SWAMID Incident Management Procedures

The SWAMID Incident Management Procedures should be followed when a suspected security incident at a Federation Participant is expected to affect other Federation Participants. More specifically, the procedures applies to all suspected federated security incidents unless their extent is known, contained within the Federation Participant and cannot affect any other party. In addition to federated identities, threats to federated entities such as Identity Providers, Service Providers, Attribute Authorities and federation infrastructure such as Metadata repositories are also in scope.

- SWAMID Incident Management Procedures

Responsibilities

Federation Participants and the Federation Operator are mutually responsible for diagnosing and resolving the ongoing security incident by ensuring that it is contained, coordinating the response between the affected parties, tracking the progress of the incident response process, disseminating information, and providing expertise and guidance. In case of a security incident suspected to affect other federations or their participants, their security procedures should be respected.

The Federation Operator and any affected Interfederation Operators' security function (for example the eduGAIN Security Team for the interfederation eduGAIN) are expected to marshal concerned Federation Participants and Federation Operators to participate in the response to a security incident.

Federation Participants report in-scope incidents to their Federation Operator, and the Federation Operator reports in-scope incidents to the Interfederation Operators' security function. Centralising incident awareness in this manner improves the chance that other affected parties can be identified and alerted sooner than might otherwise occur, much as a University CSIRT would wish departments within the University to notify them rather than silently resolve just that portion of the incident visible within their department.

The incident management procedures use the Traffic Light Protocol (TLP, https://www.first.org/tlp/), as defined by REFEDS Sirtfi, to mark information being shared according to its sensitivity and the audience with whom it may be shared. Specified TLP rules have to be strictly abided during any communication.

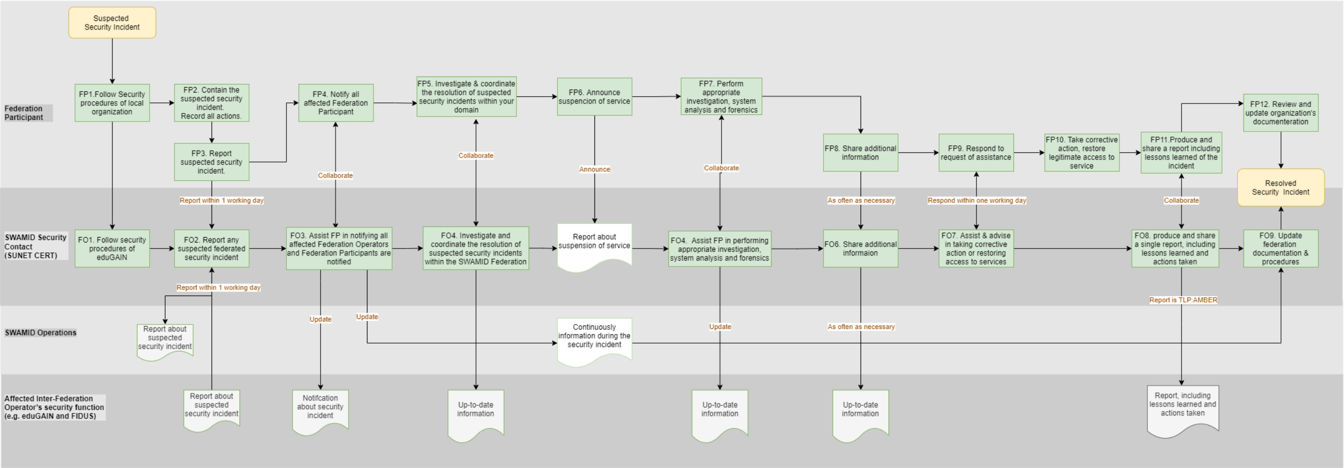
Security Incident Response Procedures

All ongoing suspected security incidents posing a risk to any Federation Participants within or outside the SWAMID Identity Federation is subject to these procedures.

The SWAMID Incident Management Procedures (including additional information) are described in a PDF-document and must be read and followed for a suspected security incident.

- SWAMID Incident Management Procedures
- Contact information for SUNET CERT: abuse@cert.sunet.se

The diagram below shows the correlation between all steps and involved parties for when a suspected security incident is in progress. Steps for federation participants are further explained after the diagram.



Suspected Security Incident
Federation Participant
FP1.Follow Security procedures of local organization
FP2. Contain the suspected security incident. Record all actions.
FP3. Report suspected security incident.
FP4. Notify all affected Federation Participant
FP5. Investigate & coordinate the resolution of suspected security incidents within your domain
FP6. Announce suspencion of service
FP7. Perform appropriate investigation, system analysis and forensics
FP8. Share additional information
FP9. Respond to request of assistance
FP10. Take corrective action, restore legitimate access to service
FP11.Produce and share a report including lessons learned of the incident
FP12. Review and update organization's documenteration
Resolved Security Incident
Collaborate
Announce
Report within 1 working day
As often as necessary
Respond within one working day
SWAMID Security Contact (SUNET CERT)
FO1. Follow security procedures of eduGAIN
FO2. Report any suspected federated security incident
FO3. Assist FP in notifying all affected Federation Operators and Federation Participants are notified
FO4. Investigate and coordinate the resolution of suspected security incidents within the SWAMID Federation
Report about suspension of service
FO4. Assist FP in performing appropriate investigation, system analysis and forensics
FO6. Share additional informaion
FO7. Assist & advise in taking corrective action or restoring access to services
FO8. produce and share a single report, including lessons learned and actions taken
FO9. Update federation documentation & procedures
Report is TLP:AMBER
Update
SWAMID Operations
Report about suspected security incident
Continuously information during the security incident
Affected Inter-Federation Operator's security function (e.g. eduGAIN and FIDUS)
Notifcation about security incident
Up-to-date information
Report, including lessons learned and actions taken

Procedure for Federation Participants, i.e. Identity Providers, Service Providers and Attribute Authorites

- **FP1.** In parallel with this procedure, follow all security incident response procedures established for your organisation.
- **FP2.** Contain the suspected security incident to avoid further propagation to other entities, while preserving evidence and logs. Record all actions taken, along with accurate timestamps.
- **FP3.** Report on the suspected security incident to Sunet CERT as soon as possible, but within one local working day of becoming aware of the suspected incident.

- **FP4.** In collaboration with Sunet CERT, ensure that all affected Federation Participants are notified, including those belonging to other federations. Include relevant information, when possible, to allow them to take action.
- **FP5.** Investigate and coordinate the resolution of the suspected security incident within your domain of operation and keep Sunet CERT and other involved parties updated appropriately.
- **FP6.** Announce suspension of services (if applicable) to Sunet CERT.
- **FP7.** Perform appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident and its full extent.
- **FP8.** Share additional information as often as necessary to keep all affected parties up to date with the status of the security incident and enable them to investigate and take action should new information appear. It is strongly encouraged for such updates to occur at regular intervals, to include the time of the next update within each update and to issue a new update sooner if significant new information becomes available.
- **FP9.** Respond to requests for assistance from others involved in the security incident within one local working day. In case of limited trust or doubt regarding the party behind a given request, involve Sunet CERT.
- **FP10.** Take corrective action, restore legitimate access to services (if applicable).
- **FP11.** In collaboration with Sunet CERT, produce and share a single report, including lessons learned and actions taken, of the incident with all Sirtfi-compliant organisations in all affected federations within one month of its resolution. This report should be labelled TLP AMBER or higher. If the participant is not Sirtfi-compliant, Sunet CERT assists in sharing the outcome of the action with Sirtfi-compliant organisations.
- **FP12.** Review and update your own organisation’s documentation and procedures as necessary to prevent recurrence of the incident in the future.

Sunet CERT may be contacted and involved at any time for security advice, recommendations, technical support and expertise, regardless of the severity of the suspected incident, at the discretion of and based on the needs of the Federation Participant.