
SWAMID
Swedish Academic Identity Federation

SWAMID

REFEDS SIRTFI

Webinar 2016-11-10

SUNET

SWAMID

Vad är SIRTFI?

- Förkortning av ”The Security Incident Response Trust Framework for Federated Identity”
- Ny internationell säkerhetsprofil från samarbetsorganisationen REFEDS för Best Current Practice inom federerad inloggning
- Ersätter gamla IdM-checklistan som SWAMID tog fram tillsammans med SUSEC i samband med SWAMID 2.0

SUNET

Vad rekommenderar SWAMID?

- SWAMID Board of Trustees, dvs. styrgruppen för SWAMID, rekommenderar starkt federationens medlemmar att använda säkerhetsprofilen REFEDS SIRTFI

- Detta betyder primärt att SWAMID Operations kommer aktivt stödja och informera alla identitetsutgivare (IdP) om REFEDS SIRTFI
- Tjänster (SP) som vill använda REFEDS SIRTFI får stöd vid behov

SWAMID

Varför ska vi använda REFEDS SIRTFI?

- REFEDS SIRTFI är ett bra sätt att veta om en organisations identitetsutgivare (IdP) eller tjänster (SP) sköts på ett säkerhetsmässigt bra sätt
- Vissa tjänster kommer att kräva att identitetsutgivare uppfyller SIRTFI för att inloggning ska tillåtas från aktuell organisation
  - Redan idag kräver forskningsorganisationen CERN att användare som ska få tillgång till federerade tjänster vid CERN måste komma från identitetsutgivare som uppfyller kraven för REFEDS SIRTFI, andra användare kan inte längre logga in.

Hur gör vi för att bli godkända för SIRTFI?

- Ni läser igenom och kontrollerar att ni uppfyller kraven för SIRTFI
- Om ni anser att ni uppfyller kraven för SIRTFI:
  - Meddela SWAMID Operations att ni uppfyller kraven för SIRTFI
  - Meddela även e-postadress, och gärna även telefonnummer, till organisationens IT-säkerhetsfunktion

- OBS! SWAMID Operations kommer inte att granska om ni uppfyller kraven eller inte, det är helt ert eget ansvar!

Mer och djupare information

- Information om REFEDS SIRTFI finns på adressen https://refeds.org/sirtfi

- SWAMID Operations kommer att publicera råd och rekommendationer om hur ni använder REFEDS SIRTFI på SWAMIDs wiki, mer information kommer till saml-admins

- Följande bilder innehåller ytterligare information runt kraven med fokus på identitetsutfärdare (IdP)

SWAMID

REFEDS SIRTFI för identitetsutfärdare (IdP)

SUNET

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS1] Security patches in operating system and application software are applied in a timely manner**
- Kravet innebär att
  - säkerhetsuppdateringar till programvaror i kontohanteringsmiljön ska installeras inom rimlig tid
  - programvaror i kontohanteringsmiljön som inte längre uppdateras eller supporteras av leverantören ska inte användas (indirekt krav)

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS2] A process is used to manage vulnerabilities in software operated by the organisation**
- Kravet innebär att
  - det finns definierade rutiner för att åtgärda säkerhetsproblem i programvaror som finns vid organisationen
- Kravet innebär ***inte*** att
  - organisationen måste offentligt publicera dessa rutiner

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats**
- Kravet innebär att
  - organisationen använder system för att upptäcka och skydda system från stora och akuta hot via t.ex. intrångsdetektering i brandvägg eller aktiv logganalys
  - det är lämpligt att identitetsutgivaren konfigureras på sätt att antalet olämpliga inloggningsförsök begränsas

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS4] A user's access rights can be suspended, modified or terminated in a timely manner**
- Kravet innebär att
  - en användares rättighet till federativ inloggning vid behov kan begränsas eller stängas av i samband med säkerhetsmässigt felaktig användning
- Kravet uppfylls av motsvarande krav i SWAMID AL1 och SWAMID AL2

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS5] Users and Service Owners (as defined by ITIL) within the organisation can be contacted**
- Kravet innebär att
  - organisationen har möjlighet att kontakta en användare vid behov
    - För anställda, och övrigt verksamma eller motsv., finns oftast kontaktvägar såsom mobiltelefon registrerat i katalog- eller personalsystem. Anställda brukar dessutom ha en e-postadress i tjänsten.
    - För studenter finns kontaktuppgifter i Ladok men även privat e-postadress om studenten eftersänder sin e-post vid lärosätet.

SWAMID

Operativa krav i REFEDS SIRTFI

- **[OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident**
- Kravet innebär att
  - det finns en incidenthanteringsfunktion vid organisationen som har tillräckliga rättigheter för att tillse att effekterna av en säkerhetsincident mildras, begränsas och till sist åtgärdas

SWAMID

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organisation belongs**
- Kravet innebär att
  - det finns definierade kontakter, helst funktion inte person, för incidenthantering vid organisationen
- Kravet innebär ***inte*** att
  - incidenthanteringsfunktionen är bemannad dygnet runt

SUNET

SWAMID

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner**
- Kravet innebär att
  - incidenthanteringsfunktionen svarar på förfrågningar från andra organisationer som följer REFEDS SIRTFI inom rimlig tid
- Kravet innebär ***inte*** att
  - incidenthanteringsfunktionen är bemannad dygnet runt

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trustframework**
- Kravet innebär att
  - incidenthanteringsfunktionen deltar och samarbetar vid säkerhetsincidenter tillsammans med andra organisationer som följer REFEDS SIRTFI
  - incidenthanteringsfunktionen även följer rutinen för SWAMIDs incidenthantering (indirekt krav) https://www.sunet.se/swamid/incidenthantering/

SWAMID

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR4] Follow security incident response procedures established for the organisation**
- Kravet innebär att
  - organisationen har definierade rutiner hur organisationen besvarar anmälningar om säkerhetsincidenter
  - incidenthanteringsfunktionen följer dessa rutiner
- Kravet innebär ***inte*** att
  - organisationen måste offentligt publicera dessa rutiner

SWAMID

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR5] Respect user privacy as determined by the organisations policies or legal counsel**
- Kravet innebär att
  - organisationen måste vid kommunikationen med tredje part, t.ex. incidentanmälaren, ta hänsyn till användarens behov av integritet enligt Personuppgiftslagen (SFS 1998:204) och i förekommande fall bestämmelserna i Offentlighets- och sekretesslagen (SFS 2009:400)

SWAMID

Incidenthanteringskrav i REFEDS SIRTFI

- **[IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy**
- Kravet innebär att
  - organisationen respekterar och använder begränsingarna i Traffic Light Protocol så länge som organisationen följer gällande svensk lagstiftning, t.ex. Personuppgiftslagen (SFS 1998:204), Offentlighets- och sekretesslagen (SFS 2009:400) och Tryckfrihetsförordningen (SFS 1949:105)

Definition av TLP: https://www.us-cert.gov/tlp

Spårbarhetskrav i REFEDS SIRTFI

- **[TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures**
- Kravet innebär att
  - säkerhetsrelaterade loggar ska sparas för kontoförändringar samt lyckade och misslyckade inloggningar
- Kravet uppfylls av motsvarande krav i SWAMID AL2 men bara delvis av kraven i SWAMID AL1

SWAMID

Spårbarhetskrav i REFEDS SIRTFI

- **[TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices**
- Kravet innebär att
  - loggar ska sparas enligt de rutiner som är definierade i organisationens incidenthanteringsrutiner
- Kravet innebär ***inte*** att
  - organisationen måste offentligt publicera dessa rutiner

SWAMID

Orgaisationskrav i REFEDS SIRTFI

- **[PR1] The participant has an Acceptable Use Policy (AUP)**
- Kravet innebär att
  - organisationen måste ha användarregler som gäller för identitetsutgivaren
- Kravet uppfylls av motsvarande krav i SWAMID AL1 och SWAMID AL2

SWAMID

Orgaisationskrav i REFEDS SIRTFI

- **[PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process**
- Kravet innebär att
  - organisationen måste ha rutiner som gör att användarna godkänner att de följer användarreglerna vid t.ex. kontoaktivering och lösenordsåterställning
- Kravet uppfylls av motsvarande krav i SWAMID AL1 och SWAMID AL2

SWAMID

Nu är det dags för frågor…

SUNET