draft-ietf-core-stateless

Has been stuck since May on review comments

Eleven (11) issues identified that had not been resolved in some way.

https://github.com/core-wg/stateless/issues

Pull requests for four:

https://github.com/core-wg/stateless/pulls

https://www.rfc-editor.org/cluster_info.php?cid=C310

has 11 ROLL/6tisch/6lo IDs waiting on core-stateless

Issues and suggestion resolution

I think we can simply explain a wontfix on:

#3 is stateless updating 7252 on distinguishing unrecognized vs invalid extension?
https://github.com/core-wg/stateless/issues/3

#4 how does freshness window of client/intermediate interact?
https://github.com/core-wg/stateless/issues/4

#6 can larger tokens fill responder memory?
https://github.com/core-wg/stateless/issues/6

#7 how to size the replay window?
https://github.com/core-wg/stateless/issues/7

#9 look ma, no state!
https://github.com/core-wg/stateless/issues/9

https://mailarchive.ietf.org/arch/msg/core/Y8c0mSR6THFP97JIyQqllLFF3Ok

Issues and suggestion resolution

We should replace confusing I-D text here:

#8 use automated key management due to AES-CCM/BCP107

https://github.com/core-wg/stateless/issues/8

https://github.com/core-wg/stateless/pull/11

Too long for the slide.

https://mailarchive.ietf.org/arch/msg/core/Y8c0mSR6THFP97JIyQqllLFF3Ok

Issues and suggestion resolution

Cabo says:

```
Overall, I think we should generate I-D text for:

#10 60 minutes for address change
   https://github.com/core-wg/stateless/issues/10
   https://github.com/core-wg/stateless/pull/12

#5  lack of integrity protection results in spoofed responses
   https://github.com/core-wg/stateless/issues/5
   https://github.com/core-wg/stateless/pull/13
```

https://mailarchive.ietf.org/arch/msg/core/Y8c0mSR6THFP97JIyQqllLFF3Ok

Issues 10, PR 12: why 60 mins?

https://github.com/core-wg/stateless/pull/12

```
        <t>
          Since network addresses may change,
          a client SHOULD NOT assume that extended token lengths are supported
          by a server later than 60 minutes after receiving the most-recent response with an extended
          token length.
          Since network addresses may change, a client SHOULD NOT assume that extended token
          lengths are supported by a server for an unlimited duration.
          Unless additional information is available, the client should assume that addresses (and therefore extended token lengths) are
valid for a minimum of 1800s, and for a maximum of 86400s (1 day).
          A client may use additional forms of input into this determination.
          For instance a client may assume a server which is in the same subnet as the client has a similiar address lifetime as the
client.
          The client may use DHCP lease times or Router Advertisements to set the limits.
          For servers which is not local, if the server was looked up using DNS, then the DNS resource record will have a Time To Live, and
the extended token length should be kept for only that amount of time.
        </t>

        <t>
```

https://mailarchive.ietf.org/arch/msg/core/Y8c0mSR6THFP97JIyQqllLFF3Ok

Issues 5, PR 13 – spoofed response

https://github.com/core-wg/stateless/pull/13

```
      However, a careful analysis of any potential attacks to the security
       and privacy properties of the system might reveal that there are cases
       where such cryptographic protections do not add value in a specific
       case.
       It is this reason that at least the use of integrity protection on
       the token is always recommended.
    </t>

    <t>
      It maybe that in some very specific case, as a result of a careful
      and detailed analysis of any potential attacks,  that there may be cases
      where such cryptographic protections do not add value.  The authors
      of this document have not found such a use case as yet.
    </t>
```

https://mailarchive.ietf.org/arch/msg/core/Y8c0mSR6THFP97JIyQqllLFF3Ok