Authentication and (D)TLS Profiles for DNS-over-TLS and DNS-over-DTLS

draft-ietf-dprive-dtls-and-tls-profiles-01

S. Dickinson Sinodun
D. Gillmor ACLU
T. Reddy Cisco

BUENOS AIRES D-PRIVÉ WG IETF 95

Recap

- DNS-over-TLS is now approved as RFC
- DNS-over-DLTS is at version -06

Originally both described authentication

- DNS-over-TLS RFC still contains
  - Strict Authentication using SPKI pinsets
  - Opportunistic security

A standard authentication mechanism enables deployment

Recap

- IETF 94: WG agreed to create a ‘combined’ document for other authentication mechanism
- Authentication removed from DNS-over-DTLS
- Also agreed a combined (D)TLS profile should move to this draft (from I-D: “DPRIVE TLS/DTLS Message Flows”)
- Adopted by WG January 2016 (revved to -01)

What is in the draft?

- Scope is
  - Both DNS-over-TLS and DNS-over-DTLS
  - Authentication of Recursive DNS Server by client
    - Not client authentication, not Authoritative
  - Domain name based authentication
    - Normative ref to DNS-over-TLS RFC
- “Privacy Enabled DNS Server”

Terminology

- **“Usage Profiles”**
  - Describe *security properties*, without reference to a specific authentication mechanism
  - Strict
  - Opportunistic
  - No Privacy

- Comment: Unclear/confusing?
- Slightly different to DNS-over-TLS draft…
- Both will be clarified!

Usage Profile: No Privacy

- Usage Profiles
  - Strict
  - Opportunistic
  - **No Privacy**

Clear text 🔓

Usage Profile: Opportunistic

- Usage Profiles
  - Strict
  - **Opportunistic**
  - No Privacy

[RFC7435]
"... the use of **cleartext** as the baseline communication security policy, with encryption and authentication negotiated and applied to the communication when available." 🔓

Detecting attacks

Usage Profile		Passive Attacker	Active Attacker
Strict		P	P
Opportunistic	Auth + Enc	P	P
	Enc	P	N (D)
	Clear text	N (D)	N (D)
No Privacy		N	N

Usage Profile: Strict

- Usage Profiles:
  - **Strict**
  - Opportunistic
  - No Privacy

Authenticate or die 🔒

BUT…

- meta queries can be Opportunistic but
- MUST be DNSSEC validated

Super Strict?

- Usage Profiles
  - Strict
  - Opportunistic
  - No Privacy

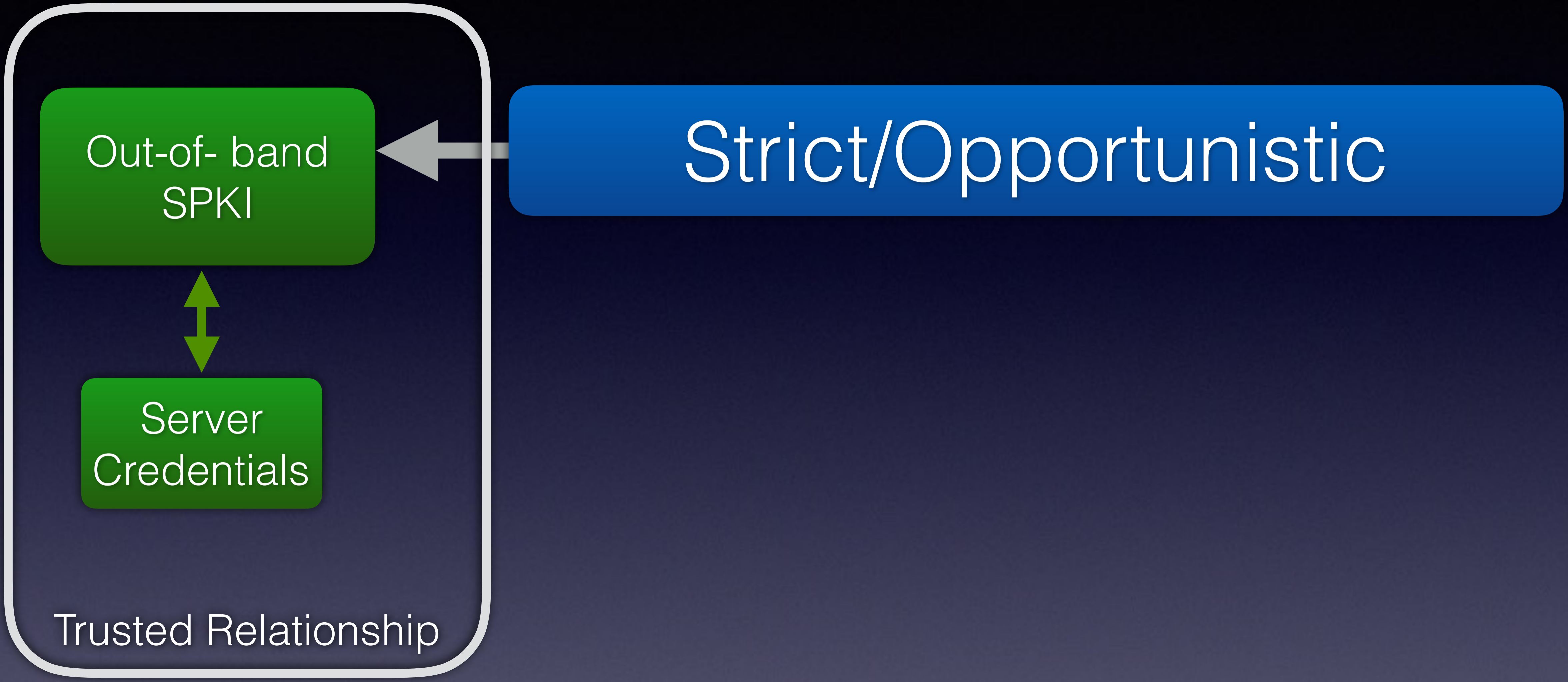
Q: What about requiring ALL queries (including meta queries) to be private?

Relaxed?

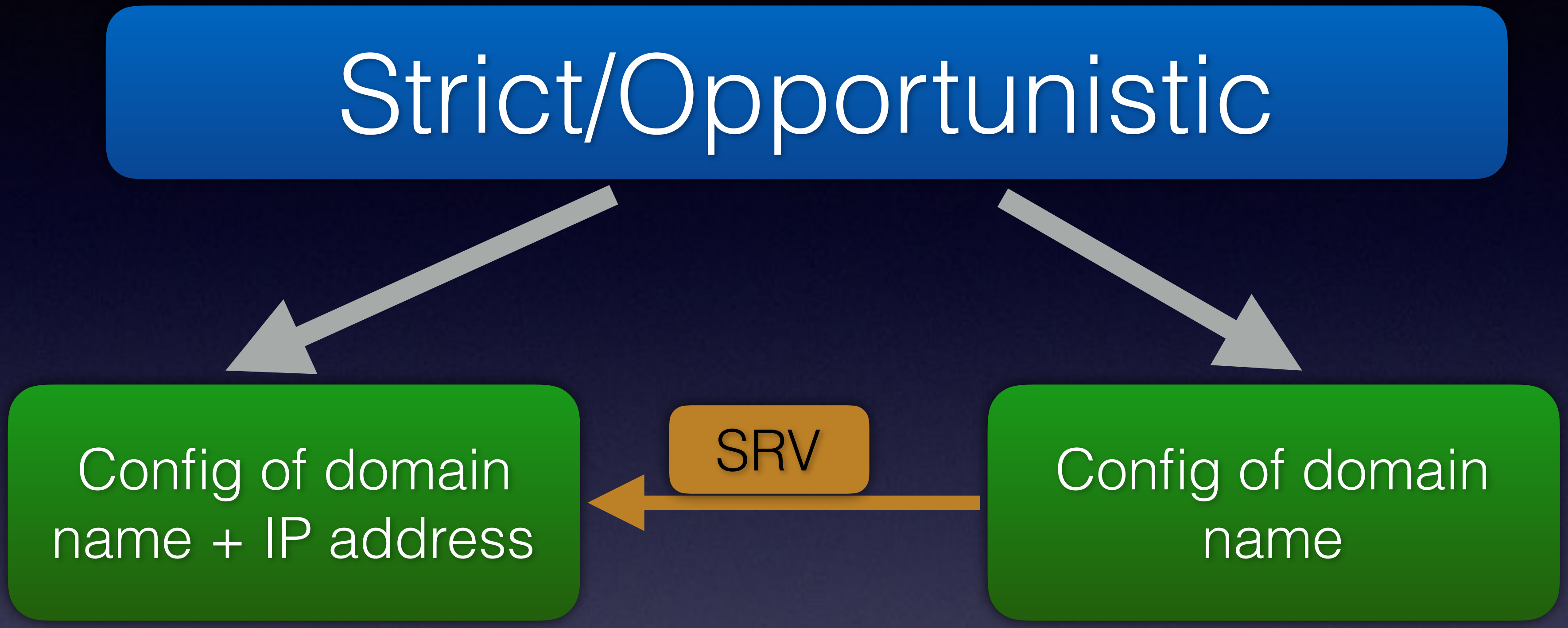
- Usage Profiles
  - Strict
  - Opportunistic
  - No Privacy

Q: What about requiring encryption but no authentication?

Auth mechanisms



Auth mechanisms



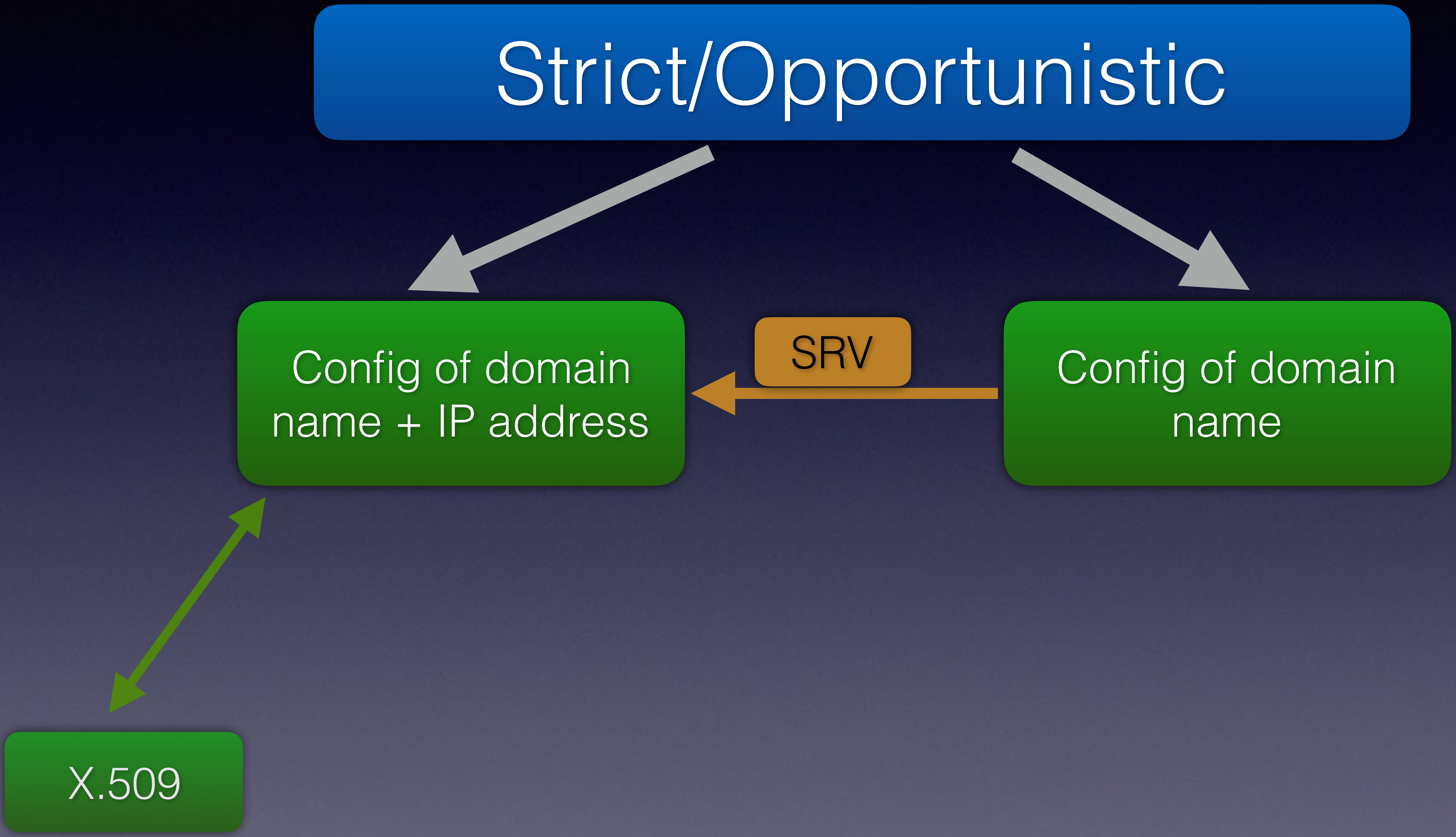
Strict/Opportunistic

Config of domain name + IP address

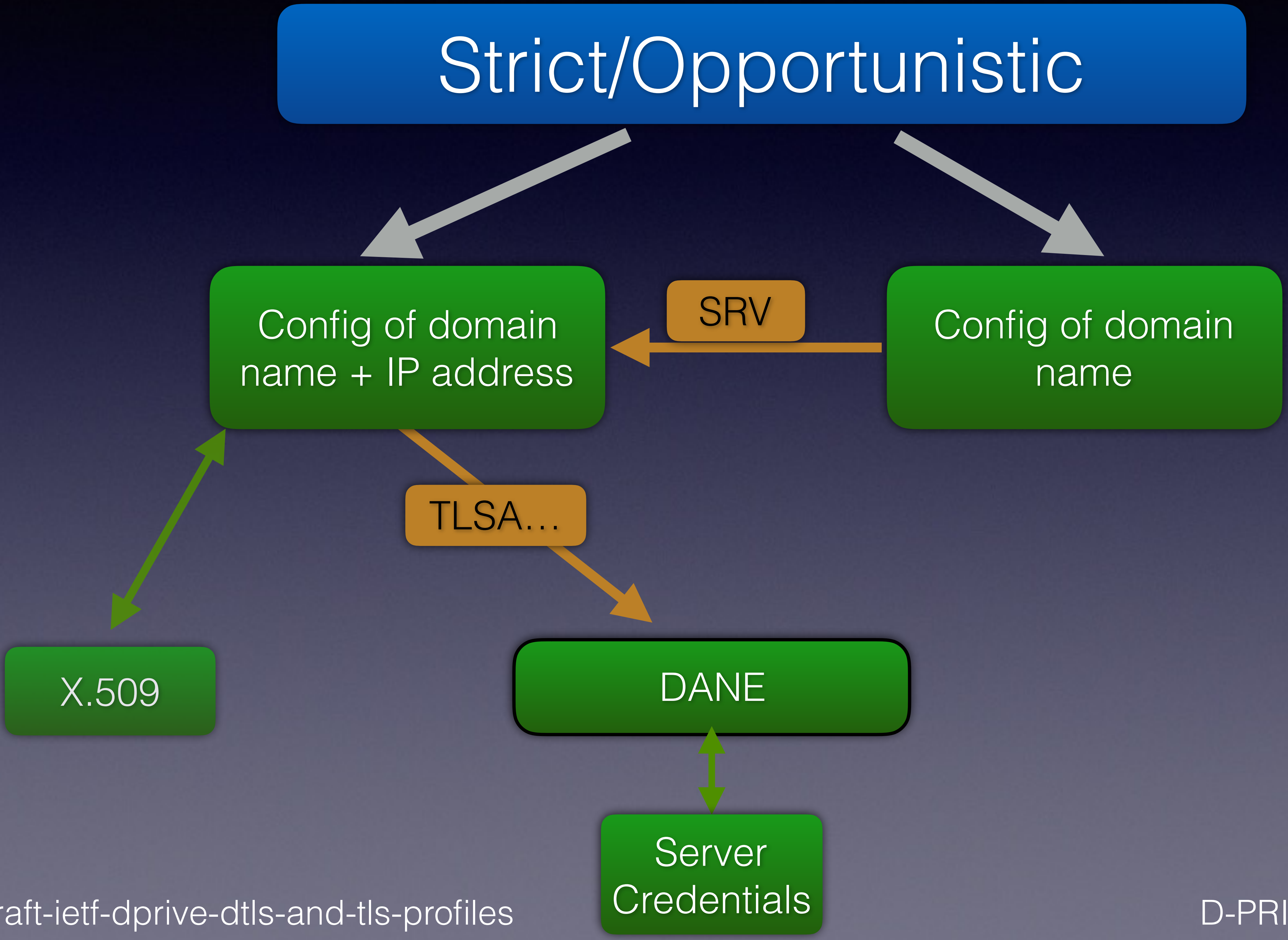
SRV

Config of domain name

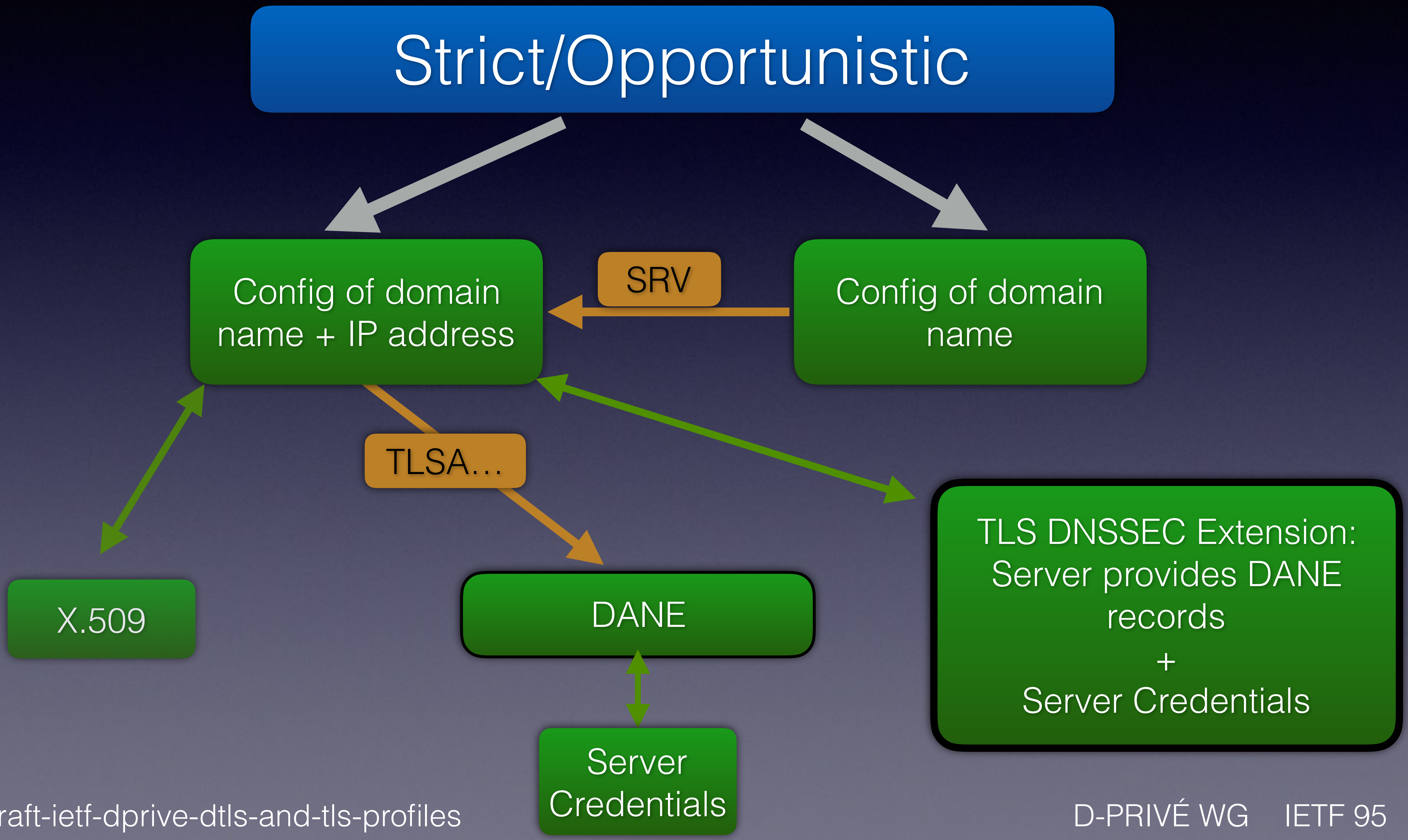
Auth mechanisms



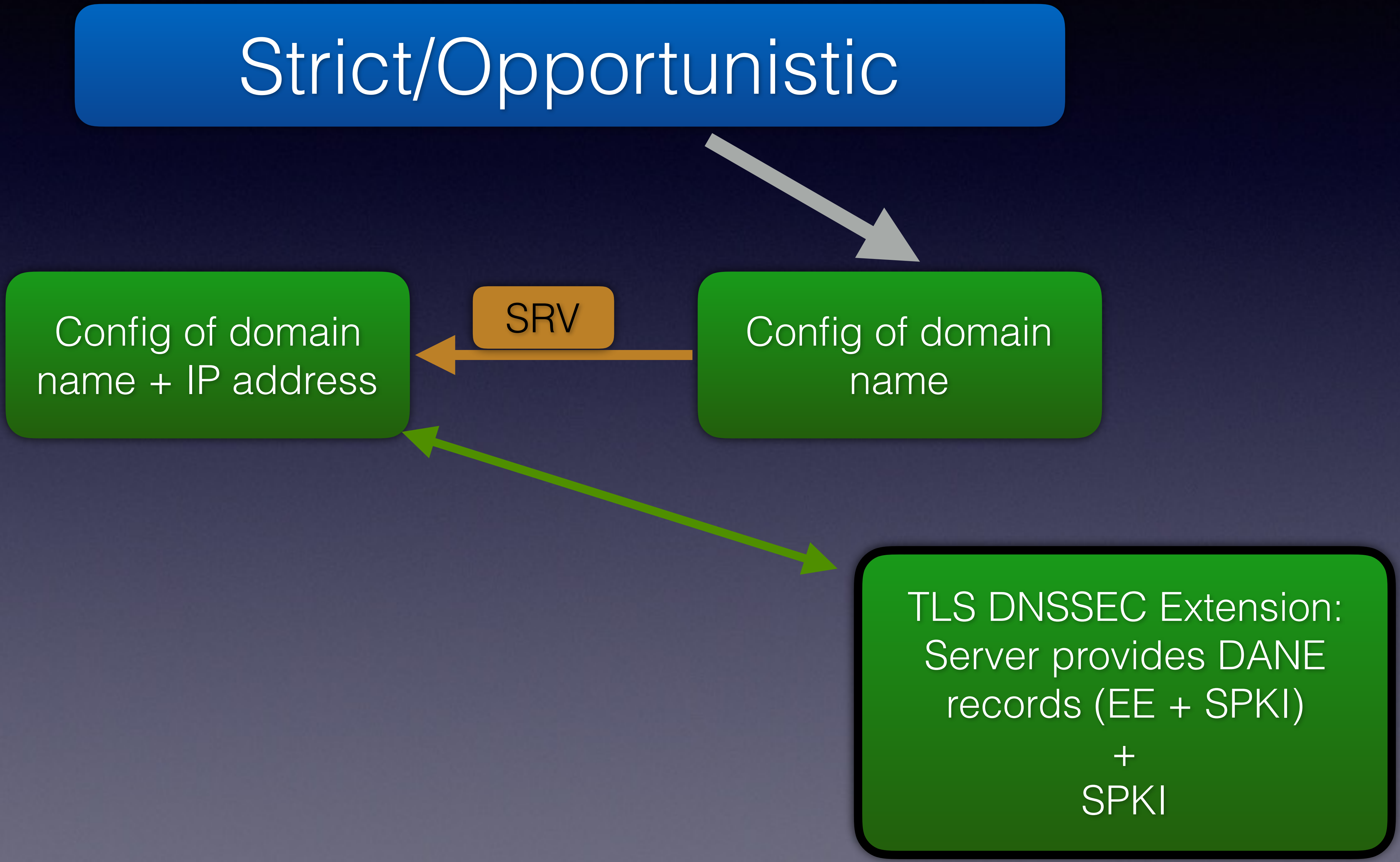
Auth mechanisms



Auth mechanisms


Strict/Opportunistic
Config of domain name + IP address
SRV
Config of domain name
TLSA…
X.509
DANE
TLS DNSSEC Extension: Server provides DANE records + Server Credentials
Server Credentials

Auth mechanisms



Strict/Opportunistic

Config of domain name + IP address

SRV

Config of domain name

TLS DNSSEC Extension: Server provides DANE records (EE + SPKI)

+

SPKI

DHCP

- To securely auto configure IP address **and** domain name would require a new options
  - and secure, trusted connection to DHCP server

Q: Should we pursue this option?

(D)TLS profile

- BCP 195
- Session resumption
- (False start)

- Expect to address TLS 1.3 in future version

Implementation Status

- Client: ***getdns***
    - Strict and Opportunistic
        - SPKI pinset
        - Hostname validation of cert
        - (WIP) DANE mechanisms
- Servers
    - Unbound
    - Knot (as of Hackathon!)

Feedback and review please!