Senast uppdaterad: 2022-09-26

UPPSALA UNIVERSITET

1 Teknisk konfiguration för SAML 2.0

Detta dokument beskriver hur du konfigurerar din tjänst/produkt för att använda Gemensam webbinloggning, en tjänst inom Uppsala universitet som möjliggör enkel inloggning för anställda och studenter.
Observera! Innan konfiguration sker ska förberedande steg ha genomförts för att påbörja arbetet; se checklista för mer information.
Innehållsförteckning:

Förväntningar:
Du som leverantör förväntas

- vara orienterad inom området SAML 2.0. Läs mer om SAML 2.0 här.
- ha kännedom om hur din tjänst/produkt kopplas till en IdP med SAML 2.0.

OBSERVERA: All auktorisering (behörighetshantering) och rollhantering måste ske i din tjänst/produkt. Tjänsten Gemensam webbinloggning utför ingen behörighetshantering eller rollhantering åt din tjänst/produkt.

Läs mer under Principer för autentisering och auktorisering (avsnittet Auktorisering).

2 Formella krav, regler och rekommendationer

Krav/regel/rekommendation	Förtydligande	Exempel
Alla SAML-nycklar/-certifikat du skapar i samband med att du sätter upp din SP bör ha - en **nyckellängd** om minst 4096 bitar (RSA) - en **giltighetstid** som är mycket lång (t.ex. 100 år)	För att uppfylla aktuella rekommendationer och krav samt för att slippa behöva generera om SAML-certifikaten löpande.	
Tjänstens **entityID** ska vara i **URL-format**.	Tjänstens entityID måste vara unikt och sätts vanligen till att vara en bas-URL till den del av tjänsten som hanterar SAML 2.0. Att ha en metadata-URL som entityID rekommenderas av Assertions and Protocols for the OASISSecurity Assertion Markup Language(SAML) V2.0 (avsnitt 8.3.6 Entity Identifier).	• `https://myservice.uu.se/Shibboleth.sso/Metadata` Om man använder SP-programvaran Shibboleth SP så är detta URL:en till dess metadatagenerator. • `https://myservice.uu.se/Shibboleth.sso` Om man använder SP-programvaran Shibboleth SP så är detta vanligtvis dess bas-URL. • `https://myservice.uu.se/shibboleth` Detta indikerar att URL:en har något med Shibboleth och SP-programvaran Shibboleth SP att göra. • `https://myservice.uu.se/saml` Detta indikerar att URL:en har något med SAML att göra.

Krav/regel/rekommendation	Förtydligande	Exempel
		• `https://myservice.uu.se/` Detta är en URL som är unik för tjänsten.
Det finns ansökningsprocesser till entitetskategorierna som måste följas för att tjänsten ska kunna knytas till (”taggas med”) dessa.	Det är de formellt ansvariga för tjänsten som bör kunna ta fram den information som krävs, se till att de informationssidor och liknande som behövs finns tillgängliga, och se till att alla krav för en ansökan är uppfyllda.	Se Entity Categories for Service Providers för detaljer för respektive entitetskategori.
Din SP och tjänstens metadata ska uppfylla alla krav i SWAMID SAML WebSSO Technology Profile avsnitt 6 Operational Requirements for Relying Parties.		

3 Förutsättningar

Steg	Instruktion	Rekommendation
1	**Identifiera lämplig entitetskategori** Entitetskategorin ska innehålla informationen (attributen) som behövs.	Se Entity Categories for Service Providers respektive den jämförande översikten Entity Category attribute release in SWAMID och välj en av dessa. För tjänster som inte behöver personnummer duger oftast REFEDS Research & Scholarship. För tjänster som behöver personnummer krävs GÉANT Data Protection Code of Conduct.
2	**Kontrollera att tjänstens syfte överensstämmer med syftet för entitetskategorin**	Mer information om syftet för några av de tillgängliga entitetskategorierna finns på följande sidor:

Steg	Instruktion	Rekommendation
	Om t.ex. tjänsten inte helt eller delvis används för att genomföra studier eller forskning så kan inte REFEDS Research & Scholarship användas.	• REFEDS Research & Scholarship (samarbetsverktyg för att genomföra studier och forskning; se Definition) • GÉANT Data Protection Code of Conduct (god, korrekt, kontrollerad, säker och minimerad hantering av personuppgifter)
3	**Ta reda på ifall tjänsten behöver få användar-ID skickad till sig via s k SAML2 Persistent NameID istället för via ”vanligt” attribut** Många tjänster använder sig av denna teknik eftersom det är ett mer standardiserat sätt att överföra just användar-ID.	

4 Uppsättning och konfiguration

Steg	Instruktion	Vägledning och exempel
1	**Skapa en Service Provider (SP) för tjänsten** Installera och konfigurera programvara som kan hantera SAML 2.0 för tjänsten. Om tjänsten har inbyggt stöd för SAML 2.0 så är det snarare konfiguration i tjänstens administrationsgränssnitt som du behöver utföra.	Se SAML SP Best Current Practice för vägledning.
2	**Använd en specifik inloggningsserver (IdP) eller val av lärosäte (DS) i tjänstens SP** Om IdP:	Se Discovery Service Integration för mer information.

Steg	Instruktion	Vägledning och exempel
	entityID: `https://weblogin.uu.se/idp/shibboleth` Om DS: discoveryURL: `https://service.seamlessaccess.org/ds/`	
Alternativ 3 a URL	**Ladda metadata för IdP via URL** För att din SP ska veta hur den ska kommunicera med (eller tolka data från) IdP:n – antingen den IdP du valt eller som användaren valt vid val av lärosäte (DS) – behöver den ha tillgång till metadata för IdP:n. Signeringscertifikat används för validering av IdP-metadata. Om standard: IdP-metadata: `http://mds.swamid.se/md/swamid-idp.xml` Signeringscertifikat: `http://mds.swamid.se/md/md-signer2.crt` Här förutsätter vi att IdP:n tillhör en organisation som är medlem i identitetsfederationen SWAMID, vilket är fallet med tjänsten Gemensam webbinloggning vid Uppsala universitet. Om undantag: IdP-metadata: `https://weblogin.uu.se/idp/shibboleth` Signeringscertifikat: `https://weblogin.uu.se/md/uu-signer.crt` Detta alternativ bör endast användas ifall minnesbegränsningar eller begränsningar i parsningen av metadata gör att standardalternativet inte kan användas.	
Alternativ 3 b	**Ladda metadata för IdP via statisk data**	SSO = Single Sign On = inloggning SLO = Single Log Out = utloggning

Steg	Instruktion	Vägledning och exempel
Statisk data	Om din SP inte stödjer att ladda IdP-metadata från en URL (se alternativ 3 a), t.ex. om du endast kan ange ”statiska” uppgifter i ett administrationsgränssnitt eller liknande. Notera att följande statiska strängar är specifika för tjänsten Gemensam webbinloggning. Signeringscertifikat för SAML-meddelanden: `MIIDJDCCAgygAwIBAgIVAMAqC57ZiqOY9LvU7W7YjaZ2U8GtMA0GCSqGSIb3DQEB CwUAMBkxFzAVBgNVBAMMDndlYmxvZ2luLnV1LnNlMB4XDTE2MDcxMDIwNDgxNloX DTI2MDcxMDIwNDgxNlowGTEXMBUGA1UEAwwOd2VibG9naW4udXUuc2UwggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXwo9+t6G/fp7dFcap5s8vygdIGWEx h7zDfKW43aSXBlT3hQXmyUNR8E1wynpswZz9OG57vklte6BwCpj6/+o/T4S6DDrz E80YKwF08Y9JMoyXB6YWk5awu4BBU1k1QDyz6wy+o27NK+dS07ZaEhbiFxZjgjkM UQSE1qBeOTX91uyp/Oud3VpyV31AbAN9Wcw33HvoRSeIy3njq3XBmW5Xbuae8SSY BDqR+M6Fu+YSk04EblIcl0zFtBDh6N9U+OCR+G8YsZvyUfs8WSx1Y4uOxygxOGgZ /f2Raiq8WuE8uy4o2UQL7NqJ9PyhTTk+94HsxT0haLOrS/MNI1l5Zw9XAgMBAAGj YzBhMB0GA1UdDgQWBBROpn9mvA5O1XugKjgnthIFsRwCBzBABgNVHREEOTA3gg53 ZWJsb2dpbi51dS5zZYYlaHR0cHM6Ly93ZWJsb2dpbi51dS5zZS9pZHAvc2hpYmJv bGV0aDANBgkqhkiG9w0BAQsFAAOCAQEAXR4BLVIAwqZTzz3iwjGskMw2WzfBQ/nG l3rjpj5tpayQ1NrEbidLiyUQD4m9PBS/zTsxIB9TJ5r/Ye3jf39+9plG51tQALUq Psz27W4CGdEe0CBeiGTJ0gnlSVNqezXsRzk+EXTkzQbQ4sov9eWeWe9c/5Cbyf6l wRUoSoZ5j0Lo9+03ZiNBBD2PRpfyrXjXuIEw5xDeE2YR/2W++3J79hWjydJPlzl/ K0lTdUS/JfVbNpxufJxPp/R1iLjU4hypLi+N3fh4xh0HOdLskIV+xCPzwn6uLsPG AbrZzItGWOuUunKpQBejEO5F+q+z1dU41x2m4oONHzdQ+3IX75GUEg==`  Krypteringscertifikat för SAML-meddelanden:  `MIIDIzCCAgugAwIBAgIUU/H0eVODSSmZoDRn6Lz3GR/1kzMwDQYJKoZIhvcNAQEL BQAwGTEXMBUGA1UEAwwOd2VibG9naW4udXUuc2UwHhcNMTYwNzEwMjEwNDMzWhcN MjYwNzEwMjEwNDMzWjAZMRcwFQYDVQQDDA53ZWJsb2dpbi51dS5zZTCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKvjMIOzZJS4B6CpNZ2aAcMlHDPloeGm cmiAIoC5odr2b1qutyj2X1k0TnlEGLVnQMbgsIZR0qz0/0Dd0RL15+SnNswBB5wa ShHiTkkZATaFaed2kmO9DDXV7m3dxgF8a3DWaSWF12jNiGwxmvCIeEmQUsSVY52r uoKbv04q+vQB2aJPTdKGzrSqGxZw6pWPjZotiuT/Hn6aWVfSeya6OTgtOgybsWsn a4A/ncMhj8tl5lnpQGxWwJWFBQm9T3mEDrzgJND4E+ZxdFmrUZGFSRmkWe+ma9Ii`  `AbrZzItGWOuUunKpQBejEO5F+q+z1dU41x2m4oONHzdQ+3IX75GUEg==`	

Steg	Instruktion	Vägledning och exempel

	`Y1z1IXNedOZMshrMelD9UMEnc3ZCZJCeWfsdpe6ecZU+T4l5kWuALqkCAwEAAaNj`
	`MGEwHQYDVR0OBBYEFM3QZFFxSaebrz860E57FdtWScA7MEAGA1UdEQQ5MDeCDndl`
	`YmxvZ2luLnV1LnNlhiVodHRwczovL3dlYmxvZ2luLnV1LnNlL2lkcC9zaGliYm9s`
	`ZXRoMA0GCSqGSIb3DQEBCwUAA4IBAQCXHAy+YMui0rPK83sEU2MEYvrD7ehI0Wff`
	`EcrQCroT1i2x2ajBkQ/4TVge2F9KHgiiKfgEG8saqdgTgwq3wP6UPGTMwgdMIlAX`
	`AN16kAibmTOZ4Kx+yqy+roFj919i9uPI998TlXJG85LpjqsX+gDoVzKw68F2fw8W`
	`Vgl9zHmoBnf765evetN8aJkQ/t2nNkqHiV83LXQ80fdtu52T2lkb6GM9nXN81jNt`
	`OiJ3wNKvx2hkOJqEs+p9ESI8IiNxjPyjdk5V9VlIl65W0WO1WfrT0qur5NhdZsl+`
	`nQPiHsyW3apD4+IJzI2nGQfeL4XO6MPUPVvn+7TiduFaCe+TXJQW`
	
	URL:er för SAML-meddelanden:
	
	SSO:
	HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SSO`
	
	HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SSO`
	
	SLO:
	HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SLO`
	
	HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SLO`
	
	Vilken variant av URL du ska använda beror på vad din SP stödjer, men HTTP POST är vanligast.	

4 Om MFA krävs	**Lägg till multifaktorautentisering (MFA)** Tjänsten Gemensam webbinloggning stödjer i dagsläget multifaktorautentisering enligt två olika standarder: • FIDO U2F, med av Uppsala universitet utdelade och hanterade Yubico YubiKey-USB-nycklar. Dessa knyts till användaren i Uppsala universitets behörighetssystem AKKA enligt särskilda rutiner.	Se t.ex. How do I actually use the REFEDS MFA Profile to request MFA?, Requiring Multi-Factor Authentication, Configure a Service Provider for Two-Factor Authentication och Multi-Factor Access för närmare information och SP-konfigurationsexempel.

Steg	Instruktion	Vägledning och exempel

	• TOTP, där man använder en app i sin smarta telefon eller surfplatta för att få fram tidsbaserade engångskoder. Användare aktiverar själva möjligheten att kunna nyttja TOTP på kontowebben.
	
	Det är i normalfallet tjänstens SP som ska indikera att multifaktorautentisering krävs och med vilken teknik.
	
	Viktigt:
	
	• att tjänstens SP endast anger **en** önskad teknik för multifaktorautentisering i inloggningsbegäranden! Tjänsten Gemensam webbinloggning har i dagsläget ingen möjlighet att veta vilken eller vilka tekniker som stöds för en given användare.
	
	• att tjänstens SP **verifierar** att multifaktorautentisering utfördes och med rätt teknik! Se `require authnContextClassRef` i exemplen.
	
	• att tjänstens SP **förhindrar manipulering** av inloggningsbegäranden så att inte kravet på multifaktorautentisering kan kringgås!
	Slå på signering av inloggningsbegäranden i tjänstens SP och lägg till `<SPSSODescriptor AuthnRequestsSigned="true" ...>` i tjänstens metadata. Då kräver tjänsten Gemensam webbinloggning att alla inloggningsbegäranden signeras av tjänstens SP.
		För FIDO U2F heter autentiseringsklassen (AuthnContextClassRef):
		`https://refeds.org/profile/mfa`
		
		För TOTP heter autentiseringsklassen (AuthnContextClassRef):
		`urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken`

5 Metadata

Steg	Instruktion	Vägledning och exempel
1	**Skapa metadata i XML-format**	Exempel på hur metadata ser ut för *andra* tjänster kan du finna på https://metadata.swamid.se/.

Steg	Instruktion	Vägledning och exempel
	Den mest grundläggande delen av detta är rent tekniska detaljer såsom tjänstens unika ID (entityID), nycklar (för signering och ev kryptering av SAML-meddelanden) och URL:er (SAML endpoints). Oftast kan SP-programvaran användas för att generera dessa metadata. Se dokumentationen för SP-programvaran för detaljer.	Välj någon tjänst och sedan `Show XML` eller `Download XML` och titta på filen med något lämpligt textvisningsprogram. Detta kan också vara till hjälp för att se om du verkar ha ”missat” något i metadata för din tjänst jämfört med andra.
2	**Komplettera med användarinformation** Komplettera med information som visas för användaren i samband med inloggning, s k MDUI-information. Det kan t.ex. gälla formella krav, tjänstens användning och hantering av personuppgifter.	Se SWAMID SAML WebSSO Technology Profile (avsnitt 6.1.12–6.1.13 Metadata Extensions for Login and Discovery User Interface (MDUI)) för de formella kraven. Se Service Provider Metadata Extensions for Login and Discovery User Interface (MDUI) för exempel. Se Service Provider Privacy Policy Template för lämplig mall att använda för sidan om tjänstens användning och hantering av personuppgifter.
3	**Komplettera med kontaktinformation** Kontaktinformation behövs så att ansvariga kan nås.	Se SWAMID SAML WebSSO Technology Profile (avsnitt 6.1.21 Organization samt 6.1.22–6.1.27 ContactPerson*)* för de formella kraven. Se Contact and Organization information for Service providers för exempel.
4 Om DS	**Komplettera med speciell tag för DS** Vid val av lärosäte (DS) måste du komplettera tjänstens metadata med en `<DiscoveryResponse>`-tagg innanför `<SPSSODescriptor>`-taggens `<Extensions>`-tagg.	Se Identity Provider Discovery Service Protocol and Profile (avsnittet Use of Metadata*)*, för information om denna säkerhetsdetalj. Se Enabling OpenAthens Wayfinder: Shibboleth för illustrerande exempel hur konfigurationen kan göras. Se Redirect to SSO Service at the IdP för allmän information om hur webbflödet går vid val av lärosäte (DS).

Steg	Instruktion	Vägledning och exempel
	Detta är en säkerhetsdetalj för att undvika att godtyckliga webbsidor ska kunna missbruka val av lärosäte och lura till sig användaren efter inloggning. I princip styr detta vilken webbadress som användaren tillåts omdirigeras till efter inloggning, och därmed vart inloggningsinformationen tillåts skickas.	
5 Om SAML2 Persistent NameID används	**Ange NameID-format** Om tjänsten använder SAML2 Persistent NameID för överföring av användar-ID så ska NameID-formatet `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` anges i tjänstens metadata eller i inloggningsbegäran. **OBS!** Det är **mycket viktigt** att NameID-formatet `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` **inte** finns listat som ett tillgängligt alternativ i tjänstens metadata. Annars ignoreras **alla** NameID-format i metadata och NameID riskerar att inte skickas överhuvudtaget. **Du behöver meddela oss** ifall tjänsten behöver användarens faktiska användar-ID (t ex abcd1234@user.uu.se) eller värdet av något	

Steg	Instruktion	Vägledning och exempel
	annat SAML-attribut skickat som SAML2 Persistent NameID. I annat fall skickas som standard en anonymiserad variant av användarens användar-ID.	

6 Publicering av metadata

Steg	Instruktion	Fördjupad information
1	**Verifiera metadata innan publicering** Kontrollera att din SP och tjänstens metadata uppfyller alla krav i SWAMID SAML WebSSO Technology Profile (avsnitt 6 Operational Requirements for Relying Parties*)*.	
2	**Skicka in tjänstens metadata till SWAMID för publicering** Metadata ska publiceras antingen i metadataströmmen `SWAMID` (IdP) eller `SWAMID and eduGAIN` (DS). Från och med januari 2022 gör man i regel detta själv (se blogginlägg) via SWAMID:s metadataverktyg. Inloggning i metadataverktyget görs här med konto från någon organisation som är ansluten till SeamlessAccess via eduGAIN. **OBS!** När man begärt publicering av metadata inifrån metadataverktyget så får man ett e-postmeddelande som man manuellt måste vidarebefordra till SWAMID Operations för att publiceringen ska utföras.	För närmare information om metadataverktyget och dess användning, vänligen kontakta SWAMID.
3	**Klart! Din tjänst är nu redo att använda tjänsten Gemensam webbinloggning**	

Steg	Instruktion	Fördjupad information
	OBS! Det är inte förrän metadata är publicerade (plus en viss tidsfördröjning, upp till 8 timmar) som Gemensam webbinloggning får kännedom om din tjänst och kan användas för att logga in i denna.	

Har du frågor? Kontakta IT-support och be om kontakt med driftansvariga för tjänsten Gemensam webbinloggning.