Document SWAMID Incident Management Procedures
Identifier http://www.swamid.se/incident
Version V2.0
Last modified 2021-06-03
Pages 6
Status FINAL

SWAMID Incident Management Procedures

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

1.1. Definition of terminology

Federation Participants operate the entities, which belong to or are accessible via SWAMID or any inter-federation partners of SWAMID, including Service Providers, Identity Providers, Attribute Authorities, Research Community Authentication and Authorization Infrastructures, identity and service provider Proxies or other Federation e-Infrastructures.

Federation Operator of SWAMID is Sunet. The operations of the federation is managed by the SWAMID Operations team within Sunet. Sunet CERT is the security contact of SWAMID regarding security incidents.

Interfederation Operator operates interfederations (for example eduGAIN) that SWAMID is a member of. The eduGAIN Security Team manages incident response at the eduGAIN interfederation level providing security coordination between federations.

Traffic Light Protocol (TLP) as defined by Forum of Incident Response and Security Teams (FIRST). The Traffic Light Protocol was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. For more information about TLP visit https://www.first.org/tlp/.

Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. For more information about Sirtfi visit https://refeds.org/sirtfi.

2. Introduction

The *Swedish Academic Identity Federation* (SWAMID) facilitates and simplifies access to shared services across the Identity Federation. This is accomplished by using Federation Technologies to extend the scope of a Digital Identity issued by one Federation Participant of the Identity Federation to be trusted across the whole Identity Federation.

The SWAMID Incident Management Procedures define procedures and practices which allows Federation Participants to handle federated security incidents. These procedures apply to all SWAMID Federation Technology Profiles.

3. Scope

The procedures below should be followed when a suspected security incident at a Federation Participant is expected to affect other Federation Participants. More specifically, this document 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.

4. 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.

4.1. Federation Participants

Federation Participants follow the Security Incident Response Procedures for Federation Participants (in Chapter 5.1 below).

For Federation Participants supporting the Sirtfi framework, the Sirtfi security contact is the channel to engage their incident response team.

4.2. Federation Operator

Sunet as the SWAMID Federation Operator follows the Security Incident Response Procedures for Federation Operators (in Chapter 5.2 below).

The security contact of the SWAMID Identity Federation is Sunet CERT. The responsibility of Sunet CERT is to coordinate and assist the security incident response.

In order to fulfil this role adequately, Sunet CERT may be supported by the SWAMID Operations Team, Federation Participants, the eduGAIN Security Team, external parties, Research Communities, or e-Infrastructure security teams, as appropriate.

5. 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 procedures below use the Traffic Light Protocol (TLP), as defined by 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.

If a suspected security incident is discovered to be a false positive, the procedure may be stopped after appropriate notification of the involved parties.

All actions detailed below are understood to be on a best-effort basis and that some parties at times may not be able to do all that are specified by these procedures.

Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort invested in doing so should be commensurate with the scale of the problem and with the potential damage and risks faced by affected parties.

In the event of conflict between this procedure and other applicable policies or procedures for your organisation, local policies and procedures take precedence. If for any reason this procedure cannot be followed, the security contact of the Federation Operator (for Federation Participants) or the eduGAIN Security Team (for the Federation Operator) must be notified.

5.1. Federation Participants

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.

5.2. Federation Operator (represented by Sunet CERT)

FO1. Follow all security incident response procedures established for the federation and, if applicable, for eduGAIN.
FO2. Report any suspected federated security incident, unless its extent is known, contained within SWAMID and cannot affect any other party, to the Interfederation Operator's security function of any potentially affected interfederations (for example the eduGAIN Security Team for the interfederation eduGAIN), as soon as possible, but within one local working day of becoming aware of the suspected incident.
FO3. In collaboration with the Interfederation Operator's security function of any potentially affected interfederations, ensure that all affected Federation Operators and Federation Participants are notified. Include relevant information, when possible, to allow them to take action.
FO4. Investigate and coordinate the resolution of the suspected security incident within the SWAMID Federation and keep the Federation Participants, the Interfederation Operator's security function of any affected interfederations and other involved parties updated appropriately.
FO5. Assist Federation Participants in performing appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident and its full extent. Keep the Interfederation Operator's security function of any affected interfederations and other involved parties updated appropriately.
FO6. 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.

FO7. Assist and advise Federation Participants in taking corrective action or restoring access to services (if applicable) and legitimate user access.
FO8. In collaboration with Federation Participants and the Interfederation Operator's security function of any affected interfederations, 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.
FO9. Update the federation documentation and procedures as necessary to prevent recurrence of the incident in the future.

Sunet CERT continuously informs SWAMID Operations during the security incident.

The eduGAIN Security Team 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 Operator.