STIR TNs for ACME

IETF 100

ACME WG

Jon - Singapore - Nov 2017
STIR and ACME

• What is STIR? Secure Telephone Identity (Revisited)
  – ART Area WG
  – Providing cryptographic authentication for telephone calls
  – Detecting impersonation is crucial to blocking illegal robocalling and other attacks on the telephone network

• STIR uses certs to attest authority over telephone network resources
  – draft-ietf-stir-certificates
  – Supports certs with extensions for TNs and SPCs
  – We need ways to issue and provision these certs
In-band STIR Logical Architecture

- Logical Authority
  - PBX Endpoint
  - Inter-Mediary
    - Credentials Provisioning
    - Unsigned Requests
  - User Endpoint
  - Inter-Mediary
    - Signed Requests
  - Endpoint

Credential Validation
ACME (through a STIR lens)

- Proof
- Proofing
- Certificate Provisioning
- Validate
- Communication

- ACME Client
- Certificate Authority
- Relying Party
What are interesting proofs?

• How to test effective control of a telephone number?
  – Return routability of SMS or similar mechanisms
  – Combined with some network data, maybe some crypto in SIM cards
    • Basic idea is in draft-ietf-acme-telephone

• Alternatively, we could use top-down attestation of assignment
  – This would require some kind of token
    • Carrier gives a token to an enterprise, who can redeem the token via ACME to get a cert for a TN
  – draft-ietf-acme-service-provider draft does this for SPCs
Generic tokens for proofs

• This seems like something pretty generic
  – Surely any number of namespaces have authorities who could generate tokens
  – Provided the ACME server has some trust relationship with the authority

• draft-peterson-acme-authority-token
  – Framework for tokens that allow authorities trusted by the CA to attest ownership for names
    • CA can then issue certs via ACME for particular names
  – Need some sort of typing mechanism for tokens, and a means to contact authorities
"challenges": [ 
  
  {  
    "type": "token-01",  
    "token-type": "TNAuthList-JWT",  
    "token-authority": "https://authority.example.org/authz",  
    "url": "https://boulder.example.com/authz/asdf/0"  
    "token": "IlirfxKXXAsHtmzK29Pj8A"  
  } 
]  

• The token-type would be governed by some sort of registry  
  – Specifies the syntax of the token: maybe a JWT, or whatever  

• The token-authority lets you know who to contact to get a token  
  – Optional, may be well known for some use cases
Next Steps

• Need to get some agreement on the right way forward for this
• Hopefully build it into both the ACME STIR drafts
  – For TNs and for SPCs