Category:
Status: IGTF Global Consultation
trusted-credential-stores-1.0.docx
Editor: David Groep
Last updated: Thu, 25 May 2017
Total number of pages: 5

IGTF Trusted Credential Stores Guidelines

Version 1.0-2017

Abstract
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

This document describes the minimum requirements and recommendations for the operation of Trusted Credential Stores.

This document is an EUGridPMA Guidelines Document, to be referred to as the "Guidelines for the Operation of Trusted Credential Stores" (version 1.0 2017).

Identifications
This document: **urn:oid:1.2.840.113612.5.4.1.1.1.8.1**

Table of Contents

1 About this document

This document describes the minimum requirements and recommendations for the operation of a Credential Store (CS) by a trusted CS Operator. A trusted CS is a system that holds re-usable credentials on behalf of another party and conforms to the requirements of this document.

Possible architectures to which these guidelines may be applicable include Token Translation Services such as those defined in the AARC blueprint, MyProxy stores issuing derived RFC3820 proxies, third parties performing full credential management for end-entities, escrow services, and services acting on behalf of users based on server-held long-term user credentials.

In this document the key words **must**, **must not**, **required**, **shall**, **shall not**, **recommended**, **may**, and **optional** are to be interpreted as described in RFC 2119. If a **should** or **should not** is not followed, the reasoning for this exception must be documented such that relying parties can decide whether to accept the exception.

2 Introduction

This document describes the minimum requirements and recommendations for the operation of a Credential Store (CS) by a trusted CS Operator. A trusted CS is a system that holds re-usable credentials on behalf of another party and conforms to the requirements of this document.

Possible architectures to which these guidelines may be applicable include Token Translation Services such as those defined in the AARC blueprint, MyProxy stores issuing derived RFC3820 proxies, third parties performing full credential management for end-entities, escrow services, and services acting on behalf of users based on server-held long-term user credentials.

3 Naming

In order to facilitate traceability, any generated derived credentials should include a human-readable, globally unique, and readily identifiable name of the CS[1].

4 Operational Requirements

CS systems must run no other services than those needed for the CS implementation and operations. Any virtualization techniques employed (including the hosting environment) must not degrade the context as compared to any secured physical setup[2].

The CS system must be located in a secure environment where access is controlled and limited to designated, trusted, and appropriately trained personnel. A list of CS operator staff functioning in trusted roles must be maintained.

CS operators must protect their operator credentials to a level of assurance that exceeds that of any credentials stored in the service.

It is advised that CS Operators review their operations against IT industry best practices for security operations, such as the ISO27002 or NIST SP800-53 assessment criteria and state the risk qualification at which the CS aims to operate[3].

---

[1] for example a MyProxy store that signed subordinate RFC3820 proxies could embed its name in the generated proxy credentials, and an SP-IdP Proxy may use its SAML EntityID embedded in the subsequent assertions.

[2] i.e., a virtualized system should not be co-hosted with for example public login services or web content management systems

[3] It is recommended to consider the recommendation by the [ISSeG] Group, http://isseg-training.web.cern.ch/ISSeG-training/Recommendations/Recommendations.htm

The CS should follow guidance of Sirtfi[4] in terms of Operational Security, Incident Response, and Traceablity.

4.1 Protection of stored key material and activation data

The controls protecting stored key materials should mitigate the risk of unauthorized access to the materials. It is recommended that these protections include:

- the exclusive use of security reviewed or certified software
- software should be run in its secure or certified mode
- keeping software up-to-date and all security patches applied
- data needed to activate and use credential material must not be held by the system on persistent storage. With the exception of short lived credentials stored in the CS, activation data and any plain text private keys should be removed when the user so requests, or after 24 hours of user inactivity
- exclusive use of confidential, integrity protected, and authenticated channels for the transfer of activation data and any private key material. The keys used to authenticate and protect the channel must have a strength equivalent to or better than an 2048 bit RSA key. The keys must be suitably protected by the operating system or an HSM, and must only be accessible by the service and trained personnel with procedural controls.

4.2 Life time considerations

If the CS issues derived credentials[5], the CS Operator must publish the default and maximum permitted life times of such derived credentials.

4.3 Network configuration

The network to which the CS is connected must be highly protected and suitably monitored. It is recommended to consider deploying the following controls:

- network intrusion detection systems
- pro-active monitoring of successful and failed connection attempts
- pro-active inspection of log files and network traffic
- record all interactive and operator access to the system, and correlate this with known and declared activity
- access to networked services be limited to the smallest number of sources commensurate with service operations
- separation of the system holding the credentials from the system offering customer-facing services, where the interaction to the credential-holding system is minimal and all transactions are logged
- logging of all records on a separate (central) log server

as well as following current defined best practices in secure service provisioning.

4.4 Incident Response

The CS operator must meet all relevant Sirtfi requirements.

The CS operator should maintain pro-active relationships with any CSIRT capabilities of the qualified relying parties and communities it serves, and must promptly inform their security incident response teams in case of a compromise or suspected compromise of the credential store.

---

[4] See https://refeds.org/SIRTFI
[5] such as RFC3820 proxy certificates

5 Site Security

The CS operator must evaluate the risk profile according to established standards[6], and implement and maintain physical site security controls in a state consistent with the security requirements of the hosted CS.

These controls must be the equivalent of but are not limited to:

- the CS system must be located in a secure environment where physical access is controlled and limited to designated, appropriately trained, and authorized personnel
- the hosting machines are in an access controlled data centre where access is logged
- the hosting machines are in cabinets that are locked with distinct keys, numeric padlocks with unique combinations, or biometrics
- the access to systems management and power management interfaces is limited to designated, trained, and authorized personnel

The implementation must be documented.

6 Publication and Repository Responsibilities

The CS operator must publish to the community:

- persistent operational and security contact details for the CS operator, including at least one email address and one postal contact address
- a URL of the CS operator for general information

The CS operator must disclose on request from qualified relying parties and to credential owners those aspects of the operational environment that are necessary for their evaluation of the security and trust of the CS.

The repository must be run at least on a best-effort basis, with an intended continuous availability.

7 Audits

The CS operator must record at least the following to meet traceability requirements:

- all requests for credential release or delegation
- all submission attempts for credential storage
- all authentications against the CS
- any configuration change to the service relevant to the access control of the CS
- all login, logout, and reboot actions of the CS systems

The CS operator must be accessible for at least 180 days after termination of the effects of the auditable event unless this is inconsistent with the applicable legislation.

The CS operator should accept being audited following reasonable requests from a relying party or by a community it serves to verify its compliance with these guidelines. Such an audit or a self-review should be performed at least once per year. The resulting statement of compliance must identify who is making the claim, and such a statement should be provided on request to qualified relying parties or communities it is willing to serve.

Where the CS is run by an operator which is also acting as an accredited authority of the IGTF, the CS associated with the authority will be included in the IGTF accreditation process.

[6] specific reference risks and controls are enumerated in ancillary documents, such as SP800-53 and relevant ISO standards

8 Privacy and confidentiality

CS operators must publish an appropriate privacy and data release policy, and wherever possible notify credential owners, qualified relying parties and communities it serves of any changes therein. The CS operator must not violate the confidentiality of credentials and related meta-data stored in the repository.

9 Business continuity and disaster recovery

The CS must have an adequate business continuity and disaster recovery procedure, and must be willing to discuss this with the qualified relying parties and communities it serves.