

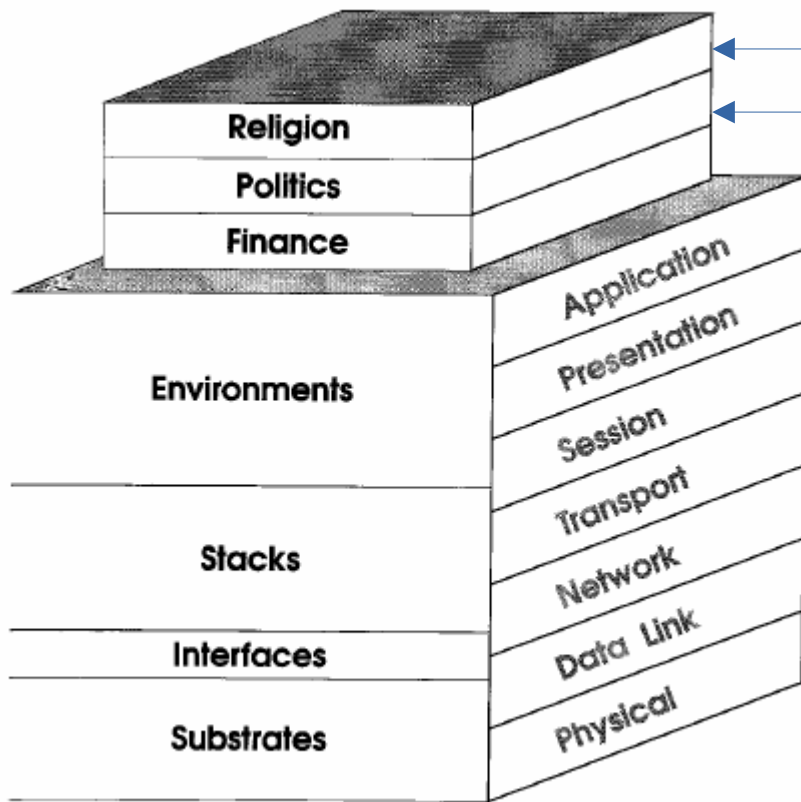
The DRIP DET Key Infrastructure

draft-moskowitz-drip-dki-05

June 14, 2023

Robert Moskowitz

Of DKIs and PKIs



You are here

Or Maybe here?

Some conversations never change

Figure 1-3 The 7 Layer Revised Model

“Stacks” – Carl Malamud, 1992

WHY?

- I tried to implement a test environment based on draft-ietf-drip-registries-09
 - And couldn't
 - Lots of unknowns
 - No tools
 - And potential security risks
 - That's due to my not clear thinking back early in the process (more later)

Two documents

- What is currently missing in drip-registries
 - Keep registries to technical matters
 - Reduce work for completion
 - Implementational matters in drip-dki
 - Items that may take time to resolve

- Now some details

Found trying to test was trying

- No open tool for creating DETs
- No open tool for creating Endorsements
- No clear understanding of HIP and TLSA and CERT RR contents
- So I learned some python. :(
 - Snaky stuff for sure; kept getting twisted in it

Need to document

- Jim Reid was kind enough to set up testing DNS
 - driptesting.org
 - apex.driptesting.org → raa.apex.driptesting.org
 - And ip6.arpa.driptesting.org → 3.0.1.0.0.2.ip6.arpa.driptesting.org
 - This exposed a serious delegation requirement and need of RAA assignment/delegation procedure
 - In the end ICAO can not step into this in time (2+ years?)₆

DNS choices

- drip-registries authors want ip6.arpa. structure
- I want apex.arpa. structure
 - As infrastructure stuff goes in .arpa.
- Both have challenge finding management entity
- I am willing to have a go at the ip6.arpa. direction
 - With reservations

Trust in Key handling

- All diagrams showing 3 levels of Endorsements flawed
 - HDA frequent signing of UA DET Endorsements a major security risk
 - Why we have always had an “Intermediate CA” in X.509 PKI
 - “Issuing” level added at HDA
 - But not at RAA

Trust in Key handling

- Needed to create clear naming for types of Endorsements
 - Authorization/Issuing/Operation
 - Authorization/Issuing the new risk mitigation piece
 - This impacts Broadcast RID Trust Chain transmissions

The missing Apex

- What is the Entity to function as the DRIP Apex?
 - Don't look to ICAO to easily step into this role
 - IATF PKI has been pushing for this for over 3 years for their "Bridge CA"
 - FAA/EUROCONTROL SWIM testing proceeding with direct cross-certification and no Bridge
 - Why did I think it would be easier for DRIP?
 - Need an alternative (like we did 25 years ago)

The missing Apex

- Three alternatives put forth
 - Trust Lists of RAAs
 - Recommended, but how to distribute
 - And no Apex in Auth transmissions?
 - RAA cross-endorsing
 - N^2 scaling problem – Acceptable for initial testing
 - RAA Bridges
 - Who runs them

Simplify Apex activities

- Simplify RAA assignment/delegation process
 - Base Nation State RAA on ISO 3166-1 numbers
 - UAS Manufacturer RAA/HDA allocation
 - Based on CTA codes
 - Test RAA
 - Others?
 - Regional agencies?
- Apex non-political? IANA/ICANN can do this?

“Shadow PKI”

- There are some out there in Aviation that REALLY want X.509 certificates
 - How to do this as backup to DKIM
 - And as light as possible
 - PKIX CSR as vehicle for DET registration?
 - But this belongs in drip-registries
 - Two profiles provided
- How much of this should be in drip-registries?

Integration with ICAO IATF PKI

- This could be a major move for DRIP
 - DETs in IATF ECDSA certificates
 - Leverage DET/DNS for IATF
 - Use IATF certificates in A2A communications
 - DET certificates in IATF
 - Further enhance IATF A2A activities
 - Further position DRIP in Aviation security
- Discussions in progress

Conclusion

- drip-dki grew out of filling gaps in drip-registries
- Is everything now addressed in both documents?
- Sort out what belongs were
- Get drip-registries moving to last call
 - drip-dki will take more work
 - Let dki “take the heat (politics and the like)”