Signature based Handling of Asserted information using Tokens

October 2015

COMCAST LABS

COMCAST

Overview

- SHAKEN will define the architecture and NNI dependencies around the usage of the PASSporT and 4474bis based framework
- SHAKEN (phase 1) will define:
  - Authentication Service
  - Verifier
  - Originating Provider Certificate Management

PASSporT and 4474bis Overview

- PASSporT 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

4474bis and PASSporT

- For 4474bis-07
  - unified identity header
  - “info” parameter corresponds to x5u header parameter in token
  - “alg” parameter corresponds with alg in token defining crypto algorithm
  - optional “canon” parameter to provide full PASSporT header.claims, for optimizing construction of token for validation

4474bis and PASSporT - extensibility

- Two mechanisms for extensibility
  - Extension of PASSporT base claims to add additional claims
  - Extension of PASSporT to create new set of claims
- Extending base claims involves adding a “ppt” header parameter with a spec defined unique string (e.g. foo)
  - This spec would define any additional claims to be added to the base set of defined claims in PASSporT
- Creating a entirely new set of claims involves creating a new “typ” MIME type, PASSporT suggests using “passport-“
  - For usage in SIP and 4474bis, alg and info parameters on identity header will still correspond to x5u and alg in token, but likely will want to use “canon” parameter to deliver the new set of claims, unless the new claims can be specified and mapped inside the SIP INVITE similar to iat/orig/term

Map between SIP message and PASSporT claims

SIP INVITE

```
INVITE sip:+12155551213@biloxi.com SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:+12155551213@biloxi.com;
user=phone>
From: Alice <sip:+12155551212@atlanta.com;
user=phone>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Date: Sat, 13 Nov 2015 23:29:00 GMT
Identity: “sv5CTo05KqpSmtHt3dcEiO/ICWTS
  ZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dIxkWzoeU
  7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI
  3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOg1uX
  ndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=“;
  info=<https://biloxi.example.org/
biloxi.cer>;alg=RS256
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

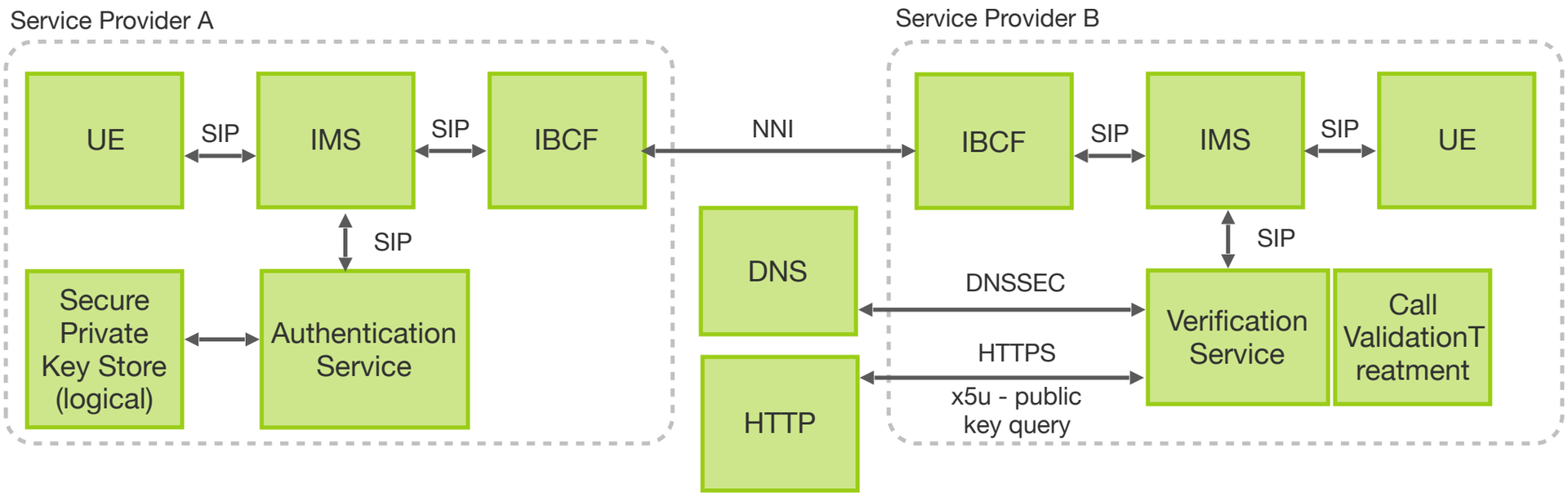
Header

```
{ “alg”:"RS256",
  "typ":"passport",
    “x5u”:"https://biloxi.example.org/
           biloxi.cer" }
```

Claim

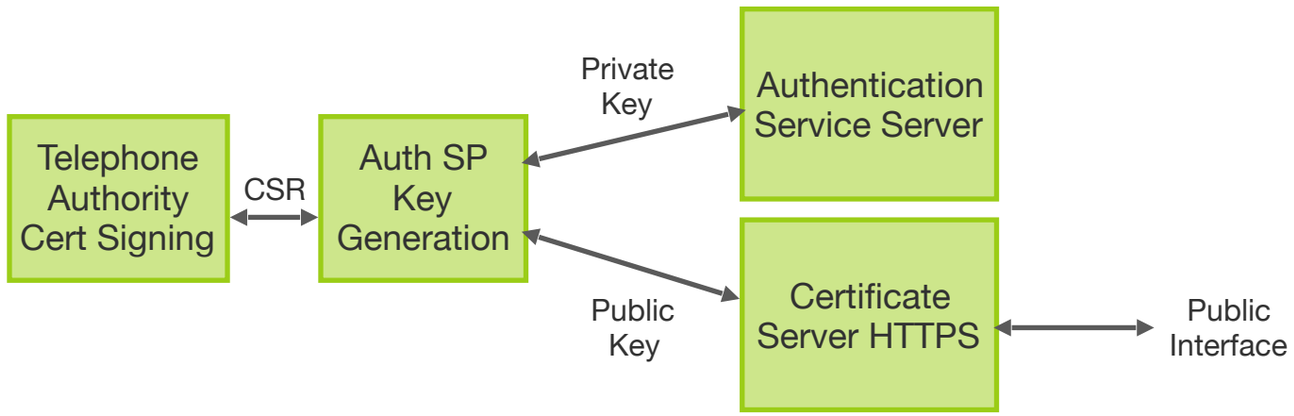
```
{"iat": “1443208345”,
  "orig":"12155551212",
  "term":"12155551213"}
```

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 PASSporT token added to identity header of SIP INVITE via canon
- 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)

Certificate Management - Manual

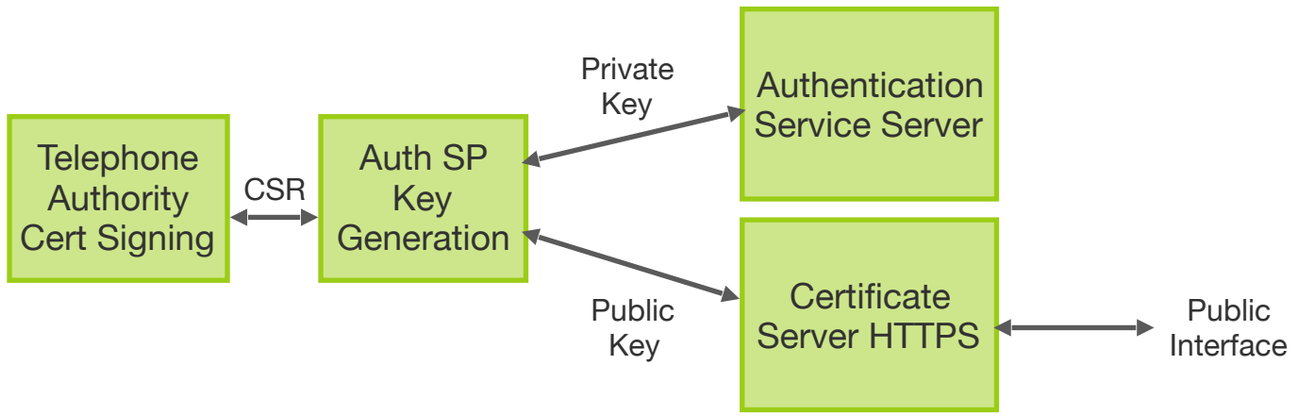


- From ACME spec, modified to fit SHAKEN, describing existing manual process
  - Generate a PKCS#10 [RFC2314] Certificate Signing Request (CSR).
  - Cut-and-paste the CSR into Telephone Authority (TA) web page.
  - Prove ownership of the domain by one of the following methods:
    - Put a TA-provided challenge at a specific place on the Authentication service server.
    - Put a TA-provided challenge at a DNS location corresponding to the target domain.
    - Receive TA challenge at a (hopefully) administrator-controlled e-mail address corresponding to the domain and then respond to it on the TA's web page.
  - Download the issued certificate and install it on their Certificate Server

Certificate Management - Manual

- Discussion:
  - How should Telephone Authority verify service provider
    - Email/postal mail/telephone call/D&B search
    - Do we need a short term semi-automated process? DNS?
    - Do we need to define a HASH or Token based mechanism? For future certificate requests?

Certificate Management - ACME/automated



- From ACME spec, modified to fit SHAKEN
  - The ACME client prompts the operator for the domain that the Authentication Service is to stand for.
  - The ACME client presents the operator with a list of TAs from which it could get a certificate.
  - The operator selects a TA.
  - In the background, the ACME client contacts the TA and requests that a certificate be issued for the intended domain.
  - Once the TA is satisfied, the certificate is issued and the ACME client automatically downloads and installs it, potentially notifying the operator via e-mail, SMS, etc.
  - The ACME client periodically contacts the TA to get updated certificates, stapled OCSP responses, or whatever else would be required to keep the server functional and its credentials up-to-date.

Certificate Management - Discussion

- Use Cases to validate:
  - When certificates get updated, what happens to calls in progress
  - Can we just use CRL or do we need OCSP stapling

Certificate Management - SP vs TN

- May not be a “versus” but likely more of an evolution
- Initial focus on Service Provider level certificates
  - Likely SP should have multiple certificates representing multiple geographic deployment regions and other uses
  - Establish good practices around these scenarios for certificate management
- Introduce TN level certificates for “important” telephone numbers, government, schools, etc.
- Evaluate moving towards wider TN level certificates and what granularity makes sense from a scale and an effectiveness point of view