



SWAMID Identity Management Practice Statement

Röda Korsets Högskola 2022

Gällande version från 2022-11-01

SWAMID Identity Management Practice Statement av Röda Korsets Högskola

Kontaktperson	Maria Johansson
Telefonnummer	08-587 516 03
E-post	maria.johansson@rkh.se
Årtal för Statement	2022



Innehållsförteckning

1. Inledning.....	3
4. Organisational Requirement	3
4.1 Enterprise and Service Maturity	3
4.1.1 Rutiner för destruering av lagringsmedia	4
4.2 Notices and User Information.....	4
4.2.1 – 4.2.4.....	4
4.2.5.....	4
4.3 Secure Communications	5
4.4 Security-relevant Event (Audit) Records.....	5
5. Operational Requirements.....	5
5.1 Credential Operating Environment.....	5
5.1.1 – 5.1.2.....	5
5.1.3 – 5.1.4.....	6
5.2 Credential Issuing.....	6
5.2.1 – 5.2.2.....	6
5.2.3 – 5.2.4.....	6
5.2.5	6
5.2.6	7
5.2.7	7
5.2.8	7
5.3 Credential Renewal and Re-issuing.....	7
5.3.1	
5.3.3	7
5.4 Credential Revocation.....	8
5.4.1	8
5.4.2	8
5.4.3	8
5.5 Credential Status Management	8
5.5.1	8
5.5.2	8
5.6 Credential Validation/Authentication	9



1. Inledning

Röda Korsets Högskola (benämnt vidare som "RKH"), är en enskild högskola. RKH är medlem i Sunet och nyttjar dess tjänster samt är även medlem i identitetsfederationen SWAMID.

RKH har idag många rutiner på plats som följer AL2 eller högre tillitsnivå. RKH ansöker härmed om, och avser bli godkänd för tillitsnivå AL2.

4. Organisational Requirement

The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

Röda Korsets Högskola, organisationsnummer [802002-8695], är en enskild utbildningsanordnare som styrs av Stiftelsen Rödakorshemmet, vars huvudman är Svenska Röda Korset. Detta gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), högskolelagen (SFS1992:1434), högskoleförordningen (1993:100) och Lag (1993:792) om tillstånd att utfärda vissa examina. Regleringsbrevet utställs årligen av regeringen och styr högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets identitets- och behörighetssystem Microsoft Active Directory 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 enligt aktuell personuppgiftslagstiftning.

Som enskilt lärosäte arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.



4.1.3 Rutiner för destruering av lagringsmedia

All lagringsmedia som avser kasseras gör så med leverantörer för återvinning av elektroniskt material. Vald leverantörs rutiner kontrolleras så att lagringsmedia nollställs enligt väl genomtänkta rutiner (t.ex. genom flertalet överskrivningar) eller att dessa kasseras på ett sådant sätt att dessa media blir permanent obrukbara.

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

4.2.1 – 4.2.4

RKH har idag användarvillkor för både medarbetare samt studenter (se bilagor).

Studenterna kan se användarvillkoren när de vill, de finns publicerade på lärplattformen Canvas. Medarbetarna kan se användarvillkoren när de vill, de finns publicerade på RKH:s intranät, Medarbetarportalen.

För anställda sker ID-kontroll vid start av anställning innan processen går vidare. Godkännande av användarvillkor sker via en e-portal varvid den anställda tilldelas sitt användarkonto. Användarvillkoren finns även tillgängliga på vår medarbetarportal.

Studenter får och godkänner användarvillkoren när de kvitterar ut sitt konto. Användarvillkoren finns även på vår lärplattform.

Vid uppdatering eller förändring av användarvillkor informeras och signerar personalen via utskick som ska undertecknas via Verified e-signering. Studenterna informeras via e-post.

Arkivering för personalgodkännande sker i Verified. Studenterna godkänner inte aktivt men de informeras aktivt om förändring via e-post.

4.2.5

Tjänstedefinition finns specificerat på <https://rkh.se/tjanstedefinition>

Information om behandling av personlig information: <https://rkh.se/gdpr>



4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

Endast behörig personal och behöriga konsulter har åtkomst till ADFS och SAML2. Kontroll sker via ordinarie åtkomstkontroll i operativsystem och applikationer.

RKH använder Microsoft Active Directory för all kontohantering. Tillsammans med en struktur baserad på ADFS och SAML2 gör det att informationen är säkrad vad gäller klartext. Radius används primärt som autentiseringsprotokoll som är krypterad enligt certifikat med EAP-MSCHAPv2.

RKH IT tillsammans med systemägare säkerställer att HTTPS används som standard i övriga lösningar som kommunicerar med vår interna miljö. De fristående system vi nyttjar ska följa samma standard.

Certifikat för kryptering och signering i ADFS är minst 2048 bitar RSA.

4.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

Inom kontohanteringen så loggas allt per standard enligt Active Directory samt Azure Active Directory. Microsoft för också loggning per standard vad gäller kontoobjekt.

Enligt Microsoftstandard sker också loggning på event för mail och filhantering inom dessa plattformar som raderas efter 90 dagar, men avsikten är att ändra till minst 180 dagar.

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.



5.1.1

RKH använder sig av rekommenderad standard från Microsoft vad gäller lösenordspolicy (minst 10 tecken, måste innehålla både gemener och versaler, måste innehålla specialtecken eller siffror). Användarnamn plus lösenord används.

5.1.2

Standardprotokoll som används: SSL/TLS, SHA 256 kryptering

Vi konfigurerar ADFS och SAML2 enligt de rekommendationer som SWAMID ger.

5.1.3 – 5.1.4

I användarvillkoren anges att lösenord eller kontouppgifter ej får spridas.

Konton låses automatiskt ner vid 10 felaktiga försök att logga in.

Brandvägg hanterar all datatrafik. För epost använder vi Microsoft Defender och vi har DKIM, DMARC och SPF påslaget. Alla säkerhetsuppdateringar installeras alltid.

5.2 Credential issuing

5.2.1 – 5.2.2

DNS-domänen rkh.se används för inläsning av attribut så som eduPersonPrincipalName med mera. ADFS använder EntityID som unik identifierar för varje tjänst som konfigureras. Vi använder DNS records för att identifiera radius-servrar till eduroam i domänen.

5.2.3 – 5.2.4

Alla konton skapas unikt och återanvänds inte. Samtliga studenter mottar unika konton då dessa skapas med hänsyn till vilken termin dessa börjar och "UserPrincipleName" sätts därefter. Anställda mottar unika konton där "UserPrincipleName" aldrig är samma. Användare har inte flera konton idag. Om en anställd blir student eller vice versa så kommer den personen ha två konton.

5.2.5

Identifieringsmetod vid utdelande av kontouppgifter för personal är fysisk ID-kontroll. För studenterna sker också fysisk ID-kontroll vid utdelande av kontouppgifter. RKH godtar giltig Svensk ID-handling för personal och student. Med giltig legitimationshandling menas: ett pass eller identitetskort som uppfyller Polisens krav: "Giltiga id-handlingar när du



ansöker om pass eller nationellt id-kort", ett pass som uppfyller ICAO Doc 9303 eller ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordning 562/2006.

Vid utdelande av kontouppgifter, vilket sker fysiskt, delas lösenord ut som måste ändras efter första inloggning.

Resulterande tillitsnivå blir AL2 för både personal och studenter.

Förregistrerade identifierare för personal är namn och personnummer. Uppgifterna är verifierade genom en signering via en elektronisk signeringstjänst. Detta kontrolleras genom fysisk identifiering med ID-kontroll vid kontoutlämning. För studenter hämtas förregistrerade uppgifter som namn och personnummer och eventuellt T-nummer från Ladok. Vid kontoutlämning sker fysisk identifiering vid ID-kontroll.

Personal eller student utan svenskt personnummer kontrolleras fysiskt mot utländsk ID-handling, tex pass. Här görs en riskbaserad bedömning baserad på foto, namn och födelsedata och eventuellt T-nummer.

5.2.6

Alla användare uppfyller idag AL1 vid anställning eller start av studier. Möjlighet att hantera olika tillitsnivåer styrs via gruppstillhörighet. Förberedelser för att signalera att en användare uppfyller kraven för tillitsnivå AL2 är förberett på både teknisk och administrativ nivå så att när vi blir godkända för AL2 kan signalera rätt tillitsnivå.

5.2.7

Anmälan om ändring av självuppgiven information kan göras av enskild. Anmälan görs till HR eller Utbildningsadministrationen (personal/student). Studenter har möjlighet att ändra e-post i Ladok och ändring av personuppgifter görs genom anmälan till skattemyndigheten varifrån Ladok i sin tur hämtar de nya uppgifterna.

Ansvarig, HR/Utbildningsadministrationen, meddelar IT som utför eventuellt nödvändiga förändringar.

5.2.8

All kontoadministration sköts av personal som är godkända för SWAMID AL2 (IT-partner eller intern personal).

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.



5.3.1-5.3.2

Frivilligt byte sker via Microsoft självbetjäningsportal för studenter och primärt via den lokala datorn för anställda (när de befinner sig på kontoret). Man måste ange nuvarande lösenord innan man anger nytt lösenord.

5.3.3

När nuvarande kontouppgifter ej är kända, till exempel om en användare inte längre har tillgång till uppgifter om sitt kontonamn och/eller lösenord till kontot, sker ny ID- kontroll på samma sätt som 5.2.5 för att användaren ska kunna motta nytt lösenord som sen måste bytas. Detta gäller både medarbetare och studenter. Metod för verifiering via BankID för att hämta ut sina uppgifter finns också tillgänglig.

5.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

5.4.1

Om anställd lämnar RKH så inaktiveras kontot efter sista arbetsdagen. Studentkonton raderas efter examensrapportering eller avbrott. Vid bekräftat missbruk stängs konto omgående ner och person informeras. Under uppehåll har studenten rätt att ha kvar sitt konto för att slutföra nödvändiga tentor, dock efter ett uppehåll på 4 terminer inaktiveras kontot.

I de flesta fall sker detta med ett fast datum för att konto skall återaktiveras. Användaren kan själv begära att inaktivera sitt konto.

Anmälan om detta sker via servicedesk och måste ske efter fysisk ID-kontroll. Användarkonton kan stängas tillfälligt vid säkerhetsincident.

5.4.2

När ett konto inaktiveras i samband med en säkerhetsincident kontaktas användaren via registrerade externa kontaktuppgifter, till exempel telefon



eller e-post, alternativt personligt möte. Ett konto som återaktiveras får ett nytt lösenord och ID-kontroll sker enligt 5.2.5 innan kontouppgifter lämnas ut.

5.4.3

Efter hanterad säkerhetsincident så sker en intern utredning där eventuella åtgärder ses över. Dessa åtgärder utförs och informeras till berörda personer. Vid behov så sker även kompletterande utbildning.

Vid incidenter används kommunikationskanaler som e-post, läroplattform, medarbetarportal och även vid behov publik hemsida.

Säkerhetsrutiner ses över årligen för att identifiera förändringsbehov och/eller kompletteringar som måste ske. Dessa informeras enligt 5.4.2.

Användarvillkor nyttjas i förstahand för att meddela att missbruk kan beivras och att åtkomst kan komma att begränsas eller stängas av på begränsad eller obegränsad tid. Vid misstänkta fall kontaktas berörd person.

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.5.1

Flertalet system utgör en helhetsbild över nuvarande och historiskt utfärdade identiteter. De system som RKH kontroller loggas enligt 4.4 samt tas daglig backup på.

För studenter använder RKH en metod som går ut på att konton vid skapande får namn baserat på termin och år.

5.5.2

RKH har så pass hög tillgänglighetsgrad att åtkomst till interna system som är beroende av identitetsutgivare uppfyller organisationens krav.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.



RKH nyttjar endast konfigurationer och protokoll som följer SWAMIDs standard och best practices. Med hjälp av ADFS toolkit konsumerar vi SWAMIDs metadata och dess konfiguration i Microsoft ADFS.

Active Directory hanterar autentisering av användare och tillåter ej konton som är inaktiverade eller har upphört. Livslängd för SSO är högst 8h för alla konfigurerade tjänster.