

European Student Identifier en påminnelse

2022-11-07

European Student Identifier (ESI)

Var används European Student Identifier?

- Lärosäten som deltar i Erasmus+-programmet måste hantera ESI för alla studenter som ska göra utbyte inom programmet
- Utbytesadministrationssystem kan använda SAML-baserad inloggning för studenterna och även få ESI från lärosätet
 - Observera att lärosätets IdP och ev. tjänst för administration av studentutbyte måste använda samma värde på ESI!
- ESI användas inte endast för administrationen mellan lärosätena utan även vid inloggning till kringtjänster såsom ansökan och prioritering till utbytesstudentbostäder

Vilka skickar idag inte ESI?

- Chalmers tekniska högskola
- Enskilda högskolan i Stockholm
- Handelshögskolan i Stockholm
- Högskolan i Gävle
- Högskolan i Skövde
- Karolinska institutet
- Konstfack
- Linnéuniversitetet
- Mälardalens universitet
- Röda korsets högskola
- Stockholms konstnärliga högskola
- Södertörns högskola
- Uppsala universitet

Denna lista är från 5 november och innehåller alla lärosäten som har provat logga in i MyAcademicId eller i attributtestaren för MyAcademicId

Vad behöver ett lärosäte göra och när?

Lärosätet ska redan idag kunna hantera ESI för alla studenter som ska på utbyte inom ramen för Erasmus+!

Finns inte i stöd så ska följande göras:

- Inför stöd för ESI i lärosätets identitetshanteringsystem (IAM)
- Se till så att den tjänst som används för studentutbyte har tillgång till samma värde för ESI som i IAM
- Konfigurera lärosätets identitetsutfärdare så att det får tillgång till ESI i attributet schacPersonalUniqueCode
- Konfigurera lärosätets identitetsutfärdare så att det kan skicka ESI med hjälp av kommande entitetskategori för ESI

Krav på ESI

En ESI ska alltid vara

- en långsiktigt unik identifierare för studenten
 - Bör vara utformat som en pseudonym (inte direkt identifierande)
 - Ska inte innehålla en e-postadress
 - Ska inte innehålla personnummer
- samma under hela perioden ett studentutbyte pågår
 - Får gärna vara samma under studentens hela studieperiod
 - En student kan samtidigt ha flera ESI så länge som att det är samma som används för ett specifikt studentutbyte
- på formen (gäller i Sverige)
 - `urn:schac:personalUniqueCode:int:esi:<sHO>:<code>`
 - `<sHO>` är ett domännamn som unikt identifierar organisation som utfärdar `<code>`
 - `<code>` är studentens unika identifierare vid utfärdande organisationen

Wikisida med rekommendation

Dagens presentation bygger på wikisidan

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

<https://wiki.sunet.se/x/E4ArBg>

Alternativ för att skapa ESI

Rekommendationen innehåller två olika modeller för att skapa ESI:

- **Använda ExterntStudentUID från Ladok**
 - Detta är en gemensam unik identifierare mellan NyA och Ladok som alla studenter som antas via Antagning.se eller registreras i Ladok har
 - ExterntStudentUID är en GUID som skapas under antagningsprocessen
 - För lärosäten som använder Ladok rekommenderas denna variant
 - eduID stödjer denna modell
- **Använda lokal användaridentitet vid lärosätet**
 - Det lokala användaridentiteten kan vara samma som används vid inloggning

Varför en egen entitetskategori för ESI?

- ESI har inget eget attribut utan använder det multivärda attributet schacPersonalUniqueCode (OID 1.3.6.1.4.1.25178.1.2.14)
 - Attributet kan innehålla flera olika värden för flera olika tillämpningar och kan därför ur ett integritets- och säkerhetsperspektiv inte hanteras inom en generell entitetskategori, t.ex. CoCo.
- ESI har en egen entitetskategori för att möjliggöra attribut-release av värdet för ESI till aktuella tjänster.

Konfigurera Shibboleth IdP \geq v4

- Hämta och populera schacPersonalUniqueCode i attribute-resolver.xml
 - SWAMIDs [exempelresolver](#) innehåller två exempel:
 - ESI-värdet finns redan i LDAP-attributet schacPersonalUniqueCode
 - Den personliga identifieraren i ESI-värdet finns som separat LDAP-attribut och som byggs ihop till ett värde i schacPersonalUniqueCode
 - ExterntStudentUID i exemplet ska bytas mot det attribut som används
- Skapa filter för attributrelease i attribute-filter.xml
 - SWAMIDs [exempelfilter](#) innehåller ett exempel med skydd så att endast ESI-värdet släpps

Konfigurera ADFS Toolkit

- **Version $\geq 2.1.0$** har stöd för ESI:s entitetskategori genom SWAMIDs federationskonfigurationsfil
- **Version 2.0.0 och 2.0.1** har efter manuell konfiguration stöd för ESI entitetskategori.
- **Version 1.0, och tidigare,** har inte stöd för ESI via entitetskategori
- Aktuell version av ADFS Toolkit är 2.2.0 och denna innehåller förutom stöd för ESI även stöd för nya GDPR-vänliga entitetskategorier, se pass på Sunetdagarna den 20 oktober.
 - Program och presentationsbilder finns på <https://wiki.sunet.se/x/yJyvBg>

Manuell konfiguration av attributrelease

Endast om attributrelease av entitetskategori inte kan användas!

- entityID för MyAcademicID:
<https://proxy.prod.erasmus.eduteams.org/metadata/backend.xml>
- Attribut för ESI-värdet: 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 använder CoCo för övriga attribut
 - eduPersonAssurance, eduPersonPrincipalName, eduPersonScopedAffiliation, givenName, mail, schacHomeOrganization och sn
- Även övriga tjänster som behöver ESI behöver konfigureras

ESI i eduID

- eduID har stöd för ESI via Ladok
 - Kräver godkännande för aktivering av de lärosäten som vill använda
- eduID har endast stöd för ESI, inte om användaren är student vid ett visst lärosäte
- Lärosätet kan hämta ESI från eduID via attributrelease
- eduID Connect kommer när tjänsten lanseras kunna hantera ESI inkl. om användaren är student vid lärosätet

Testverktyg för ESI

- SWAMID har i testsuiten på release-check.swamid.se med en flik för ESI
 - <https://release-check.swamid.se/#esi>
 - Testanvändare är ok men de måste vara unikt kopplade till en fysisk person och ha korrekta personuppgifter för denna person.
- MyAcademicId har ett bra verktyg för att testa fullständig attributrelease till tjänsten
 - <https://myacademicid.devtest.eduteams.org/sp/>
 - Observera! Ni får inte logga in med några testanvändare utan ni får be om hjälp av en student.

Aktuell status för testverktygen

- 10 lärosäten släpper inte ESI varken till MyAcademicId eller till SWAMIDs testtjänst
- 3 lärosäten släpper inte ESI till MyAcademicId har inget testresultat hos oss
- 3 lärosäten har under oktober fått ok testresultat i vår testtjänst men har inte testat i MyAcademicId efter det
- 21 lärosäten får ok hos MyAcademicId

Frågor och funderingar?