**ATIS IP-NNI**

**January 24, 2022**

**Contribution**

**Title: 608 JWT freshness requirement**

**Source**\***: Charter Communications**

**Issue Number:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Abstract

Contribution proposes removal of the 608 JWT freshness requirement

RFC 8688 in section 3.2.2 specifies

“The payload contains two JSON values. The first JSON Web Token (JWT) claim that MUST be present is the "iat" (issued at) claim [RFC7519]. The "iat" MUST be set to the date and time of the issuance of the 608 response. This mandatory component protects the response from replay attacks.”

The requirement that the “iat” be set tot the date and time of the issuance of the 608, creates great complexity. E.g. it requires per call signing of the JWT and implicitly a requirement to keep these per call JWTs for some unspecified time for retrieval by the called party.

The argument for this requirement is to prevent replay attacks. Even if replay attacks was a serious problem, the “iat” requirement at best makes it only slightly harder to do. A 608 response has to be generated by an entity in the call path – such an entity could obtain a “fresh” JWT from other calls transiting it or by placing calls that would result in a 608 response.

Given the added complexity and little to no benefit the requirement that the “iat” be set at time of issuance of the 608 should be dropped.

This change would also eliminate the requirement in section 3.3 of RFC 8688 for the UAC to check the “iat”.