DRIP WG

Interim Meeting

2023-03-01

Chairs: Daniel Migault & Mohamed Boucadair

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

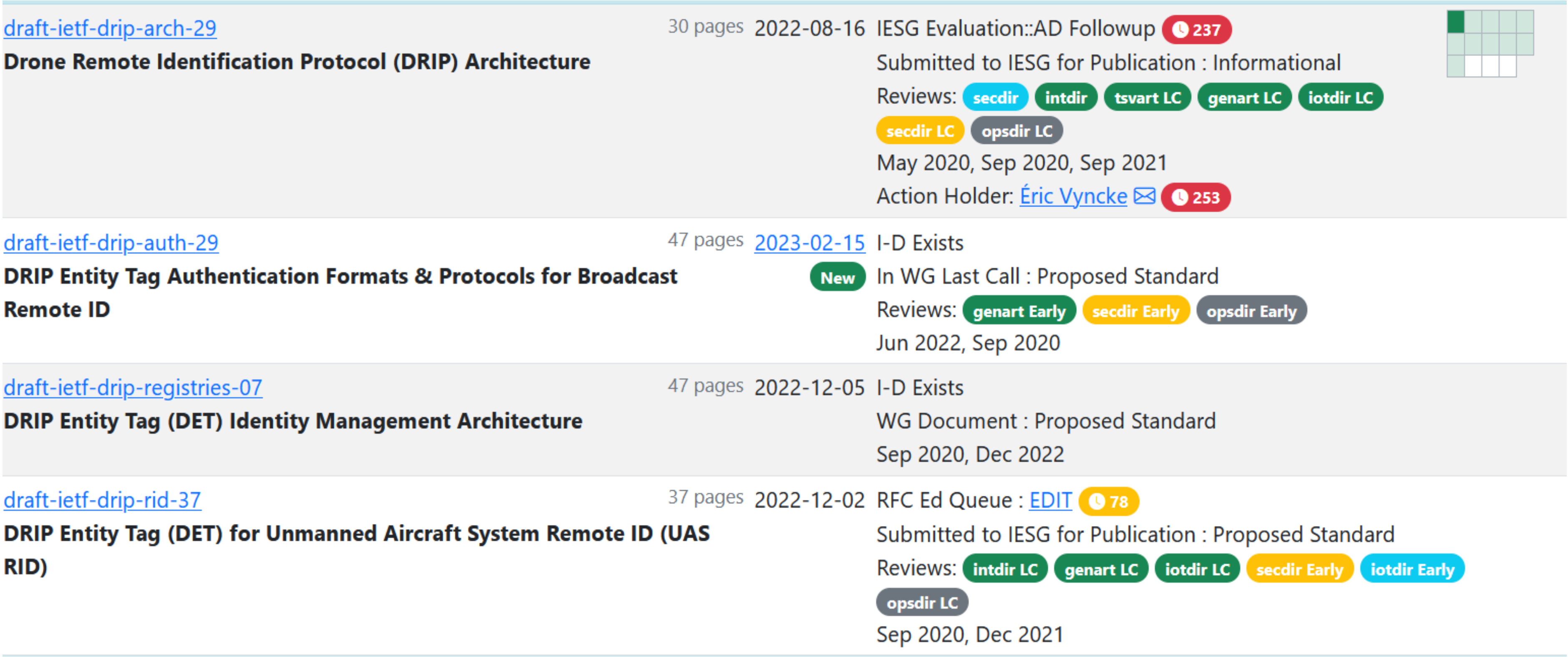
- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

I E T F

Agenda

- Introduction
- WG Status Update
  - Section 8.5
- DRIP Authentication (Adam – 15 min)
- DRIP Registries (Adam – 30 min)
- Misc
  - IETF#116 meeting plan

WG Status



draft-ietf-drip-arch-29 **Drone Remote Identification Protocol (DRIP) Architecture**	30 pages	2022-08-16	IESG Evaluation::AD Followup 🕓 237 Submitted to IESG for Publication : Informational Reviews: secdir intdir tsvart LC genart LC iotdir LC secdir LC opsdir LC May 2020, Sep 2020, Sep 2021 Action Holder: Éric Vyncke ✉ 🕓 253
draft-ietf-drip-auth-29 **DRIP Entity Tag Authentication Formats & Protocols for Broadcast Remote ID**	47 pages	2023-02-15 New	I-D Exists In WG Last Call : Proposed Standard Reviews: genart Early secdir Early opsdir Early Jun 2022, Sep 2020
draft-ietf-drip-registries-07 **DRIP Entity Tag (DET) Identity Management Architecture**	47 pages	2022-12-05	I-D Exists WG Document : Proposed Standard Sep 2020, Dec 2022
draft-ietf-drip-rid-37 **DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)**	37 pages	2022-12-02	RFC Ed Queue : EDIT 🕓 78 Submitted to IESG for Publication : Proposed Standard Reviews: intdir LC genart LC iotdir LC secdir Early iotdir Early opsdir LC Sep 2020, Dec 2021

Section 8.5: AD Comment

Section 6 and more fundamentally Section 3.3 both require timestamps. In Broadcast RID messages, [F3411-22a] specifies both 32-bit Unix style UTC timestamps (seconds since midnight going into the 1st day of 2019 rather than 1970) and 16-bit relative timestamps (tenths of seconds since the start of the most recent hour or other specified event). [F3411-22a] requires that 16-bit timestamp accuracy, relative to the time of applicability of the data being timestamped, also be reported, with a worst allowable case of 1.5 seconds. [F3411-22a] does not specify the time source, but GNSS is generally assumed, as latitude, longitude and geodetic altitude must be reported and most small UAS use GNSS for positioning and navigation. [F3586-22], to satisfy [FAA_RID], specifies use of the US Government operated GPS (with its sub-microsecond accuracy but only 1.5 second precision) and tamper protection of the entire UAS RID subsystem. Thus, in messages sourced by the UA, timestamp accuracy and precision each can be assumed to be 1.5 seconds at worst. GCS often have access to cellular LTE or other time sources better than the foregoing, and such better time sources would be required to support multilateration in Section 6, but such better time sources cannot be assumed generally for purposes of security analysis.