How-To - European Student Identifier (ESI) för European Digital Student Service Infrastructure (EDSSI)

Inledning

MyAcademicID / EDSSI och Erasmus+

MyAcademicID levererade under 2020 en arkitektur för digital identitet som ger studenter möjlighet att autentisera sig för sina studier utomlands med sitt lärosätes studentkonto. Detta kunde genomföras genom att eduGAIN kopplades ihop med sveriges nationella eIDAS-nod. På så sätt kopplas de akademiska identiteterna samman med medborgaridentiteter och en unik identifierare för studenter kan utlovas genom att införa en European Student Identifier (ESI).

Projektet resulterade i en plattform för identitets- och åtkomsthantering för autentisering i e-tjänster relaterade till Erasmus+-programmet, såsom Erasmus+ App eller Online Learning Agreement.

Implementeringen av plattformen för e-tjänster relaterade till Erasmus+ i kombination med användning av ESI via eduGAIN och Erasmus Without Paper beräknas komma att medföra avsevärt minskad administrativ arbetsbörda för personal och studenter.

Projektresultaten vidareutvecklas nu i projektet European Digital Student Service Infrastructure - EDSSI - som kommer att utveckla ett system som gör det möjligt för lärosäten att utbyta och autentisera studentdata på ett sömlöst och säkert sätt.

Erasmus+ är EU:s program för internationellt samarbete och utbyte inom bland annat utbildning. Under 2021 startar en ny sjuårig programperiod där en av de övergripande målsättningarna är att digitalisera programmet. Initiativet har som målsättning att digitalisera administrationen av utbytesprocessen, från att förnya utbytesavtal till urval av studenter. Detta görs genom att lärosäten ansluter till något som kallas *Erasmus Without Paper-nätverket*.

Anslutningen till nätverket kan ske på ett av tre olika sätt:

- Genom en direktanslutning.
- Genom att lärosätet ansluter sitt upphandlade systemstöd för utlandsstudier från tredje part (ex. *Mobility Online eller MoveOn)*.
- Genom att lärosätet ansluter ett egenutvecklat systemstöd för utlandsstudier.

European Student Identifier (ESI)

ESI är ett särskilt attribut som används vid administration av europeiska studentutbyten, t.ex. inom Erasmus+-programmet samt vid de virtuella europeiska universiteten (ex. Unite! och ECIU), för att primärt underlätta att personuppgifter och studieresultat överförs korrekt mellan de inblandade lärosätena.

> Erasmus+-programmet kommer att börja kräva ESI vid både administration och självadministration av studentutbyten. Europeiska kommissionen har beslutat att från och med 1 januari 2023 måste ESI användas vid all administration vid studentutbyte med Erasmus+. Detta betyder att lärosätena måste vara klara i god tid innan det med sin implementation. De lärosäten om har upphandlat ett administrativt system för studentutbyten måste se till så att det systemet använder samma ESI-värde för en specifik student som lärosätets identitetshanteringssystem. Om detta inte görs kommer det inte att gå att göra en koppling mellan ansökan till utbytesstudier via Erasmus+ och studentens självadministration i Erasmus+ webbtjänster.

En ESI är en unik, permanent och stabil identifierare som byggs upp av ett *prefix* som är unikt för organisationen eller organisationerna och ett *suffix* som är unikt inom en eller en grupp av organisationer. Det är möjligt att en person "samlar på sig" mer än en ESI under sin studietid men, det är enklare ju färre ESI:er man behöver hålla reda på. Det finns också fördelar om en ESI kan följa med en student genom hela livet.

ESI representeras i SAML som schacPersonalUniqueCode (se nedan för detaljer).

Implementationen av ESI vid ett lärosäte kretsar kring följande två frågor:

1. Vad har en student för ESI och ska det skapas en lokal ESI eller ska den hämtas från annan källa?

2. Hur görs ESI-attributet tillgängligt i samband med inloggning till de tjänster som ska konsumera attributet?

Tänk på följande:

- Det underlättar om en student har få ESI:er men det är hanterbart även om en student har flera ESI:er under sin studietid, tex i samband med flytt till eller från ett lärosäte som inte ingår i Ladok eller för studenter som inte gått igenom central antagning och därmed inte har ett ExterntStudentUID från Ladok/NyA/Antagning.se.
- Lärosätet kan behöva hantera studenter som gått igenom lokal antagning på ett annat sätt än vanliga "NyA-studenter". Detta kan ge flera olika ESI-strukturer inom lärosätet. Detta är inte ett problem för ESI-samarbetet.
- ESI är inte knuten till personnummer och kräver inte "bekräftade" användare. En ESI är frikopplat från nationella identifieringssystem och är gemensamt för hela EU.
- Genom att samordna ESI med eduID kan en student behålla sin ESI över lång tid, även efter ett eventuellt val av lärosätet att rensa bort ett lärosäteskonto. Detta främjar livslångt lärande på sikt.
- Den modell som väljs för ESI måste både vara tillgängligt både för den tjänst som används för administration av studentutbytet och lärosätets identitetsutgivare (IdP).

Olika alternativ vid implementation av ESI

På grund av GDPR så är det inte lämpligt att använda studenters personnummer som ESI. För studenter så finns två andra nationella identifierare som kan vara lämpliga att använda som bas för ESI, ExterntStudentUID från Ladok/NyA/Antagning.se respektive unikt id i eduID. Ett tredje alternativ är att skapa en lokalt ESI direkt kopplat till studentens identitetsutfärdare.

Använda ExterntStudentUID från Ladok som ESI

Rekommendation

För de lärosäten som använder Ladok rekommenderas att ExterntStudentUID i Ladok används för att bilda ESI. Fördelen med just denna variant är att studenten behåller samma ESI-värde även om de börjar studera vid annat lärosäte med förutsättning att även det nya lärosätet använder ESI från Ladok.

Denna variant går även använda för de lärosäten som inte använder Ladok men använder NyA/Antagning.se för antagning. Detta värde kan då hämtas från NyA/Antagning.se.

I Ladok finns ett ExterntStudentUID för varje student. Värdet kommer från UHR:s studentregister där samordning sker med Ladok och NyA/Antagning.se för att varje student som etableras i Ladok eller NyA/Antagning.se ska få en unik gemensam identifierare. För att i möjligaste mån se till att studenter har samma ESI oberoende vilket lärosäte/inloggningstjänst studenten loggar in via så bör ExterntStudentUID användas för ESI. Notera att Ladok respektive NyA/Antagning.se även har egna, interna UID:er för studenter (som i Ladoks fall (StudentUID) bland annat kan användas i norEduPersonLIN). Dessa är inte samma som ExterntStudentUID.

ExterntStudentUID i Ladok är ett uuid, exempelvis 9e342e78-5b6c-4902-966e-50e28a21e601.

Värdet på schacPersonalUniqueCode blir då: **urn:schac:personalUniqueCode:int:esi:ladok.se:externtstudentuid-9e342e78-5b6c-4902-966e-50e28a21e601**

Observera att värdet från ExterntStudentUID ska från Ladok/NyA/Antagning.se ska vara skrivna med gemener (små bokstäver). Vissa verktyg får ut dessa i versaler (stora bokstäver) som då behöver konverteras till gemener.

Denna ESI kan användas på två sätt:

1. Genom en integration i den egna inloggningstjänsten mot Ladok eller NyA-Open.
2. Genom att eduID uppdras att integrera mot Ladok/NyA-Open och sedan antingen bygga en integration mot eduID i sin inloggningstjänst eller att därefter hänvisa sina studenter till eduID för inloggning i de fall studenten vill ha med sig ESI.

Läsa ut ExterntStudentUID från Ladok

ExterntStudentUID följer med i lärosätets egna feed i Ladok. Händelsen heter **LokalStudentEvent** och attributet i händelsen heter **ExterntStudentUID**. Notera att händelsen även har attributet **StudentUID**, som är den interna UID:n för studenten i Ladok.

REST-dokumentationen för LokalStudentEvent i Ladok: https://www.start.ladok.se/restdoc/schemas/schemas.ladok.se-studentinformation-events.html#type_LokalStudentEvent.

Ett exempel på ett LokalStudentEvent:

```
<si:LokalStudentEvent xmlns:si="http://schemas.ladok.se/studentinformation" xmlns:base="http://schemas.ladok.se"
xmlns:dap="http://schemas.ladok.se/dap" xmlns:events="http://schemas.ladok.se/events">
  <events:HandelseUID>9f920641-9647-4c39-88ec-aae708516014</events:HandelseUID>
  <events:EventContext>
    <events:AnvandareUID>6cf85d57-1662-42bf-93aa-1b5fdea16386</events:AnvandareUID>
    <events:Anvandarnamn>feedevent@ladokintern.se</events:Anvandarnamn>
    <events:LarosateID>96</events:LarosateID>
  </events:EventContext>
  <events:Handelsetyp>UPPDATERAD</events:Handelsetyp>
  <si:Efternamn>Johansson</si:Efternamn>
  <si:ExterntStudentUID>e32accbe-4915-4e4f-8d66-08961b6542de</si:ExterntStudentUID>
  <si:Fodelsedata>1986-09-30</si:Fodelsedata>
  <si:Fornamn>Maria</si:Fornamn>
  <si:Kon>1</si:Kon>
  <si:Personnummer>198609309888</si:Personnummer>
  <si:StudentUID>a044b2d3-eb0d-4ece-89e0-7fa8b4a008a4</si:StudentUID>
</si:LokalStudentEvent>
```

Läsa ut ExterntStudentUID från NyA/Antagning.se

ExterntStudentUID går även att läsa ut från NyA-Open (speciellt för lärosäten som inte har Ladok men som använder NyA för antagning). Där återfinns det i tabellen STUDENT_PERSON_ID_MAP:

```
select p.PNR, m.STUDENT_UID from NYA.PERSON p join NYA.STUDENT_PERSON_ID_MAP m on p.PERSON_ID = m.PERSON_ID where
p.PNR = '<pnr>'
```

I vissa fall behöver frågan ändras för att det ska blir rätt beroende på drivare mot Nya/Antagning.se, upptäckt problem vid utsökning med .Net

```
select p.PNR, HEX(m.STUDENT_UID) from NYA.PERSON p join NYA.STUDENT_PERSON_ID_MAP m on p.PERSON_ID = m.PERSON_ID
where p.PNR = '<pnr>'
```

Synkronisering av ExterntStudentUID med eduID

eduID kan på uppdrag från ett lärosäte tillhanda ESI för dess studenter. Efter att lärosätet godkänt användningen kan en student vid lärosätet aktivera ESI i sin användarprofil. eduID kan dock inte skicka i attributrelease att det är en student vid lärosätet beroende på säkerhetsbegränsningar.

Oavsett om ett lärosäte väljer att implementera ESI i sin identitetsutfärdare eller ej så finns skäl att synkronisera studenters ESI med eduID. Exempel på detta:

- Lärosätet hämtar ESI från Ladok/NyA till sin egen IdP och lärosätets studenter använder ibland, eller i framtiden främst, eduID för inloggning
- Lärosätet har sina studenter i Ladok men hämtar inte ESI från Ladok/NyA/Antagning.se och låter istället sina studenter använda eduID för inloggning mot Erasmus+

För mer information om att synkronisera studenters ESI med eduID i Ladok, se Synkronisera ESI med eduID (åtkomst till Ladoks dokumentation krävs).

eduID har integrationsmöjligheter med Ladok både för att koppla ESI till användare i eduID och för att hämta ut användares ESI från eduID:

Synkronisering av ESI	Beskrivning
Ladok -> eduID	Lärosätet kan tillåta eduID att hämta ESI för lärosätets studenter från Ladok (via Ladoks REST-API)
eduID -> Lärosäte	Lärosätet kan hämta ESI för sina studenter från eduID (via en användarinloggning)

Använda lokal användaridentitet vid lärosäte som ESI

> ⚠ Använd denna variant endast om ExterntStudentUID från Ladok (och NyA/Antagning.se) inte kan användas!

Varje användare vid ett lärosäte har en unik användaridentitet som aldrig återanvänds för annan individ (används normalt i eduPersonPrincipalName i SWAMID).

Användaridentiteten är en textsträng, exempelvis *abcd1234*, och lärosätet har en DNS-domänen (SAML Scope), exempelvis *larosate.se*.

Värdet på schacPersonalUniqueCode blir då: **urn:schac:personalUniqueCode:int:esi:*larosate.se*:*abcd1234***

Att göra attributrelease av ESI från en identitetsutfärdare

MyAcademicID använder entitetskategorin Géant Data Protection Code of Conduct för alla attribut som överförs från lärosätenas identitetsutfärdare förutom för European Student Identifier (ESI). Det beror på att ESI använder det multivärda attributet schacPersonalUniqueCode. Detta attribut kan innehålla många olika värden med olika syfte och det är av integritets- och säkerhetsskäl endast lämpligt att släppa ESI till tjänster som har rätt att använda det.

European Student Identifier har en egen entitetskategori vilken har som enda uppgift att endast släppa ESI-värdet i attributet schacPersonalUniqueCode till de tjänster som efterfrågar ESI via entitetskategorin. Övriga attribut som tjänsten behöver efterfrågas via annan entitetskategori, t.ex. CoCo. Den tekniska identifieraren av denna entitetskategori är **https://myacademicid.org/entity-categories/esi** och den formella definitionen på entitetskategorin finns på den adressen..

Shibboleth Identity Provider

För Shibboleth Identity Provider har SWAMID uppdaterat SWAMID:s exempelfiler för resolver och filter på hur ESI-värdet släpps genom ett automatiserat beslut. Se wikisidorna "Example of a standard attribute resolver for Shibboleth IdP v4 and above" och "Example of a standard attribute filter for Shibboleth IdP v4 and above" och sök på attributet **schacPersonalUniqueCode** för att se exempelkonfigurationerna.

Active Directory Federation Services (ADFS)

ADFS Toolkit från och med version 2.1.0 har inbyggt stöd för entitetskategorin för ESI, som gör att ESI släpps med automatik till tjänster som är markerade för entitetskategorin. Version 2.0 av ADFS Toolkit kan manuellt konfigureras för att hantera ESI via en uppdatering av SWAMID-inställningarna. Det finns inget stöd i version 1.0 och tidigare.

Instruktion för att hantera ESI i ADFS Toolkit från och med v2.1.0

För att snabbt få stöd för ESI-kategorin innan den byggts in i ADFS Toolkit har SWAMID släppt en utökad federationsfil som kan importeras via ett kommando, se nedan. Federationsfilen innehåller dels specifika entitetskategorier för SWAMID, dels defaultvärden för ADFS Toolkit så att man inte behöver ta reda på URL:en till metadatat eller certifikatets fingerprint som signerar metadatat.

Steg 1 - Ladda ner den nya versionen av SWAMID:s federationsfil

Använd följade kommando för att ladda ner och uppdatera SWAMID:s federationsfil(er):

```
Get-ADFSTkFederationDefaults -URL https://mds.swamid.se/md/SWAMID_FederationDefaults.zip -InstallDefaults
```

Federationsfilen packas upp och lägger sina filer i mappen "C:\ADFSToolkit\config\federation\SWAMID".

Den intressanta filen i det här sammanhanget är "C:\ADFSToolkit\config\federation\SWAMID\SWAMID_entityCategories.ps1".

I filen har vi lagt till ett kodblock, #European Student Identifier Entity Category, som i sin tur innehåller två delar, en av dem är utkommenterad (raderna som startar med #).

```
    #European Student Identifier Entity Category
    $TransformRules = [Ordered]@{}

    $TransformRules.schacPersonalUniqueCode = [PSCustomObject]@{
        Rule=@"
        @RuleName = "compose schacPersonalUniqueCode for ESI"
        c:[Type == "urn:mace:dir:attribute-def:schacPersonalUniqueCode", Value =~ "^urn:schac:
personalUniqueCode:int:esi:"]
         => issue(Type = "urn:oid:1.3.6.1.4.1.25178.1.2.14",
         Value = c.Value,
         Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:
oasis:names:tc:SAML:2.0:attrname-format:uri");
"@
        Attribute="urn:mace:dir:attribute-def:schacPersonalUniqueCode"
        AttributeGroup="ID's"
    }

#     $TransformRules.schacPersonalUniqueCode = [PSCustomObject]@{
#         Rule=@"
#         @RuleName = "compose schacPersonalUniqueCode for ESI"
#         c:[Type == "urn:mace:dir:attribute-def:schacPersonalUniqueCode"]
#          => issue(Type = "urn:oid:1.3.6.1.4.1.25178.1.2.14",
#          Value = "urn:schac:personalUniqueCode:int:esi:ladok.se:externtstudentuid-" + c.Value,
#          Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:
oasis:names:tc:SAML:2.0:attrname-format:uri");
# "@
#         Attribute="urn:mace:dir:attribute-def:schacPersonalUniqueCode"
#         AttributeGroup="ID's"
#     }

    $IssuanceTransformRuleCategories.Add("https://myacademicid.org/entity-categories/esi",$TransformRules)

    ###
```

1. Det övre stycket släpper alla värden i schacPersonalUniqueCode som böjar på "urn:schac:personalUniqueCode:int:esi:".
2. Det nedre stycket tar alla värden i schacPersonalUniqueCode och släpper ett nytt värde som byggs ihop av "urn:schac:personalUniqueCode:int:esi:externtstudentuid-" + värdet.

Har ni behovet att bygga ihop ESI-strängen, *kommentera ut* det övre stycket och *avkommentera* det undre.

Steg 2 - Konfigurera var ADFS Toolkit kan hämta värden för schacPersonalUniqueCode

Fil att ändra är C:\ADFSToolkit\config\institution\config.Swamid.xml (standardplats).
Lägg till följande rad någonstans i filen inom <attributes> taggen (långt ner i filen).

```
<attribute type="urn:mace:dir:attribute-def:schacPersonalUniqueCode" store="Active Directory" name="
externtstudentuid" />
```

Observera att attributnamnet *externtstudentuid* måste ersättas med det attribut där ni lagrar ESI-värdet i Active Directory.

Värdet kan lika gärna hämtas från en annan källa, t.ex. SQL/Custom Store om så önskas.

Steg 3 - Gör en import av en SP och tvinga en entitetskategori

För att testa konfigurationen ovan kan man antingen importera en SP som har rätt entitetskategori i metadatat eller tvinga en entitetskategori på en test-SP. Man kan också "torrsimma" och emulera vilka attribut som kommer släppas med kommandot Get-ADFSTkToolsIssuanceTransformRules.

Använd följande kommando för att se attributreglerna som kommer skapas för SWAMID:s testtjänst för ESI:

```
Get-ADFSTkToolsIssuanceTransformRules -entityId https://esi.release-check.swamid.se/shibboleth
```

Använd följande kommando för att tvinga en entitetskategori på MyAcademicID:

```
Import-ADFSTkMetadata -EntityId 'https://proxy.prod.erasmus.eduteams.org/metadata/backend.xml' -ConfigFile 'C:
\ADFSToolkit\config\institution\config.Swamid.xml' -ForcedEntityCategories 'https://myacademicid.org/entity-
categories/esi' -ForceUpdate
```

För att se resultatet av importen, använd följande kommando:

```
Get-AdfsRelyingPartyTrust -Identifier 'https://proxy.prod.erasmus.eduteams.org/metadata/backend.xml' | Select -ExpandProperty IssuanceTransformRules
```

Manuell konfiguration av entitetskategori för ESI

Om inte lärosätets identitetsutfärdare inte kan hantera attributrelease av ESI via entitetskategori eller om lärosätet manuellt konfigurerar attributrelease behöver ni tänka på följande vid konfigurationen.

- Identifieraren för entitetskategorin är **https://myacademicid.org/entity-categories/esi**.
- Värdet för ESi ska skickas i attributet **schacPersonalUniqueCode (urn:oid:1.3.6.1.4.1.25178.1.2.14).**
    - Observera att det är endast ESI-värdet som ska skickas till MyAcademicID, inga andra!

Manuell konfiguration av attributrelease till MyAcademicID om inte entitetskategori kan användas

Om inte lärosätets identitetsutfärdare inte kan hantera attributrelease av ESI via entitetskategori eller om lärosätet manuellt konfigurerar attributrelease behöver ni tänka på följande vid konfigurationen.

- entityID för MyAcademicID är **https://proxy.prod.erasmus.eduteams.org/metadata/backend.xml**.
- Värdet för ESi ska skickas i attributet **schacPersonalUniqueCode (urn:oid:1.3.6.1.4.1.25178.1.2.14)**.
    - Observera att det är endast ESI-värdet som ska skickas till MyAcademicID, inga andra!
- MyAcademicID begär även attributen **eduPersonAssurance**, **eduPersonPrincipalName**, **eduPersonScopedAffiliation**, **givenName**, **mail**, **schacHomeOrganization** och **sn** via entitetaskategorin CoCo.

Presentationer från webinarer

Presentationer som beskriver hanteringen av ESI:

- 2021-04-06 - Webbinarium MyAcademicID/EDSSI och ESI
- 2021-10-27 - European Student Identifier och den sista pusselbiten - Sunetdagarna Hösten 2021
- 2022-11-07 - Implementering av ESI UHR och SUNET
- 2022-11-07 - Webinarium European Student Identifier en påminnelse

På wikisidan Presentationer från webbinarium 2021 finns ytterligare webbinar om MyAcademicID och EDSSI.

Specifikationer

Specifikation av European Student Identifier (ESI)

Specfikationen för ESI finns publicerad på adressen https://wiki.geant.org/display/SM/European+Student+Identifier.

Specifikation av attributet schacPersonalUniqueCode

Specfikationen för attributet schacPersonalUniqueCode finns på adressen https://wiki.refeds.org/display/STAN/SCHAC+Releases.

Specifikation av entitetskategorin för European Student Identifier (ESI EC)

Specfikationen för ESI EC finns publicerad på adressen https://myacademicid.org/entity-categories/esi.