Teknisk tjänstebeskrivning Diggs-tillitsramverk - eduID

Sammanfattning

eduID är en identitetsutfärdare som är tillgänglig för alla fysiska personer som omfattas av någon process inom forsknings- och utbildningsektorn i Sverige. Detta betyder att även utländska forskare, studenter eller annan personal kan använda eduID sålänge det finns en koppling till Svensk forskning och utbildning. Användare i eduID får ej kopplas till juridiska personer som inte är fysiska individer. En eduID-användare är personlig men kan i vissa fall associeras med information som bifogas från en organisation inom forsknings- och utbildningssektorn. Sådan information kontrolleras av respektive organisation. Detta sker genom tjänsten eduID Connect.

Denna tekniska tjänstebeskrivning gäller för Digg:s tillitsramverk. För teknisk tjänstebeskrivning inom SWAMID:s tillitsramverk klicka på denna länk.

Vad krävs för att kunna logga in mot en tjänst som kräver Digg tillitsnivå 2 (Level of Assurance, LoA2)?

1. Att kontot är verifierat med någon av nedan metoder
2. och att en multifaktor lagts till och använts för att logga in.

Källkod

eduID bygger på öppen källkod. Källkoden kan läsas på GitHub genom att klicka på denna länk.

Deployment- och implementationsprofiler

Följande profiler för SAML stödjs:

- https://saml2int.org/

Identitetsverifiering

Identitetsverifiering betyder att associera en eduID-användare med en fysisk person. Det finns ett antal alternativa processer för att genomföra identitets-verifiering:

1. Kontrollkod till folkbokföringsadress eller digital brevlåda
2. ID-växling med e-legitimation enligt DIGG:s valfrihetssystem

Dessa processer resulterar i en koppling mellan en fysisk person och en eduID-användare. Vid inloggning till en tjänst skickar eduID information om förtroendenivå och säkerhetsnivå genom attribut och andra protokollelement (tex AuthenticationContextClassRef för SAML eller ACR för OpenID Connect) i enlighet med de profiler som eduID implementerar.

Om något steg i verifieringen misslyckas så räknas hela processen som misslyckad och eduID-användaren kopplas inte med den fysiska personen. Detta är en säkerhetsåtgärd.
Koppling mellan fysisk person och eduID-användare sker efter framgångsrik process genom att information om vilken process som genomförts lagras i eduID tillsammans med tillräcklig information för att identifiera de dokument eller andra objekt som användes för verifiering. Nedan beskrivs processernas sk happy path - dvs lyckade verifieringsflöden.

Kontrollkod via brev till folkbokföringsaddress eller digital brevlåda

Här verifieras identiteten genom att vi kontrollerar vilken fysisk adress eller digital adress som är kopplad till ett visst personnummer och sedan att användaren har tillgång att ta emot och läsa brev som skickas till den adressen.

1. Användaren uppger ett personnummer
2. Personnumret slås upp i Navet (folkbokföringen)
3. Personnumret slås upp i FaR (DIGG:s tjänst för kontroll om person har digital brevlåda)
    a. Om har digital brevlåda, skickas verifieringskod ut till den digitala brevlådan
    b. Om inte har digital brevlåda, skickas verifieringskod ut brevledes
4. En verifieringskod genereras och skickas till addressen som uppges i folkbokföringen eller den digitala brevlådan för personnummret. Verifieringskoden har en begränsad giltighetstid.
5. Användaren uppger verifieringskoden. Om verifieringskoden inte har gått ut i tid och överensstämmer med den verifieringskod som skickades så har processen lyckats.

Ger tillitsnivå e-leg LoA2 enligt Diggs ramverk. (detta gäller från senare under 2023 när eduID godkänns för att utfärda DIGG e-leg)

ID-växling med e-legitimation enligt DIGG:s valfrihetssystem

Här verifieras identiteten genom att man efter lyckad process ärver verifikationen man fått vid utfärdandet av sin e-legitimation.

1. Användaren uppger ett personnummer
2. Användaren anmodas logga in med en e-legitimation som omfattas av ett valfrihetssystem som medger ID-växling
3. Om det uppgivna personnumret överensstämmer med personnumret från inloggningen så har processen lyckats.

Ger tillitsnivå e-leg LoA2 enligt Diggs ramverk. (detta gäller från senare under 2023 när eduID godkänns för att utfärda DIGG e-leg)

Inloggningssäkerhet

eduID stödjer inloggning via användarnamn och lösenord i kombination med FIDO2-tokens (via WebAuth-API:et) där förhöjd säkerhet krävs. Inloggning med förhöjd säkerhet (sk MFA) sker på begäran från en ansluten tjänst via protokollelement (tex AuthenticationContextClassRef för SAML eller ACR för OpenID Connect). Kontroll av MFA sker mot FIDO Alliance register över godkända intyg (attestations) eller Passkeys. Exakt vilka protokollelement som resulterar i inloggning med MFA finns beskrivet i respektive implementationsprofil som eduID stödjer.

eduID förväntar sig att FIDO2-token är någon av följande "key protection":

- "faceprint_internal",
- "passcode_external",
- "passcode_internal",
- "handprint_internal",
- "pattern_internal",
- "voiceprint_internal",
- "fingerprint_internal",
- "eyeprint_internal",

Samt kräver att protection uppfylls med någon av följande "user verification":

- "remote_handle",
- "hardware",
- "secure_element",
- "tee",

Och att FIDO2-token skickas med en attestation, eller är av typen Passkey.

Autentisering

Vid skapande av konto genereras ett lösenord som är svårt att gissa. Användaren loggar in genom att ange detta. Efter inloggning kan användaren byta till ett annat säkert lösenord. Användaren måste också lägga till ytterligare säkerhetsnyckel för att kunna verifiera sitt konto på Digg LoA2. Eventuell verifiering av kontot nollställs om lösenordet till kontot återställs.

Återställning av lösenord och eventuell borttagning av verifiering

Om användaren glömt sitt lösenord kan den återställa lösenordet. Instruktioner för återställning skickas då till den primära e-postadressen kopplad till användarens konto.

Om användaren har verifierat sitt konto så uppmanas användaren att använda säkerhetsnyckeln när man skapar ett nytt lösenord. Använder man säkerhetsnyckeln när man skapar sitt nya lösenord så behåller man sin verifierade identitet på den tillitsnivå man hade. Har man inte tillgång till den extra säkerhetsnyckeln och återställer lösenordet så försvinner den personliga verifieringen från kontot, och kontot behöver verifieras på nytt med någon av verifieringsmetoderna för att nå upp till Digg LoA2.

Teknisk anslutning

Anslutning till eduID beror på det tekniska gränssnitt som används (se listan på understödda profiler ovan). För profiler som har stöd för federationer används befintliga federationer. För profilen SAML2Int gäller att tjänster ansluts till eduID genom någon av de identitetsfederationer som eduID är kopplad till. I dagsläget är eduID ansluten till följande federationer:

- SWAMID
- FIDUS (via SWAMID)
- eduGAIN (via SWAMID)

Teknisk anslutning till eduID kan även ske genom tjänsten eduID Connect som är en integrationsproxy som medger att en organisation kan provisionera attribut kopplade till en användare i eduID. Sådana organisations-attribut kan inte ersätta attribut som är kopplade till den fysiska person som är kopplad till eduID-användaren via identitetsverifiering. Tjänsten eduID Connect används för att komplettera och normalisera säkerhet och uppfyllelse av federationsprofiler, tex i syfte att ansluta IdP:er som inte uppfyller SAML2int eller i syfte att komplettera en IdP som saknar stöd för MFA. I vissa fall används eduID Connect med eduID som IdP och som MFA-lösning, dvs utan att någon extern IdP används. eduID Connect ska ses som en plattform för virtuella IdP:er som använder eduID helt eller delvis för hantering av identiteter medans ytterligare attribut kan påföras från respektive organisation som ansvarar för den virtuella IdP:n

Kvalitetsmärken, federationer och trustmarks

Kvalitetsmärken är normalt tillämpbara för eduID samt för eduID Connect i de fall eduID helt och fullt används som bakomliggande IdP. Normalt ska alltså virtuella IdP:er i eduID Connect ses som separata medlemmar i respektive federationer och förtroenderamverk men i fallet då eduID Connect använder eduID som bakomliggande eduID så är i de flesta fall dessa förtroenderamverk tillämpliga.

Namn	Aktuellt	Extern review	Länk
DiGG LoA2	ja	DIGG	