DRIP Architecture Update

S. Card, A. Wiethuechter, *
R. Moskowit, **
Shuai Zhao ***
A. Gurtov ****
Update summary

• Current revision https://tools.ietf.org/html/draft-ietf-drip-arch-05
• Issues addressed from reviewers
• Proposed suggestions to move forward

We put Notes where we will take actions in the following revisions, so do review those sections lightly.
Overview of current DRIP drafts

<table>
<thead>
<tr>
<th>#</th>
<th>DRIP Drafts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DRIP Requirement (draft-ietf-drip-reqs-06)</td>
<td>RID problem space:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• N-RID, B-BRID, USS/UTM, DRIP focus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requirements in 4 dimensions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General, Identifier, privacy, registries</td>
</tr>
<tr>
<td>2</td>
<td>DRIP Architecture (draft-ietf-drip-arch-05)</td>
<td>• Describe the DRIP ecosystem:</td>
</tr>
<tr>
<td>3</td>
<td>UAS Remote ID (draft-ietf-drip-rid-04)</td>
<td>HHIT as UAS RID with modern encryption approach</td>
</tr>
<tr>
<td>4</td>
<td>Crowd Sourced Remote ID (drip-crowd-sourced-rid-05)</td>
<td>A gateway for Broadcast RID to Network RID</td>
</tr>
<tr>
<td>5</td>
<td>UAS Operator Privacy for RemoteID Messages (draft-moskowitz-drip-operator-privacy-06)</td>
<td>Encrypt operator/pilot sensitive data using hybrid ECIES</td>
</tr>
<tr>
<td>7</td>
<td>DRIP Authentication Formats (draft-wiethuechter-drip-auth-05)</td>
<td>include trust into B-RID</td>
</tr>
<tr>
<td>8</td>
<td>DRIP Identity Claims (draft-wiethuechter-drip-identity-claims-03)</td>
<td>UAS ID Proofs (in the form of Claims, Certificates and Attestations) for DRIP and UTM</td>
</tr>
</tbody>
</table>
My two cents on the scope of DRIP architecture.

- DRIP architecture should not be focusing on external UAS RID related architectures such as
- My personal view is that DRIP Arch shall only focus on the "UAS RID ecosystem", which may include only the domains mentioned in the current DRIP drafts:
  - The Design of the RID to comply with UAS RID standardization (ex: ASTM F3411-19)
    - A RID MAY a HHIT, with modern encryption method
  - The communication among N-RID, B-RID, Register, DNS, operator, GCS, USS/UTM and the internet
  - The security/trustworthiness of a RID
  - The Privacy
  - The RID authentication
  - The RID identification
Addressed comments from Michael

• Section 1.1, extend ASTM F3411-19 to the extends that fits into DRIP’s architecture.
• Add Section 1.2.1 and Section 1.2.2 for N-RID and B-RID intro
• Section 1.4 updated issue list
• Add section 3 the “Definition and Abbreviations” to explain TLAs
• Add Section 4 HHIT for UAS ID with notes to be addressed in the following revisions
• Comments about informational language usage align with BCP14 yet needs to be fixed.

• Are those agreeable?
More comments from Daniel, Carsten, Amelia

• Removed hybrid RID subsection
• Added section 1.2.2 for B-RID figure
• refinement of safety vs security distinction, yet to be addressed:
  • May clarify it in section 10: “Security Consideration”

• Are those agreeable?
Way to move forward...

• In Section 1:
  • Update N-RID (Sec 1.2.1) and B-RID (Sec 1.2.2) figures to show the UA, GCS and DNS interacts
  • In Section 1.2.2 to clarify what Broadcast RID can do with or without Observer Internet connectivity (Crowd sourced?)
  • in Section 1.4, “Overview of the DRIP Architecture”, to clarify the connectivity requirements among UA, GCS, SP, DP...

• In Section 4, “HHIT for UAS RID”
  • Clarify how HHIT may be used as a RID solution for the listed issues.

• In section 5, “DRIP RID Entities”
  • May add “DNS register” subsection to address Daniel’s comment regarding:
    • What information is static/dynamic and when register may access DNS through network
    • Why should RID be in reverse DNS lookup?

• In Section 6,” UAS Remote Identifiers”
  • Clarify “why should RID be in reverse DNS lookup?”
  • Address the possibility of naming collision using HHIT
  • Justify why X.509 and PKI will not address the DRIP requirement
  • explain continuing role of some kind of CA even w/o X.509 PKI??
  • expand on different uses of & relationship between optional manufacturer-assigned HI & subsequent single-use HIs??

• Are those agreeable?

11/17/20
Thanks,