Metaswitch-logo-color

Version 1.0 | Issue 1 | 11 Feb 2020

Document Number VPM-1472-000

# API comparison

1. This document summarizes the minor, but notable, differences between the SHAKEN HTTP interfaces defined in 3gpp TS 24.229 V16.40 (referenced as "3gpp" below) and ATIS 1000082 (referenced as "ATIS").

## General differences

* + 1. The ATIS spec requires some additional parameters in the HTTP headers: X-RequestID (optional) and X-InstanceID (optional) in any request and X-RequestID (mandatory) in the responses.
    2. 3gpp requires the telephone numbers sent to the signing endpoint to be canonicalized (although the verification endpoint doesn't), ATIS requires the service to canonicalize them.
    3. The dest parameter on signing requests is an array of objects in 3gpp and an object of arrays in ATIS. 3gpp cites RFC 8225 (PASSporT) for the format but we believe agreement is with ATIS in general.
    4. A couple of the parameter names are slightly different: where ATIS uses "identity", 3gpp uses "identityHeader"; where ATIS uses "verstat", 3gpp uses "verstatValue".
    5. The "to" parameter in a verification request is an array of telephone numbers in ATIS and is a single string (tn or uri) in the 3gpp spec.
    6. Error handling:
       1. 3gpp has a set of service errors and policy errors that should be returned as an unspecified JSON object (e.g. " Error: Missing request body.") in the body of a http response with a specified status code (e.g. 400).
       2. ATIS has the same set of service and policy errors however the body is a JSON object containing slightly more information than the 3gpp errors contain, while the http status code is set identically to that in the 3gpp spec. However, ATIS also has a set of errors specific for verification requests that are returned in a different format to the service and policy errors and with an http status of 200 OK - these are used to provide more detail as to why the verification failed.
       3. ATIS-1000085 has a requirement that if an SP receives an INVITE containing one or more Identity headers, and the most recently added Identity header contains a stale PASSporT, then remove all Identity headers (to avoid issue where a subsequent div authentication makes the stale PASSporTs look fresh). To support this, the HTTP API verification response needs to indicate when verification fails due to a stale PASSPorT.

## STIR-Div issues

1. This consideration is based on 3gpp TS 24.229 V16.40 - the relevant sections are 5.10.10 and Annex V. The issue with the 3gpp spec focuses on its assumption that each div identity can be individually validated.
   * 1. Annex V specifies endpoints /divSigning and /divVerification but nowhere in the document are they defined or used
     2. The verification endpoint returns separate "verstat" values for each individual identity (div and shaken), but verification is not defined per identity - it is a property of a collection of identities. The spec makes no reference as to how to produce these values. Comment: I guess there are some individual PASporT failures (like bad signature). But your're right, there is also the overall "the chain is broken" failure that can't be pinned to a single PASSporT.
     3. Section 5.10.10.2 contains this statement: "if the … response included verification results for the diverting identities, the IBCF shall based on local policy add the "verstat" tel URI parameter to the verified diverting identities in the History-Info header field if this field is available.", which doesn't align with the way the IETF div spec describes validating a call. Specifically, you can only validate the current destination of a call. Comment: I'm not exactly sure why 5.10.10.2 specifies this, but I don't think it contradicts the IETF div draft, but rather, is something outside of and separate from the draft. I don't quite understand the point being made by your final sentence in this item.
     4. Instead of defining a separate resource URL to verify each type of PASSporT (/verification vs. /divVerification), why not verify all PASSporT types with a single "/verification" URL? The verification procedures to be applied for each case should be unambiguous to the STI-VS, since the PASSporT type is conveyed in the "ppt" parameter; I.e., if it’s a single shaken PASSporT then do base-shaken verification; if it’s a shaken plus one or more div passports then verify each passport plus check the authority chain, if it's an rph passport the verify that, etc.

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Issue | Author | Description |
| 11-Feb-20 | Issue 1 | PCB | Initial release |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |