Deploying DNSSEC in a Large Enterprise

Han Zhang, Allison Mankin, Salesforce

- Introduction
- Hybrid DNSSEC Architecture on 3rd Party Providers
- Summary

Introduction

Reasons for a Large Enterprise to Deploy DNSSEC

Security and Compliance

- We were mostly aware of US FedRAMP but recently we've received other national compliance needs for DNSSEC
- ICANN advised that all use DNSSEC at a very opportune time

And equally important, though not as measurable: Trust Benefits for Users

- DNSSEC increases trust for users
- We had to decide between a separate small namespace for the regulated groups or DNSSEC for all
- Our decision, supported by leadership: deploy DNSSEC for all

Introduction

Characteristics of Our Enterprise

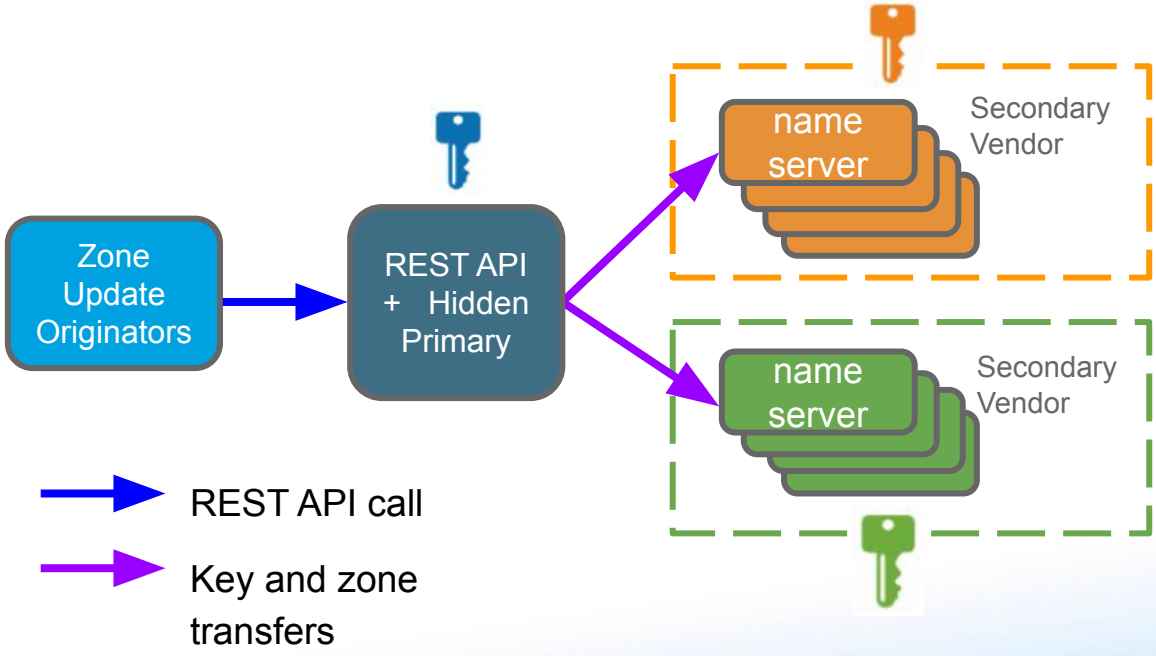
- Use of Managed DNS
  - Outsourcing to get sufficient authoritative footprint
  - Using multiple providers for resilience
- Some zones are very dynamic
  - Up to 1 million changes per day, 700 changes per minute (aggregate)
  - Dynamic zones are not unique: consider web hosting companies
  - Changes can cause update propagation delays *
- Some customer-facing zones are very large *before signing*

* DNS Service Monitoring at Salesforce, **Han Zhang, OARC 27**

- Introduction
- Hybrid DNSSEC Architecture on 3rd Party Providers
- Summary

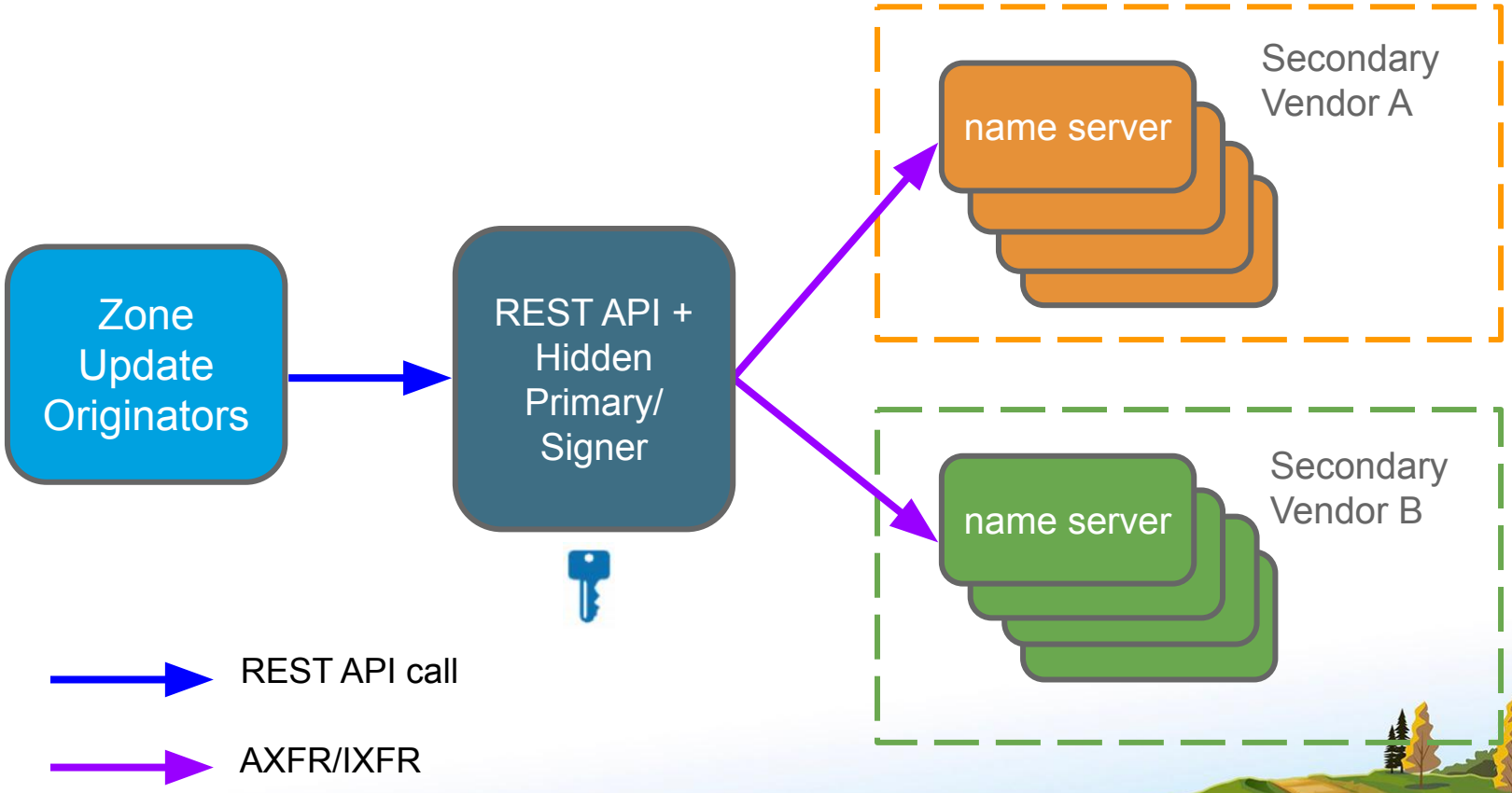
Ideal Model * - Multi-signer

- Multi-signer DNSSEC has two models
- Not enough providers supported these models

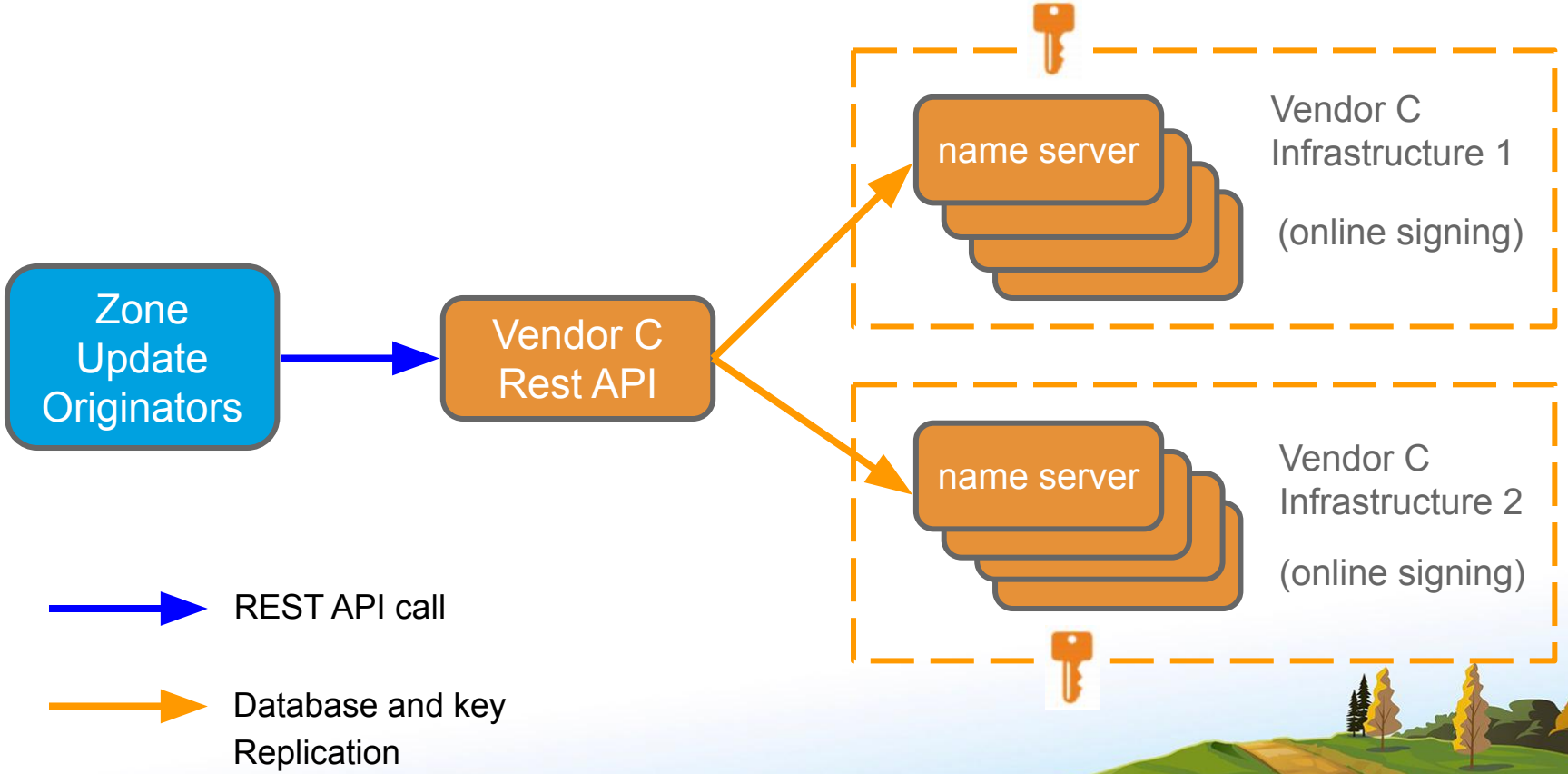


* Multi-signer DNSSEC Models, **Shumon Huque, Jan Včelák, OARC 30**

Hidden Signing Primary Model



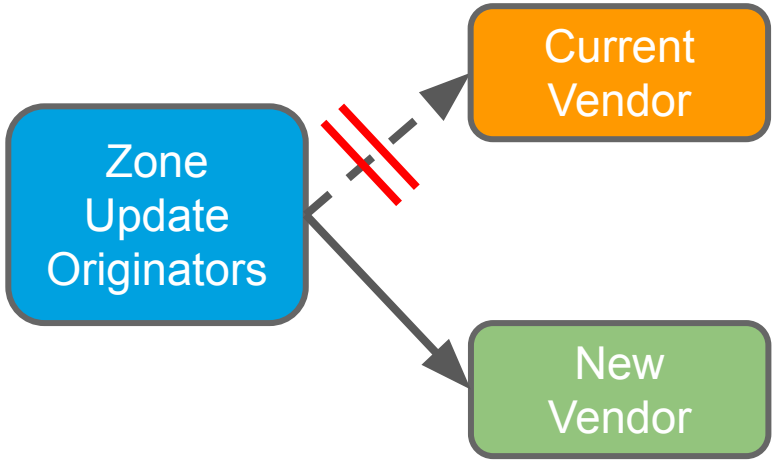
Third-party Signing Vendor Model



Zone Migrations in all the models

- Moves of zones between providers were needed
  - For provider features - DNSSEC and other and for clean-up

Is Zone Migration Simple?



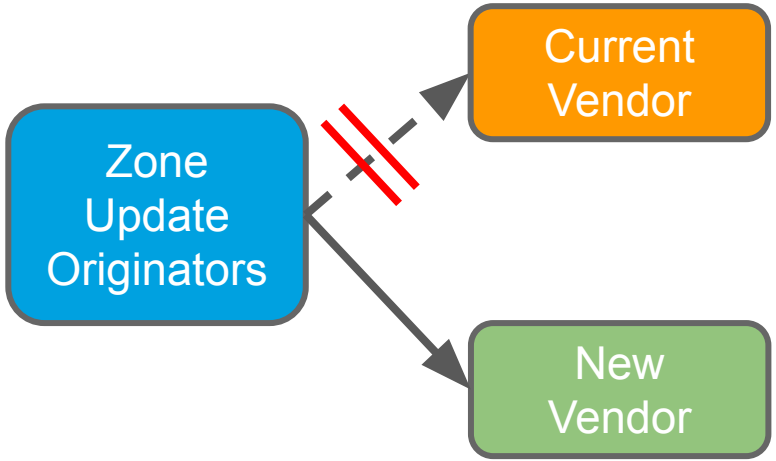
- Moves of zones between providers were needed
  - For provider features - DNSSEC and other and for clean-up

- Zone migration is simple, isn't it?

  Just changes to send updates to new vendor

  Then change the NS records, right?

Lesson Learned - Migration Can be Fragile



Goal: Mitigate risks by doing multi-step migration

Observation: Separate migration from DNSSEC signing to minimise impact.

For live, dynamic zones a hard cut-over is risky:

- Provisioning: REST API calls fail
- Resolution: customers see outdated inconsistent answers

Delegation and Child Zones

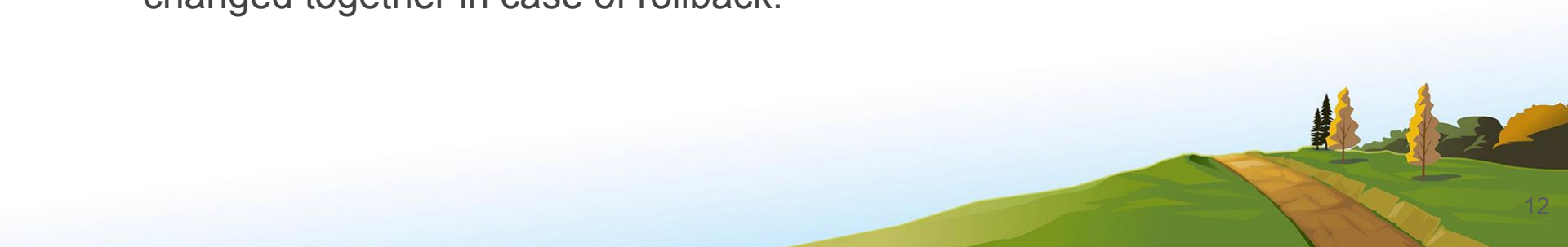
- Zones being migrated remain on the old provider until migration completed.
- If both parent and child are on the same provider and **ONLY** the child is migrated then old provider might still server the child zone after the NS change.

Solution:

Migrate the parent zone and child zone at the same time

Pro -> No down time. No impact on provisioning

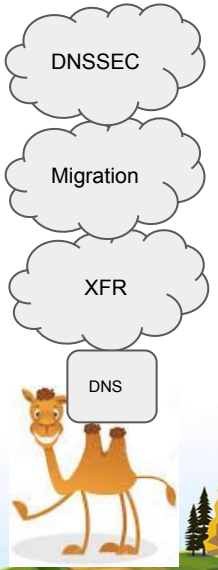
Con -> The NS records of the parent zone and child zone need to be changed together in case of rollback.



- Introduction
- Hybrid DNSSEC Architecture on 3rd Party Providers
- Summary

Takeaways

- There are challenges and surprises in deploying DNSSEC in a large enterprise, but it can be driven to success
- DNSSEC deployment needs preparation, clean-up, migrations, and monitoring, in addition to the DNSSEC specific tasks
- The DNS camel's burden from old standards is also tough
  - Examples include the delegation issues and the XFR issues we've discussed
  - This is distinct from the burden of new standards



Thank You

- The DNSSEC deployment at our enterprise was accomplished by a great team. Everyone on the team is an author of this talk. Other authors: Pallavi Aras, Sara Dickinson, Shumon Huque, Neda Kianpour, David Lawrence, Shivan Sahib & Baula Xu.

- We have been immeasurably aided by engineers and product managers at our vendors (A, B, C, D, and E). They know who they are.