Sirtfi compliance of SAFIRE

This is a self-assessment of the South African Identity Federation's compliance with the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi) version 1.0[1]. Such an assessment is necessary because the Federation uses a hub-and-spoke architecture, and thus some Federation components are in scope for identity- and service- providers own Sirtfi assessments. For this reason, SAFIRE's own assessment includes more detail than it normally requires of Federation Participants (who need only provide the expression of compliance).

Scope

The scope of this review is limited to systems that are directly involved in the operations of the South African Identity Federation, as compliance is only requested for the Federation Hub and associated IdP proxies. It does not consider other, unrelated systems operated by the SA NREN (either the Tertiary Education and Research Network of South Africa or the SANReN Competency Area).

Systems in scope

Federation metadata registry and aggregator; Federation hub; Federation IdP proxies; Consent administration; Databases; Logging systems. These are hosted on the following servers: md-cpt-01.safire.ac.za, hub-cpt-01.safire.ac.za, db-cpt-01.safire.ac.za. Some of the underlying data is hosted in private repositories on Github, and assessment of those is based on Github's publically accessible documentation.

Systems excluded from scope

Federation's web presence, test service provider, metadata validator, and ancillary non-critical services. These are all hosted on web-cpt-01.safire.ac.za.

Individual identity- and service providers are explicitly excluded from scope (including the SA NREN's own identity- and service providers). However, the Federation may assert compliance for such providers on receipt of an equivalent confirmation of compliance from such providers (i.e. this document is an adjunct to the documentation provided by such providers, and additionally covers systems such as the IdP proxies they may use due to the Federation's architecture.)

Comments on Sirtfi normative assertions

Operational Security [OS]

[OS1] Security patches in operating system and application software are applied in a timely manner.

The Federation runs a currently-supported, long-term-support release of Ubuntu. All servers are configured to automatically install operating system security patches as soon as they're released by the vendor.

Federation staff are subscribed to the security announcement mailing lists of critical software components (e.g. SimpleSAMLphp), and will apply patches or mitigate risk as soon as practical after an announcement.

[OS2] A process is used to manage vulnerabilities in software operated by the organisation.

A network monitoring system automatically tracks whether or not there are outstanding operating system patches. This is reviewed every working day and an informed decision is made on remediation. Moreover, should critical operating system security patches fail to install timeously, automated notifications will be sent to relevant staff irrespective of whether it is a working day or not.

[1] https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

As a general policy, all servers are configured with a default-to-deny firewall and only relevant services are added to the ruleset. This mitigates the risk of exposing inadvertently installed software to outside threats.

The Federation has undergone a third-party vulnerability assessment conducted by the SA NREN's CSIRT and has mitigated or responded to all identified risks[2]. All systems included in the scope of this review were also in scope for the assessment. It is anticipated that this assessment will be periodically re-conducted.

[OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats

At present only informal mechanisms are employed in this role. Real-time logging information is constantly displayed in the Federation's offices, and it relies on staff knowledge to pick up anomalies in the routine patterns. Some automated monitoring tools are available to assist with this.

[OS4] A user's access rights can be suspended, modified or terminated in a timely manner.

The only relevant users in this case are those with underlying access to the operating systems, or who can log into systems such as the Federation hub or metadata aggregator. This is only SA NREN staff, and limited on a need-to-have basis. Rights can be easily modified via an Ansible playbook.

The Participation Agreement does provide for Federation Participant's right to be suspended.

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

Users of the system are Federation Participants. The on-boarding process includes collecting of relevant contact details for all users, and this information must further be published in metadata. The Service Owner is the Federation, and accurate contact details are published in metadata. Such contact details are automatically added to the metadata of identity providers where IdP proxies are used.

[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.

An informal security response capability exists in the form of the Federation staff. They have sufficient organisational authority to mitigate, contain, and remediate the effects of a security incident and are empowered to do so on behalf of Users by the Participation Agreement.

Incident response [IR]

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

SAFIRE publishes a security contact in metadata using the prescribed form.

[IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.

Security incidents will be prioritised by Federation staff.

Note, however, that SAFIRE does not have a mandate to respond on behalf of its Participants and no such assertion can be made for the individual identity providers it may proxy for.

[IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.

It is in the Federation's interests to collaborate. Moreover, there is a contractual requirement to do so in the Participation Agreement. This must, of course, be within the bound of South African law.

[2] https://safire.ac.za/safire/news/vulnerability-assessment-20161221/

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

Federation staff have full authority to respond to security incidents, and are required to report them upwards to organisational management. They will collaborate with the SA NREN CSIRT staff as required.

[IR5] Respect user privacy as determined by the organisations policies or legal counsel.

This is a contractual requirement of staff, and is further included in the Participation Agreement.

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

Federation staff will be sensitised to the traffic light protocol.

Traceability [TR]

[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.

All relevant logs are retained locally for a week and are retained on a remote logging server for 183 days. All servers are configured to synchronise their clocks via NTP, and synchronisation is monitored. Logs are available for use subject to the processes outlined in the Participation Agreement.

[TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

The information in [TR1] is collected in accordance with the responsibilities outlined in the Participation Agreement and the corresponding technical profiles.

Participant Responsibilities [PR]

[PR1] The participant has an Acceptable Use Policy (AUP).

The Federation Participation Agreement fulfils the role of an acceptable use policy in this context.

[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.

All Users of the Federation are required to formally sign and ascent to the Participation Agreement before they may participate in the Federation's activities. Federation staff are not empowered to make exceptions to this.

Expression of compliance

To whom it may concern:

Re: Expression of Sirtfi compliance for the South African Identity Federation

This serves to certify that the Tertiary Education and Research Network of South Africa (RF) NPC completed a self-assessment of the South African Identity Federation on 21 June 2017. TENET hereby confirms that at the time of assessment it satisfied the aforementioned normative assertions set out in the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi) v1.0.

This expression of compliance is scoped to the following SAML entities:

- https://iziko.safire.ac.za/
- https://proxy.safire.ac.za/…

Sincerely,

G.A. Halse
Project Director: South African Identity Federation
Tertiary Education and Research Network of South Africa (RF) NPC