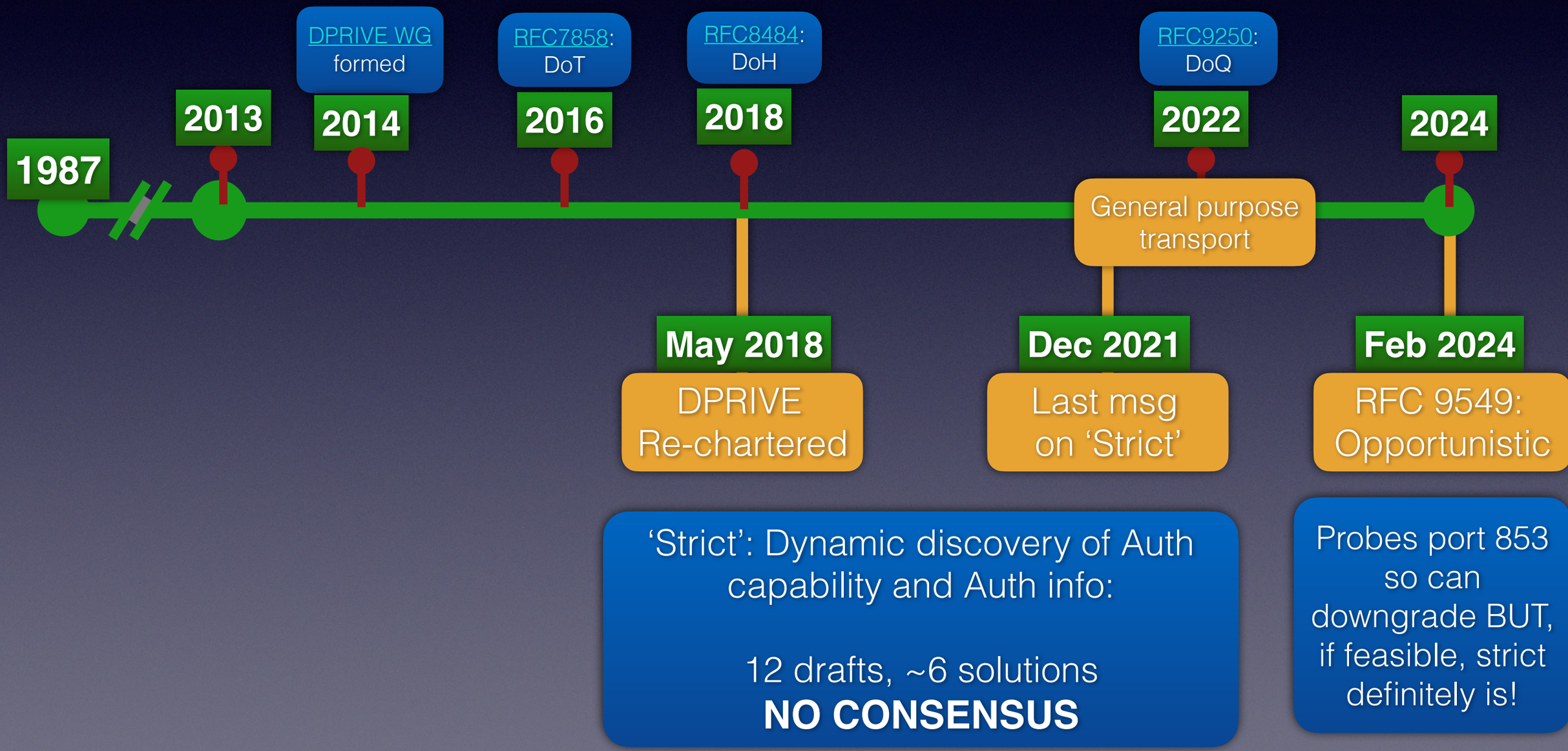
Recursive to Authoritative Encrypted DNS - Where are we?

Sara Dickinson sara@sinodun.com

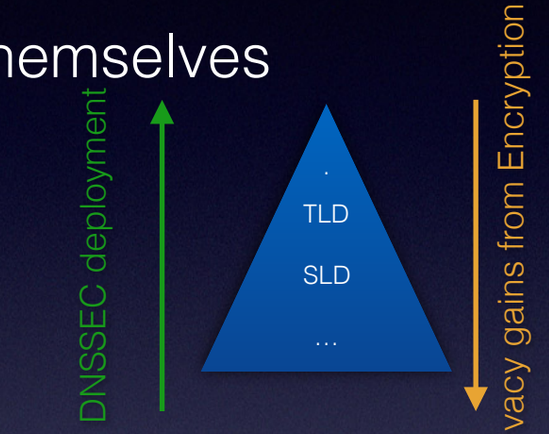
DPRIVE Work on Rec-Auth



Why is Strict hard?

1. **DNSSEC**: In-band credentials (name or SPKI) MUST be secure themselves
   - DNSSEC deployment is inverse to gains from privacy

2. **DELEGATIONS ARE NOT SIGNED**: Neither is glue



3. **ADoT IS A PROPERTY OF**…. a zone, nameserver or IP address?

Per zone delegation	• Fine grained control, BUT • Updating 1 nameserver -> many zones (child+parent)
Nameserver names	• Aliasing -> name mismatch complications • Effect all zones on nameserver at same time
IP based	• But IP certs are not common…

Note: compared to DNSSEC this adds secondary zone operator to deployment chain

Why is Strict hard?

		A (nameserver)	B (zone)
1	New Parent side RR	TLSA/SVCB for nameserver that can be signed	i. A new delegation model (using DNSSEC) ii. DSPKIs for zone
2	Parent side hack	Overload NS - put SPKI in name (DNSCrypt like) Not signed/slow	Overload DS (new algo) with SPKI or SVCB for child Too hacky, risky
3	Child side RR	TLSA/SVCB for nameserver	DSPKI like records

Full Ecosystem change (EPP, ICANN, etc.,)
Impractical

- **Child MUST be signed**
- Glue not signed/**slow**
- Leaky
- Slows all zones?

If not DELEG, how?

- Proposal to create new DNSSEC signed delegation path
  - Potential solution to include encryption credentials
    - Current status - BoF/WG forming… years away if at all

- In the meantime….
  - Need the results from opportunistic on speed and attacks
  - 80/20 option - encrypt biggest resolvers to most SLDs/CDNs…