

# DNSSEC for a large Enterprise

Shumon Huque & Pallavi Aras, Salesforce

March 8<sup>th</sup> 2018

DNS-OARC 28 Workshop; San Juan, Puerto Rico

## **DNSSEC for a large Enterprise Network**

This talk will give an overview of our planning and efforts so far to deploy DNSSEC for a large enterprise with a complex infrastructure, involving the services of several managed DNS providers. It will start by outlining our specific requirements and design choices (e.g. signing algorithms, authenticated denial mechanisms, signing of dynamically generated records, key rollover schedules, scaling and performance considerations, etc.). Many prominent managed DNS providers have significant limitations in the extent of their DNSSEC support. We will survey DNSSEC capabilities in several of the managed DNS providers, pointing out where they excel, and where they fall short, based on testing we've performed. We will discuss relevant discussions with the vendors and the status of several feature enhancement requests that we've made. A key challenge is the requirement for supporting multiple distinct DNS providers simultaneously, which further complicates the planned implementation, and we will outline several strategies around this. One additional desired goal of this talk is to stimulate a community discussion of what capabilities need to be widely available in DNS providers for successful DNSSEC deployment at many large enterprises.

# Outline

- Our rationale for DNSSEC
- Our DNS infrastructure overview
- DNSSEC specific planned requirements
- Vendor features and limitations
  - We won't mention specific vendors by name.
  - But many vendors are collaborating on addressing these.

# DNSSEC Use Case

# DNSSEC Use Case

- Obviously, for the security benefits ..
- Specific Business Needs:
  - We have many US government agency customers
  - Compliance with FedRAMP and DoD certification levels

# FedRAMP and DoD certifications

- US Federal Risk & Authorization Management Framework
  - <https://www.fedramp.gov/>
  - <https://www.fedramp.gov/cloud-service-providers/>
  - Specific security controls relevant to DNS/DNSSEC: SC20, SC21, SC22
- US DOD IL4/5/6
  - Cloud Security Information “Impact Levels”
  - [https://iase.disa.mil/cloud\\_security/cloudsrg/Pages/ImpactLevels.aspx](https://iase.disa.mil/cloud_security/cloudsrg/Pages/ImpactLevels.aspx)

# Basic Overview of our DNS infrastructure

# A basic overview of our external DNS infra.

- Many DNS zones
- Some are very large (several million records) and rapidly changing
- Multiple (2) DNS providers in use concurrently for all zones
- Some leaf zones are delegated to load balancing appliances
- Use of several non-standard DNS features:
  - Traffic management (geol responses, load distribution, failover, etc.)
  - Zone apex aliases
- Large number of automated tools making record updates



# DNSSEC Specific Requirements

# DNSSEC specific requirements

- Initial thought: Can we scope the project in the short term?
  - Migrate US Gov customers onto dedicated DNS zones and sign only those.
  - Reconsidered due to (1) large operational impact on current customers and (2) why not extend DNSSEC to all of Salesforce customers - our long term goal was always to deploy DNSSEC across the company.
- Sign all zones associated with the core Salesforce applications
  - On the order of ~ 20 to 30 zones
  - Includes the largest and busiest of our zones

# DNSSEC specific requirements

- Signing Algorithm
  - Widely supported: RSASHA256 or ECDSAP256/P384
  - Ideally, resistant to attack by the strongest adversary:
    - $\geq$  2048-bit RSA or,  $\geq$  ECDSAP256SHA256
    - This is difficult to achieve in practice because the weak link in the DNSSEC chain is the very common 1024-bit RSA ZSK seen to be deployed at most Top Level Domains
- Authenticated Denial of Existence
  - Zone enumeration defense:  $\rightarrow$  NSEC3 or equivalent

# DNSSEC specific requirements

- Support for signing non-standard, and often dynamic features:
  - Traffic Management (geo/GSLB, probe & failover, M of N pools).
- Ability to work across multiple providers.
- Performance and scalability: needs to be able to scale to our largest zones with no performance impacts.

# DNSSEC Deployment models

- **Serve Only** (treat providers as secondary servers)
  - We manage master zone, sign & push out to providers
  - More secure since we manage the signing keys
  - Challenges: supporting non-standardized features
  
- **Sign and Serve**
  - We update zone data at provider using their APIs
  - Provider manages keys, signs and serves the data to the world
  - Can support signing non-standard features if vendor supports it

# DNSSEC Deployment models

- **Serve Only** (treat providers as secondary servers)

- We manage master zone, sign & push out to providers
- More secure since we manage the signing keys
- Challenges: supporting non-standardized features

MOST BIG ZONES WITH  
VANILLA FEATURES

- **Sign and Serve**

- We update zone data at provider using their APIs
- Provider manages keys, signs and serves the data to the world
- Can support signing non-standard features if vendor supports it

ZONES WITH TRAFFIC  
MANAGEMENT RECORDS

# Managed DNS provider capabilities

# Managed DNS providers capabilities

We've examined DNSSEC capabilities of several managed DNS providers and have broadly classified them into two categories:

- Pre-Compute signer: Providers that pre-compute DNSSEC signatures over the zone record sets.
- Online signer : Providers that perform online signing (“on-the-fly signing”) of zone record sets.

We have focused on few key criteria for this presentation.






# 1. Zone Signing Algorithm Support

Zone signing algorithms, that DNS providers support when they are signing a zone versus serving a signed zone.

Vendor	Sign and Serve (Primary provider)			"Serve Only" ( Secondary provider)		
	RSA256	ECDSAP256	ECDSAP384	RSA256	ECDSAP256	ECDSAP384
A	✓		✗	✓	✓	(untested)
B	✗	✓	(untested)	✗		
C	✓	✓	✓	✓	✓	✓
D	✓	✓	✓	✓	✓	✓
E	✗	✓	✗	✗		
F	✓		✗	✓	✓	(untested)

## 2. Zone Enumeration Defense

-  One vendor only supports NSEC mode for denial of existence. (!)
-  Most of the Pre-compute signers support NSEC3.
-  Online signers that we tested use “black lies” [1] for denial of existence.

**Important :** Since the zones are corporate zones

[1] <https://tools.ietf.org/html/draft-valsorda-dnsop-black-lies-00>

# 3. Zone Signing Efficiency

*Our zones are large and very dynamic and receives several updates per minute.*

- *One of the important criteria was speed of zone signing/propagation after zone receives a single update.*

✓ For Online signers, zone updates are generally very fast, since they only sign at response time, not update time.

✓ Some of the Pre-compute signers can incrementally sign only the updated records (without having to sign the entire zone).

✗ One Pre-compute signer re-signed the entire zone for every update (they are working on a release to fix this).

# 4. Zone Sizes support

*Our current zone sizes are large and challenge the capabilities of our vendors*

- We're working closely with vendors to address these scaling challenges*

## **Sign and Serve mode :**

- Pre-compute signers have difficulty signing zones of sizes greater than 100k records (unsigned).
- Online signers, since they do not store signature can sign zones of larger size (we do not yet know the limit).

## **Serve Only mode :**

- Most providers can serve signed zones upto 2 million records.

# 5. Signature Validity Periods

The signature validity period affects the window of time in which old responses can be replayed by an attacker. Shorter is more secure, but imposes costs for some providers associated with more frequent re-signing.

- Online signers had shorter signature validity periods (2 or 3 days), since they generate signature for every query and do not have to resign the entire zones.
- Pre-compute signers had longer signature validity period (15-30 days).

(As far as we can tell, no provider allows configurable values)

# 6. Key Rollover support

- Many providers support well-defined automated ZSK rollover periods.
  - The period is fixed for some, configurable for others (ranging from 1 week to months or years)
- None supported automated KSK rollovers. But this is also probably not realistic until there is wider adoption of mechanisms like CDS and CDNSKEY\*

\* RFC 8078: Managing DS Records from the Parent via CDS/CDNSKEY -- <https://tools.ietf.org/html/rfc8078>

# 7. Signing non-standard traffic management records



- ✓ Online signers can sign traffic management records ( geo-location, failover records etc).
- ✗ Most of the Pre-compute signers cannot sign traffic management records.
- ✓ Only one Pre-compute signer could sign traffic management records (by pre-computing signatures over all the possible sets of answers).

**Important** : Multiple zones with Geo-location features and failover records.


# 8. Chain of trust

*We have multiple zones with sub-zones and secure delegation is important for us.*

## **Sign and Serve mode :**

-  Two of the providers did not support adding a DS record for a subzone via their interfaces. (one of them allows through backend DB channels)
-  The other providers supported adding DS records.

## **Serve Only mode :**

-  The providers can support DS record when serving a signed zone.



# 9. Authenticated Zone transfers

*DNSSEC is not designed to protect the transfer of full zones. Channel security mechanisms like TSIG need to be used.*

✓ **Inbound zone transfer:** All the providers that we tested, support TSIG for inbound zone transfer (when they act as a secondary)

✗ **Outbound zone transfer:** 4 out of 6 DNS providers do not support TSIG for outbound zone transfer (when they act as primary)

# Feature Enhancement Requests

# No single vendor satisfies all our reqs

- We're collaborating with vendors and hope the outcome will be improved and much more scalable implementations for DNSSEC.

# A few enhancement requests we've made

- Support NSEC3 for primary signing
- Scale to much larger zone sizes
  - Some vendors have already made improvements in this area
- Supporting DNSSEC signed zone as secondary
- Supporting adding DS for child zone.
- Supporting automated ZSK rollover
- Support for incremental signing.

(for the vendors missing those specific features)

# Multi-provider active-active signing

# Multi-provider active-active signing

- (This is “Sign and Serve” with multiple providers)
- Needed for zones containing dynamic traffic management features.
- Most managed DNS providers have not yet contemplated such a configuration (“You’re the first customer to ask us for this?”).
- Each provider acts signs zone data independently.
- Key Requirement: DNSKEY and DS RRset contents are coordinated such that validation is always possible no matter who is queried.

# Model 1

- Customer (Zone owner) holds the KSK and manages the associated DS record.
- Each provider has their own ZSK which is used to sign zone data.
- Providers have an API that customer uses to query the ZSK, and insert a combined DNSKEY RRset comprising both ZSKs, signed by the KSK.
- Key rollovers are always initiated by the Customer (details omitted here)

# Model 2

- Each Provider has their own KSK and ZSK key pairs
- Providers DNSKEY RRset also includes the ZSK of the other provider
  - Communicated by customer using a vendor API mechanism
- DNSKEY RRset is signed by the providers KSK (respectively)
- DS record in parent, managed by Zone owner, includes both KSKs
  
- Actively speaking to some providers about implementing this.
- For more details, see:
- <https://tools.ietf.org/html/draft-huque-dnsop-multi-provider-dnssec>



# Load Balancers etc

# Zones on Load Balancers

- Some of our data center designs employ leaf zones configured on load balancer appliances.
- These will need to support DNSSEC too.

# In Summary ...

# Take Aways

- We had a set of DNSSEC requirements we thought were fairly standard.
  - We found no single vendor satisfied all our requirements.
  - We're working with vendors on addressing these.
  - Multi-provider DNSSEC signing is a more novel requirement.
- 
- **Q. What can we do as a community to improve this situation?**

# Acknowledgements

- All the other members of the Salesforce Public DNS team:
- Sara Dickinson, Allison Mankin, Tim Wicinski, & Han Zhang.
- Engineers and product managers at the vendors we've spoken to.

Questions and/or comments?

# Appendix: Extra Slides (not covered in talk)

# Key Size Support

- ECC algorithms (ECDSAP256, ECDSAP384 etc) use fixed key sizes, and they are adequately strong.
  - e.g. P256 - 512-bit key approximately equal to 3,000 bit RSA key.
- But RSA supports variable length keys
  - Is often deployed with quite weak keys
  - 1024-bit ZSKs are very common, and these are widely considered to be compromisable by powerful adversaries (nation state, large corp, etc)
  - Vendors should support RSA key lengths much larger than 1024-bit (ideally 2048-bit), even for ZSKs.
  - We found many vendors that only supported 1024-bit for the ZSK.



# What if we wanted to roll our own?

- We're not a DNS company, so unlikely to happen.
- But if we wanted to take all of this in-house, would it be feasible?
- In theory, we run data centers and infrastructure around the world, so could deploy a network of authoritative DNS servers on them.
- We'd likely run open source DNS server software, but that leads to the question of supporting non-standardized DNS features, which are often absent or poorly supported in them.