

SHAKEN PASSporT extension

draft-ietf-stir-passport-shaken-04

STIR Working Group
IETF103

Some Comments to discuss

- Request for a Privacy Considerations section
- Proposed Text

Privacy Considerations

As detailed in [RFC3261] Section 26 as well as [RFC3323], SIP as a protocol inherently carries identifying information of both the initiator or 'caller' as well as the terminating party or 'callee'. 'origid', as defined in SHAKEN [ATIS-1000074] and described in this document is intended to be an opaque and unique identifier that is used by an originating telephone service provider to trace and identify where within their network (e.g. from a gateway or a particular service within their network) the call was initiated, so that either bad actors that may be either trying to illegitimately spoof identities or making fraudulent calls can be identified and likely stopped or held responsible for the fraudulent activities. While the opaqueness of the 'origid' identifier is intended to keep any direct or implied information regarding the origination of a set of calls that may have the same 'origid' to a minimum, it should be recognized that potential patterns whether intended or not may be able to be discovered.

New Terminology text

- Added to existing Terminology section to address two comments:

In addition, the following terms are used in this document:

- o Verified association: is typically defined as an authenticated relationship with a device that initiated a call, for example, a subscriber account with a specific SIM card or set of SIP credentials.
- o PASSporT: Defined in [RFC8225] is a JSON Web Token [RFC7519] defined specifically for securing the identity of an initiator of personal communication. This document defines a specific extension to PASSporT.

New Abstract text

- To address two comments regarding providing the reader a bit more context of the details of the document vs talking about SHAKEN and IP-NNI task force, etc:

Abstract

This document extends PASSporT, which is a token object that conveys cryptographically-signed information about the participants involved in communications. The extension is defined, corresponding to the SHAKEN specification, to provide both a specific set of levels-of-confidence to the correctness of the originating identity for a SIP based Communication Service Provider (CSP) telephone network originated call as well as an identifier that allows the CSP to uniquely identify the origination of the call within its network.

Other comments

- Most other comments were editorial
- There was some other comments/questions that i provided clarification on the list.
- All of these changes are ready to go into a 05 release of the document unless there is any comments regarding the proposed new text.