Trustworthy Multipurpose Remote Identification (TM-RID) Proposed WG Charter v1

Governmental agencies worldwide, including the United States Federal Aviation Administration (FAA), are embarking on rule making processes to define Remote Identification (RID) requirements for Unmanned Aircraft Systems (UAS). ASTM International (formerly the American Society for Testing and Materials) F38 Committee Work Item WK65041, "Standard Specification for UAS Remote ID and Tracking", addresses such anticipated requirements. Broadcast RID defines a set of messages for UAS to send one-way over Bluetooth or IEEE 802.11. Network RID defines how the same information (and potentially more) can be made available via the Internet. The ASTM draft does not address how to ensure or at least assess trustworthiness of information communicated via RID.

TM-RID will build upon the Host Identity Tag (HIT) from the Host Identity Protocol (HIP) as an RID and augment it and supporting HIP and other IETF technologies to add trustworthiness to the ASTM messaging suite. The goal is to provide trustworthiness both in an Internet connected environment and emergency, unconnected situations within the highly constrained environment of UAS.

The Host Identity Tag (HIT) is ideally, in fact uniquely, suited to work within this RID effort. The Host Identity (HI) behind the HIT can be used to sign Broadcast Authentication Messages, thus proving ownership of the RID (HIT) and signed messages. HITs provide significantly superior privacy compared to other allowed RID types while providing greater assurance to authorized observers that they are accessing the proper PII for the UA.

TM-RID will create specifications for HIP-augmented ASTM RID messages. Initially this will consist of additional RID Authentication Messages that use the HI in public key signing operations: to prove UAS ownership of a Hierarchical HIT (HHIT); to authenticate other claims made via RID, such as position and velocity, as having been made by the owner of that HHIT; and to provide observers lacking current Internet connectivity with locally verifiable UAS proof-of-registration objects.

For this, HIP would be amended to be used effectively in this environment:

- Hierarchical HITs (HHIT) enabling scalable and trustable UA registration and information retrieval: HHIT was part of the original design of HIP, but was dropped for lack of a clear use case. RID messages containing HHITs will enable use of DNS and potentially RDAP to access information about the UAS.

- expanded HIP Registration for HHITs: This registration process will provide proof of authenticity and prevent duplicate HHITs from occurring. Further, these Registries will provide the UAS DNS information and other services (e.g. RDAP and support of RVS for Network RID and related applications).

- new cryptographic algorithms: Extremely compact keys and signatures (such as are enabled by EdDSA and Keccak functions) are needed to meet the severely constrained UAS environment.

Further work will emerge as experience is gained in using HIP for UAS RID. For example, some UAS Traffic Management (UTM) systems envision using OAuth for Ground Control Systems (GCS) and authorized safety personnel. HIP as an OAuth method may help in merging HIP into these systems.

The goal is to complete these updates to HIP and publish the TMRID RFCs by the end of 2020.