Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 06, 2014

L. Johansson, Ed.
SUNET
S. Winter
Restrena
October 03, 2013

F-Ticks - A Federation Log Format
draft-johansson-fticks-00

Abstract

This document describes a log format for distributed identity federations that can be used as a tool for meetering and statistics gathering.

Requirements Language

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 RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 06, 2014.

Copyright Notice

Table of Contents

1. Introduction and Motivation

Identity federations are often built as loosly coupled systems of

identity providers and relying parties. In such a system it is often important to collect statistics and meetering in a consistent way.

This document describes a simple (yet extensible) tex logformat which can be to communicate the essential aspects of authentication events to log reception software (eg syslog [RFC5424]).

2. F-ticks Semantics

An F-ticks log stream consists of a series of F-ticks log messages, each one represents a single authentication event. Each log message is generated at a federation entity (eg an identity provider or a relying party).

3. F-ticks Format

An F-ticks log message is a text string that fulfills the following ABNF [RFC5234]:

```
fticks = "F-TICKS/" federation-identifier "/" version attribute-list
label = ( ALPHA / DIGIT / '_' / '-' / ':' / '.' / ',' / ';')
federation-identifier = label
version = label
attribute-list = 1*("#" attribute "=" value ) "#"
value = label
attribute = ( ALPHA / DIGIT )
```

The federation-identifier and version can be used by federations and other communities to indicate the type of attributes used. This document does not describe any mandatory attributes but instead provides a list of attributes in use in various communities today.

Future versions of this document may want to define an IANA registry for f-tick attribute definitions.

Because of size constraints common to several log systems it is expected that f-ticks attributes are kept short.

4. Common F-ticks Attributes

In general a log consumer should not assume that any one attribute is present. Depending on the situation any one of these (or any other defined attributes) may be missing from an F-ticks message.

4.1. REALM

The REALM attribute is used to convey the AAA-realm (eg RADIUS) of the authentication event. The presence of the REALM attribute implies that the message was generated by a AAA-based identity provider.

4.2. VISCOUNTRY

The ISO country code of the entity that generated the log messages.

4.3. VISINST

TODO

4.4. CSI

The Calling Station ID of the subject associated with the authentication event. The presence of this attribute implies that the message was generated by an AAA-based identity provider.

4.5. RESULT

The result of the authentication event - either 'OK' or 'FAIL'.

4.6. RP

Relying Party identifier. A string uniquely identifying the relying party invoved in the authentication event.

4.7. AP

Asserting party identifier. A string uniquely identifying the party making the claim towards the relying party. For an authentication event this is the identity provider. For an attribute authority lookup event this is the AA identifier.

4.8. TS

A timestamp (seconds since the epoch) associated with the authentication event. If this attribute is absent the consumer MAY choose to use a timestamp provided by the log message system (eg syslog) instead.

4.9. AM

Authentication Method identifier.

4.10. PN

A unique identifier for the subject involved in the event.

5. Examples

TBD

6. Acknowledgements

The f-ticks log format has been in use in the eduroam community since TTT and was originally conceived as a usage-tracking mechanism by Stefan Winter.

7. Security Considerations

Improperly configured logging may leak sensitive user information. In particular the PN attribute value (subject identitier) should be masked with a cryptographically keyed hash function before transmission.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

Authors' Addresses

Leif Johansson (editor)
SUNET

Email: leifj@sunet.se

Stefan Winter
Restrena

Email: stefan.winter@restrena.lu