SWAMID

Swedish Academic Identity Federation

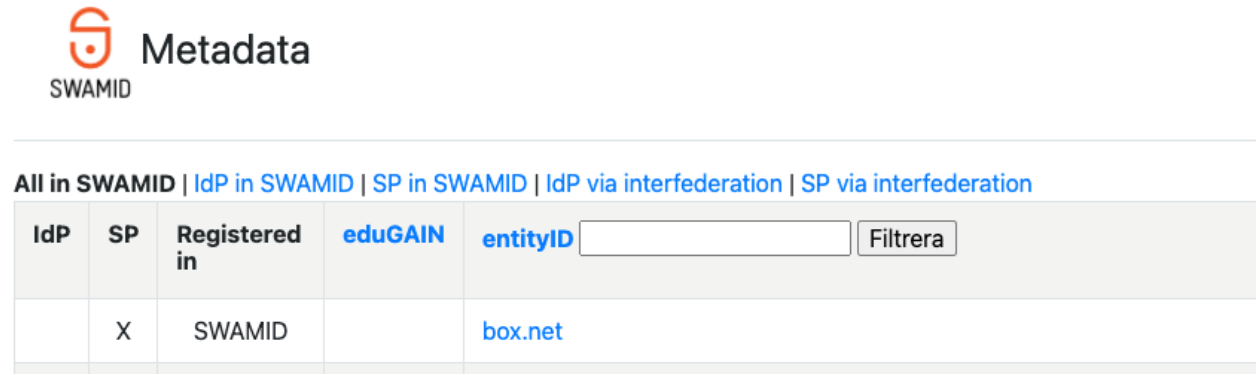
Genomgång av metadata.swamid.se

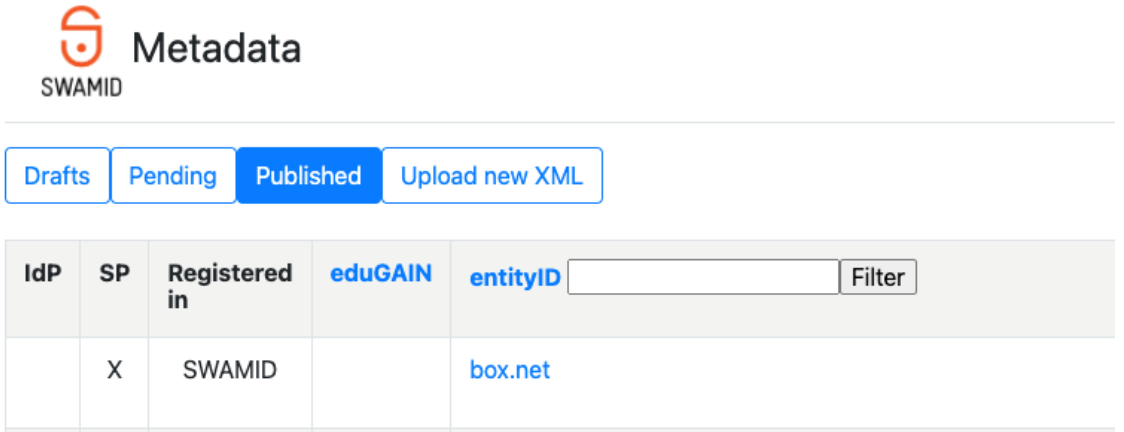
2022-01-20

SWAMID

View / Admin

- View
  - Alla kan se allt
  - Listar publicerade
  - Visar även eduGAIN
- Admin
  - Kräver inloggning
  - Möjlighet att redigera





SWAMID

Metadata.swamid.se

- Validerar emot
  - SWAMID SAML WebSSO Technology Profile
  - Felaktig SAML-XML
  - GÉANT CoCo (v1)
  - REFEDS R&S
- Övrig info
  - Länkar som är fel
  - Resultat från Release-check (om EntityCategorySupport saknas / felaktig)
  - Cert som är på väg att gå ut
  - Felaktiga FriendlyName

SWAMID

Metadata.swamid.se

- Visar vad som är fel / behöver uppdaterats / läggas till
  - Mindre mail mellan er och Operations
  - Snabbare hantering av era ärenden
  - Flagga upp cert som är på väg att gå ut / gått ut
- Mail (kommer under våren)
  - Cert som går ut / gått ut
  - Länkar som är fel
  - Dags att verifiera en entity

SWAMID

Metadata.swamid.se

- Enbart konton med affiliation employee kommer att kunna logga in.
  - Fler krav har diskuterats men inte implementerats ännu.
- 3 nivåer
  - Warning – bra om ni fixar till
  - NonBreakning Error – Hindrar inte aktuell uppdateraing. Åtgärda snarast!
  - Error – MÅSTE åtgärdas innan vi accepterar uppdateringen
- Entiteter med fel (Error) i metadata kommer efter årsskiftet 22/23 att avregistreras ur SWAMID under januari 2023.

SWAMID

XML-fel

- Warnings
  - SPSSODescriptor/Extensions should not have a DiscoHints.

- Errors
  - DiscoveryResponse found in Extensions should be below SPSSODescriptor/Extensions.
  - Scope found in Extensions should be below IDPSSODescriptor/Extensions.
  - EntityAttributes found in IDPSSODescriptor/Extensions should be below Extensions at root level.
  - Scope found in SPSSODescriptor/Extensions should be below IDPSSODescriptor/Extensions.
  - Index is Required in SPSSODescriptor->AttributeConsumingService.
  - A Name attribute is Required in SPSSODescriptor->AttributeConsumingService[index=1]->RequestedAttribute.

SWAMID

Diverse varningar

- Warnings
  - NameFormat "urn:oasis:names:tc:SAML:2.0:attrname-format:basic" for mail in RequestedAttribute for index 1 is not recomended.
  - NameFormat is missing for urn:oid:0.9.2342.19200300.100.1.3 in RequestedAttribute for index 1. This might create problmes with some IdP:s
  - Certificate (signing) metadata.swamid.se will soon expire. New certificate should be have a key strength of at least 4096 bits for RSA or 384 bits for EC.
  - One or more old certs found. Please remove when new certs have propagated.

SWAMID

Certifikat

- Warnings
  - SWAMID Tech 5.2.1/6.2.1: Certificate is RECOMMENDED NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 4096-bit RSA key.
  - SWAMID Tech 5.2.3/6.2.3: Signing and encryption certificates SHOULD be self-signed.
- Error NonBreaking
  - SWAMID Tech 5.2.1/6.2.1: (NonBreaking) Certificate MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 2048-bit RSA key.
  - SWAMID Tech 5.2.2/6.2.2: (NonBreaking) Signing and encryption certificates MUST NOT be expired.
- Errors
  - SWAMID Tech 5.2.1/6.2.1: Certificate MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 2048-bit RSA key. New certificate should be have a key strength of at least 4096 bits for RSA or 384 bits for EC.
  - SWAMID Tech 5.2.2/6.2.2: Signing and encryption certificates MUST NOT be expired. New certificate should be have a key strength of at least 4096 bits for RSA or 384 bits for EC.

SWAMID

REFEDS Research and Scholarship

- Warnings
  - REFEDS Research and Scholarship 4.3.3 RECOMMEND a MDUI:DisplayName and a MDUI:InformationURL with lang=en.

- Errors
  - REFEDS Research and Scholarship 4.3.3 Require a MDUI:DisplayName and a MDUI:InformationURL.
  - REFEDS Research and Scholarship 4.3.4 Require that the Service Provider provides one or more technical contacts in metadata.

SWAMID

GÉANT Data Protection Code of Conduct

- Warnings
  - GÉANT Data Protection Code of Conduct Recomend a MDUI - DisplayName with at least lang=en.
  - GÉANT Data Protection Code of Conduct Recomend a MDUI - Description with at least lang=en.

- Errors
  - GÉANT Data Protection Code of Conduct Require a MDUI - PrivacyStatementURL with at least lang=en.
  - GÉANT Data Protection Code of Conduct Require a MDUI - Logo with lang=en for all present elements.
  - GÉANT Data Protection Code of Conduct Require MDUI with lang=en.
  - GÉANT Data Protection Code of Conduct Require at least one RequestedAttribute.

SWAMID

Release-check

- Warnings
  - SWAMID Release-check: (2022-01-14 14:53:00) CoCo OK, Entity Category Support missing.
  - SWAMID Release-check: (2022-01-14 14:52:59) R&S attributes OK, Entity Category Support missing.

- Error NonBreaking
  - SWAMID Release-check: (2022-01-14 14:53:00) CoCo is not supported, BUT Entity Category Support is claimed.
  - SWAMID Release-check: (2022-01-14 14:52:59) R&S attributes missing, BUT Entity Category Support claimed.

SWAMID

Övriga varningar

- Warnings
  - SWAMID Tech 5.1.5/6.1.5: Missing MDUI/Organization/... with lang=sv.
  - SWAMID Tech 5.1.7/6.1.7: entityID SHOULD NOT start with urn: for new entitys.
  - SWAMID Tech 5.1.11: Support for Entity Categories SHOULD be registered in the entity category support entity attribute as defined by the respective Entity Category.
  - SWAMID Tech 5.1.11: Support for Entity Categories SHOULD be registered in the entity category support entity attribute as defined by the respective Entity Category.
  - SWAMID Tech 6.1.20: FriendlyName for urn:oid:0.9.2342.19200300.100.1.3 in RequestedAttribute for index 1 is email (recomended from SWAMID is mail).
  - SWAMID Tech 6.1.26: Missing ContactPerson of type support.
  - SWAMID Tech 5.1.28/6.1.27: Missing security ContactPerson.

- Error NonBreaking
  - Entity Category Error: (Non breaking) The entity category http://www.swamid.se/category/sfs-1993-1153 is deprecated.

SWAMID

Övriga fel

- Errors
  - SWAMID Tech 5.1.2: More than one mdui:InformationURL with lang=en in IDPSSODescriptor.
  - SWAMID Tech 6.1.2: More than one mdui:InformationURL with lang=en in SPSSODescriptor.
  - SWAMID Tech 6.1.2: More than one ServiceName with lang=en in AttributeConsumingService (index=1).
  - SWAMID Tech 6.1.2: More than one ServiceDescription with lang=en in AttributeConsumingService (index=1).
  - SWAMID Tech 5.1.2/6.1.2: More than one OrganizationName with lang=en in Organization.
  - SWAMID Tech 5.1.3: Missing lang=en for mdui:InformationURL in IDPSSODescriptor.
  - SWAMID Tech 6.1.3: Missing lang=en for mdui:InformationURL in SPSSODescriptor.
  - SWAMID Tech 6.1.3: Missing lang=en for ServiceName in AttributeConsumingService.
  - SWAMID Tech 5.1.3/6.1.3: Missing lang=en for OrganizationName in Organization.
  - SWAMID Tech 5.1.4/6.1.4: Missing MDUI/Organization/... with lang=en.
  - SWAMID Tech 5.1.7/6.1.7: entityID MUST start with either urn:, https:// or http://.
  - SWAMID Tech 5.1.8/6.1.8: entityID MUST NOT exceed 256 characters.
  - SWAMID Tech 5.1.13: IdP:s MUST have a registered errorURL.
  - SWAMID Tech 5.1.15: IdP:s MUST have at least one Scope registered.

SWAMID

Övriga fel

- Errors
  - SWAMID Tech 5.1.16: IdP Scopes (sunet.se) MUST NOT include regular expressions.
  - SWAMID Tech 5.1.17: Missing mdui:DisplayName in IDPSSODecriptor.
  - SWAMID Tech 6.1.12: Missing mdui:DisplayName in SPSSODecriptor.
  - SWAMID Tech 5.1.9: SWAMID Identity Assurance Profile compliance MUST be registered in the assurance certification entity attribute as defined by the profiles.
  - SWAMID Tech 6.1.17: ServiceName is Required in SPSSODescriptor->AttributeConsumingService[index=1].
  - SWAMID Tech 6.1.19: RequestedAttribute is Required in SPSSODescriptor->AttributeConsumingService[index=1].
  - SWAMID Tech 5.1.20: Identity Providers there MUST have at least one signing certificate.
  - SWAMID Tech 5.1.21: All SAML endpoints MUST start with https://. Problem in IDPSSODescriptor->SingleSignOnService[Binding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST].
  - SWAMID Tech 6.1.14: Service Providers there MUST have at least one encryption certificate.
  - SWAMID Tech 6.1.15: All SAML endpoints MUST start with https://. Problem in SPSSODescriptor->SingleLogoutService[Binding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST].

SWAMID

Övriga fel

- Errors
  - SWAMID Tech 6.1.16: Binding with value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect is no allowed in SPSSODescriptor->AssertionConsumerService[index=1].
  - SWAMID Tech 5.1.22/6.1.21: Missing OrganizationName in Organization.
  - SWAMID Tech 5.1.23/6.1.22: ContactPerson [support] elements MUST have an EmailAddress element.
  - SWAMID Tech 5.1.23/6.1.22: ContactPerson [support] EmailAddress MUST start with mailto:.
  - SWAMID Tech 5.1.24/6.1.23: There MUST NOT be more than one ContactPerson element of type = support.
  - SWAMID Tech 5.1.28/6.1.27: GivenName element MUST be presenten for security ContactPerson.
  - SWAMID Tech 5.1.25/6.1.24: Missing ContactPerson of type administrative
  - SWAMID Tech 5.1.26/6.1.25: Missing ContactPerson of type technical.
  - SWAMID Tech 5.1.27: Missing ContactPerson of type support.
  - SWAMID Tech 5.1.30/6.1.29: entityID MUST NOT include RoleDescriptor elements. Have been removed.
  - SWAMID Tech 5.1.31: The Identity Provider IDPSSODescriptor element in metadata MUST NOT include any Attribute elements. Have been removed.

SWAMID

Och nu är det dags för demo...

Tack för att ni kom och lyssnade!

Nu är det är det frågestund...