign.sunet.se sköter validering och utfärdande av sk valideringsintyg
- Signerade dokument innehåller både en digital signatur och en sista sida där informationen om den som signerat dokumentet visas upp.
- I den digitala signaturen finns all information om den som genomförde signaturen.

Hur ser flödet i tjänsten ut?

1. Logga in på edusign.sunet.se
2. Ladda upp ett dokument för signering
3. Förhandsgranska dokumentet och godkänn för signering
4. Klicka på signera-knappen
5. Du blir skickad till samma IdP som du loggade in på och får logga in en gång till för att genomföra signaturen på signservice.edusign.sunet.se
6. Du blir skickad tillbaka till edusign.sunet.se där det signerade dokumentet kan laddas ner.

Är signerade dokument juridiskt bindande?

- Fråga din jurist.

Har eduSign en privacy policy?

- Ja, eduSigns privacy policy går att läsa på Sunets wiki under information och processer.

Vilka avtal krävs, och vad kostar tjänsten?

- Ni tecknar avtal med Sunet om användandet av tjänsten. Se mer information på Sunet hemsida för eduSign och kontakta tjänsteförvaltaren om ni har frågor.

Räknas dokument som skickas till tjänsten som inkomna handlingar?

- Vi utgår ifrån att svaret är nej eftersom tjänsten inte sparar dokument som skickas.
- Se även frågan om avtal ovan samt svaret om huruvida data lagras i tjänsten.

Hur många kan signera ett dokument i eduSign?

- I dagsläget finns en begränsning att upp till och med 12 personer kan signera ett och samma dokument i eduSign. Detta beror på att det är antalet signaturer som får plats på den grafiska representationen av signatursidan. Vi upplever inte detta vara ett problem, men skulle det vara så att många organisationer vill att vi ökar denna begränsning kommer vi se över frågan.

Varför använder eduSign tidzonen UTC?

- Det handlar till viss del om att minska tvetydigheten. Dels rent teknisks då UTC är vanligare att använda än t.ex. CET, speciellt internationellt då många utgår från just UTC när tider skall konverteras. En annan fördel är att UTC alltid är UTC, om man väljer CET som exempel så skiftar det mellan CET till CEST på sommaren.

Jag har en ide om en ny feature!

- Skicka ett mail till tjänsteförvaltaren som anges som kontaktperson på Sunet hemsida för eduSign.

Hur stora dokument går att signera med eduSign?

- I dagsläget har vi satt en gräns på 20MB på storleken på dokument som går att ladda upp i eduSign och signera.

Går det att se statistik för eduSign?

- Vi har i dagsläget ingen dedikerad statistiktjänst för just signeringar. Däremot går det att få en indikation på användandet genom att se på Géants f-ticks tjänst.
    - Gå till https://f-ticks.edugain.org/index.html
    - Klicka på Statistics -> SPs
    - Välj last 12 month uppe till höger
    - Välj er IdP som idp (om det inte kommer upp något resultat betyder det förmodligen att er IT-avdelning inte slagit på fLog mot Sunet /Swamid)
    - Välj signservice.edusign.sunet.se som sp
- I ovan förfarande ser man hur många autentiseringar som gjorts från en IdP mot signservice. Dvs hur många gång en användare har signerat i eduSign. Att notera är dock att "en signering" kan även vara en bulksignering i eduSign, så själva antalet dokument som signeras kan vara högre än antalet autentiseringar mot signservice.
- OBS Kör en IdP ADFS går det inte att rapportera f-ticks just nu, men en uppdatering av ADFS toolkit som väntas till våren (2024) kommer kunna ändra på just detta.

Validering av signaturer

Vad innebär en validering?

- Att gå från en process att manuellt skriva sin namnunderskrift på papper till att gå över till en digital process och använda e-signaturer kan kräva vissa förändringar för många organisationer. I grunden är det ofta samma funktion som eftersträvas men processerna behöver ofta ändras eller se något annorlunda ut. Nedan är några liknelser mellan namnunderskrifter för hand på papper och validering av e-signaturer för att skapa en större förståelse för hur det går att relatera till dessa nya processer. Sunet tjänst eduSign följer de rekommendationer som DIGG och PTS har i relation till digitala signaturer och validering, det går att läsa mer om dessa begrepp i PTS utredning om Betrodda tjänster.
- En validering av en e-signatur kan generellt jämföras med att ta ett dokument som har namnunderskrifter gjorda med penna på papper och kontakta alla personer som signerat och jämföra underskrifterna med deras signaturer på deras respektive identitetshandlingar.
  Det är dock väldigt sällan som ovan jämförelse görs, så varför behöver vi då validera e-signaturer? Det är faktiskt inte säkert att det behövs. MEN om det uppstår en tvist eller oklarhet i relation till ett signerat dokument så är det fördelaktigt att det är väldigt enkelt att göra just denna jämförelse i relation till e-signaturer, dvs göra en validering av signaturen. En annan fördel med den digitala valideringen är att det även blir tydligt ifall integriteten på dokumentet är intakt, dvs ifall någon har ändrat något sedan dokumentet signerades.

Vad spelar giltigheten på certifikat av en signatur för roll?

- En signatur i eduSign är generellt möjlig att validera under ett år efter signaturen gjordes. Detta kan jämföras med en ID-handling som också har en giltighetstid. Dvs om en person skulle behöva jämföra en namnunderskrift på ett papper mot en ID-handling så kan det ju finnas en risk att den ID-handlingen som personen ägde när namnunderskriften gjordes inte längre är giltig, det betyder ju dock nödvändigtvis inte att namnunderskriften i sig är ogiltig. På liknande sätt kan man tänka att t.ex. ett avtal inte nödvändigtvis blir ogiltigt för att en e-signatur inte längre går att validera.

Vad är ett Valideringintyg?

- Om det är viktigt att kunna validera signaturerna på ett dokument signerat med eduSign över en längre tid är det rekommenderat att skapa ett valideringsintyg. Ett valideringsintyg kan jämföras med att vidimera en namnunderskrift med penna på ett papper. Dvs om någon validerar ett dokument i Sunets valideringstjänst och sedan skapar ett valideringsintyg i den tjänsten kan det liknas med att Sunet vidimerar signaturerna. Detta gör att signaturerna går att validera i en mycket längre tid än ett år, ett valideringsintyg kan generellt valideras i ca 50 år.

Varför ser signaturen ogiltig ut i Adobe Acrobat/Reader?

- eduSIGN följer DIGGs tekniska ramverk för digitala signaturer för svenska myndigheter.
- DIGGs ramverk fokuserar på säkra signaturer och följer CEF byggblock för signaturer inom EU som fungerar på annat sätt än Adobes egna signaturer.
- Inom projektet undersöker vi möjligheterna att koppla signaturerna till certifikat utfärdade av någon publik certifikatsfabrik
- Redan idag kan man välja att lista eduSIGNs certifikat som en betrodd certifikatsutfärdare i Adobe Acrobat/Reader

Signatursidan på slutet av min PDF är tom trots att jag signerat dokumentet!

- Detta fel beror sannolikt på att någon har "sparat" PDF:en genom att skriva ut den och välja alternativet "spara som fil".
- Att på detta sätt "spara" en PDF förstör de elektroniska signaturerna och dessa måste göras om för att vara giltiga.
- Om man laddar upp en sådan fil i valideringstjänsten kommer denna naturligtvis inte kunna validera signaturerna.

Hur fungerar valideringstjänsten?

- Det finns ingen officiell standard till hur en PDF-fil ska signeras. Det skiljer mycket mellan olika programvaror i deras sätt att hantera signerade PDF:er.
- eduSign:s valideringstjänst validerar PDF-signaturer som gjorts i eduSign.
- Läs gärna följande informationsblad: Informationsblad Valideringstjänst
- En mer omfattande beskrivning av hur valideringstjänsten fungerar finns på denna youtube-video (för engelsk version klicka här: english).
- SUNET följer arbetet inom ETSI kring standardisering av validering av PDF-signaturer och eduSIGN kommer successivt att anpassas för att uppfylla denna standard.
- Valideringstjänsten kan även erbjuda ett sk valideringsintyg - detta är en elektronisk stämpel som placeras i dokumentet som intygar att validering skett vid ett visst klockslag. Detta syns i Valideringstjänsten när dokument med valideringsintyg laddas upp dit.
- Ett valideringsintyg kräver att dokumentet sparas från valideringstjänsten genom att klicka på knappen "Valideringsintyg" som visas efter att validering skett.
- Ett dokument med valideringsintyg kan arkiveras utan vidare åtgärd i minst 50 år - därefter kan ytterligare valideringar genomföras för att förlänga arkivbeständigheten.

Valideringstjänsten klagar på ett dokument som skrivits under genom en annan tjänst än eduSIGN

- Alla signaturtjänster är inte likvärdiga - vissa tjänster som använder begrepp som "digital underskrift" och producerar PDF-filer använder inte ens digitala signaturer.
- De enda externa signaturer (dvs signaturer som producerats av andra tjänster än eduSIGN) som valideringstjänsten accepterar är äkta digitala PDF-signaturer från utfärdare som eduSign litar på.

- Kontakta oss gärna med synpunkter på vilka externa tjänster som valideringstjänsten litar på!

Valideringstjänsten klagar på en signatur som utfärdats av adobe sign

- Se svarat på frågan ovan
- Adobe har en lista på certifikatsutfärdare som får utfärda certifikat för signaturer som Adobe-produkter litar på
- Denna lista (AATL - Adobe Approved Trust List) är inte publik och får enligt Adobe inte användas utanför Adobes egna produkter.
- Det är alltså inte möjligt för eduSIGNs valideringstjänst eller någon annan tjänst som inte säljs av Adobe att validera PDF-signaturer på samma

Det står att signaturen är ogiltig i Acrobat! Vad betyder det?

- Signerade dokument måste valideras genom en sk valideringstjänst. En sådan är på väg att etableras inom ramen för eduSign-tjänsten men det finns även en utredning kring frågan att etablera gemensamma valideringstjänster i statens regi.

Säkerhet och identifiering av användare

Kan signaturer förfalskas?

- Varje signatur sker med en nyckel som skapas just för tillfället.
- Efter signaturen kastas nyckeln bort och kan alltså inte användas för andra signaturer.
- eduSIGN följer de standarder och rekommendationer som etablerats genom DIGGs tekniska ramverk.

Används molnet/Var körs tjänsten?

- Inga molntjänster används för eduSign
- Alla delar av tjänsten körs av Sunet på Sunets egna servrar som är placerade i Sunet datacenter.

Lagras data i tjänsten?

- Nej!
- Uppladdade dokument finns endast i minnet medans signaturen genomförs. Om användaren inte laddar ner dokumentet försvinner det helt.
- När en användare bjuder in andra att signera så finns dokumentet på Sunets servrar temporärt fram tills dess att alla har svarat på inbjudan eller den som bjuder in andra att signera tar bort dokumentet.
- Information om inloggade användare finns också bara i minnet medans signaturen genomförs - det skapas med andra ord inga permanenta identiteter i tjänsten

Vad händer om en användare tar bort ett dokument ur eduSign?

- Det finns två scenarios att ta hänsyn till när en användare tar bort dokument från eduSign.
  - Det som kallas Personliga dokument och Mallar i eduSign lagras i användarens lokala webbläsare, dvs deras egen dator. Om en användare tar bort detta dokument ur eduSign så tas det bort från den användarens lokala webbläsares lagringsyta.
  - De dokument som en användare bjuder in andra att signera lagras temporärt på Sunets servrar fram tills dess att signeringsflödet avslutas. Om användaren som bjudit in andra att signera tar bort detta dokument kommer information om detta dokument tas bort från Sunets servrar och de som varit inbjudna att signera dokumentet blir notifierade via ett e-post att signeringsförfrågan har avbrutits.

Vilka attributkrav gäller för tjänsten?

- Signaturtjänsten består av två SPs (entityIDs):
  - https://signservice.edusign.sunet.se/sigservice
  - https://edusign.sunet.se/shibboleth
- Följande attribut används av tjänsterna - samma attribut måste släppas till båda tjänsterna:
  - givenName
  - sn
  - mail
  - eppn
  - eduPersonAssurance (valfritt)
- Se även frågan om säkerhetskrav nedan

Vilka säkerhetskrav gäller för inloggning till tjänsten?

- SPn begär inloggning med AuthenticationContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
- I framtiden kan tjänsten komma att höja säkerhetskraven.
- Se även frågan om styrkan i signaturen nedan

Hur säker är signaturen?

- Svaret på den frågan är komplext - tekniskt är signaturen väldigt säker: vi använder nycklar med hög säkerhet och återanvänder aldrig en nyckel för mer än en signatur till exempel.
- Säkerheten i signaturen beror också på hur mycket man litar på säkerheten i inloggningen.
- För närvarande finns inga hårda krav på högre förtroendenivå i tjänsten men information om vilken förtroendenivå som används (se tex SWAMID Assurance Profiles) kommer lagras i signaturen.

Kan användare logga in med BankID?

- Det går inte för närvarande och vi har heller inga konkreta planer på just BankID. Orsaken är att vi ser uppenbara risker med att bryta mot BankIDs licensvilkor som förbjuder så kallad identitetslänkning. Se vidare frågan om Svensk e-leg och eIDAS nedan.

Kan användare logga in med Svensk e-legitimation och/eller eIDAS

- Det går inte för närvarande men vi har planer på att ansluta tjänsten till Sweden Connect vilket ger tillgång till eIDAS och alla e-legitimationer som finns i Valfrihetssystem 2017 (där dock BankID ej ingår).
- eduSign följer dock redan nu den definition av signaturer som eIDAS tagit fram som kallas Advanced electronic signature. Det pågår även arbete inom Géant att få till en Qualified electronic signature som skall kunna användas av eduSign också.
- Formaten på PDF och XML signaturer som genereras av eduSign överensstämmer även med eIDAS definitionerna.

Finns det något sätt att hantera användare utanför högskolesektorn?

- Det enklaste är att be användaren skaffa och logga in med eduid.se som är fritt för alla och kan erbjuda upp till LoA2-nivå på inloggningen.

För tekniker och integratörer

Går det att bjuda in personer att signera i eduSign via e-postalias?

- Som standard går det bara att bjuda in personer att signera via den e-post de har kopplat till sitt "mail" attribut i deras IdP.
  Men om en organisation konfigurerar att släppa även mailLocalAddress från deras IdP till eduSign så går det också att bjuda in personer att signera via deras e-postalias. Förutsatt att mailLocalAdress populeras med de lokala e-postalias som används inom organisationen.
  Attributet som behöver släppas till eduSign är alltså mailLocalAddress enligt http://www.geant.net/uri/dataprotection-code-of-conduct/v1 entitets kategori (aka CoCov1) eller https://refeds.org/category/code-of-conduct/v2 entitets kategori (aka CoCo v2).
  Se även mer information på SWAMIDs wiki.

Kan jag köra en egen instans av edusign.sunet.se?

- Ja det är möjligt men det krävs en del förberedelser. Läs Teknisk Dokumentation för att få en uppfattning om insatsen.
- OBS att olika instanser har olika signerings-certifikat och av säkerhetsskäl finns det för närvarande ingen rutin för att olika instanser ska kunna signera varandras dokument. Dokument som signeras av fler parter måste alltså för närvarande signeras inom samma instans.

Hur håller jag min egen instans i synk med Sunets version?

- Så länge denna tjänst finns i Sunet tjänsteportfölj så kommer Sunet erbjuda alla tillgång till samma programvara som vi själva kör - sedan är det upp till var och en att hålla sin version uppdaterad.

Finns det ett API till tjänsten?

- Det finns ett internt lågnivå-API till signeringstjänsten baserat på OASIS DSS - detaljerna finns beskrivet i tekniskt ramverk för Svensk e-legitimation. Vi rekommenderar inte detta API för annat än mycket avancerade användare. Kontakta oss för detaljer.
- Det finns ett Java-baserat högnivå-API (kallas även integrations-API): API:et finns på: https://github.com/idsec-solutions/signservice-integration-api och Java-impl finns på https://github.com/idsec-solutions/signservice-integration. Detta API kan användas av Java-baserade applikationer men vi rekommenderar att de flesta applikationer använder REST-gränssnittet till detta API. Se Teknisk dokumentation för mer information.