Signature based Handling of Asserted information using Tokens

October 2015
Overview

• SHAKEN will define the architecture of Verified Token and 4474bis based framework

• SHAKEN (phase 1) will define:
  • Authentication Service
  • Verifier
  • Originating Provider Certificate Management
Verified Token and 4474bis Overview

• Verified Token uses the JWT and JWS formats and defines a standard set of base claims and signature allowing secure cryptographic validation of the owner of the claims made, specifically targeting originating caller-id

• 4474bis defines how Verified Token is formatted in a SIP message using the identity header
Auth/Verify Service - Basic Call Flow

- Originate Call on UE, Authentication constructs one or more signatures using one of the following options:
  - 4474bis signature and adds identity header to SIP INVITE
  - 4474bis signature with full Verified Token added to identity header of SIP INVITE
  - Verified Token is applied to Message Body as a multi-part MIME
- Terminating network receives INVITE, fetches (likely highly cached) public key certificate from x5u claim and uses Validation Service to validate signature
- In addition, there are other mitigation techniques that can be used to perform service provider specific CVT (Call Validation Treatment)
Originating SP Certificate Management

• Each provider will create a public key/private key X.509 certificate pair

• It will generate a CSR (Certificate Signing Request) to the chosen Trust Anchor or authority that can validate with absolute certainty that the requestor is an authorized PSTN provider

• The provider will receive back a signed public key and certificate chain with the public key of the Trust anchor.

• The provider will use the certificate chain as the public key certificate and distribute this public key via HTTPS and/or DNSSEC as indicated in the “x5u” claim used in the verified token.

• The validation of the signature and the certificate chain back to the trust anchor will be the trust mechanism for authenticating the originating providers certificate.