

Roadmap - eduID

Utveckling kring eduID - i korthet

Vi har lyckats om,

- Eduid fortsätter sträva efter att hålla en god användbarhet, med en hög tillgänglighet och prestanda
- Studenter från inom- och utom EU kan använda universitetens och högskolornas tjänster genom eduID
- Vi fortsätter sträva efter att erbjuda metoder för att logga in som är säkra, enkla att använda och aktuella för marknaden
- och Sunet har börjat använda eduID Connect som sin IdP, där anställda loggar in med sitt eduID för att arbeta i interna och externa system.

Fokus är ett uppdaterat gränssnitt där våra användare lyckas verifiera sitt konto på rätt tillitsnivå för de tjänster de ska användas mot, där bland annat tillägg av säkerhetsnyckel och verifiering av densamma blir aktuellt.

Vi vill göra det möjligt för tjänster att signalera om det räcker att användaren loggar in med lösenord eller om man kräver MFA. Med det klart kan vi också erbjuda användare att logga in med sin fysiska enhet som identifierare, och kommer som följd av det också bygga upp en säkerhetsmässigt förstärkt hantering av det egna kontot gällande ändring av lösenord samt tillägg och borttag av MFA.

Aktiviteter för Eduid och när de beräknas vara klara

Datum som anges ska inte tolkas som det datum då funktionen finns tillgänglig att använda i produktionsmiljö. Datum finns för innevarande kvartal. Många funktioner har beroenden till varandra och kan inte göras tillgängliga i produktionsmiljö förens alla funktioner i samma kluster är klara.

Aktiviteter	Beskrivning och motivering av behov	Vi beräknar att vi är klara med arbetet i denna aktivitet till den
Compliance-process för LoA2 med DIGG	I och med detta godkännande kan eduID användas även för de tjänster som kräver en nivå 2 enligt DIGGs ramverk för tillit.	Klar, godkända för e-legitimation Digg tillitsnivå 2
eIDAS	Möjliggöra att fler studentgrupper genom eduID kan använda högskolors och universitets tjänster.	Finns driftsatt i produktion
Verifiera identitet genom resehandling	Erbjuda möjlighet att med hjälp av en resehandling (pass, nationell identitetshandling) verifiera sin identitet på nivå SWAMID AL2 i eduID.	Finns driftsatt i produktion
Följa SWAMID:s uppdaterade rekommendationer	SWAMID har lanserat nya rekommendationer (länk till dessa riktlinjer). För att följa dessa behöver vi för eduID:s del lägga till och uppdatera en del attribut (länk till förklaring av förändringarna) och förändringarna för eduID utskrivet: Nytt attribut mailLocalAddress som ska vara tillgängligt för CoCo v2 och v1 - CoCo v2 har tillkommit, CoCov2 och v1 ska hanteras lika med tillägg av attributen i v1. Två nya identitetsattribut: pairwise-id och subject-id Om any eller pairwise-id i metadataattributet urn:oasis:names:tc:SAML:profiles:subject-id:req ger pairwise-id, resp. subject-id ger subject-id Nya entitetskategorier: Personalized, Pseudonymous och Anonymous Ordning av de nya entitetskategorierna: Anonymous så släpp inte Pseudonymous eller Personalized Pseudonymous så släpp inte Personalized	Finns driftsatt i produktion
eduID proxy i produktionsmiljö	Del av arbetet med eduID Connect.	Finns driftsatt i produktion

Uppdatering av användargränsnitt	Ökad användbarhet med tydlighet i menyer och hur information presenteras på sidan.	Finns driftsatt i produktion
Uppdatering av flöden för verifiering	Verifiering av identitet tillgängliggörs genom att bli del av flödet när man loggat in.	Finns driftsatt i produktion
Inbjudningsflöde för Connect	Möjliggöra att man kan bjuda in någon till en eduID Connect IdP, samt se status på om någon har accepterat inbjudan.	Finns driftsatt i produktion
Bistå eduID Connect för Sunet	SUNET ska börja använda eduID som inloggning mot sin IdP i eduID Connect.	Finns driftsatt i produktion
Verifiera identitet med Digg e-leg Valfrihetssystem 2018	Verifiering med ytterligare svenska e-legitimationer (exempelvis BankID) i syfte att underlätta åtkomst till system med krav på tillitsnivå SWAMID AL2 och AL3 samt Digg e-leg LoA2. BankID som verifieringsmetod kommer finnas tillgänglig för interna tester till sommaren, och från i hösten kommer det gå att använda för att verifiera identitet på konton.	Finns driftsatt i produktion
MFA step-up	eduID kommer kunna användas för att göra en MFA step-up (efter inloggning med egen IdP som inte har MFA) för de tjänster som kräver det.	Finns driftsatt i produktion
Ombudshantering av särskilda konton	I samband med Skolverkets projekt Digitala nationella prov ska SUNET erbjuda en identitetstjänst (IdP) för skolhuvudmän som inte. Identitetstjänsten ska även erbjuda en särskild kontotyp för elever. Denna kontotyp finns inte i eduID sedan tidigare, eftersom den förutsätter att ett eduID-konto har kontroll över ett annat (kan skapa det, göra lösenordsåterställning och kan radera det).	Finns driftsatt i produktion
Bistå med eduID Connect för skolhuvudmän	Den nya tjänsten eduID Connect kommer göras tillgänglig för att skolhuvudmän utan egen IdP ska kunna identifiera sig för test mot Provtjänsten hos Skolverket inom projektet Digitala nationella prov.	Finns driftsatt i produktion
Presentera urval godkända säkerhetsnycklar	eduID förlitar sig på den standardiserade parten Fido Alliance kring säkerhetsnycklar och kontroll av dessa. Fido Alliance låter förlitande parter hämta metadata över säkerhetsnycklar, där olika nycklar har olika säkerhetsfunktioner. eduID:s bedömning är att endast en del av nycklarna uppnår de krav vi ställer. Därför ska vi presentera en lista som uppdateras automatiskt varje månad över de säkerhetsnycklar som enligt vår bedömning kan användas med eduID, samt beskriva varför vi gjort detta urval.	Finns driftsatt i produktion
Välja tiltalsnamn	Ett eduID-konto med en verifierad personkoppling kan inte ändra på namnet. Vi vill möjliggöra att man ska kunna välja vilket av ens förnamn som ska skickas med till tjänsten man loggar in mot.	Finns driftsatt i produktion
Följa SWAMID:s tillitsprofil kopplat till eduPersonAssurance	"Cappuccino" för AL2 och "Cappuccino" + "Espresso" för AL3	Finns driftsatt i produktion
Särskilja verifierationsmetoder	Olika verifierationsmetoder signalerar olika tillitsnivå i SWAMID:s - och DIGG:s ramverk. Därför kommer vi bygga upp logik respektive verifierationsmetod så att rätt signalering sker ut mot extern tjänst. Vilken metod som använts signaleras inte ut till externa tjänster, utan används bara inom eduID för att avgöra vilken tillitsnivå man kan signalera till den externa tjänst användaren loggar in mot.	Finns driftsatt i test
Styrka samordningsnummer	Tjänster inom SWAMID börjar förbereda stöd för styrka samordningsnummer. I och med detta ska eduID kunna hantera verifiering av konton för de med styrka samordningsnummer, så att kontot kan användas för att göra koppling mot en tjänst eller annan IdP som kräver det.	Finns driftsatt i test
"Säkerhetscenter"	För den användare som lagt till en MFA, och har loggat in med exempelvis lösenord eller med en betrodd device ska det krävas en ytterligare inloggning inuti tjänsten med MFA för att kontrollera och justera inställningar som gäller inloggningsmetoder - så som ändring av lösenord eller lägga till en ny MFA. Så fungerar det redan i praktiken idag, då man om lagt till MFA alltid behöver logga in med denna metod, men i och med införandet av "MFA vid behov" och "Passwordless login" kommer man kunna logga in med en metod som har en lägre säkerhetsnivå - men kommer då inte kunna göra ändringar som kan påverka åtkomsten till kontot förens dess man loggat in med MFA.	10 May 2024
Passwordless login	Möjliggöra inloggning med en betrodd device, utan att behöva ange ett lösenord.	13 Jun 2024
MFA vid behov	När användaren lagt till en metod för multifaktors-inloggning ska tjänster som använder eduID kunna signalera om det krävs en enkel- eller multifaktors-inloggning för att kunna logga in. Detta gör det möjligt att logga in med nivå AL1 för de tjänster som kräver det, och AL2 för de tjänster som kräver det.	30 Apr 2024

ESI för alla anslutna lärosäten	ESI blir ett allt mer centralt begrepp. eduID kan idag hjälpa de lärosäten som så önskar att hämta ut dessa ESI för studenter, men processen för detta kan förenklas genom att kopplingen till LADOK för eduID blir generell istället för som idag att varje lärosäte behöver förse eduID årligen med ett certifikat.	01 Jul 2024
Bistå eduID Connect för Teknik 8:an	Den nya tjänsten eduID Connect kommer användas för att digitalt kunna medverka i Teknik 8:an.	17 Sep 2024
Mina meddelanden	För att verifiera sin identitet kan man idag ta emot ett brev hem i brevlådan. Vi kommer lägga till möjligheten att även ta emot och verifiera sig genom digitala brev hos Mina meddelanden (Min myndighetspost, Kivra, m.fl.).	2024