SWAMID Identity Management Practice Statement av Röda Korsets Högskola

Kontaktperson	**Peter Altsved**
Telefonnummer	**08-587 516 77**
E-post	peter.altsved@rkh.se
Årtal för Statement	**2024**

Innehållsförteckning

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.

Stiftelsen Röda Korsets Högskola, organisationsnummer [802002-8695], är en enskild utbildningsanordnare och regleras inom lagen (1993:792) om tillstånd att utfärda vissa examina. Stiftelsen Röda Korsets Högskola följer Sveriges 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 anställde 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 finns

samt på engelska https://www.rkh.se/en/servicedefinition.

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

samt på engelska: https://www.rkh.se/en/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 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.

Från och med Januari 2025 kommer RKH att införa multifaktorautentisering (MFA) med Microsoft Authenticator med nummermatchning och Microsoft Entra inloggningsbegäran, för samtliga medarbetare och studenter, och detta i kombination med lösenord. Dessa faktorer är alltså oberoende av varandra, d.v.s. tillgång till endast den ena faktorn möjliggör inte återställning av den andra faktorn.

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 ned automatiskt 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.

https://www.rkh.se/student/stod-och-service/it-for-studenter/it-regler-och-ansvarsforbindelse/

https://www.rkh.se/om-oss/styrdokument-och-policies/

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

Vid legitimationskontroll av anställda och studenter godkänns samma identitetshandlingar som polisen godkänner för utfärdande av svenskt pass, samt utländska pass som uppfyller ICAO Doc 9303 och nationella ID-kort inom EU/EES som uppfyller EU-förordning 562/2006.

Anställda

Anställda kan hämta ut sitt konto eller höja sitt konto från AL1 till AL2 med följande metoder:

- Personligt besök i servicedesk/IT-intro med legitimationskontroll. Personnummer eller namn och födelsedata sparas som fördefinierade identifierare och jämförs med uppgifter i lönesystemet/kontosystemet. Ett engångslösenord erhålles som måste bytas vid första inloggning. Kontona blir AL2.

- Anställda med svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via svensk e-legitimation på tillitsnivå 3 eller högre. Personnummer sparas som fördefinierade identifierare och jämförs med uppgifter i lönesystemet/kontosystemet. Kontona blir AL2.

Studenter

Studenter kan hämta ut sitt konto eller höja sitt konto från AL1 till AL2

med följande metoder:

- Personligt besök i servicedesk med legitimationskontroll. Personnummer eller namn och födelsedata sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok/kontosystemet. Ett engångslösenord erhålles som måste bytas vid första inloggning. Kontona blir AL2.

- Studenter med svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via svensk e-legitimation på tillitsnivå 3 eller högre. Personnummer sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok/kontosystemet. Kontona blir AL2.

- Studenter med svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via eduID. Kontroll görs att IdP och inloggning uppfyller AL2. Personnummer från eduID sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok//kontosystemet. Kontona blir AL2.

- Studenter utan svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via eduID. Kontroll görs att IdP och inloggning uppfyller AL2. En automatiserad, riskbaserad bedömning görs att namn och födelsedata från eduID tillräckligt väl matchar uppgifter i Ladok/kontosystemet. Dessa sparas också som fördefinierade identifierare. Kontroll sker även att e-postadress från eduID matchar e-postadress i Ladok/kontosystemet. Eppn/subject-id från eduID sparas för senare lösenordsåterställning utan riskbaserad bedömning. Kontona blir AL2.

5.2.6

Alla användare uppfyller idag AL1 vid anställning eller start av studier. Möjlighet att hantera olika tillitsnivåer styrs via grupptillhörighet. 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. Förändring av tillitsnivå loggas i 180 dagar med Microsoft Sentinel.

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

Alla anställda/studenter har möjligheten att själv byta sitt lösenord via lösenordsportal.

Vid lösenordsbyte behöver nuvarande lösenord anges.

5.3.3

Metoderna under 5.2.5 kan användas för lösenordsåterställning.

De förregistrerade identifierarna som beskrivs under 5.2.5 används för att säkerställa att det handlar om samma person.

MFA kan idag inte återställas på annat sätt än:

a. Loggat in med lösenord och MFA

b. Kontaktat IT-administratör via personligt besök i servicedesk som initierar en återställning.

Återställa glömt lösenord kan göras genom Self Service Password Reset där det krävs två olika verifikationsmetoder: Mejl /sms/samtal, samt därpå MS Authenticator med nummermatchning.

Därutöver gäller personligt besök till servicedesk för lösenordsåterställning.

När portallösningen är på plats kommer man istället kunna återställa sitt lösenord enligt 5.2.5.

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.

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

Identifieringsmetoderna under 5.2.5 kan användas vid kontoåteraktivering.

De förregistrerade identifierarna som beskrivs under 5.2.5 används för att säkerställa att det handlar om samma person.

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.