Säkerhets- och incidenthanteringsprofilen REFEDS SIRTFI med fokus på identitetsfärdare (IdP)

The Security Incident Response Trust Framework for Federated Identity från REFEDS, förkortat SIRTFI, är en internationell säkerhetsprofil för Best Current Practice. SIRTFI ersätter den tidigare IdM-checklistan som SWAMID tog fram tillsammans med SUSEC i samband med SWAMID 2.0. En av skillnaderna mellan IdM-checklistan och REFEDS SIRTFI är att REFEDS SIRTFI gäller både identitetsutgivare (IdP) och tjänsteleverantörer (SP). För djupare information om REFEDS SIRTFI se https://refeds.org/sirtfi.

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

Lärosäten, och andra medlemmar, som uppfyller SWAMID AL1 eller SWAMID AL2 för sin identitetsutgivare uppfyller automatiskt flera av kraven i SIRTFI. Främst behöver de säkerställa att de uppfyller de operativa kraven i profilen samt att de har rutiner på plats för incidenthantering innan de meddelar SWAMID Operations att de uppfyller säkerhetsprofilen REFEDS SIRTFI.

På sidan wikisidan 3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTFI finns beskrivet hur tjänsteleverantörer kan kontrollera om identitetsutgivare har deklarerat att de följer REFEDS SIRTFI.

Varför ska en identitetsutgivare uppfylla och deklarera REFEDS SIRTFI?

När en identitetsutgivare deklarerar att de följer REFEDS SIRTFI ges tjänsteleverantörer en indikation på att användarhantering i aktuell organisation sköts på ett säkerhetsmässigt bra sätt, dvs. tjänsteleverantören kan känna en högre säkerhetsmässig tillit för användare från aktuell organisation.

Vissa tjänster som är kopplade till SWAMID, direkt eller genom eduGAIN, kräver att identitetsutgivare uppfyller REFEDS SIRTFI för att inloggning ska tillåtas från den aktuella organisationen. Ett tydligt exempel på detta är forskningsorganisationen CERN där användare som ska få tillgång till federerade tjänster vid CERN måste logga in via identitetsutgivare som uppfyller kraven för REFEDS SIRTFI. Ett annat exempel på en tjänst är CiLogon som kräver både REFEDS SIRTFI and REFEDS Research and Scholarship.

Hur gör en identitetsutgivare för att bli godkända för REFEDS SIRTFI?

SWAMID gör ***ingen*** granskning av att identitetsutgivaren uppfyller REFEDS SIRTFI utan det är medlemsorganisationen som ensidigt deklarerar att de uppföljer säkerhetsprofilen.

1. Medlemsorganisationen kontrollerar att identitetsutgivaren och underliggande system uppfyller kraven i REFEDS SIRTFI, se nedan.
2. Om medlemsorganisationen anser att identitetsutgivaren uppfyller kraven meddelar ni SWAMID Operations att identitetsutgivare uppfyller REFEDS SIRTFI.
    - När ni informerar SWAMID Operations måste ni även skicka med e-postadressen till incidenthanteringsfunktionen.
    - Om det är möjligt att nå incidenthanteringsfunktionen via telefon kan ni om ni vill även skicka med telefonnumret.
3. SWAMID Operations lägger in markering om att medlemsorganisationens identitetsutgivare uppfyller kraven i REFEDS SIRTFI inkl. aktuella kontaktuppgifter.

Vilka krav ska en identitetsutgivare uppfylla?

Kraven i REFEDS SIRTFI är uppdelade i fyra avsnitt och varje krav har en benämning som står inom hakparanteser. I de fall som SWAMIDs tillitsprofiler SWAMID AL1 eller SWAMID AL2 tillgodoser ett krav står detta tydligt.

För de av SWAMID:s medlemsorganisationer som är statliga myndigheter har Myndigheten för samhällsskydd och beredskap enligt 19§ i Förordning (SFS 2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap rätt att skapa föreskrifter kring myndigheters informationssäkerhetsarbete. Genomförande av MSB:s föreskrifter , t.ex. MSBFS 2016:1, MSBFS 2016:2 och MSBFS 2016:7, inom medlemsorganisationen kan vara till hjälp i analysen om identitetsutfärdaren och underliggande system uppfyller kraven i REFEDS SIRTFI.

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 samt
- att programvaror i kontohanteringsmiljön som inte längre uppdateras eller supporteras av leverantören ska inte användas.
    - Indirekt krav som följer av att programvaran inte längre uppdateras.

[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.

[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 samt
- att det är lämpligt att identitetsutgivaren konfigureras på sätt att antalet olämpliga inloggningsförsök begränsas.

[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

[OS5] Users and Service Owners (as defined by ITIL) within the organisation can be contacted

Kravet innebär

- att organisationen har en utpekad driftorganisation som är kontaktbar samt
- 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 ofta även en privat e-postadress om studenten eftersänder sin e-post vid lärosätet.

[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.

Incidenthanteringskrav i REFEDS SIRTFI

[IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs

Kravet innebär

- att det finns en definierad kontakt för incidenthantering vid organisationen.
    - Det är lämpligt att använda kontaktuppgifter till funktion, inte person.
    - E-postadress måste finnas men gärna även telefonnummer.

Kravet innebär ***inte***

- att incidenthanteringsfunktionen är bemannad dygnet runt.

[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.

[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 samt
- att incidenthanteringsfunktionen även följer rutinen för SWAMIDs incidenthantering.
    - Indirekt krav som följer av att organisationen är medlem i SWAMID.

[IR4] Follow security incident response procedures established for the organisation

Kravet innebär

- att organisationen har definierade rutiner hur organisationen besvarar anmälningar om säkerhetsincidenter samt
- att incidenthanteringsfunktionen följer dessa rutiner

Kravet innebär ***inte***

- att organisationen måste offentligt publicera dessa rutiner.

[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 gällande personuppgiftslagstiftning i Sverige och i förekommande fall bestämmelserna i Offentlighets- och sekretesslagen (SFS 2009:400).

[IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy

Kravet innebär

- att organisationen respekterar och använder begränsningarna i Traffic Light Protocol så länge som organisationen följer gällande svensk lagstiftning, t.ex. gällande personuppgiftslagstiftning, Offentlighets- och sekretesslagen (SFS 2009:400) och Tryckfrihetsförordningen (SFS 1949: 105).

Trafikljusprotokollet (TLP) underlättar utbyte av känslig säkerhetsinformation mellan olika parter. TLP är en uppsättning av beteckningar som används för att säkerställa att känslig information delas med lämplig målgrupp.

Trafikljusprotokollet har fyra färger för att ange hur avsändaren förväntar sig att mottagaren hanterar spridning av informationen, fritt översatt:

TLP: RED	Mottagaren får inte sprida informationen till någon, inte ens inom sin egen organisation.
TLP: AMBER	Mottagaren får endast sprida information till andra personer inom organisationen, eller direkt berörda partner och kunder, som behöver ha den för att hantera problemet, TLP-märkningen ska bibehållas.
TLP: GREEN	Mottagaren får sprida informationen till kollegor och partner inom sektorn, TLP-märkningen ska bibehållas.
TLP: WHITE	Inga spridningsbegräsningar förutom normal upphovsrätt, TLP-märkningen ska bibehållas.

För mer och djupare information om trafikljusprotokollet se https://www.first.org/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.

[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.

Organisationskrav 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.

[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.