RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDAC-T11

Domain Knowledge: How to Factor DNS into Your Privacy and Security Strategy

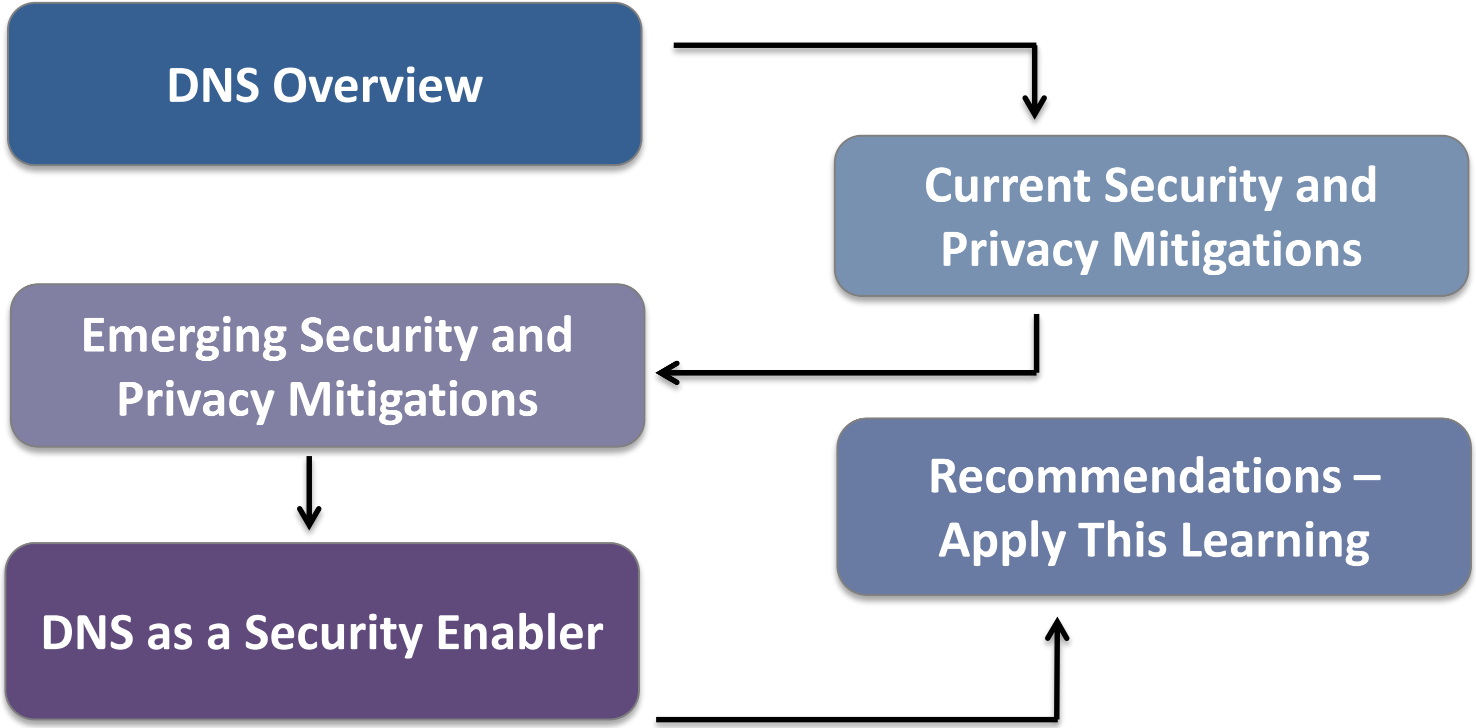
Allison Mankin,
Director – Next Lab

Burt Kaliski,
Chief Technology Officer

Verisign

#RSAC

Agenda



DNS Overview

Current Security and Privacy Mitigations

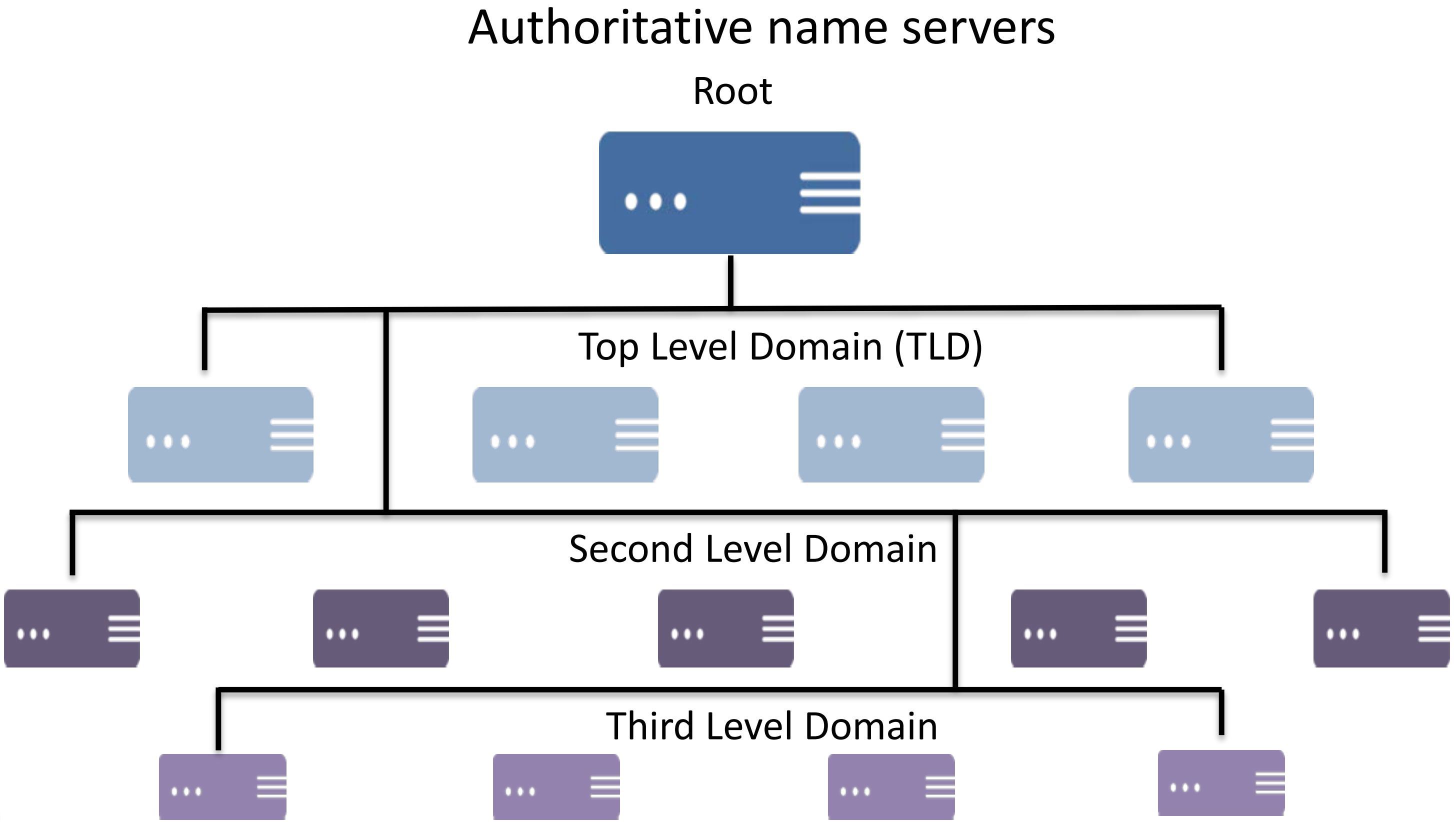
Emerging Security and Privacy Mitigations

DNS as a Security Enabler

Recommendations – Apply This Learning

DNS Overview

DNS Overview and Hierarchy


Authoritative name servers

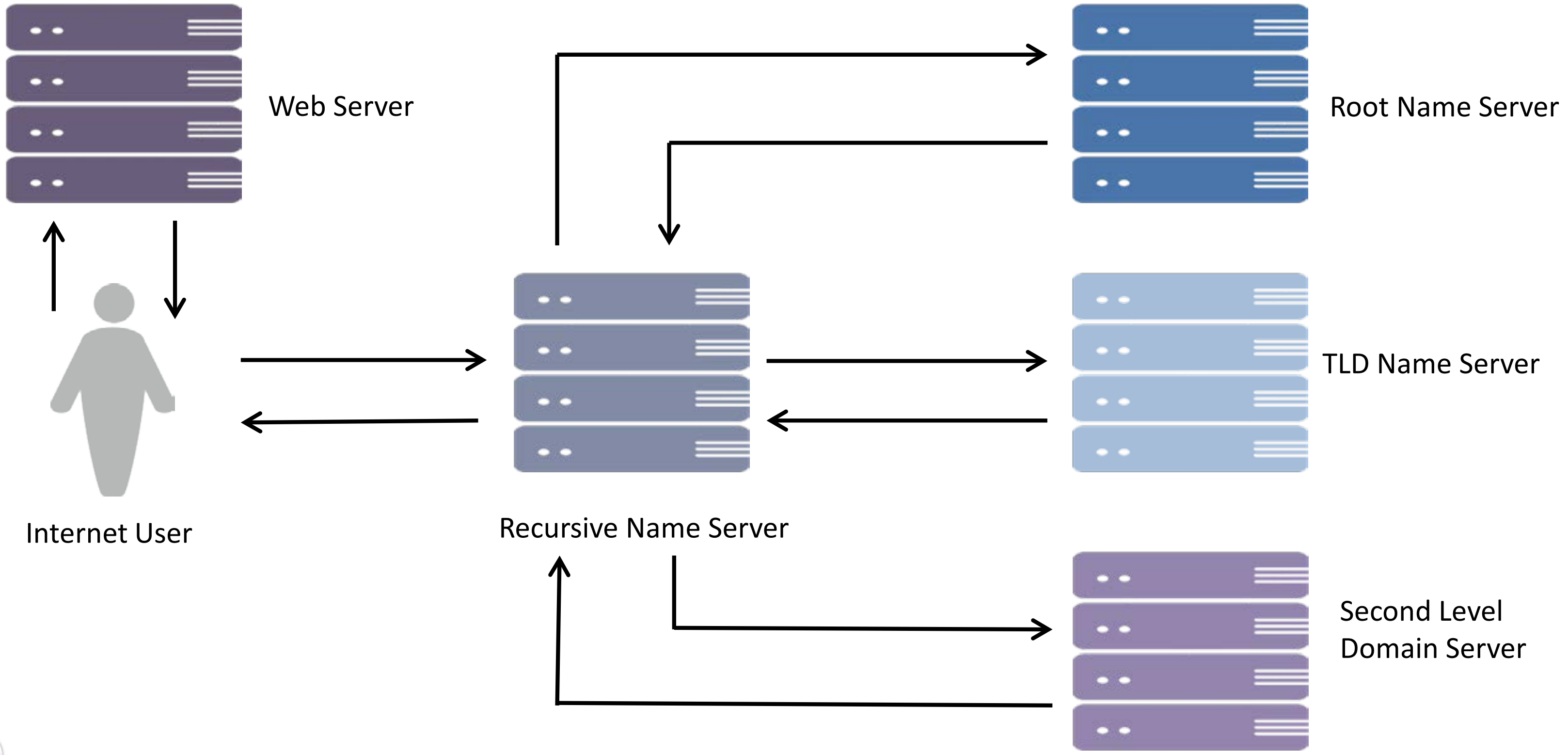
Root

Top Level Domain (TLD)

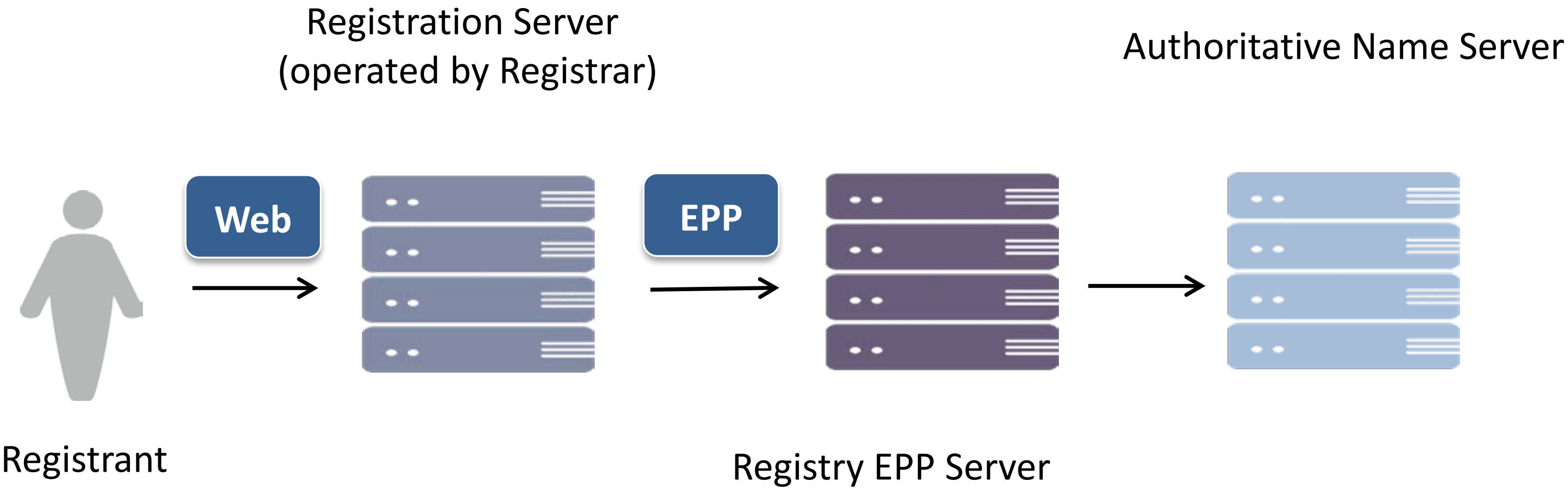
Second Level Domain

Third Level Domain

DNS Resolution Process

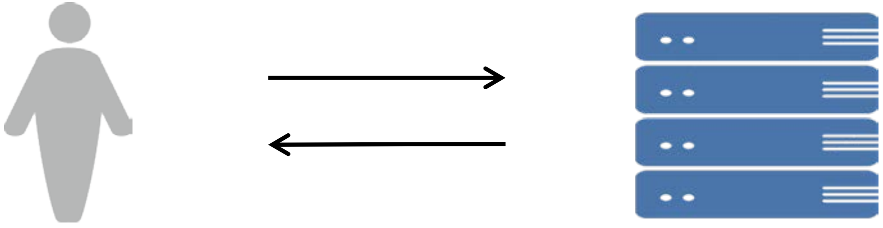


Registration and Provisioning Process



EPP = Extensible Provisioning Protocol

Registration Data Access Process

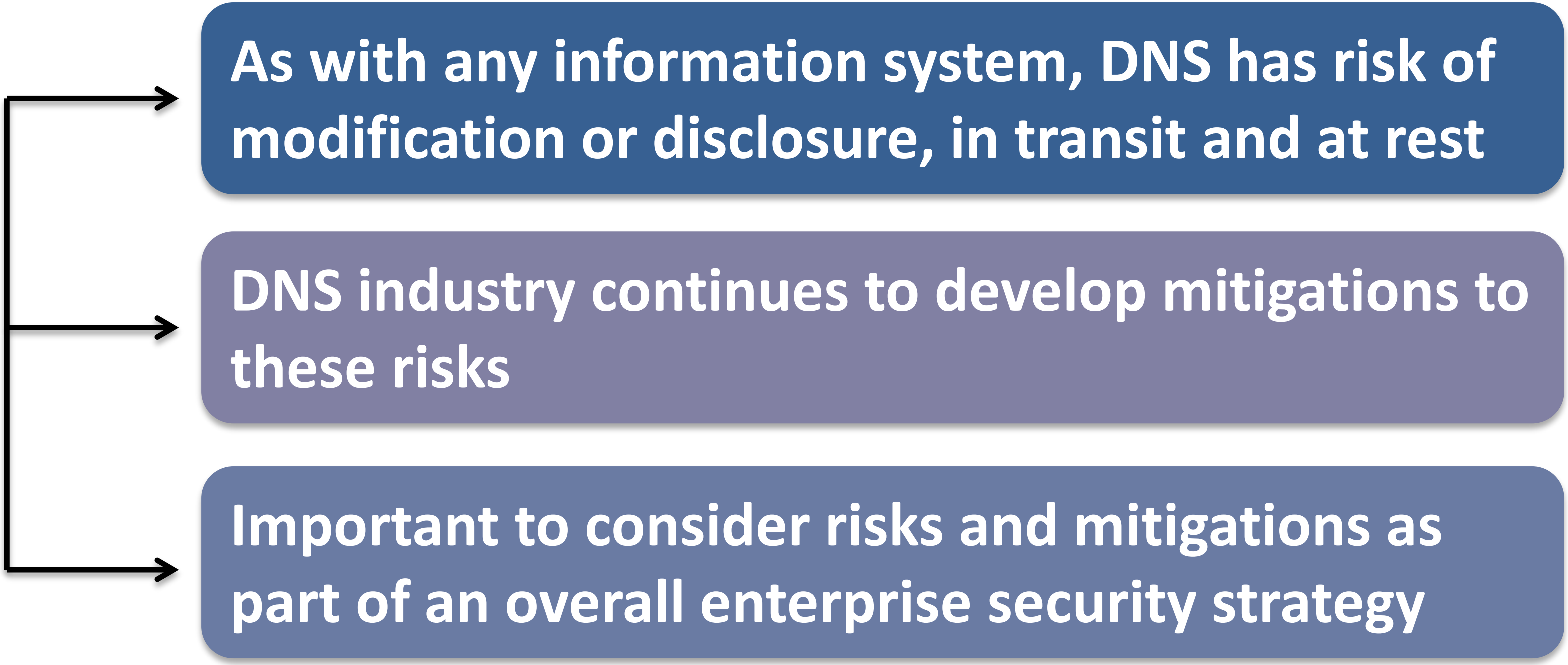


Internet User

WHOIS Registration Data Server

Current Security and Privacy Mitigations

DNS Security and Privacy Risks

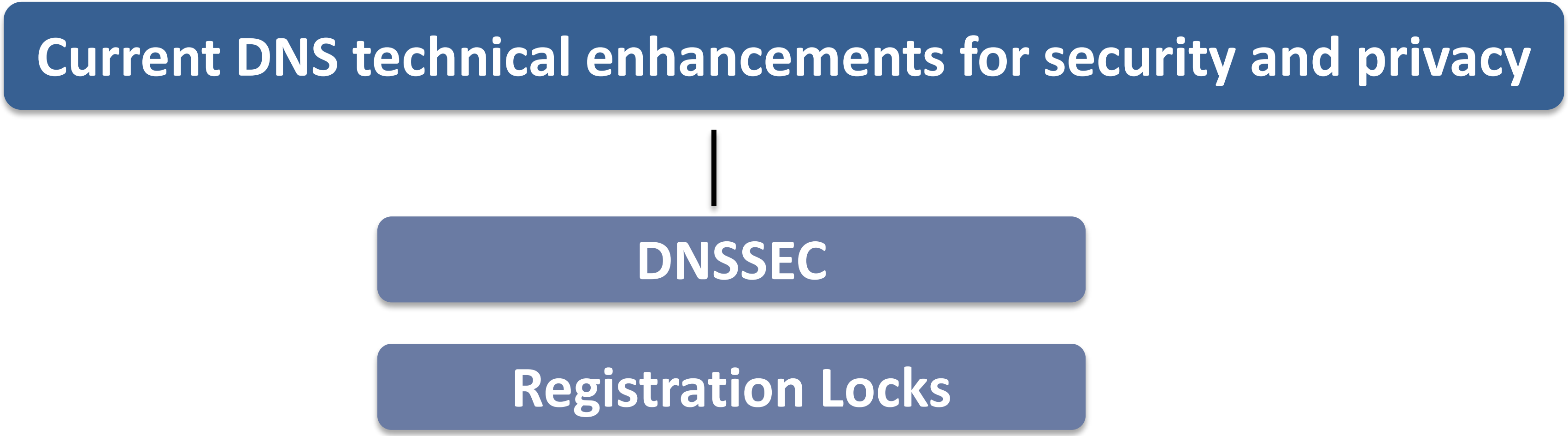


As with any information system, DNS has risk of modification or disclosure, in transit and at rest

DNS industry continues to develop mitigations to these risks

Important to consider risks and mitigations as part of an overall enterprise security strategy

Current Mitigations

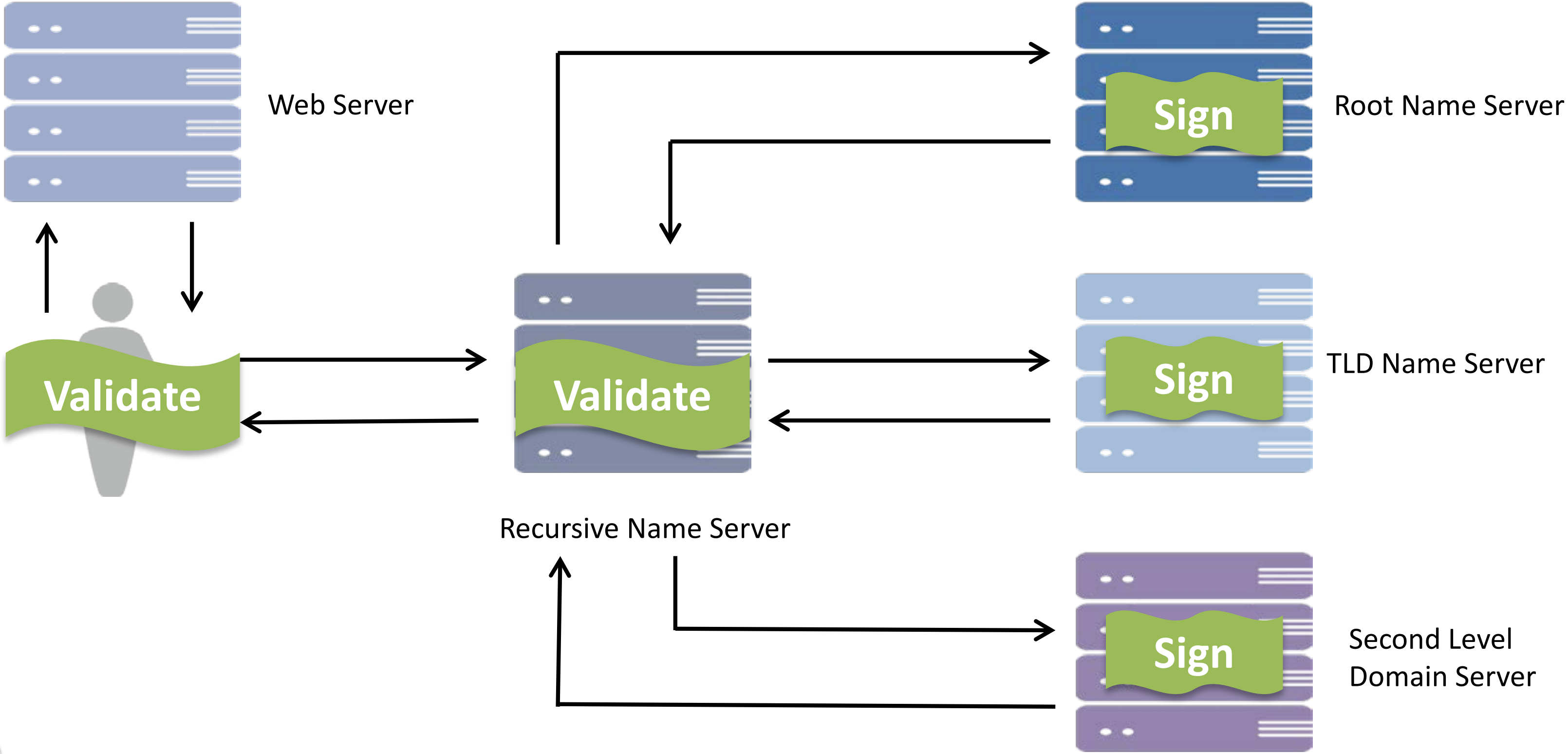


Current DNS technical enhancements for security and privacy

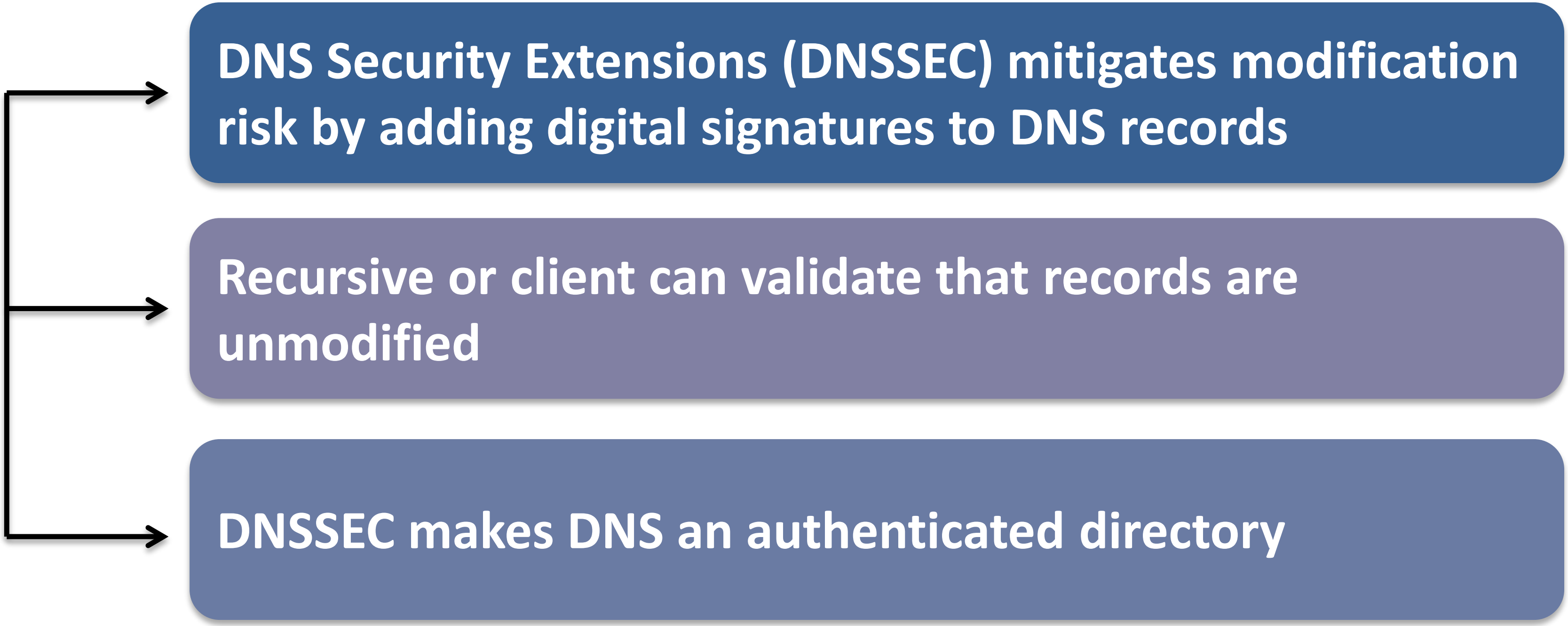
DNSSEC

Registration Locks

DNSSEC Process



DNSSEC

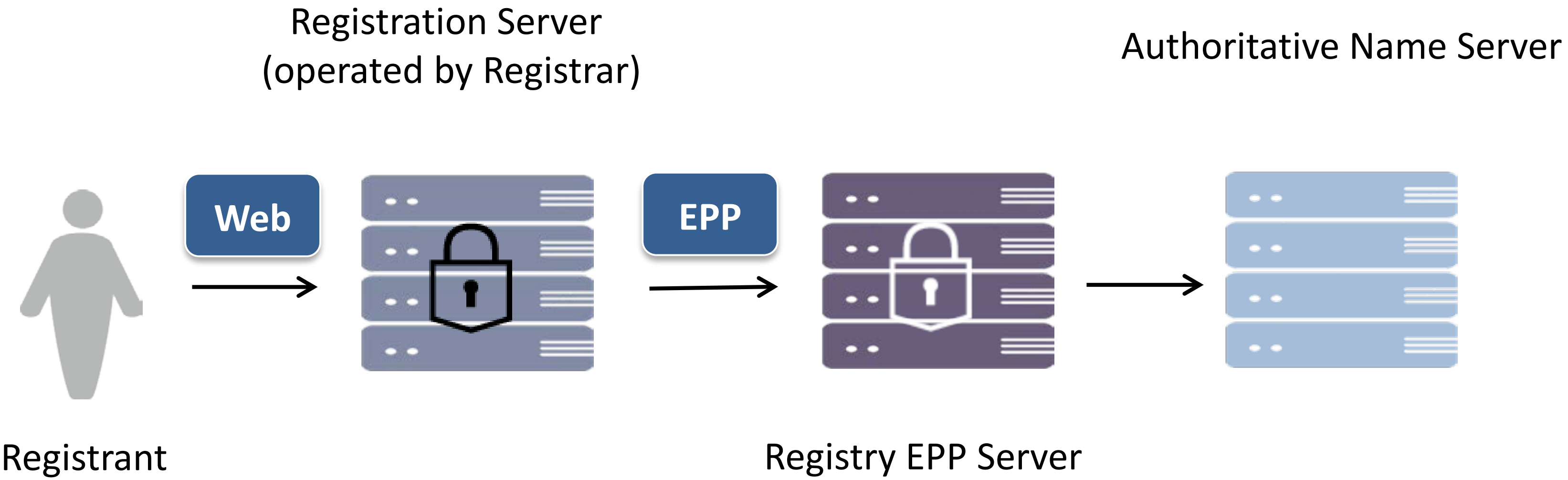


DNS Security Extensions (DNSSEC) mitigates modification risk by adding digital signatures to DNS records

Recursive or client can validate that records are unmodified

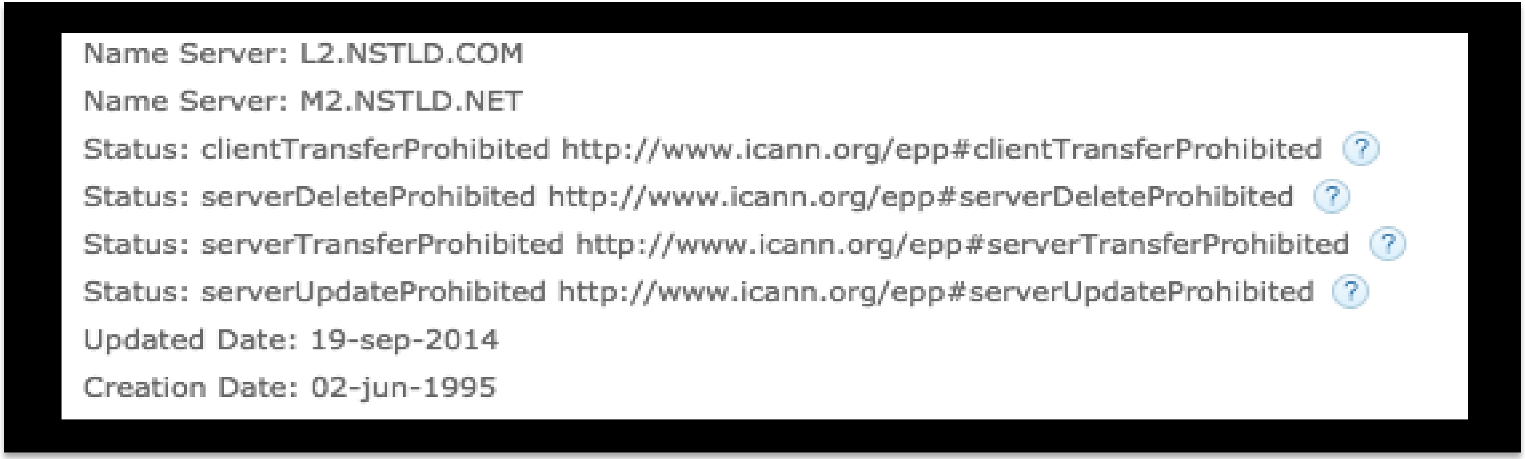
DNSSEC makes DNS an authenticated directory

Registration Locks



Registration Locks

Registrars and registries provide complementary options to mitigate registration modifications and fraudulent transfer of domains

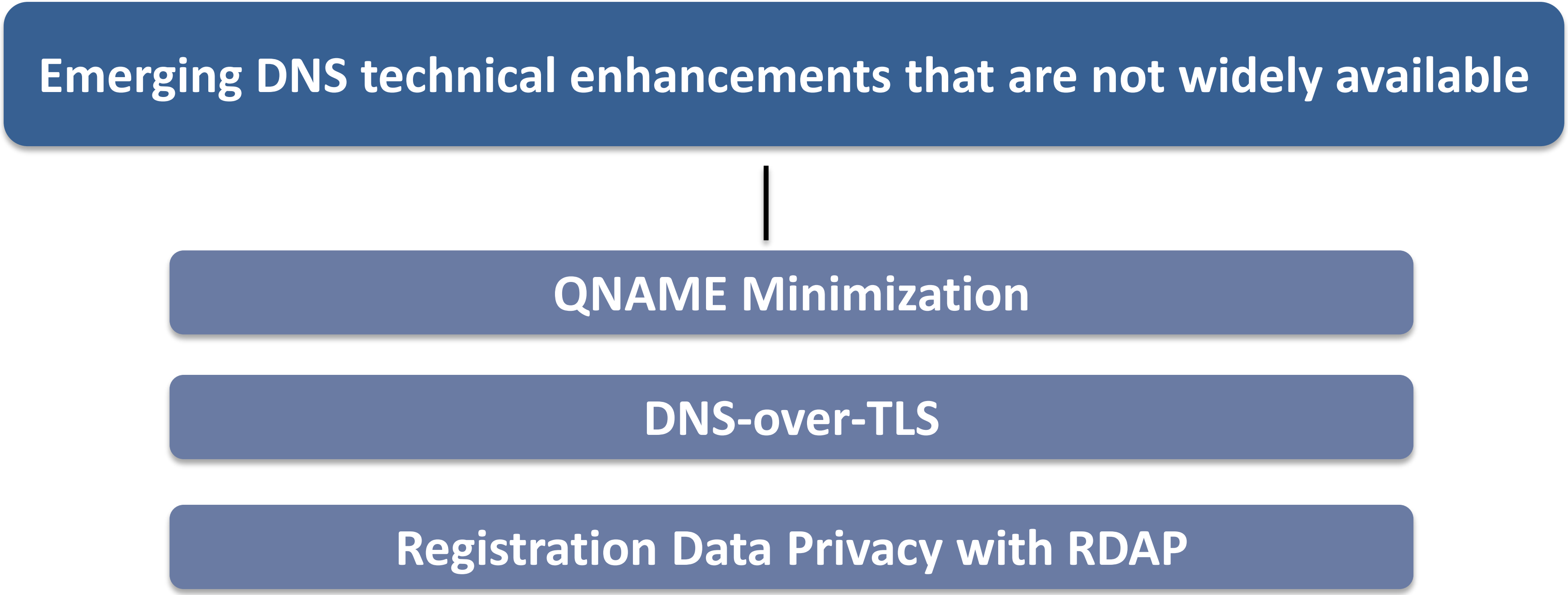


```
Name Server: L2.NSTLD.COM
Name Server: M2.NSTLD.NET
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Updated Date: 19-sep-2014
Creation Date: 02-jun-1995
```

verisign.com WHOIS data indicating a registrar lock and a registry lock

Emerging Security and Privacy Mitigations

Emerging Mitigations



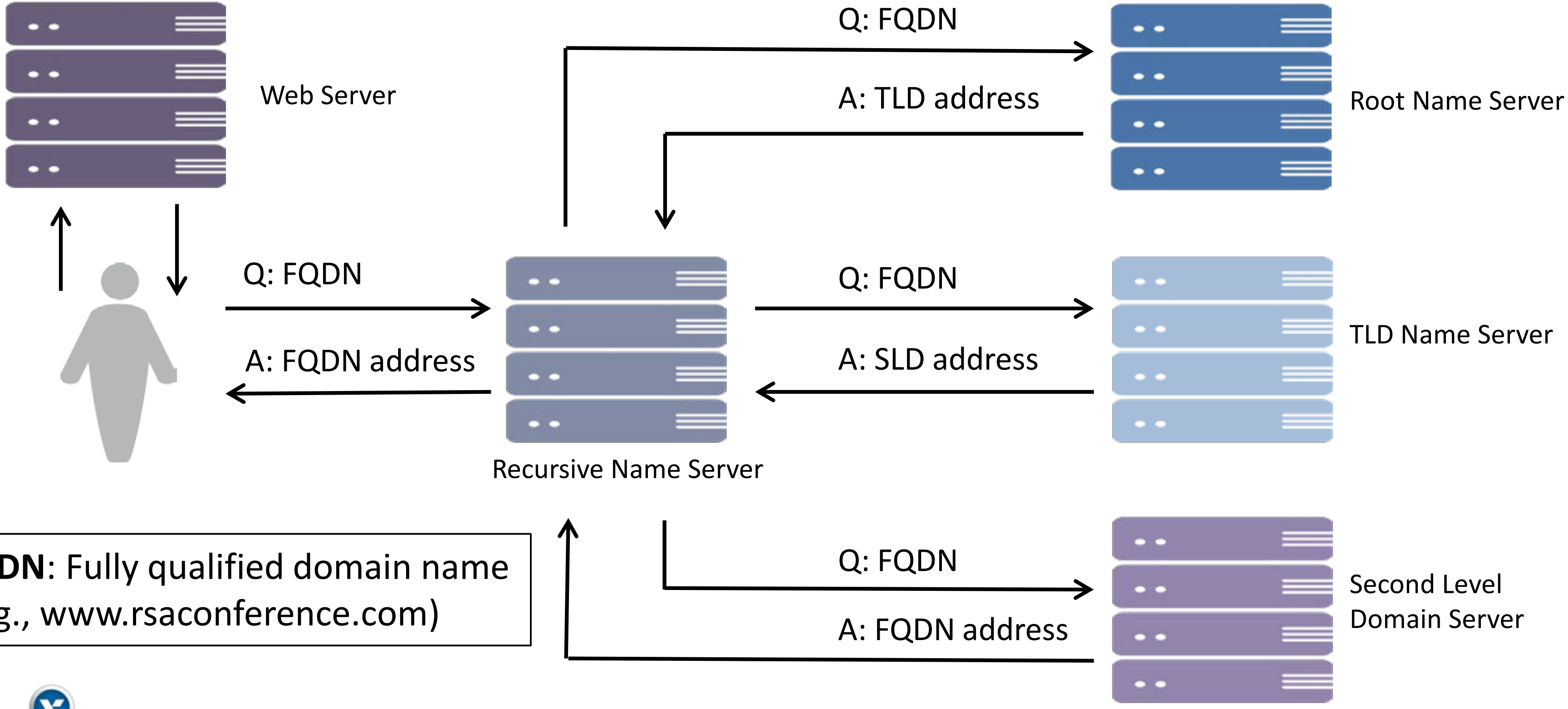
Emerging DNS technical enhancements that are not widely available

QNAME Minimization

DNS-over-TLS

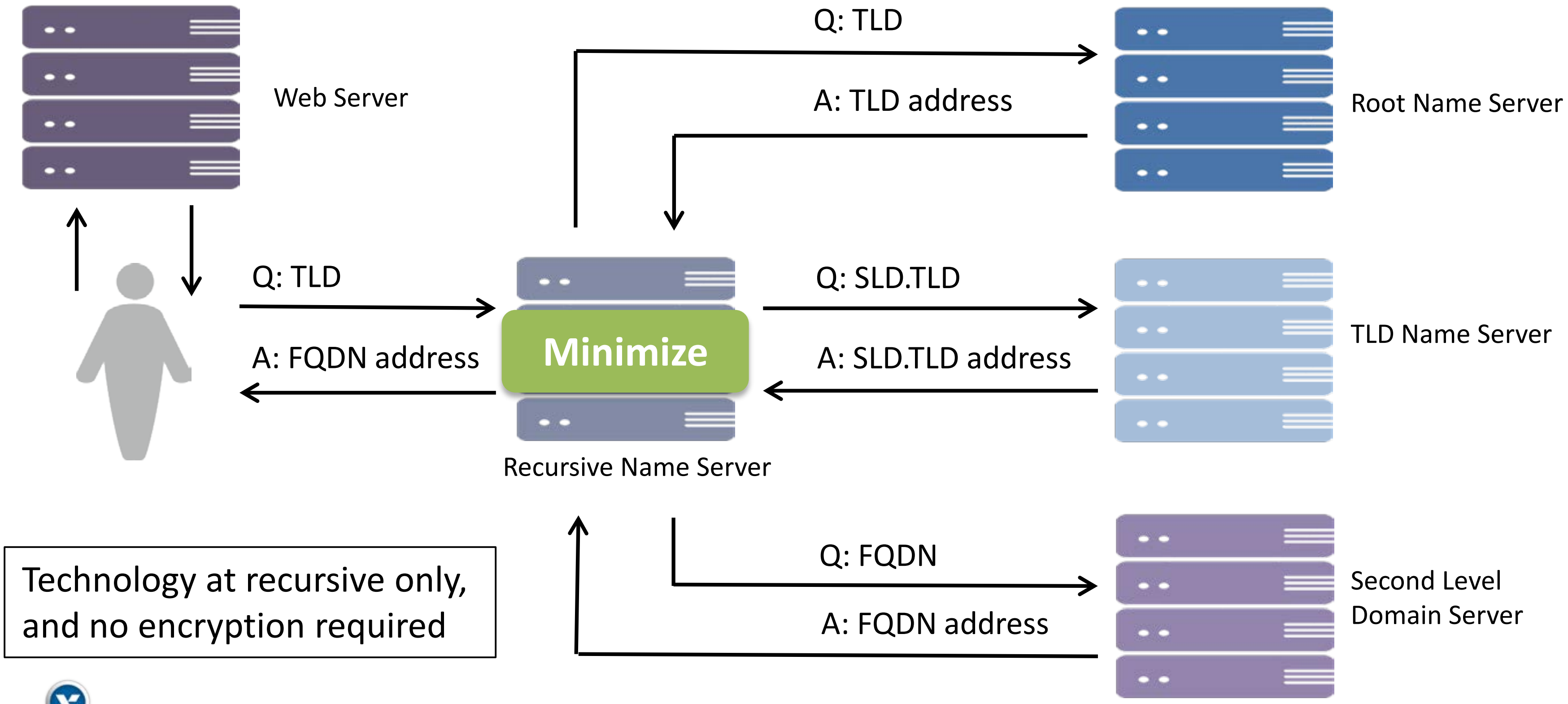
Registration Data Privacy with RDAP

DNS Resolution Process



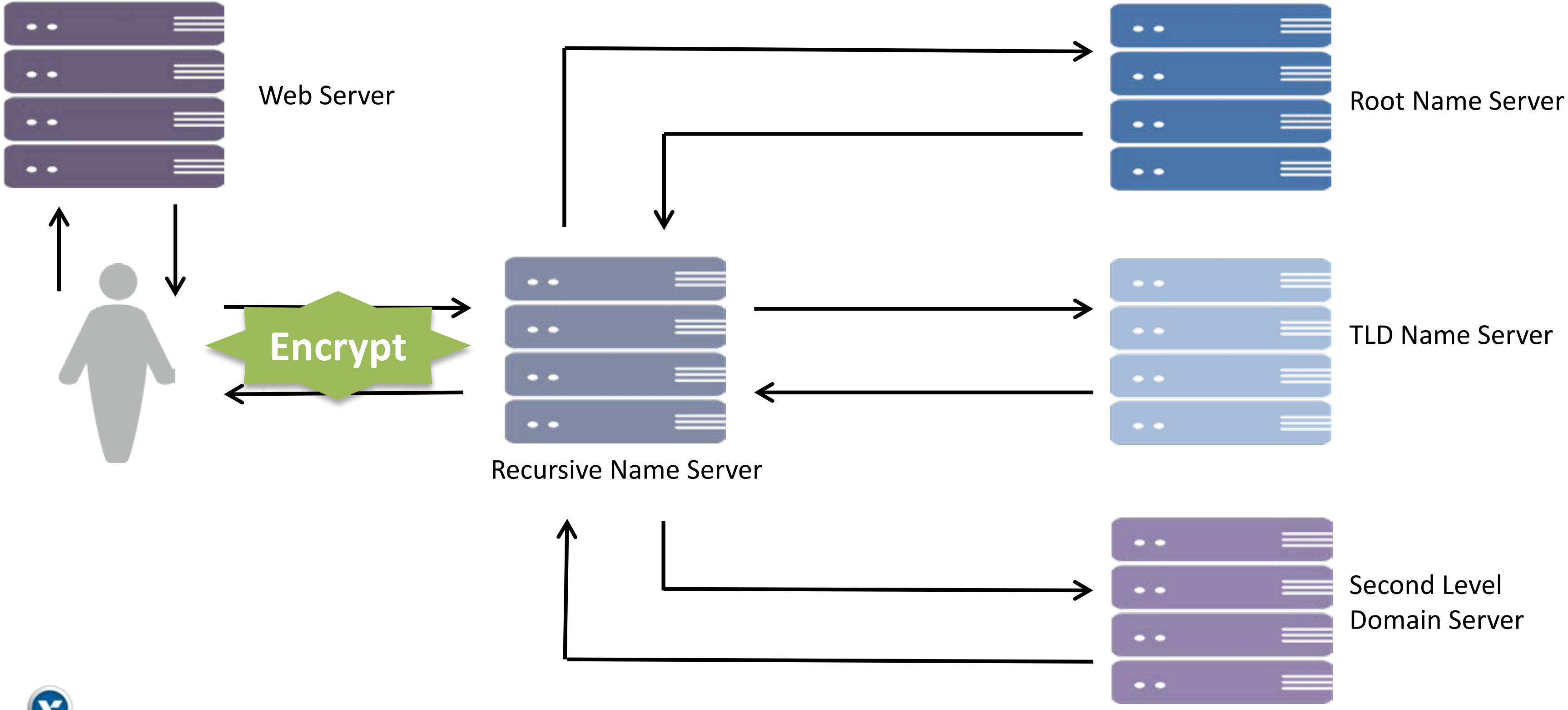
FQDN: Fully qualified domain name (e.g., www.rsaconference.com)

QNAME Minimization Process

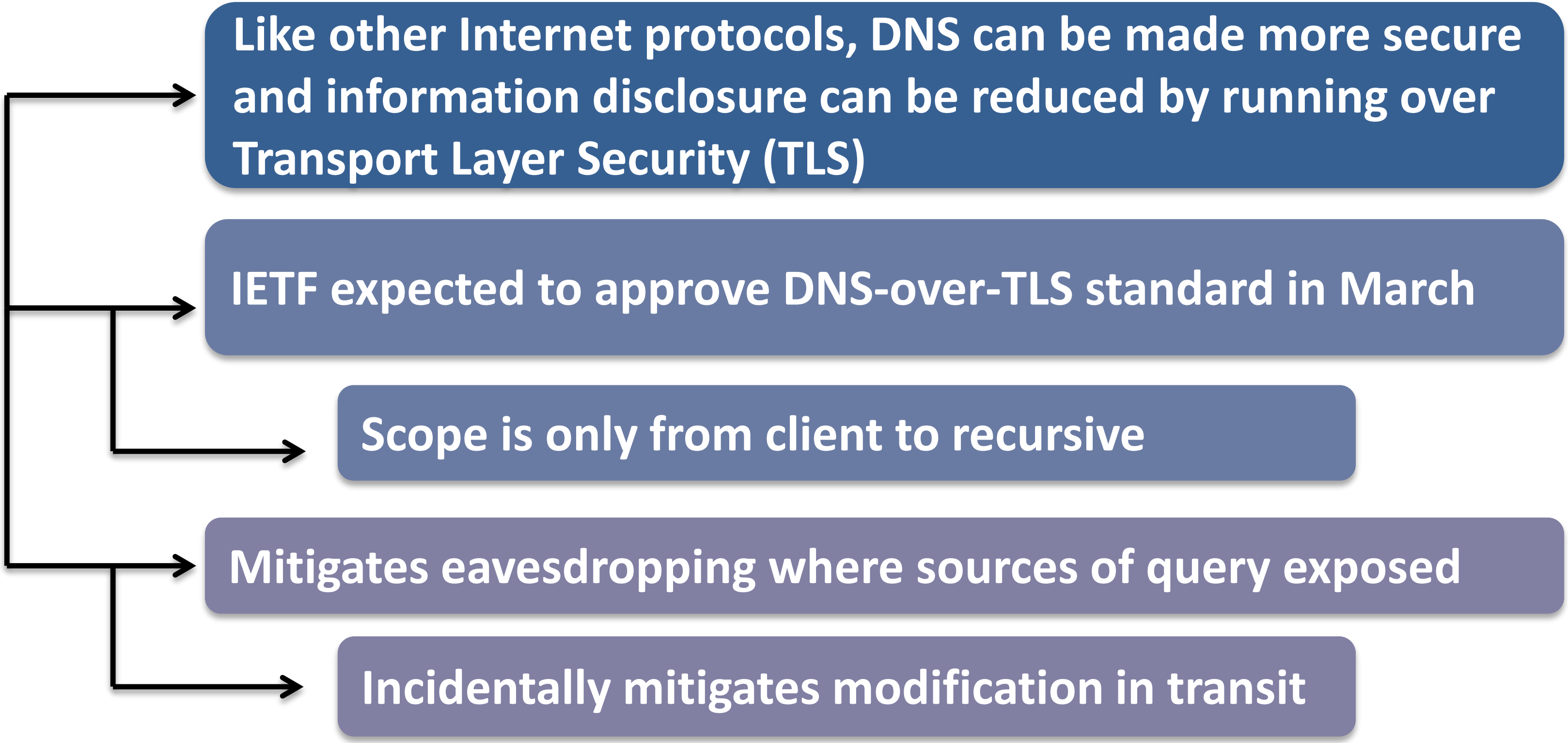


Technology at recursive only, and no encryption required

DNS-over-TLS Process



DNS-over-TLS



Like other Internet protocols, DNS can be made more secure and information disclosure can be reduced by running over Transport Layer Security (TLS)

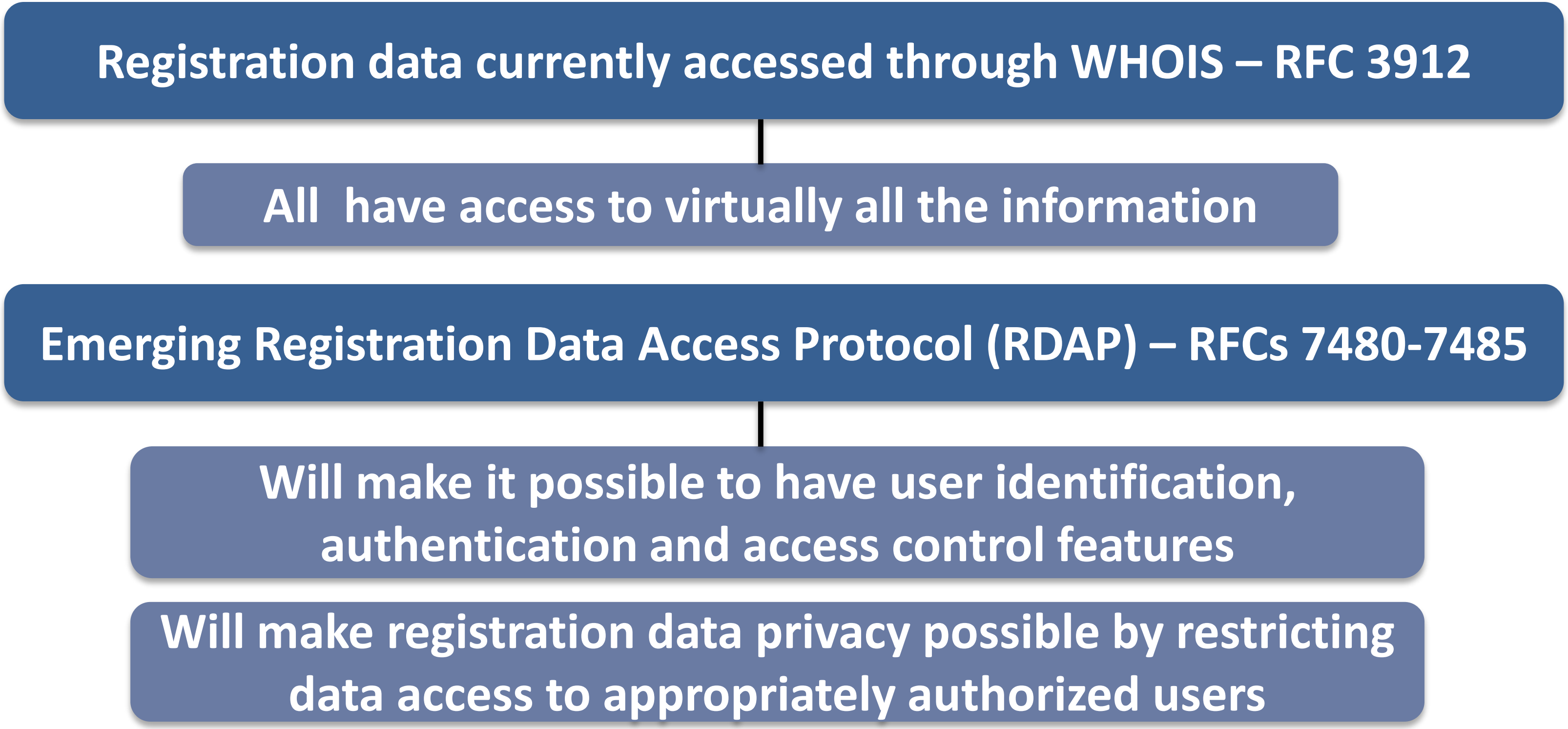
IETF expected to approve DNS-over-TLS standard in March

Scope is only from client to recursive

Mitigates eavesdropping where sources of query exposed

Incidentally mitigates modification in transit

Differentiated Access to Registration Data



Registration data currently accessed through WHOIS – RFC 3912

All have access to virtually all the information

Emerging Registration Data Access Protocol (RDAP) – RFCs 7480-7485

Will make it possible to have user identification, authentication and access control features

Will make registration data privacy possible by restricting data access to appropriately authorized users

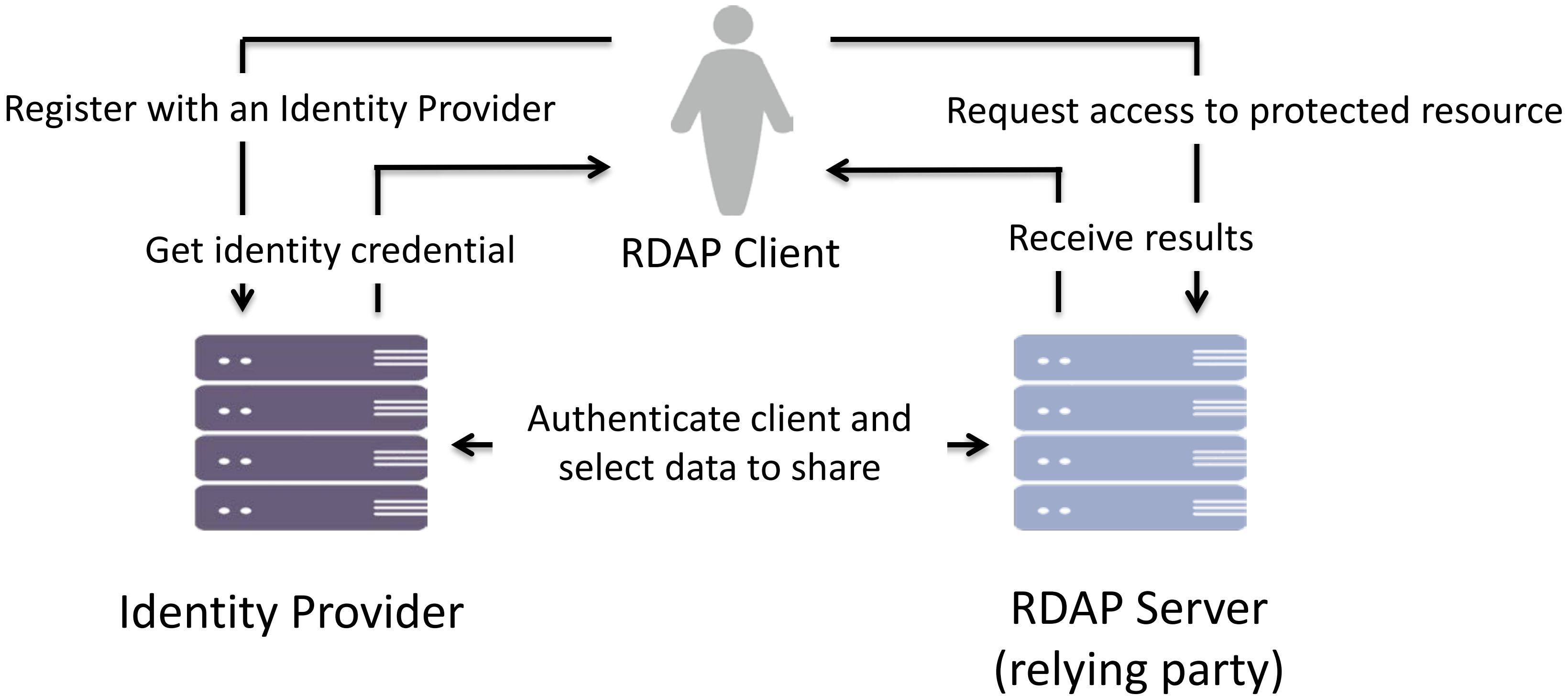
Registration Data Privacy with RDAP

WHOIS: All clients see all data (more or less)

RDAP: What a client sees can depend on:

- → **Who** is asking
- → **What** they’re asking for
- → **Where** they’re asking from
- → **Why** they’re asking
- → **How** they’re asking

How Might Data Privacy with RDAP Work?



Register with an Identity Provider

Request access to protected resource

Get identity credential

RDAP Client

Receive results

Authenticate client and select data to share

Identity Provider

RDAP Server (relying party)

Status of Emerging Mitigations

QNAME Minimization	Approved for Experimental IETF RFC, implemented by open source recursive servers (Unbound, Knot)
DNS-over-TLS	Expected IETF approval as a standard in March, implemented in reference end-user open source (getdns) and patched in Unbound
Registration Data Privacy with RDAP	One authentication specification in development in IETF, non-production (experimental) services emerging

Summary of Current & Emerging Mitigations

Mitigations	Client to Recursive	At Recursive	Recursive to Authoritative	At Authoritative
Current				
DNSSEC		Protect	Protect	Protect
Registration Locks				Protect
Emerging				
QNAME Minimization			Protect	Protect
DNS-over-TLS	Protect			
RDAP Privacy				Protect

DNS as a Security Enabler

DNS as a Security Enabler

Focus so far has been on strengthening security of DNS

DNS-based services can also strengthen security of networks and applications

Four Use Cases:

1. Web security
2. Email security
3. Network security
4. Threat intelligence

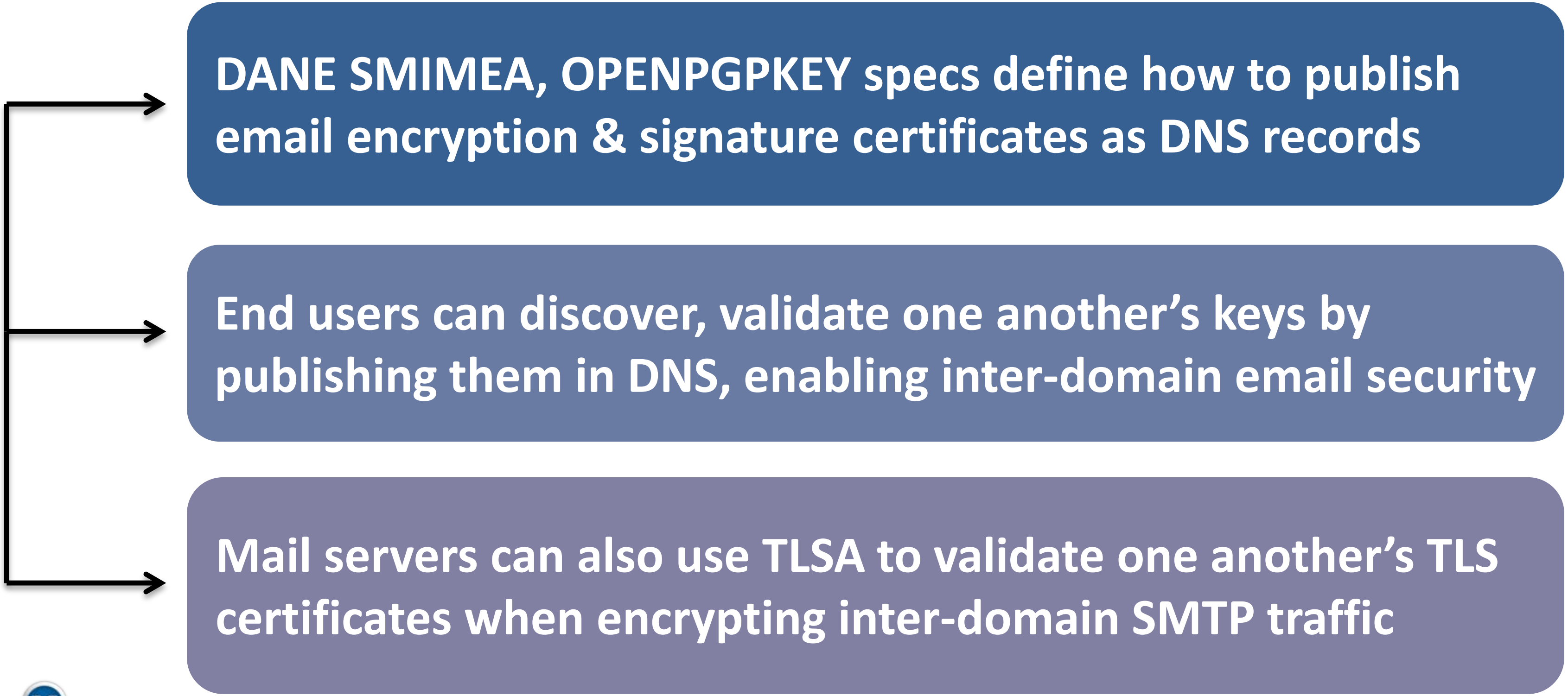
Use Case 1: Web Security

DANE TLSA spec defines how to publish web certificates, public keys, and/or their hashes as DNS records

Relying parties can thereby validate that web certificate hasn’t been substituted with one from a compromised CA

Certificate transparency logs, forensics also detect compromises, but DNS publication gives resource holders its own “voice”

Use Case 2: Email Security

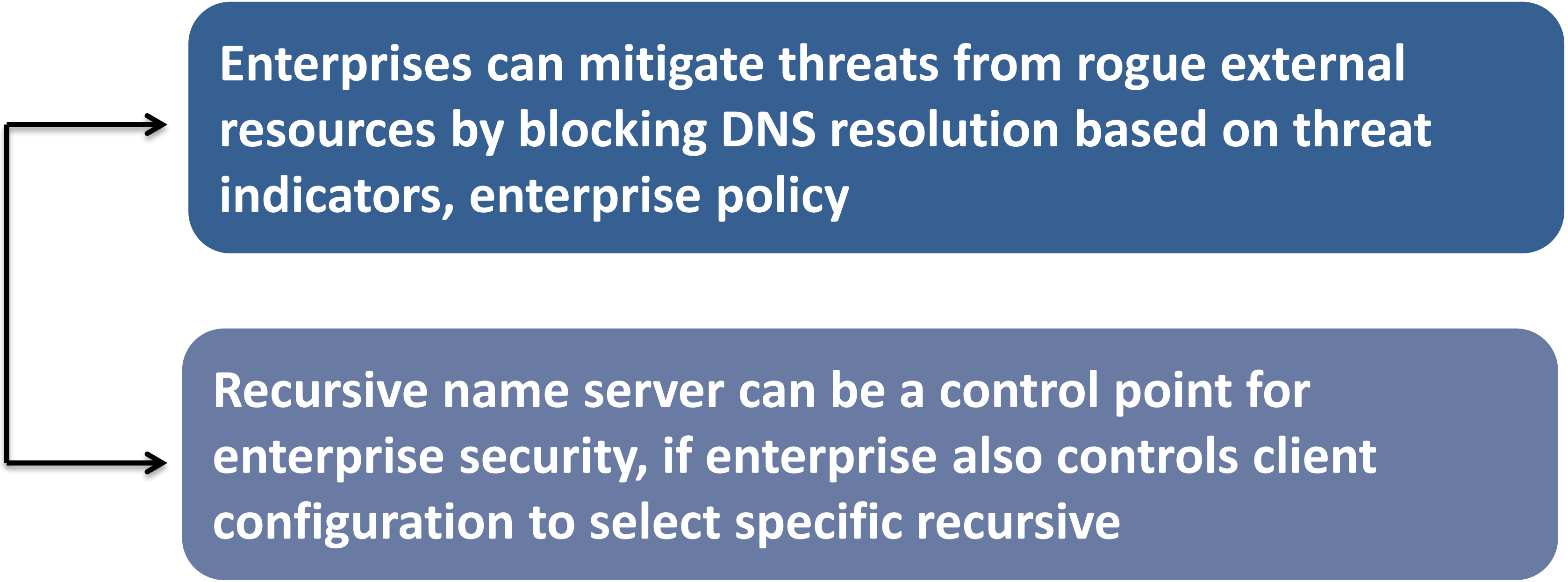


DANE SMIMEA, OPENPGPKEY specs define how to publish email encryption & signature certificates as DNS records

End users can discover, validate one another’s keys by publishing them in DNS, enabling inter-domain email security

Mail servers can also use TLSA to validate one another’s TLS certificates when encrypting inter-domain SMTP traffic

Use Case 3: Network Security



Enterprises can mitigate threats from rogue external resources by blocking DNS resolution based on threat indicators, enterprise policy

Recursive name server can be a control point for enterprise security, if enterprise also controls client configuration to select specific recursive

Use Case 4: Threat Intelligence

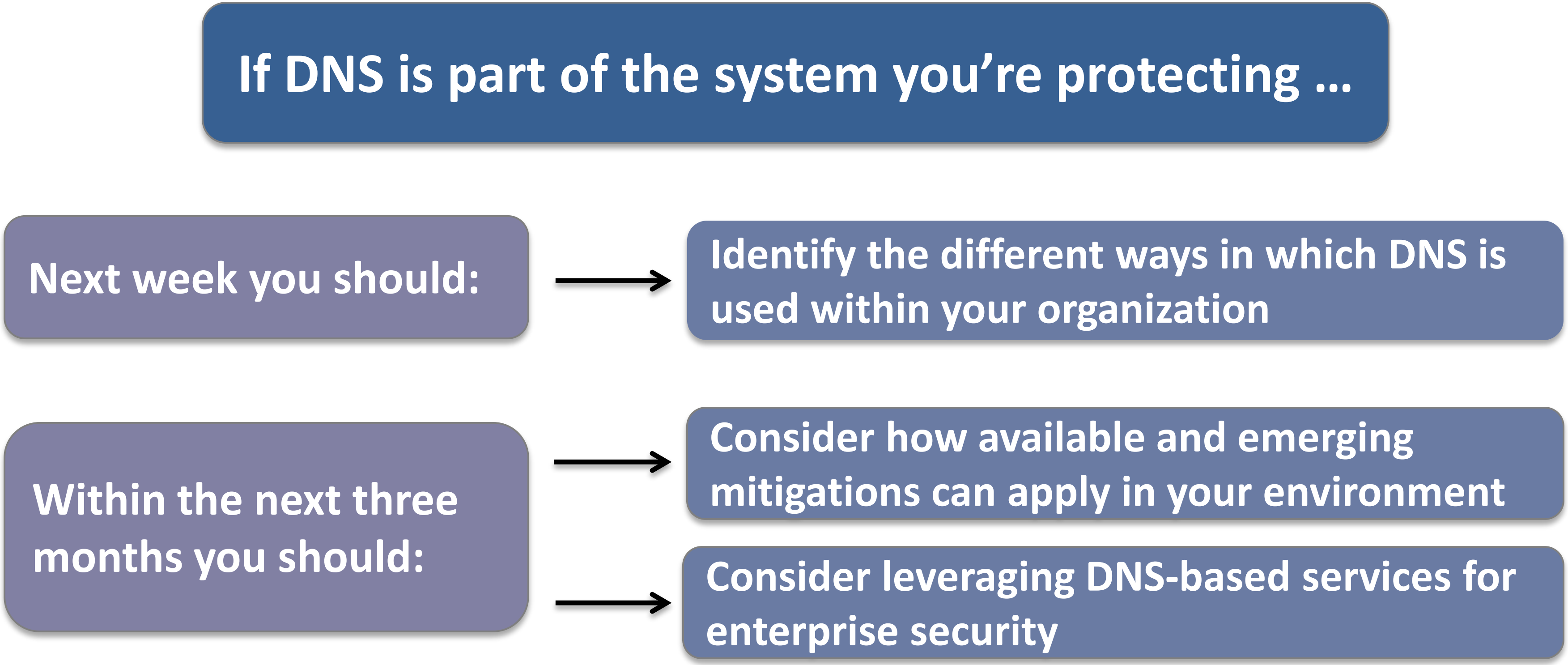
- Enterprises can also detect threats from rogue external resources by analyzing DNS resolution patterns
- Recursive name server also becomes an observation point for enterprise security
- Observations can be correlated across enterprises via "passive DNS" type approaches

Status of Use Cases

Use Case	Standards Status	Implementation and Deployment
1. Web Security	IETF Standards Track RFC (TLSA)	Early adopters only, with browser support lacking
2. Email Security	In review for IETF Experimental RFCs	Emerging use between MTAs. Minimal adoption by MUAs.
3. Network Security	Not in standards development	Emerging production offerings
4. Threat Intelligence	Not in standards development	Active production offerings

Wrapping Up

Recommendations – Apply This Learning



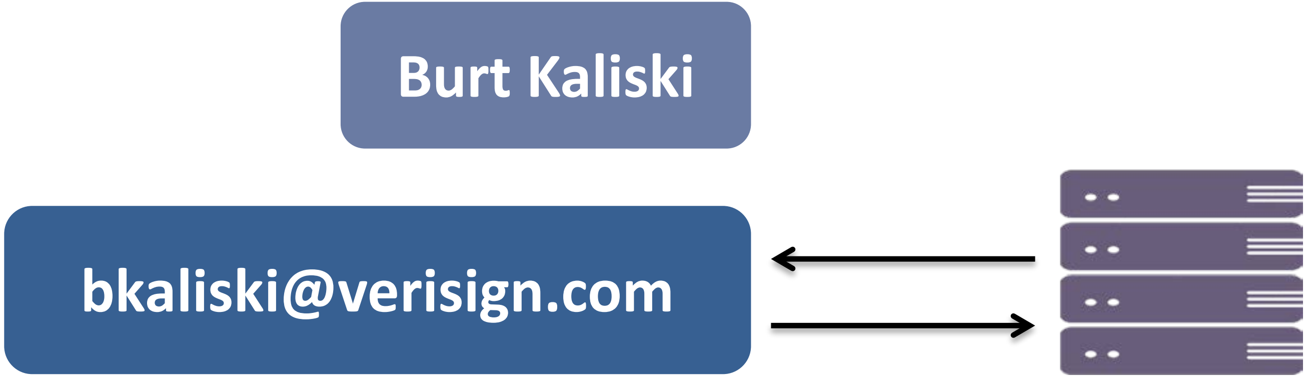
If DNS is part of the system you're protecting …

Next week you should: → Identify the different ways in which DNS is used within your organization

Within the next three months you should: → Consider how available and emerging mitigations can apply in your environment

→ Consider leveraging DNS-based services for enterprise security

For More Information



Burt Kaliski

bkaliski@verisign.com

Q & A