Verified Caller Token Proposal

August 2015
Current Status of STIR

• 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.
Proposal

• Assumptions:

  • Telephone service providers will have interworking/peering agreements for many years to come
  
  • Telephone service providers that directly manage UE devices have specific knowledge of who that customer is and whether a call was initiated by that device
  
  • Most of the legitimate calls that residential and enterprise customers care about most, family, friends, direct consumers, will initiate calls from “first party devices”
  
  • Based on these assumptions, many simplifications can be made in terms of mechanics of passing verification information and security requirements.
Proposal - Verified Caller Token

• Pass a token that verifies the calling number and the provider that originated the call.

• Use the very straight forward, efficient and widely used JSON Web Token (JWT) RFC 7519 and JSON Web Signature (JWS) RFC 7515.

• JWT 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 is a HMAC of the claim
Verified caller token (VCT) - Proposed flow

- Originate Call on UE, TAS applies VCT in INVITE for service provider managed UEs
- Terminating network receives INVITE, uses VCT validation to make decisions about call treatment, e.g. to block/forward to VM call depending on provider preference.
VCT as a Assertion validator

• VCT should be thought of as a Caller-id validation extension

• VCT would be used as a parameter of P-Asserted-ID header e.g.

  • sip:+1215551212@ims.example.net;
vct=eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJ1eHAiOiJEMDA4M
  TkdODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ.dBjftJeZ4CVP-
  mB92K27uUbJU1p1r_wWlgFWFOEjXk
Signing Key/Secret sharing

- JWT provides flexibility in terms of signing of the information, could be based on:
  - shared secret
  - X.509 certificate via URL
  - public key via DNSSEC DNSKEY RR - RFC 4034
- Rather than waiting for registries or certificate authorities to be setup, short term options would include:
  - Peering agreement provides shared secret
  - Peering agreement provides public key
  - Public Key available in public DNSKEY RR in standard domain, e.g. ims.example.com
  - Public Key available in privately shared DNS (in DNSKEY RR)