Chris Lemmons via ietf.org

Fri, Jul 12, 9:54 AM (11 days ago)

to <cdni@ietf.org>

My first observation is that this document seems to have 3 semi-related purposes. Two definitions that describe when and where the dCDN may deliver content. One that defines the details of the TLS connection. And one that I think is supposed to define client authentication and authorization requirements.

The delivery time and place definitions seem mostly fine to me. The example in the LocationACLExtended should use an RFC 6761 example domain, though, instead of an svta.org domain.

In the TimeWindowACLExtended definition, there's a reference to SVTA2032, which is an SVTA document that is very similar to the proposed work in processing-stages-metadata. If we adopt that draft, would this reference need to be updated? Likewise, this is an informative reference, but it appears that you need to understand the content of it in order to understand what "terminating objects" are. It also appears to be the source of the definition for the MI.SyntheticResponse object. It appears this document is very much normatively dependent on processing-stages-metadata.

In the section that defines the TLS parameters, the protocols are enumerated explicitly. This is a forward compatibility problem. The TLS versions should be in a registry, I suspect.

Likewise, the TLS Cipher Suites need a full definition to define their encoding. Is there an appropriate document that you can cite for encoding these strings? Or might it work better to reference the existing TLS Cipher Suite registry?

And lastly, the ClientAuthMetadata seems to be a bit of a stub? I'm not entirely clear what this section is defining. How, for example, is Mi.ClientAuthMetadata different from the MI.Auth it contains? The MI.Auth is defined as "An Auth object defines authentication and authorization methods to be used during content acquisition and content delivery, respectively." in RFC 8006. URI Signing is described as defining an Auth object. Is ClientAuthMetadata defining a new Auth interface or a wrapper for the existing interface? And why? I think this section needs a lot of fleshing out.

The introduction also might call out that we're defining new http

protocols as well. Readers may easily miss that the second IANA Consideration isn't related to the remainder of the document directly.