DRIP Authentication Formats & Protocols for Broadcast RID

draft-ietf-drip-auth-05

Adam Wiethuechter (AX Enterprize, LLC), Etal.
Changes since -03

• FEC section is now fully filled in, needs extensive review
• Link Type field and Manifest Window was removed
• Appendix A was filled in
• Appendix D added as a first past attempt for Med's comment
Pending Issues

• FEC needs review desperately
  • Do we need to specify a specific polynomial to ensure compatibility

• Appendix D review (Med)
  • Does this satisfy the comment in conjunction with Appendix A?

• Loosen some language
  • Manifest in parts of the document are the mandatory 2nd message to send, but it can be either Manifest or Wrapper – so wording update required
Next Steps

• Send for an English language review to Laura Welch
• Integrate comments from SEC DIR review
• WGLC?
Discussion (-auth)

Questions, Comments, Concerns?
DRIP Entity Tag Registration & Lookup

draft-ietf-drip-registries-01

Adam Wiethuechter (AX Enterprize, LLC), Etal.
Changes from -00

• New section in introduction for high level "story" of a typical lifecycle and use of registries in DRIP

• Attestation/Certificates now an Appendix
  • Subsection for naming conventions for files and in text

• Some text on key rollover and federation

• Attempt at merging high level points from DET Section 5 into Section 4

• Section 7 and 8 are merged into one section (Section 6)
  • Much cleaner formatting and more fleshed out

• EPP and RDAP sections
  • EPP section has examples now that are being used in AX implementation
Title Reasoning

• Draft primary focus is on the registration of and look ups of DETs
  • And other information associated with DET

• DRIP is not bound to DNS, EPP or RDAP
  • Other drafts can be written to support newer technologies
  • The use of DNS, EPP and RDAP in this draft is to lay down a **baseline** for standardization to allow DRIP deployments

• DRIP is not bound to DET
  • No other solution has been put forward – but if one comes later...
  • Draft registration architecture (the tree) is strongly tied to HID structure of DET
  • Another identifier would need to either mimic the HID, produce a whole new registration architecture, or modify existing draft format
Pending Issues

• Fix Contributors section
  • Scott H. was incorrectly pulled into it; meant to stay as Acknowledgement

• Pull in Andrei's text
  • Was an oversight that was lost in emails
  • Is this an Appendix?

• Break EPP/RDAP into separate documents?
  • Scott H. suggestion on list

• Pull in text about RAA/HDA from –rid to here

• Title change
Registration Process
Registry Tree Diagram
Typical Registration Operations

• Serial Number registration at Manufacturer (MRA)
  • DET encoded as ANSI CTA2063-A (per DET draft)

• Operator registration at USS (RIDR)
  • DET proposed to used by an Operator in Session ID Registration

• Session ID registration at USS (RIDR)
  • DET proposed to be used by UA
Serial Number MRA Registration

Diagram:
- **Manufacturer's Registry of Aircraft**: DNS, Database, Software
- **Manufacturer**
- **Unmanned Aircraft**

Procedure:
1. **Start**
2. Generate $H_0/DET_0/SA-a_2$
3. **Propose** $DET_0/Hi_0$ using $SA-a_3$
4. **Extract** $DET_0$ from $SA-a_3$
5. **DEI Collision Check**: Valid/Invalid
6. Generate $A-m.a_3$ using $SA-m + SA-a_3$
7. **Encode** $DET_0$ into $SN_{DEI}$
8. **DEI Collision Check**: Valid/Invalid
9. **SN_{DEI} RR_{x}**
10. **SN_{DEI} RR_{y}**
11. **SN_{DEI} + UA Information**
12. **SN_{DEI} + H_0 + DET_0 + SA-a_2 + A-m.a_2**
13. **Build UA**
MRA: DNS / Database Records

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <dripSerial:create xmlns:dripSerial="urn:ietf:params:xml:ns:dripSerial-1.0">
      <dripSerial:SerialNumber>MRA000000000000000000</dripSerial:SerialNumber>
      <dripSerial:make>Fast Drones</dripSerial:make>
      <dripSerial:Model>0000</dripSerial:Model>
      <dripSerial:Manufacturer>Drones & Us</dripSerial:Manufacturer>
      <dripSerial:Material>Plastic</dripSerial:Material>
      <dripSerial:Length>4.0</dripSerial:Length>
      <dripSerial:Width>3.8</dripSerial:Width>
      <dripSerial:Height>12.0</dripSerial:Height>
      <dripSerial:NumberOfMotors>4</dripSerial:NumberOfMotors>
      <dripSerial:LengthOfPropeller>2.0</dripSerial:LengthOfPropeller>
      <dripSerial:CapacityOfBattery>5000</dripSerial:CapacityOfBattery>
      <dripSerial:Voltage>12</dripSerial:Voltage>
      <dripSerial:Weight>3.2</dripSerial:Weight>
      <dripSerial:ChargingTechnology>Lithium-Ion</dripSerial:ChargingTechnology>
      <dripSerial:TakeOffWeight>15</dripSerial:TakeOffWeight>
      <dripSerial:MaxPayloadWeight>18</dripSerial:MaxPayloadWeight>
      <dripSerial:MaxFlightTime>15</dripSerial:MaxFlightTime>
      <dripSerial:MinOperatingTemp>-35</dripSerial:MinOperatingTemp>
      <dripSerial:MaxOperatingTemp>98</dripSerial:MaxOperatingTemp>
      <dripSerial:IpRatings>55</dripSerial:IpRatings>
    </dripSerial:create>
  </command>
</epp>
```

<table>
<thead>
<tr>
<th>Inputs (Optional)</th>
<th>DNS Entries (Optional)</th>
<th>Outputs (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>&lt;sn_det_fqdn&gt; HIP &lt;hsp_rr_data&gt;</td>
<td>(Attestation: MRA, UA)</td>
</tr>
<tr>
<td>(UA Self-Attestation)</td>
<td>&lt;sn_det_fqdn&gt; CERT &lt;sn_self_attestation&gt;</td>
<td>(Broadcast Attestation: MRA, UA)</td>
</tr>
<tr>
<td>UA Metadata</td>
<td>&lt;sn_det_fqdn&gt; CERT &lt;attestation_mra_sn&gt;</td>
<td>(Concise Attestation: MRA, UA)</td>
</tr>
<tr>
<td></td>
<td>&lt;sn_det_fqdn&gt; CERT &lt;concrete_attestation_mra_sn&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;sn_det_fqdn&gt; CERT &lt;broadcast_attestation_mra_sn&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Session ID RIDR Registration

Remote ID Registry

DNS

Database(s)

Software

Operator

Unmanned Aircraft

Start

Generate Session ID

SN + A-o.a_i [Additional Info]

Generate A-o.a_i using SA-o + A-o.a_i

Invalid

Generates HJ/DET/SA-a_i/A-a_i

Invalid

Invalid

AC-r.o.a_i + BA-r.a_i

BA-r.a_i

AC-r.o.a_i + BA-r.a_i

Valid/Invalid

DET Collison Check

Valid/Invalid

DET_j, RRs

SN + A-r.o + A-o.a_i

[Additional Info]

Detect Collision Check from A-o.a_i

Extract DET_j

DRIP WG -- IETF 113 -- March 23, 2022

15
## RIDR: DNS / Database Records

<table>
<thead>
<tr>
<th>Inputs (Optional)</th>
<th>DNS Entries (Optional)</th>
<th>Outputs (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation: RIDR, Operator</td>
<td><code>&lt;session_det_fqdn&gt; HIP &lt;hip_rr_data&gt;</code></td>
<td>Attestation: RIDR, Operator</td>
</tr>
<tr>
<td>Attestation: Operator, UA</td>
<td><code>&lt;session_det_fqdn&gt; CERT &lt;session_self_attestation&gt;</code></td>
<td>Broadcast Attestation: RIDR, Operator</td>
</tr>
<tr>
<td>Serial Number</td>
<td><code>&lt;session_det_fqdn&gt; CERT &lt;broadcast_attestation_ridr_session&gt;</code></td>
<td>Attestation Certificate: RIDR, Operator, UA</td>
</tr>
<tr>
<td>(Concise Attestation: Operator, UA)</td>
<td><code>&lt;session_det_fqdn&gt; CERT</code> <code>&lt;attestation_ridr_session&gt;</code></td>
<td>(Concise Attestation: RIDR, Operator)</td>
</tr>
<tr>
<td>(Mutual Attestation: Operator, UA)</td>
<td><code>&lt;session_det_fqdn&gt; CERT</code> <code>&lt;concise_attestation_ridr_session&gt;</code></td>
<td>(Mutual Certificate: RIDR, Operator, UA)</td>
</tr>
<tr>
<td>(Link Attestation: Operator, UA)</td>
<td><code>&lt;session_det_fqdn&gt;</code> <code>&lt;concise_attestation_ridr_session&gt;</code></td>
<td>(Link Certificate: RIDR, Operator, UA)</td>
</tr>
<tr>
<td>(Operational Intent)</td>
<td></td>
<td>(Broadcast Attestation: RAA, RIDR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Broadcast Attestation: Root, RAA)</td>
</tr>
</tbody>
</table>

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <dripSession:create xmlns:dripSession="urn:ietf:params:xml:ns:dripSession-1.0">
        <dripSession:serial>000000000000000000000</dripSession:serial>
        <dripSession:uid></dripSession:uid>
        <dripSession:sessionHt></dripSession:sessionHt>
        <dripSession:operationIntent></dripSession:operationIntent>
        <dripSession:operationIntentSrc>uss.example.com</dripSession:operationIntentSrc>
        <dripSession:operatorId>NNIF23456</dripSession:operatorId>
        <dripSession:operatorDet></dripSession:operatorDet>
        <dripSession:fa3>N123456</dripSession:fa3>
      </dripSession:create>
    </create>
    <c1TRID>ADD-SID</c1TRID>
  </command>
</epp>
```
Next Steps

• Feedback on EPP section examples
• Produce some RDAP examples
• Federation of registries/keys
  • Interesting topic to see how it would affect deployments and use of system
  • Any takers to explore?
• Plan for an interim to focus on deep dive of registration z-diagrams
Discussion (-registries)

Questions, Comments, Concerns?