Minutes for ACME Meeting at IETF 101

Thanks to PHB for taking notes.

Document Status (Yoav)

CAA is probably done. Will check with Hugo and if so, will submit to the IESG.

Alexei: SMIME and TLS, have made changes for clarity. Probably ready for WGLC.

Main document went back to WGLC, has completed, been updated.

One new PR posted since. Will discuss.

Jacob Hoffman-Andres, believes that the PR is editorial only and should not block.

Will push to IESG for approval.

Richard: is ready for pub request / IETF last call.
(after the session, Daniel McCarney submitted yet another editorial PR)

ACME-IP

Document adopted last year, no movement. Provides for validation by IP identifiers. Allows certs containing IP addresses to be issued.

Http and tls-alpn methods work without change.

Reverse DNS has small change.

Methods valid under CABF 3.2.2.5

EKR (hatless) Reverse DNS is valid under 3.2.2.5 but has no effect on ability to direct traffic. Can't trust IANA delegation. Subsequent management of the domains does not necessarily reflect operations.

Ryan Slevi: Disagrees with EKR on sufficiency of validation. CABForum is going through a re-evaluation of validation methods. Should define the method first and then let policy groups decide if it is acceptable as matter of policy.

Cullen Jennings: Have tried to use the reverse DNS for spam control, they don't work, the information is wrong.

Finch: Reverse DNS is a cesspit and not to be trusted.

??: Please don't do this. Large amounts of DNS not signed

Lars: Could this be perceived as secure in a local environment?

Tom Peterson: Should the challenge response be bound to IP?

PHB: Will move CABF ballot to block this use.

Richard Barnes: Agree this is ultimately a policy argument. But better to go forward without this approach.

Ryan Slevi: The property relied on to validate an IP address is the RR-NIC. People in this forum should feel free to comment on what are acceptable validation approaches.

ACME-TLS-SNI replacement

Providers allow users to claim arbitrary SNI names. Thus tls-sni validation does not work.

TLS-ALPN uses the ALPN extension. [description of method in slides]

Ben Schwartz: Do random HTTP servers allow the ALPN to be configured? All modern TLS stacks are having to add extension processing to support QUIC, why not introduce a new extension?

Ryan Slevi: ALPN requires that servers not respond to stuff they don't understand, It is a MUST.

PHB: Is cynical about servers doing the right thing. Expects ACME to become part of the server stack. Don't worry too much about legacy servers being able to implement every method provided they can do one method.

Martin Thompson: If you do an extension can do the challenge and will be much better.

Ben Schwartz: Would be relatively straightforward to render this robust.

Authority Tokens for ACME:

Objective was authenticated telephone calls. Use this to prevent spam. This got into a generalized authenticated token.

Fingerprints or nonces discussion...

Richard Barnes: No immediate use but can see potential applications.

Mary Barnes: Would it be possible to do this flexible?

??: Another vote for flexibility

Profile for RFC8226 Certs

Again for telephone service providers.

Deine new TNAuthList identifier.

Richard Barnes: Are SPCs included in auth list (yes)

Should value be a string?

Richard Barnes: Other possibility ASN.1 (nitpick: DER)

John Pierson: What we are passing around should be what is going to end up in the cert.

Richard Barns: Should this be base64 encoded ASN.1?

Mary Barnes: We have an ASN.1 situation elsewhere.

Russ Housley: TN Auth structure is a list of three strings, seems that what you want to encode is direct

Richard Barnes: If you want to ASN.1 then it is straightforward, Otherwise translate.

Matt Miller: Someone defined JSON encoding rules for ASN.1 But what matters is what goes in the cert.

Russ: CAs know ASN.1

PHB: The only time a human sees this is to debug and they are going to have to be looking at ASN.1 structures so there is no more readability from stringifying things.

Matt: I regret mentioning JER...

Disposition: Take to the list

ATC Token Claim

John Pierson: You ask for what you want.

Richard Barnes: What if you validate against a range of numbers and then ask for one specific.

John Pierson: Need to make a choice. You asked us to come back with one thing, this is one thing.

Humm: Anyone think this is not a good idea?

Is a good idea: Hmmm

Is a bad idea: <silence>

Resolved merge docs. Two docs will become two docs.

ACME Star:

Chair: ready for WGLC?

Ryan Slevi: Good for WGLC. Not going to be good for WebPKI case. The motivating cases don't cover WebPKI. Blockers include CAs include keeping OCSP revocation, operational issues.

(DIgiCert): Correct way of characterizing is that the majority of CAs don't care. A few are interested in issuing them. Biggest debate was on not wanting to remove the CRL pointers from certs even if they are shortlived.

PHB: Strongly favor short lived certs. The main blocking issue is the lack of a spec for automating the issue process. Will probably still want CRL Distribution point but not necessarily OCSP

Richard Barnes: can probably prune the non-normative text. Good way to flush out is a WGLC

Chair: Will discuss with co-chair and (probably) start WGLC