Errata for “iat” content and inclusion of “mky” (RFC8224 / RFC8225)
“iat” Content

• “iat” pertains to PASSporT token, i.e. it needs to contain the time when it is constructed
• RFC7519 JSON Web Token (JWT)
  – Arguably the “most authoritative” specification regarding “iat” content
  – 4.1.6. "iat" (Issued At) Claim
    • The "iat" (issued at) claim identifies the time at which the JWT was issued. This claim can be used to determine
      the age of the JWT. Its value MUST be a number containing a NumericDate value. Use of this claim is OPTIONAL.
    • This text clearly states that “iat” should be populated with the generation time of JWS.
• “Session initiation” and “Token generation” are two different functionalities
• Start of session (which Date header is based on) and PASSporT generation are temporarily not necessarily close
  – Example: PASSporT generated just before session is routed to a partner network after announcement/digit collection.
  – This could introduce a non-negligible artificial drift and cause freshness check issues during validation.
  – A new PASSporT claim should be defined/used if Date needs to be validated as well.
**“iat” Content / Call Flow**

**UE**
- INVITE
  - Date: t1
- Announcement played
- Digits collected
- Time is now “t1 + t2”

**SBC/MRF**
- 183

**SBC**
- INVITE
  - Date: t1
- Session will be routed to another carrier and therefore PASSPorT Token needs to be created
- Time is now “t1 + t2 + t3”
- Especially t2 could be substantial, e.g. 45 seconds, therefore using t1 from Date is problematic

**Another Operator**
- INVITE
  - Date: t1
  - Identity: ...
Inclusion of mky in PASSporT

• Always include mky when a=fingerprint present in SDP
• Do not tie it to DTLS-SRTP (RFC8224 12.1)
  – There is already one other use case: TLS with self signed certificates for MSRP
  – And there could be more in the future