F-ticks standard

1. Original document

F-Ticks - A Federation Log Format.htm (F-Ticks - A Federation Log Format; draft-johansson-fticks-01)

2. Amendments to the original document (section 4.) related to attributes used (to be edited)

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. VISCCOUNTRY

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 success-state of the event - either 'OK' or 'FAIL'. For identity providers, this implies that a successful authentication request was returned to a relying party. For relying parties it means a successful authentication response was received from an identity provider.

4.6. RP

Relying Party identifier. A string uniquely identifying the relying party involved in the authentication event. This is typically a URI and will often be technology-dependent. Implementations should expect and be able to process any string.

4.7. AP

Asserting party identifier - often an identity provider. A string uniquely identifying the party making the claim towards the relying party. For an authentication event this is the identity provider. This is typically a URI and will often be technology-dependent. Implementations should expect and be able to process any string.

4.8. TS

A POSIX timestamp (aka unix time) 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. This is normally a URI that identifies the type of authentication that was used. Values may be technology-dependent.

4.10. AL

Assurance Level Identifier. This is normally a URN that identifies the level of assurance (aka LoA) that was associated with the security association event. Level of assurance identifiers SHOULD be registered according to RFC6711 [RFC6711] and SHOULD NOT be technology-dependent. If registered identifiers are used, their short form may be used depending on the underlying technology used. Long-form (URI) and short-form level-of assurance identifiers are equivalent.

4.11. PN

A unique identifier for the subject involved in the event.

3. Proposed format

3.1 F-ticks format definition

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

```c
ABNF
```
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.

### 3.2 Proposed format for technical trial / pilot

```
F-TICKS/eduGAIN/1.0beta#VISCOUNTRY=<tld-country-of-F-tick-origin>#AP=<SAML-IdP-entityID>#RP=<SAML-SP-entityID>#RESULT=<authentication-result-code>#CSI=<SAML-session-id-hash>#PN=<depersonalised-ePTID>#TS=<timestamp>#
```