

# DRIP Authentication Protocols & Formats for Broadcast RID

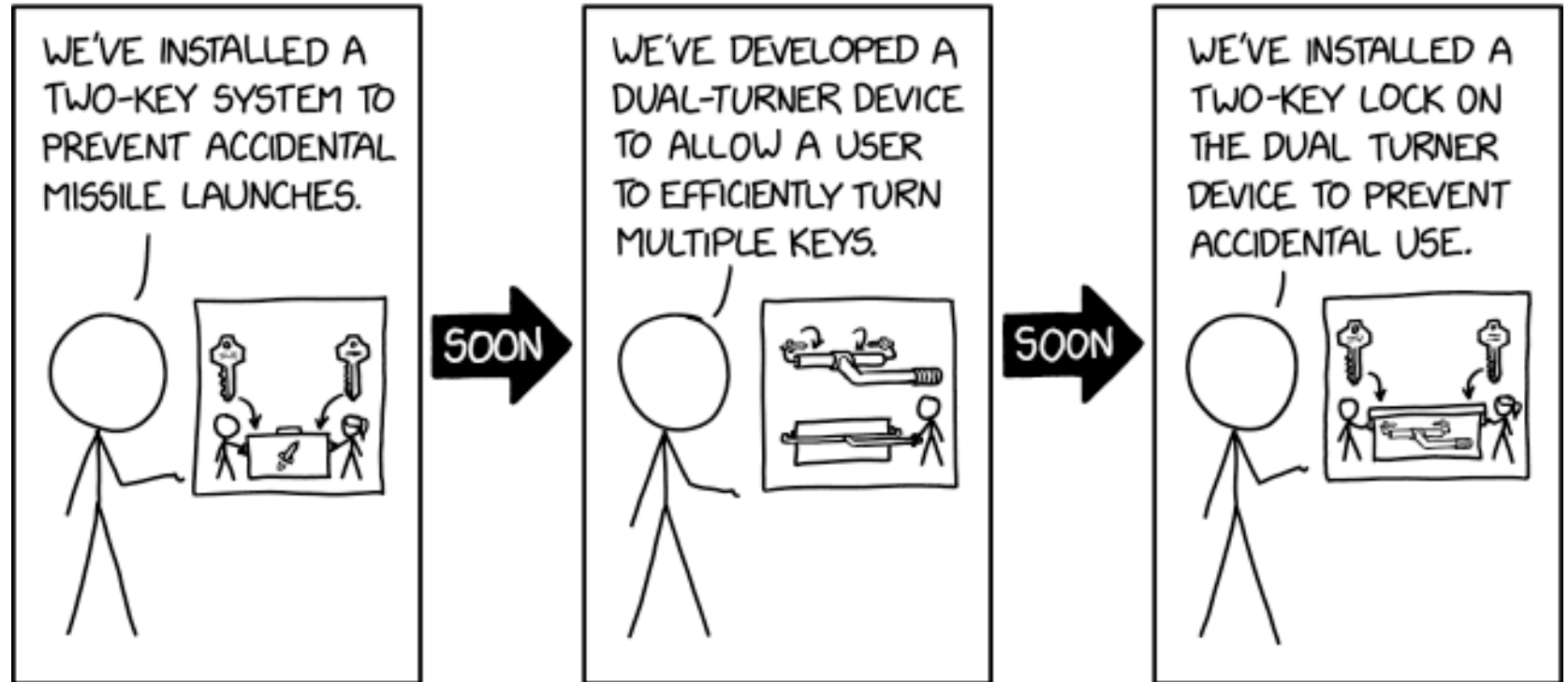
draft-ietf-drip-auth-26

Adam Wiethuechter (AX Enterprize, LLC)

# Quick Update

- ASTM + ICAO working through process now to setup registry for SAM Types
  - A formal letter of some kind to be sent between parties soon
  - Once they are ready, we can formally submit our request (to ICAO)
    - DRIP Link, Wrapper, Manifest, and Frame
- WGLC comments and issues
  - No substantive reviews
  - Med has added some issues to GitHub which are to be addressed shortly after 115

# ALL SOFTWARE DEVELOPMENT, EVENTUALLY



Hackathon 115

Our company can be your one-stop shop for decentralization.

<https://xkcd.com/2677/>

# Another successful Hackathon

- Talked with LiU students and gave some direction on drafts to implement and issues in their open-source implementation
  - Have been working on updates/changes during the week
- Two attendees physically here in London
  - Produced the first open-source implementation of a tool to generate and read Endorsements
    - Will be on the IETF WG GitHub under drip-scripts
  - Thanks Filip Debczak and Marius Kleidl!
- Was present at Hackdemo Happy Hour
  - Showing that the new tool interoperates with AX implementation over Broadcast RID

# DRIP Registry Updates

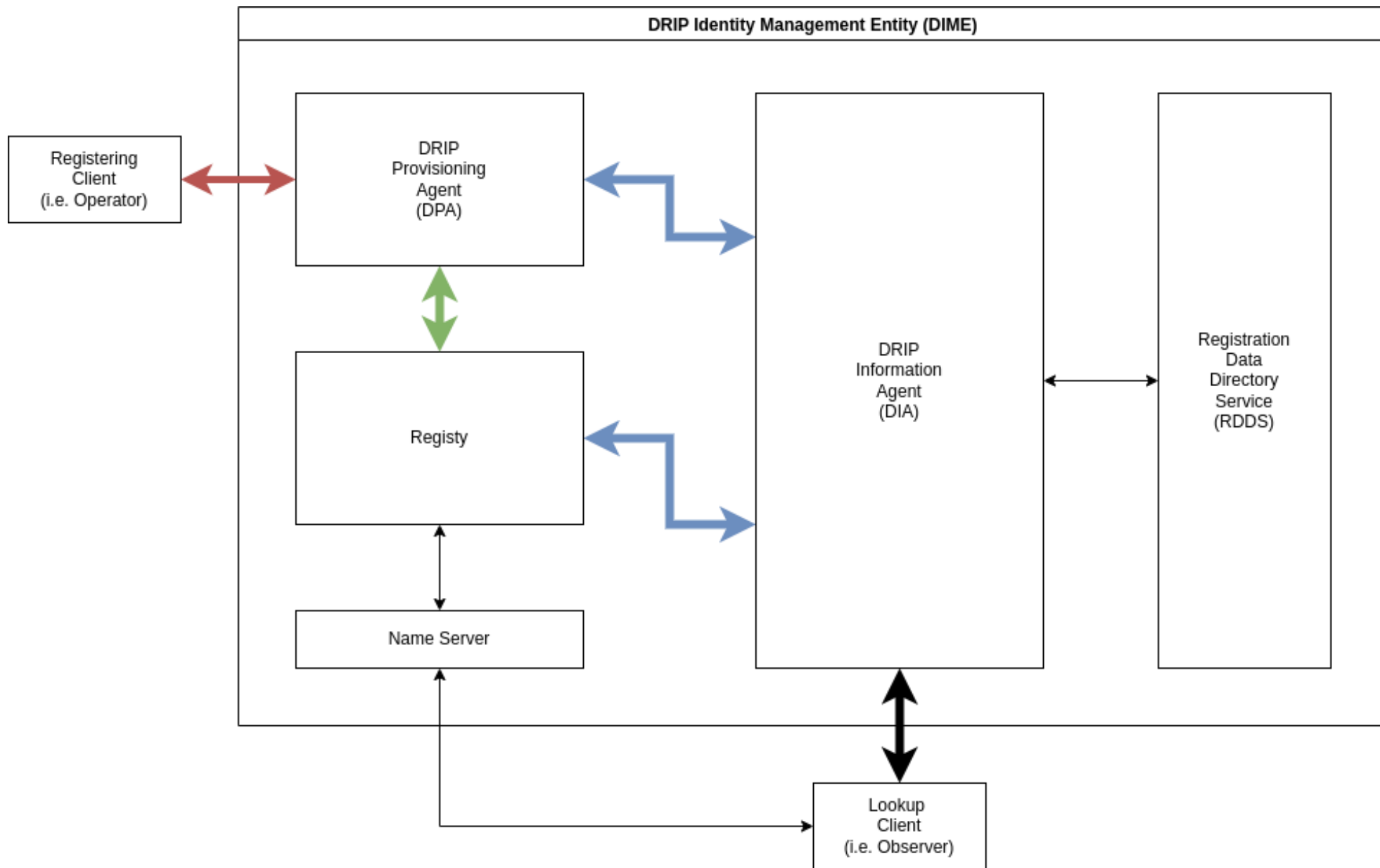
draft-ietf-drip-registries-05

draft-wiethuechter-drip-[detim-arch-00, dia-http-00, dia-rdap-00, dpa-http-00, registry-http-00, registry-epp-00]

# Current Status

- Proposed to break draft-ietf-drip-registries into multiple documents
  - Seemed like general agreement on concept, requested a 'dry-run' be done to see how the split would work
  - Resulted in an email with the raw MKD
  - Later, uploaded all as personal drafts to DRIP WG
- No comments from initial email or posting of documents
- AX live prototype fast tracking the documents

Today will focus discussion on this break up and get consensus to move forward or not



**Legend:**

Red Arrow:

-dpa-http

Green Arrow:

-registry-http  
-registry-ep

Blue Arrow:

-dia-http  
[-dia-ep?]

Black Arrow:

-dia-rdap

# -detim-arch

- The primary document for WG
- Becomes the primary architecture for DRIP registration & lookup that uses DNS technologies
- High level data models and information elements needed for interactions
- High level of different entities, roles, and logical components of a DRIP Entity Tag Identity Management (DETIM) system
- Short form...
  - DRIP Identity Management Entities (DIMEs) in the DETIM have multiple roles (Apex, RAA, HDA, etc.) and logical components (DPA, DIA, etc.) to perform functions such as registration and look up of DETs and Serial Numbers



# -detim-arch

- Document is a copy of draft-ietf-drip-registries with the following changes:
  - Updates to terminology to line up with -drip-arch if wasn't already in original document
  - Addition of sections explaining logical components
  - Update of Attestation -> Endorsement (now in main body of document)
  - Removal of EPP/RDAP implementation details
    - Tweak text as needed
    - Moved into their own documents
  - New DRIP IANA registry for key values of registration data
- Overall makes –drip-registries much easier to parse and modularizes a lot of the implementation specific details

Adopt this as a new revision/rename/replace existing –registries?

# -dpa-http

- Next most important document for WG
- Defines the interface for clients to register items to a DIME
  - Interface inputs different for items (Session ID, Serial Number, etc.)
  - Specifically JSON encoded formats
- Defined to talk to a "registry" to pass DNS information
  - Out of scope interface when integrated
  - Defined interface over HTTP (-registry-http) or EPP (-registry-epp) otherwise

Does WG wish to adopt this document?

# -dia-http

- Defines interface to add, update, delete entries in Registration Data Directory Service (RDDS)
  - Data in RDDS defined by role and interfaces supported
  - Performed by DPA or Registry
- HTTP method-based APIs (with JWT) is currently selected interface could be others as needed
  - EPP another candidate (document would be in REGEXT WG, mirror –registry-epp?)

Does WG wish adopt this document?

# Documents to move to other WGs?

- Least mature documents
  - -registry-http, -dia-rdap
- -registry-epp
  - More well defined but needs expert review

To get these documents right we need expertise from both DRIP and REGEXT WGs!

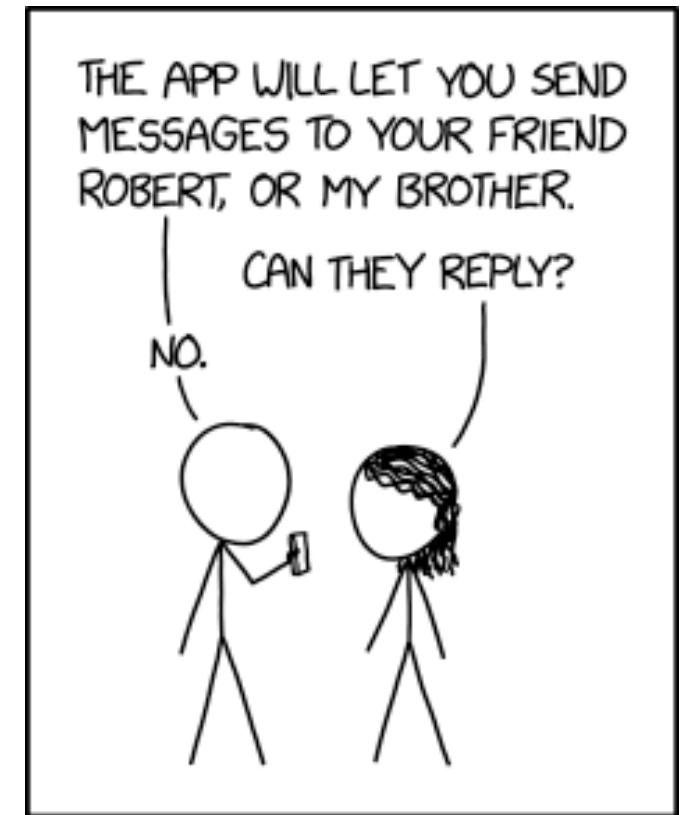
Where should this work live? Who can actively support us?

# Open Issues

- Apex of DNS tree
  - '\*.icao.int', '\*.hhit.arpa', others?
- Encryption key management
  - In support of draft-moskowitz-drip-operator-privacy
- Support of Serial Numbers for non-DRIP participants
  - Mechanism already exists for non-DRIP based Serial to be mapped to a DET (CNAME)
    - Would be done by the UA manufacturer
  - May want a mechanism to non-DRIP Serial to be 'registered' to HDA
    - Does this have value? UA probably doesn't even support Session IDs at that point
- In -detim-arch Endorsements defined using CDDL
  - In -auth this CDDL is referenced, and a subset is specified with specific encoding (binary)
  - Implementation drafts specify JSON or CBOR encodings

# Discussion

- Do we proceed with registry restructure?
  - Any issues with document scopes and names?
- Does WG approve to "adopt" -detim-arch?
  - In practice: rename existing –registries + text
- What documents stay in WG?
  - Adopt in WG?
    - -dpa-http
    - -dia-http
  - Move to other?
    - -registry-epp, -registry-http, -dia-rdap



MY NEW SECURE TEXTING APP ONLY ALLOWS PEOPLE NAMED ALICE TO SEND MESSAGES TO PEOPLE NAMED BOB.

WARNING: PEOPLE NAMED EVE ARE PROHIBITED FROM INSTALLING THIS APP!

<https://xkcd.com/2691>