SHAKEN - Secure Handling of Asserted information using toKENs

August 2015

COMCAST LABS

COMCAST

Current Status

- The current STIR IETF working group is focused on 4474bis which defines a signing mechanism for validating a calling information between two parties and form a level of trust that the caller is who he says who he is.
- The issue is that current STIR discussion scope is large (beyond current world of provider peering agreements), incorporates a lot of concepts into many new SIP headers that aren't very well understood and requires a certificate management infrastructure to be in place, whether following a proposed draft for a certificate authority with OCSP, or the landscape team proposal as part of a registry.
- This will take time and will take time for providers to understand how to best deploy into their networks.
- Further, something has been forgotten in the process is that we cannot implement a silver bullet, we are looking for indicators that allow for better informed decisions on whether a call is potentially fraudulent.

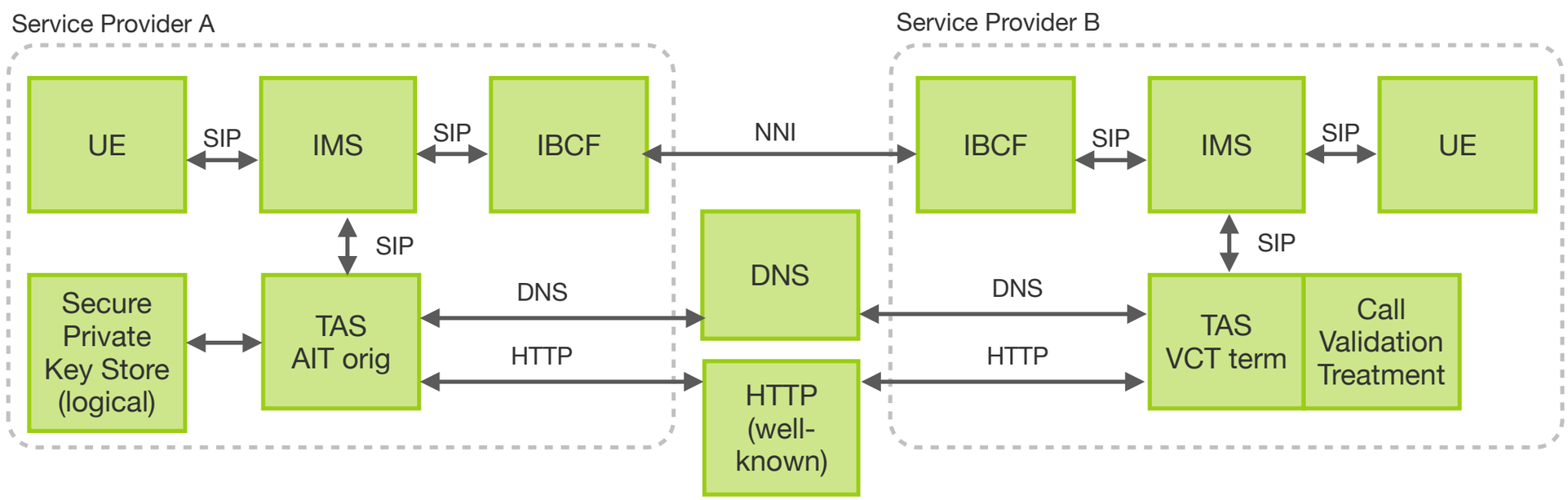
Overview

- Use of a standard, widely-used token (JWT) that is extensible and incorporates the ability to evolve signing mechanisms, crypto algorithms and other characteristics, if necessary.
- Separation of concerns with SIP and header details versus validation of asserted information via token
  - From implementation point of view, SIP state machine processing and token creation/validation should be able to be separable
  - Simplify the dependence, assert telephone number or identity information vs. SIP headers.
  - Similar framework may also be used for wholesale/transit to customer validation or legitimate caller-id spoofing validation

JWT/JWS Token

- Use the very straight forward, efficient and widely used JSON Web Token (JWT) RFC 7519 and JSON Web Signature (JWS) RFC 7515.
- JWT/JWS provides flexibility in terms of signing of the information
- JWT is a standard URL friendly string that is of the form “header . claim . signature”
- claim is the asserted information in JSON format. In this case, would be the calling number (could be easily included to incorporate calling name, etc)
- header and claim are base64 encoded, signature can be a digital signature (asymmetric key) or HMAC (symmetric key) of the claim

Asserted Information Token (AIT) - Basic Call Flow



- Originate Call on UE, TAS (telephone application server) applies AIT, signed by private key, in INVITE for service provider managed UEs
- Terminating network receives INVITE, uses AIT validation to perform service provider specific CVT (Call Validation Treatment) including both:
  - negative treatment - e.g. to block/forward to VM call
  - positive treatment - e.g. apply “verified” flag and/or validation confidence flag

Evolution of AIT Signature Validation Ecosystem

- Use simple asymmetric public/private key pairs (i.e. X.509 certificates) with limited certificate chain (i.e. provider certificate only signed by root directly)
    - X.509 framework provides more direct evolutionary path and incorporate trust anchor and chain (Could start without root signing initially, if necessary.)
    - Trust anchor is mechanism to validate authority to sign AIT, particularly as ecosystem evolve beyond direct peering relationships.
- Root signing request services could start within industry or more centralized players or both (e.g. NANPA, Cablelabs/NetworkFX, Peer providers?) Very low volume service (1000s requests per year?).
- Assume domain certificates will be wildcard for domain chosen by provider (e.g. *.pstn.example.com) until a future point that per-TN certificates is even considered, but in either case provides evolutionary path.
- Distribution of Public Key Certificates via three mechanisms:
    - Could be passed directly in peering agreements initially
    - DNS resource record in corresponding domain (DNSKEY RR)
    - HTTP via RFC 5785 based Well-Know Uniform Resource Identifiers (URIs)

AIT as a Assertion validator in SIP

- Two proposals on table:
  - AIT could be used as a parameter of P-Asserted-ID header e.g.
    - `sip:<+12155551212@ims.example.net>;`
      `ait=eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMD`
      `A4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ.dBjftJeZ4CVP-`
      `mB92K27uhbUJU1p1r_wW1gFWFOEjXk`
  - AIT could be passed as new header
    - Identity?
    - New header?