Högskolan i Gävle
Mona Åkerman

2016-05-23
Version 1

HÖGSKOLAN
I GÄVLE

Identity and Management Practice Statement

Högskolan i Gävle

Innehållsförteckning

1 Inledning ... 3
2 Elektroniska identiteter ... 3
LoA1 - obekräftad användare ... 3
LoA2 - bekräftad användare ... 3
LoA3 - kontrollerad användare ... 3
LoA4 - verifierad användare ... 3
AL1 - obekräftad användare ... 3
3 Compliance and Audit ... 4
4 Organisational Requirement ... 4
4.1 Lärosätets/myndighetens/stiftelsens organisationsnummer ... 4
4.2 Notices and User Information ... 5
4.3 Secure Communications ... 5
4.4 Security-relevant Event (Audit) Records ... 5
5 Operational Requirements ... 6
5.1 Credential Operating Environment ... 6
5.2 Credential Issuing ... 6
5.3 Credential Renewal and Re-issuing ... 8
5.4 Credential Revocation ... 8
5.5 Credential Status Management ... 8
5.6 Credential Validation/Authentication ... 8

1 Inledning

Dokumentet beskriver de olika typer av elektroniska identiteter som finns i katalogtjänsten vid Högskolan i Gävle. Dokumentets syfte är att

- kortfattat beskriva högskolans identitetstyper
- utgöra underlag för högskolans medlemskap i Swedish Academic Identity Federation – nedan kallad SWAMID
- definiera identitetstypernas förtroendenivå enligt NIST 1, OMB M-04-042 samt SWAMID Identity Assurance Level 1 Profile (AL1)3

SWAMIDs AL1-profil ersätter SWAMID 2.0 från och med december 2014 och är baserad på Kantaras Identity Assurance Framework version 3.0 som anpassar ramverket till europiska förutsättningar. SWAMID AL1-profilen är som helhet inte översättningsbar enligt LoA1 som den beskrivs i NIST SP 800-63-1 eftersom AL1 ställer högre krav på IdM-processer samt infrastruktur.

2 Elektroniska identiteter

Den gemensamma katalogtjänst vid HiG via vilken användare till de gemensamma systemen autentiserar sig utgörs av en Lightweight Directory Access Protocol (LDAP)-katalog på katalogtjänstmiljön Open LDAP. Till denna katalogtjänst finns även ett Active Directory (AD) som ett gränssnitt för de system som inte autentiserar via LDAP. Samtliga konton och delar av kontoinformationen replikeras från LDAP till AD. Autentisering mot katalogtjänsten sker krypterat.

LoA1 - obekräftad användare

LoA1 innebär att det finns liten eller ingen möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Exempel på elektroniska identiteter av typen LoA1 är Windows Live-konto och Google-konto.

LoA2 - bekräftad användare

LoA2 innebär att det finns rimlig möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Vem som ursprungligen tar emot identiteten fastställs genom att identiteten styrks vid utlämnade av identitetsinformation eller att identitetsinformationen skickas till en postadress – till exempel folkbokföringsadressen eller arbetsplatsens adress – där det är sannolikhet att den person som identitetsinformationen tillhör även är den person som ta del av den informationen.

LoA3 - kontrollerad användare

LoA3 innebär att det finns god möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Detta säkerställs via kontroll av giltig identitetshandling vid utlämnade av identitetsinformation. Med giltig identitetshandling menas nationellt identitetskort, pass, körkort, SIS-godkänt identitetskort och e-legitimation.

LoA4 - verifierad användare

LoA4 innebär att det finns mycket god möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Med avseende på att detta PM är begränsat till identitetsutgivande är det ingen skillnad mellan LoA3 och LoA4 förutom att e-legitimation inte får användas.

AL1 - obekräftad användare

AL1 innebär att det finns liten eller ingen möjlighet att fastställa vem som innehar en

elektronisk identitet, d.v.s. samma som för LoA1. Skillnaden mellan AL1 och LoA1 är att vi för AL1 är säkra på att den som innehar den elektroniska identiteten är en fysik person.

Ansvarsförbindelse innehåller dels regler för kontot samt användarnamn, lösenord och en del för signatur som skall returneras.
Kontohanteringssystemet sköter automatiskt förändringar av LoA-nivåerna.

[1] NIST Special Publication 800-63-1, Electronic Authentication Guideline, december 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[2] Executive Office of the President, Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, 16 december 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
[3] SWAMID, https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance+Level+1+Profile

3 Compliance and Audit

Revision av rutiner angivna i detta dokument, sker senast inom 12 månader från senaste revisionstidpunkt.

4 Organisational Requirement

4.1 Lärosätets/myndighetens/stiftelsens organisationsnummer

Högskolan i Gävle organisationsnummer 202100-2890 är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.1 Tillämpbara lagrum

De viktigaste lagarna och förordningarna som styr högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100). Regleringsbrevet utställs årligen av regeringen och styr högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.
Lärosätets katalog- och behörighetssystem LDAP innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Personuppgiftslagen (SFS 1998:204) och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.
Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i kontohanteringssystemet.
Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).

4.1.2 Rutiner för destruering av lagringsmedia

Rutin beslutad av avdelningen för infrastruktur 2015-12-02 ”Hantering av kasserade diskar med klassad information”.

4.2 Notices and User Information

4.2.1 Användarvillkor

Användarvillkor finns publicerad på vår webb http://www.hig.se/it/ansvarforbindelse

4.2.2 Godkännande

Användarna godkänner användarvillkoren i samband med att de hämtar ut sitt konto eller i samband med att de byter sitt lösenord.

4.2.3 Ny ansvarsförbindelse

När högskolan beslutar om att ge ut en ny version av ansvarsförbindelsen, hanteras det genom att ansvarsförbindelsen skall godkännas vid nästa lösenordbyte som inträffar senast inom 365 dagar

4.2.4 Loggning av ansvarsförbindelsen

Ett godkännande av ansvarsförbindelsen loggas i vårt kontohanteringssystem.

4.2.5 Service definition

Service definition finns publicerad på vår webb
http://www.hig.se/Ext/Sv/Organisation/Hogskolans-gemensam-administration/Avdelningen-for-infrastruktur/IT/Dokument/Service-Definition.html
Privacy policy finns publicerad på vår webb http://www.hig.se/privacy_policy

4.3 Secure Communications

4.3.1 IT-personal med teknisk åtkomst

IT personal med teknisk åtkomst till de servrar och datamedia där lösenord lagras undertecknar även särskild ansvarsförbindelse. Ansvarsförbindelse för medarbetare med dessa priviligierade behörigheter finns i vårt diarium.

4.3.2 Privata nycklar mm

Privata nycklar och hemligheter skyddas med behörighetskontroll i filsystem och serveraccess.

4.3.3 Kryptering

All nätverkskommunikation skyddas med användning av TLS eller motsvarande kryptering

4.3.4 Entity keys

Alla entity keys är 2048 bitar RSA

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser
Alla förändringar på ett datorkonto loggas.

5 Operational Requirements

5.1 Credential Operating Environment

5.1.1 Lösenord
Lösenord måste vara minst 8 tecken långa och innehålla minst en gemen (liten bokstav och en versal (stor bokstav) och minst en siffra, det innebär ca 24-bitars entropi. Lösenorden kan ej återanvändas vid lösenordsbyte.

5.1.2 Tekniska protokoll
Tekniska protokoll All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat såsom beskrivet under rubriken SWAMID AL1 4.3.3 – 4.3.4. TLSv1 och SSLv3 har inbyggda skydd mot återspelningsattacker (eng. message replay). Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering. Högskolan synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

5.1.3 Skydd mot missbruk
Rutiner för skydd mot missbruk Se SWAMID AL1 4.3.3 ovan.

5.1.4 Personligt ansvar
I högskolans ansvarsförbindelse framgår att kontoinnehavarana är personligt ansvariga för användningen av användarkontot och att det inte får göras tillgängligt för andra. Användarna godkänner detta regelverk innan de använder kontot första gången samt när de gör en lösenordsåterställning.

5.1.5 Konfiguration
Alla servrar som används för kontohantering, webbinloggning och eduroam är uppsatta och konfigurerade så att de endast är tillgängliga på avsedda tjänsteprotokoll såsom Kerberos, LDAPS, HTTPS, radius med flera för reglerade IP-adresser med hjälp av brandvägg. Vid avdelningen för IT-service finns ansvar för att hålla servrar och annan hårdvara uppdaterade med avseende på säkerhetsproblem.

5.2 Credential Issuing

5.2.1 Identitetshanterarens DNS-domän
Den administrativa DNS-domänen hig.se används alltid vid attributrelease till det system där användare vill logga in. Detta oberoende om det är SAML2 eller eduroam.

5.2.2 Hanteringen av användarnamn/konton
Samtliga identitetsservrar vid Högskolan i Gävle använder unika identifierare.

5.2.3 Unik användaridentitet

En användaridentitet används bara för en enda person och återanvändas inte för någon annan person. Motsvarande gäller även för olika typer av funktionsanvändare men dessa är inte aktuella för användning inom SWAMID.

5.2.4 Flera användaridentiteter

Om en användare har mer än ett användarkonto, dvs. är både student och anställd, väljer användaren vid inloggning vilket användarkonto denna ska använda vid det aktuella tillfället.

5.2.5 Identifieringsmetoder

Personal

När en anställd börjar arbeta vid högskolan beställer administrativt ansvarig vid respektive organisation vid högskolan ett användarkonto via ett formulär på vårt intranät. När handläggare vid IT tar emot begäran skapar handläggaren ett användarkonto för den nyanställde. Kontouppgifterna hämtas av individen hos IT-supporten. Vid uthämtandet krävs godkännande av ansvarsförbindelsen och uppvisande av giltig legitimation. I det fall en anställd inte kan besöka IT-supporten personligen kan den anställde göra en lösenordsåterställning alternativt få en blankett skickad till sin folkbokföringsadress. Kommer den underskrivna blanketten inte i retur inom 20 dagar deaktiveras datorkontot.

Studenter

Antagna studenter går till en webbsida där de väljer att fylla i persondata och en captcha, alternativt använder EduID. De får då ett konto skapat och användarnamn och lösenord på webben direkt. Om registrering i LADOK inte sker inom 85 dagar så deaktiveras kontot.
LoA1 och AL1 konton har ej tillgång till eduroam.
Konton som hämtas ut mot uppvisande av legitimation i IT-supporten blir med automatik uppgraderade till LoA3.
Kan studenten inte personligen uppsöka IT-support skickas en aktiveringskod via vanligt brev till folkbokföringsadressen. LoA2 konto erhålls när studenten skriver in personnummer, användarnamn samt aktiveringskod på därför avsedd webbsida.
Utökade konton (LoA2, LoA3 och AL2) har tillgång till samtliga federationer.

5.2.6 Förändring av AL nivåer

Inte aktuellt för AL1

5.2.7 Ändring av självuppgiven information

Studenter ändrar den personinformation som inte hämtas från folkbokföringen i Ladok genom vår studentportal.
Anställda uppdaterar sin personinformation genom att fylla i ett formulär på vårt intranät som sedan skicka till berörda avdelningar som uppdaterar informationen i högskolans olika IT-system.

5.2.8 Krav på identitetsgranskningen

Vid högskolan i Gävle är all personal som hanterar användaridentiteter verifierade med LoA3-nivå.

5.3 Credential Renewal and Re-issuing

5.3.1 Möjlighet till lösenordsbyte

Alla användare kan byta sitt lösenord genom en webbsida som kräver inloggning.

5.3.2 Lösenordsbyte

När användaren gör lösenordsbyte på detta sätt anges först det gamla lösenordet innan man anger det nya två gånger. Det nya lösenordet måste uppfylla kraven i SWAMID AL1 5.1.1 ovan. Krav SWAMID AL1 5.3.3

5.3.3 Lösenordsåterställning

Lösenordsåterställning för tillitsnivå AL1 sker via en webbsida med angivande av persondata Förutom personadata används Captcha för att säkerställa att det är en människa som återställer lösenordet.. Lösenordsåterställning för tillitsnivå AL2 sker via en webbsida med verifiering via EduID, bekräftad användare.

5.4 Credential Revocation

5.4.1 Inaktivering av användarkonton

Samtliga konton kan deaktiveras för användning

5.4.2 Återaktivering av användarkonton

Se 5.3.3

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

HiG loggar alla lösenordsförändringar

5.5.2 Tillgängligheten för identitetstjänsten

Inloggningsservern för SAML2 och inloggningsservern för eduroam har en erfarenhetsmässigt högre tillgänglighet än 95%.

5.6 Credential Validation/Authentication

5.6.1 Validering av rättigheter

Både SAML2- och radiusinstallationerna uppfyller dessa krav eftersom protokollen är konfigurerade enligt instruktioner från SWAMID och eduroam.org.

5.6.2 Autentisering av inaktiva konton

När en användare byter lösenord tas det gamla lösenordet bort ur Active Directory och ersätts med det nya. Därmed kan det gamla lösenordet inte användas för inloggning. Då kontot stängs av deaktiveras kontot i Active Directory och kontot flyttas i huvudkatalogen så att autentisering inte kan göras. Konton för studenter stängs av per automatik när de inte längre studerar vid lärosätet.

När en anställd avslutar sin tidsbegränsade anställning vid Högskolan stängs kontot av direkt. Anställda med tills vidare anställning meddelar organisationen att kontot ska stängas.

5.6.3 Autentisering vid inloggning

SAML2-baserad webbinloggning och eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Webbinloggning har en SSO-funktionalitet som aktiveras efter att användaren loggat in. Eduroam har ingen sådan men användaren kan oftast spara sina inloggningsuppgifter i den klientprogramvara som finns för eduroam

5.6.4 Sessionstider

SAML2-baserad webbinloggning och eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Webbinloggning har en SSO-funktionalitet som aktiveras efter att användaren loggat in. Eduroam har ingen sådan men användaren kan oftast spara sina inloggningsuppgifter i den klientprogramvara som finns för eduroamFör SAML2-baserad webbinloggning uppfyller Högskolan kraven med att den maximala längden för SSO-sessionen är tolv timmar. Den maximala giltighetstiden från att användaren gör inloggningen, eller använder SSO-sessionen, tills att tjänsten släpper in användaren i tjänsten är fem minuter. För eduroam finns ingen SSO-session för inloggning utan där finns en maxtid för hur lång tid en klient får på sig för att genomföra inloggningen. Denna maxgräns är mindre än en minut.