1.2 DNSSEC Vision

June 12 – DNSSEC & Security Workshop

Rod Rasmussen, Jacques Latour, Danny McPhereson

Where are we?

- DNSSEC has been around forever
  - Penetration ”pretty good” – both deployment and resolution
  - Scales well
  - Largely solves problems that spurred adoption (cache poisoning, spoofing)
  - I can “trust” DNSSEC signed DNS replies/entities to be what they ”should be”
  - Ubiquitous and well-tested – operationally solid
- Friction to ”finishing the job”
  - Lots of effort in many forums (ICANN, IETF, DNS Operators, RRs/Rys, ISPs)
  - So what’s the payoff and why do more?
  - Are the “problems” solved worth the operational risks?
  - Some thorny operational issues
- Killer app to overcome inertia?

What's this vision thing you speak of?

- DNSSEC is a unique solution for many challenges
  - Disparate trust systems need to interoperate
  - No one can create a "new" system everyone else uses, trusts, deploys
  - Scaling things to the whole Internet is really hard
  - People want to "do their own thing" but still work everywhere with others
- DNSSEC checks the boxes
  - Standards based, baked-into the base infrastructure
  - Ubiquitous/available to all networks
  - Uniquely trusted governance/acceptance
  - Proven scalability/operational experience

DNSSEC Can Be…

- The Universal Trust Anchor
- Substrata for Internet-wide interoperable trust
- Foundation for services of all types
- New products/services for existing & new players
- A way for individual entities to control their trust relationships

People have been & are working on stuff

- DANE – Named entitiy authentication
  - Verifiable information for multi-factor verification
  - Defining CAs/TLS for domains
  - Basis for other work
- Interoperable, Scalable Encrypted Email
- IoT and client authentication (DANCE)
- Object Security
- Connections for digital trust regimes

We’re not quite there yet…

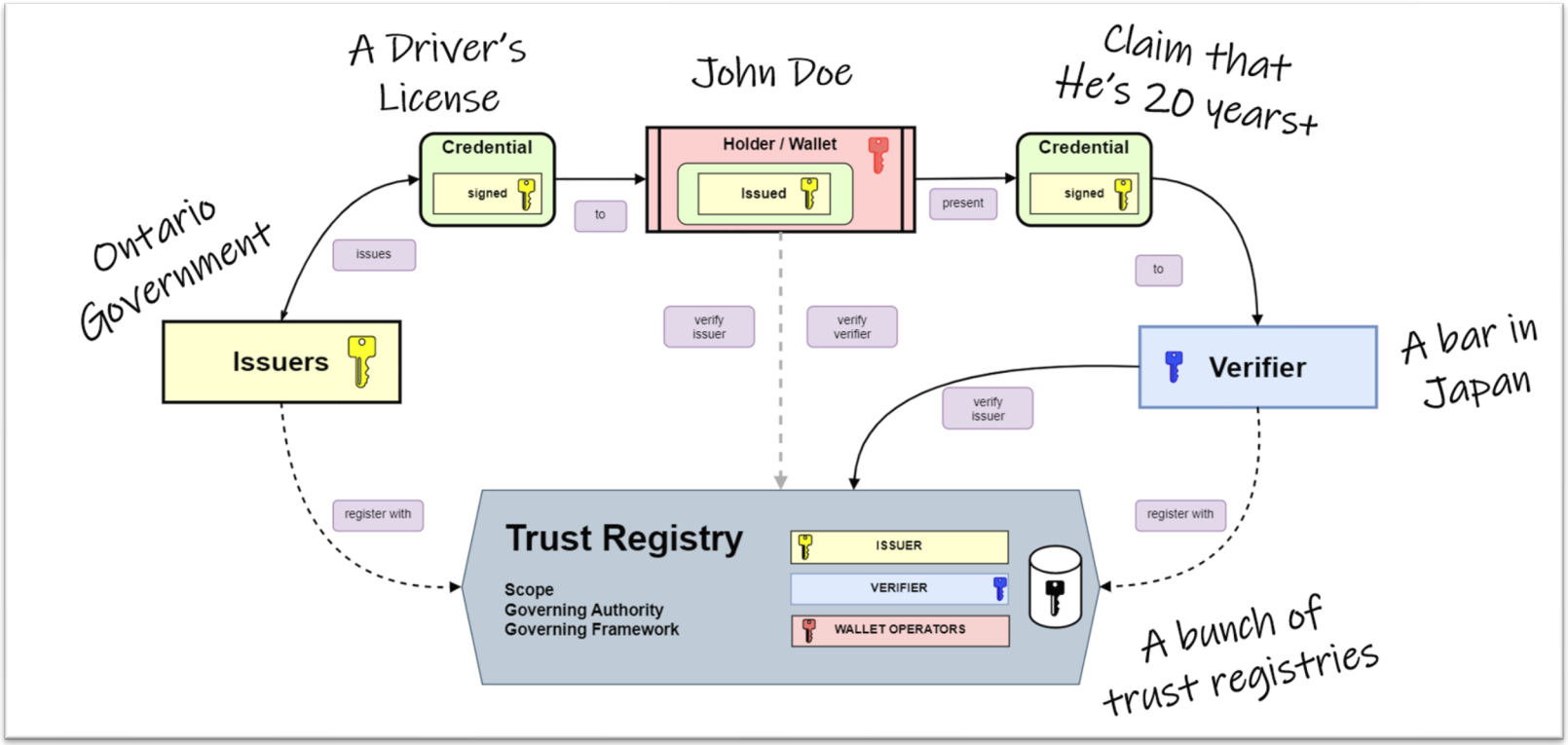
- Today’s workshop is about a particular issue in providing DNSSEC scalability
- Other issues still exist to address
- Fundamental strata infrastructure requires fully solid base
  - Risky to build “big things” or $$$ services on infrastructure with holes

Examples of Cool Stuff

Jacques' DNSSEC Vision Slides "Digital Trust and DNSSEC go hand in hand"

June 12 – DNSSEC & Security Workshop

DNS enables global Digital Trust interoperability
DNSSEC ensure authenticity of ecosystems



Digital Trust is all about verifying

< Authenticity, accuracy and authority >

DNSSEC enables authenticity in DNS transactions

When an entity is presented with a verifiable claim, there are three things they will want to ensure:

1. **That a claim hasn't been altered/falsified at any point in time**
   (Cryptographic proof verifiability, TLSA records)
2. **That a claim has accurate representation**
   (Authentication, DID Discovery/mapping within DNS)
3. **That a claim has authority**
   (Authorization, Trust Registries/trust lists, TLSA records)

The change from Opportunistic to Deterministic Protocol communications

The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

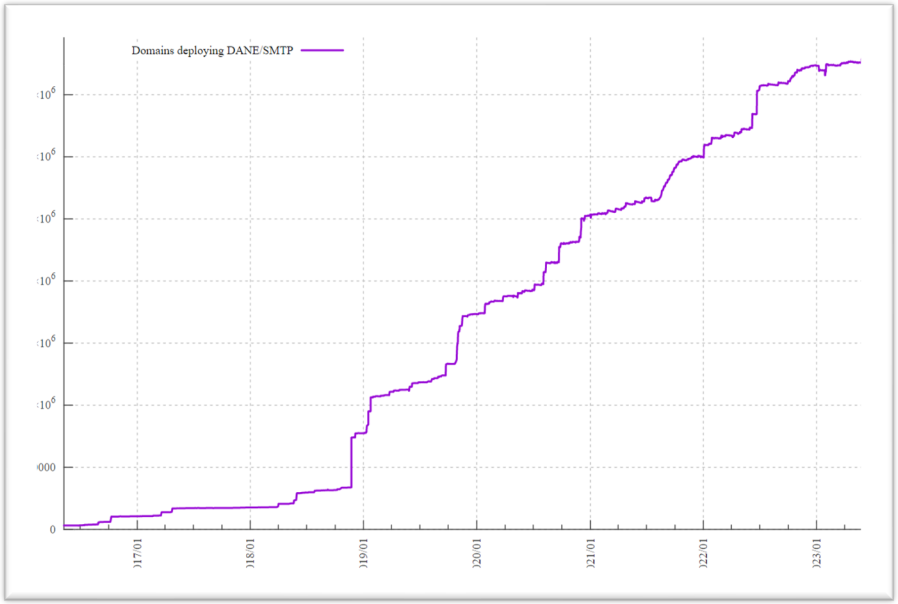
<- STARTED HERE

DOING MORE ->

The DANE Authentication for Network Clients Everywhere (DANCE) WG seeks to extend DANE (RFC 6698) to encompass TLS client authentication using certificates or Raw Public Keys (RPK).

Example: Use case for DANE/SMTP in Germany

IT WORKS ->



https://stats.dnssec-tools.org/