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

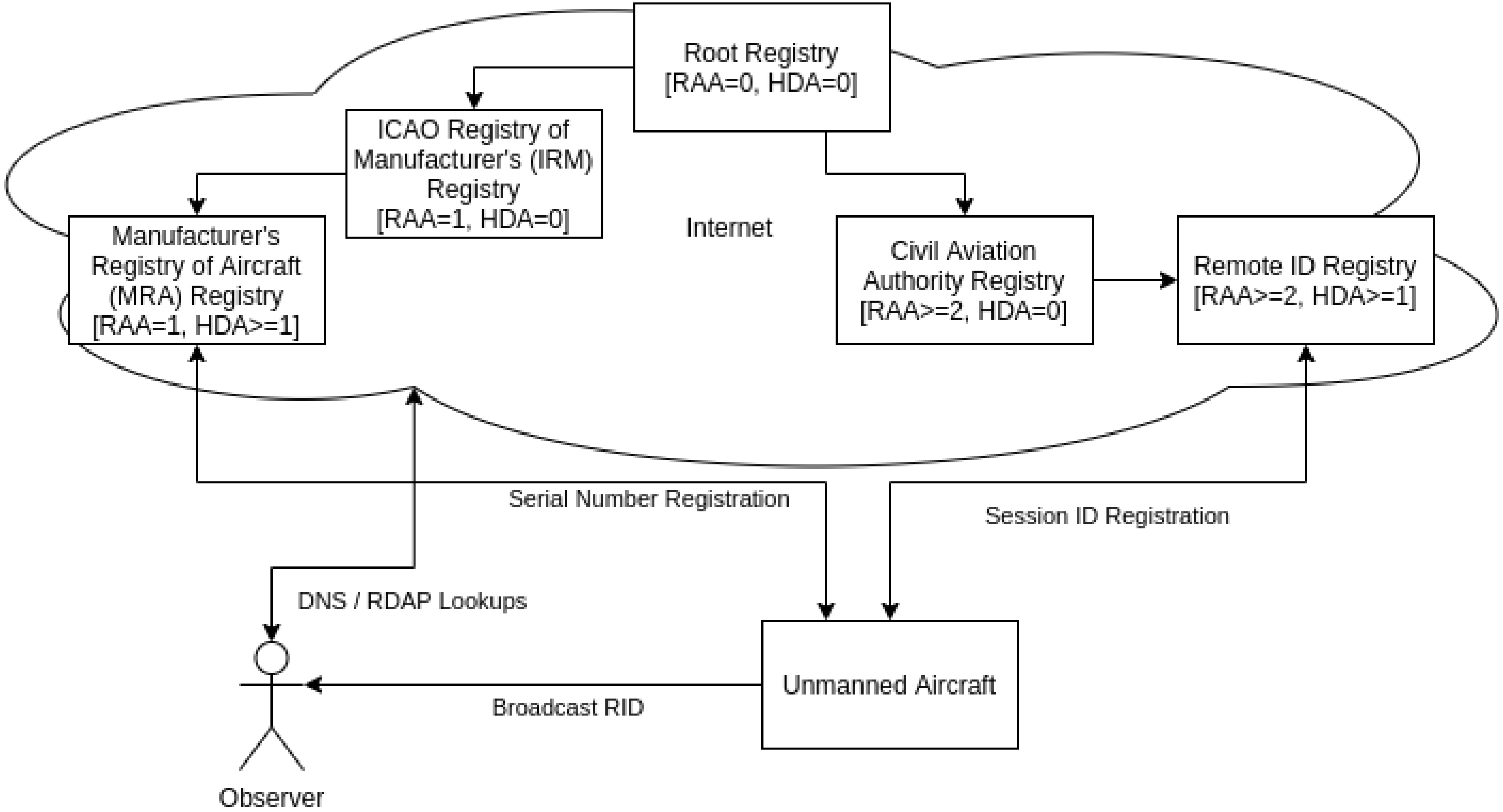
- Draft primary focus is on the registration of and look ups of DETs
  - And other information associated with DET
- DRIP is not bound to DNS, EPP or RDAP
  - Other drafts can be written to support newer technologies
  - The use of DNS, EPP and RDAP in this draft is to lay down a baseline for standardization 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

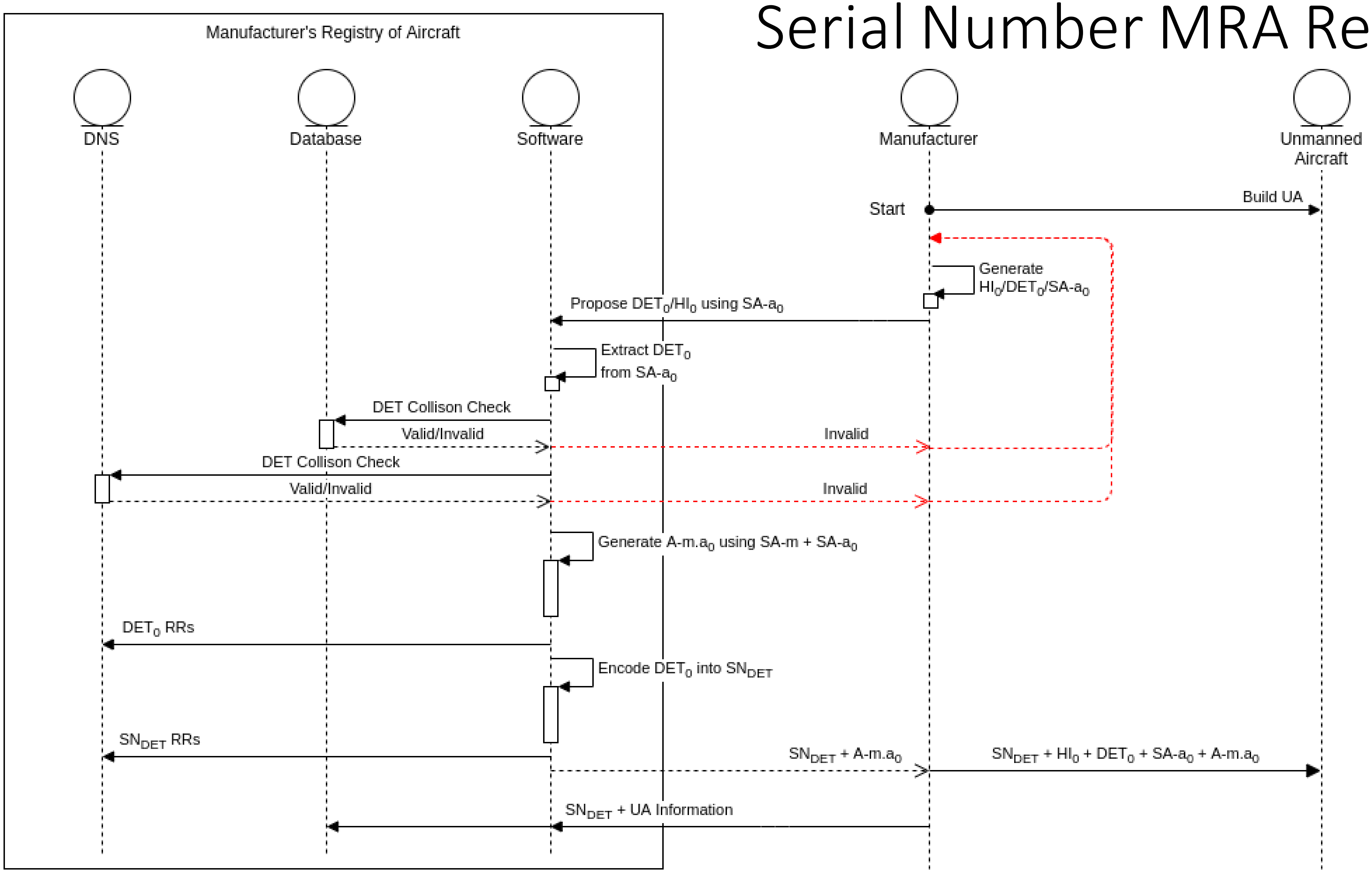
Registry Tree Diagram



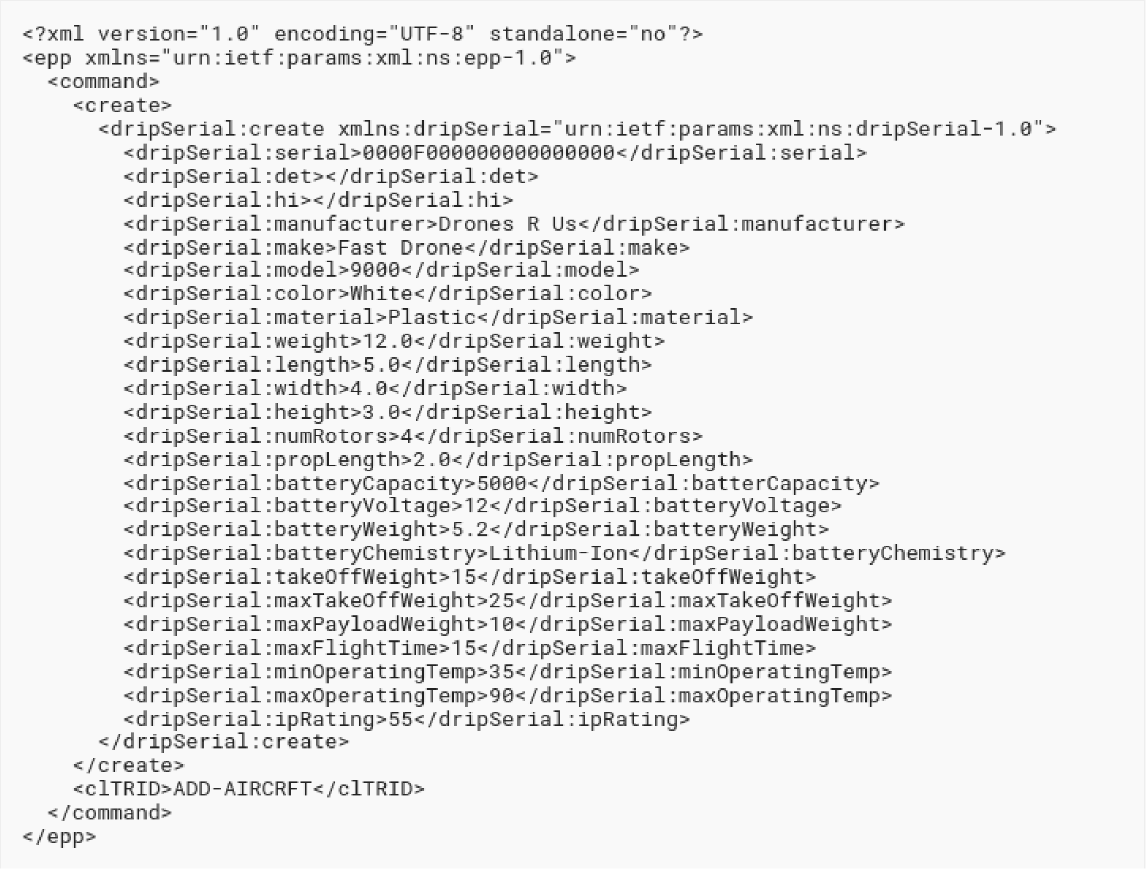
Typical Registration Operations

- 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

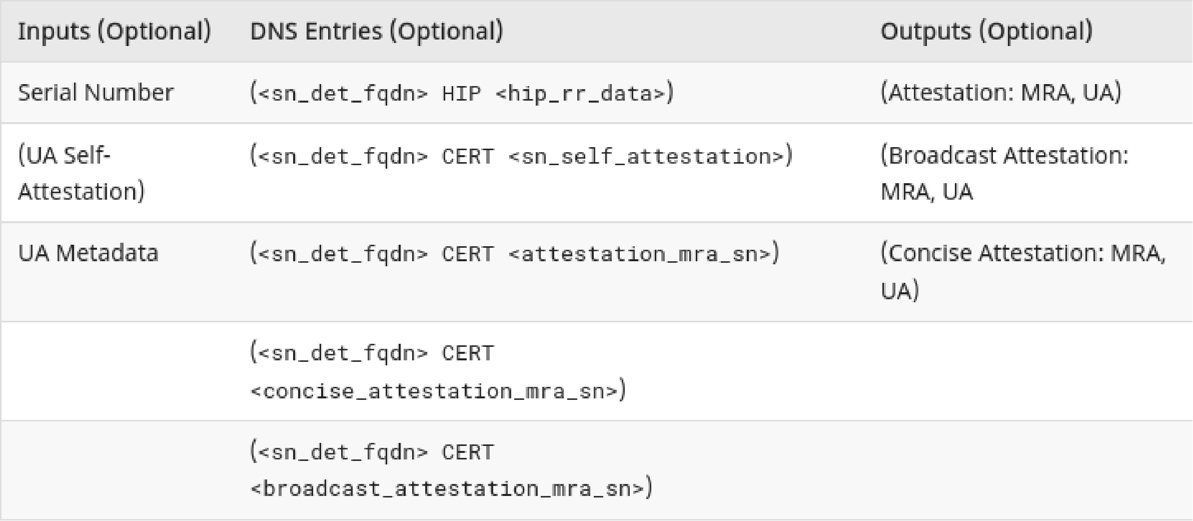
Serial Number MRA Registration


Manufacturer's Registry of Aircraft
DNS
Database
Software
Manufacturer
Unmanned Aircraft
Start
Build UA
Generate HI$_0$/DET$_0$/SA-a$_0$
Propose DET$_0$/HI$_0$ using SA-a$_0$
Extract DET$_0$ from SA-a$_0$
DET Collison Check
Valid/Invalid
Invalid
DET Collison Check
Valid/Invalid
Invalid
Generate A-m.a$_0$ using SA-m + SA-a$_0$
DET$_0$ RRs
Encode DET$_0$ into SN$_{DET}$
SN$_{DET}$ RRs
SN$_{DET}$ + A-m.a$_0$
SN$_{DET}$ + HI$_0$ + DET$_0$ + SA-a$_0$ + A-m.a$_0$
SN$_{DET}$ + UA Information

MRA: DNS / Database Records

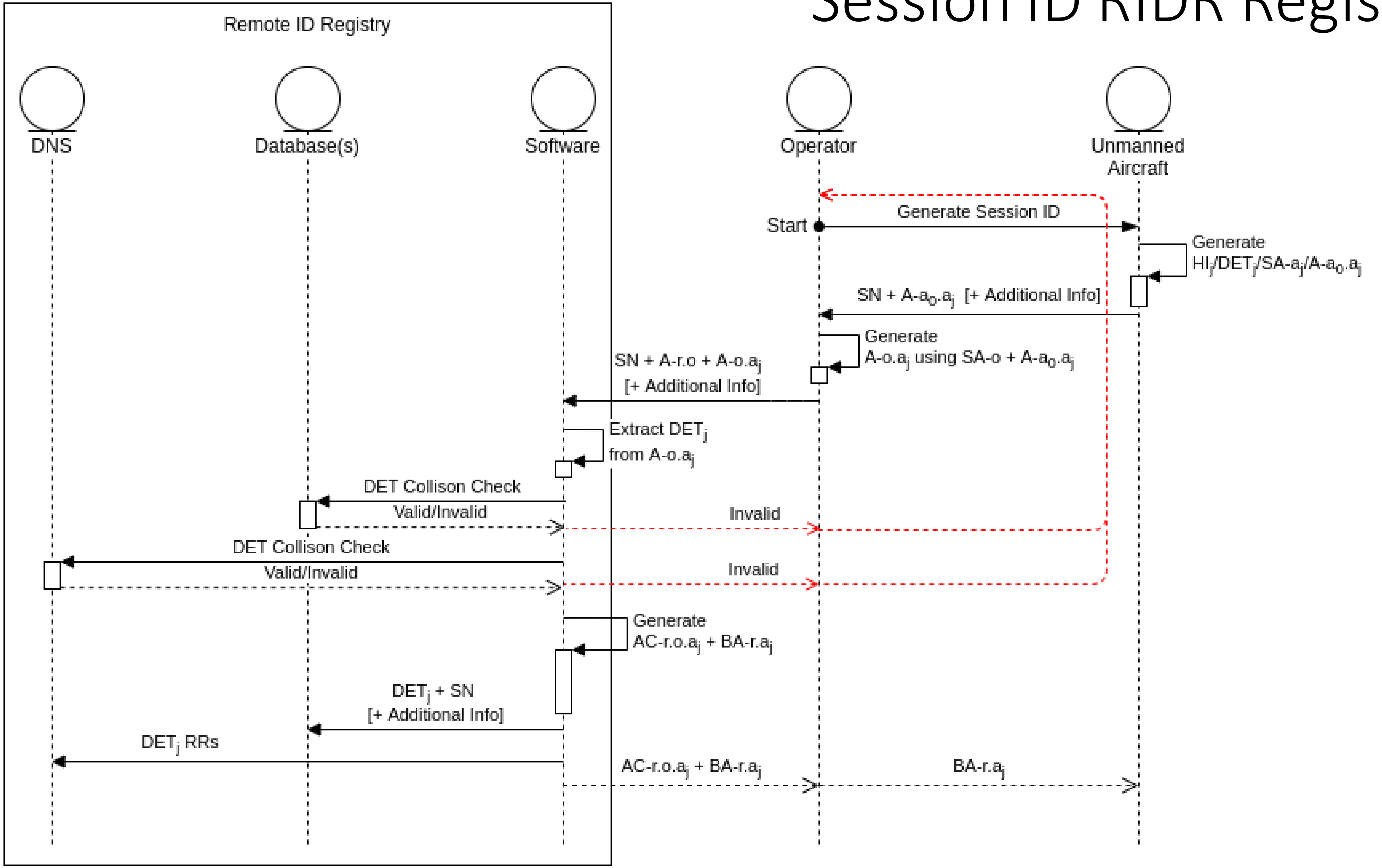


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <dripSerial:create xmlns:dripSerial="urn:ietf:params:xml:ns:dripSerial-1.0">
        <dripSerial:serial>0000F000000000000000</dripSerial:serial>
        <dripSerial:det></dripSerial:det>
        <dripSerial:hi></dripSerial:hi>
        <dripSerial:manufacturer>Drones R Us</dripSerial:manufacturer>
        <dripSerial:make>Fast Drone</dripSerial:make>
        <dripSerial:model>9000</dripSerial:model>
        <dripSerial:color>White</dripSerial:color>
        <dripSerial:material>Plastic</dripSerial:material>
        <dripSerial:weight>12.0</dripSerial:weight>
        <dripSerial:length>5.0</dripSerial:length>
        <dripSerial:width>4.0</dripSerial:width>
        <dripSerial:height>3.0</dripSerial:height>
        <dripSerial:numRotors>4</dripSerial:numRotors>
        <dripSerial:propLength>2.0</dripSerial:propLength>
        <dripSerial:batteryCapacity>5000</dripSerial:batterCapacity>
        <dripSerial:batteryVoltage>12</dripSerial:batteryVoltage>
        <dripSerial:batteryWeight>5.2</dripSerial:batteryWeight>
        <dripSerial:batteryChemistry>Lithium-Ion</dripSerial:batteryChemistry>
        <dripSerial:takeOffWeight>15</dripSerial:takeOffWeight>
        <dripSerial:maxTakeOffWeight>25</dripSerial:maxTakeOffWeight>
        <dripSerial:maxPayloadWeight>10</dripSerial:maxPayloadWeight>
        <dripSerial:maxFlightTime>15</dripSerial:maxFlightTime>
        <dripSerial:minOperatingTemp>35</dripSerial:minOperatingTemp>
        <dripSerial:maxOperatingTemp>90</dripSerial:maxOperatingTemp>
        <dripSerial:ipRating>55</dripSerial:ipRating>
      </dripSerial:create>
    </create>
    <clTRID>ADD-AIRCRFT</clTRID>
  </command>
</epp>
```

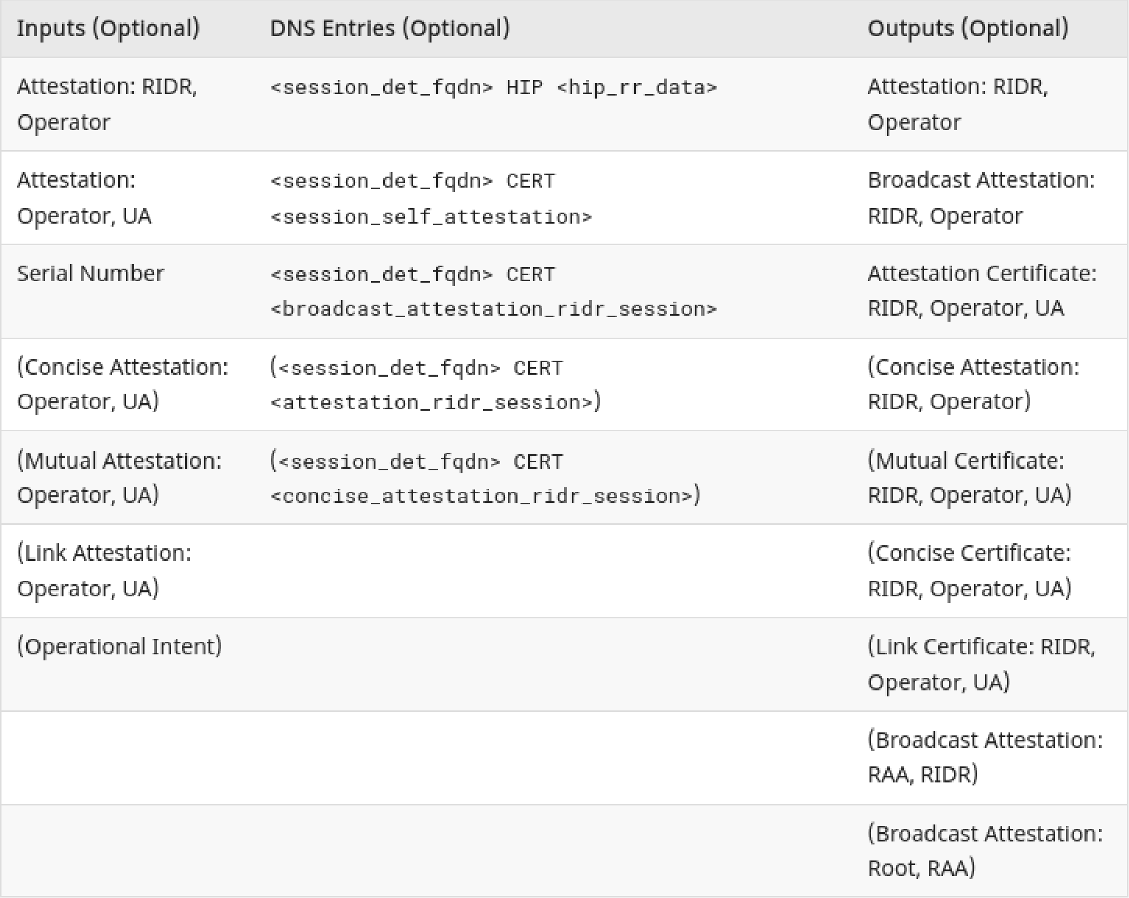


Inputs (Optional)	DNS Entries (Optional)	Outputs (Optional)
Serial Number	(`<sn_det_fqdn> HIP <hip_rr_data>`)	(Attestation: MRA, UA)
(UA Self-Attestation)	(`<sn_det_fqdn> CERT <sn_self_attestation>`)	(Broadcast Attestation: MRA, UA
UA Metadata	(`<sn_det_fqdn> CERT <attestation_mra_sn>`)	(Concise Attestation: MRA, UA)
	(`<sn_det_fqdn> CERT <concise_attestation_mra_sn>`)	
	(`<sn_det_fqdn> CERT <broadcast_attestation_mra_sn>`)	

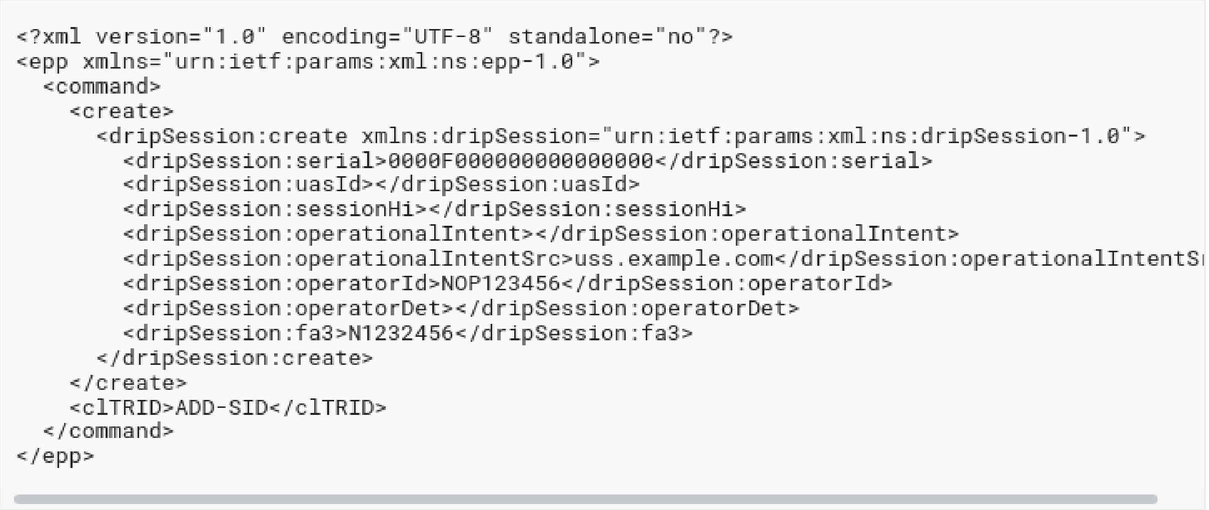
Session ID RIDR Registration


Remote ID Registry
DNS
Database(s)
Software
Operator
Unmanned Aircraft
Start
Generate Session ID
Generate $HI_j/DET_j/SA\text{-}a_j/A\text{-}a_0.a_j$
SN + $A\text{-}a_0.a_j$ [+ Additional Info]
Generate $A\text{-}o.a_j$ using SA-o + $A\text{-}a_0.a_j$
SN + A-r.o + $A\text{-}o.a_j$ [+ Additional Info]
Extract DET_j from $A\text{-}o.a_j$
DET Collison Check
Valid/Invalid
Invalid
DET Collison Check
Valid/Invalid
Invalid
Generate $AC\text{-}r.o.a_j$ + $BA\text{-}r.a_j$
DET_j + SN [+ Additional Info]
DET_j RRs
$AC\text{-}r.o.a_j$ + $BA\text{-}r.a_j$
$BA\text{-}r.a_j$

RIDR: DNS / Database Records



Inputs (Optional)	DNS Entries (Optional)	Outputs (Optional)
Attestation: RIDR, Operator	`<session_det_fqdn> HIP <hip_rr_data>`	Attestation: RIDR, Operator
Attestation: Operator, UA	`<session_det_fqdn> CERT <session_self_attestation>`	Broadcast Attestation: RIDR, Operator
Serial Number	`<session_det_fqdn> CERT <broadcast_attestation_ridr_session>`	Attestation Certificate: RIDR, Operator, UA
(Concise Attestation: Operator, UA)	(`<session_det_fqdn> CERT <attestation_ridr_session>`)	(Concise Attestation: RIDR, Operator)
(Mutual Attestation: Operator, UA)	(`<session_det_fqdn> CERT <concise_attestation_ridr_session>`)	(Mutual Certificate: RIDR, Operator, UA)
(Link Attestation: Operator, UA)		(Concise Certificate: RIDR, Operator, UA)
(Operational Intent)		(Link Certificate: RIDR, Operator, UA)
		(Broadcast Attestation: RAA, RIDR)
		(Broadcast Attestation: Root, RAA)



```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>0000F000000000000000</dripSession:serial>
        <dripSession:uasId></dripSession:uasId>
        <dripSession:sessionHi></dripSession:sessionHi>
        <dripSession:operationalIntent></dripSession:operationalIntent>
        <dripSession:operationalIntentSrc>uss.example.com</dripSession:operationalIntentS
        <dripSession:operatorId>NOP123456</dripSession:operatorId>
        <dripSession:operatorDet></dripSession:operatorDet>
        <dripSession:fa3>N1232456</dripSession:fa3>
      </dripSession:create>
    </create>
    <clTRID>ADD-SID</clTRID>
  </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?