

# Verisign's Path to RPKI

Mike Hollyman and Hasan Siddique

### Delivering critical internet infrastructure: Verisign's role

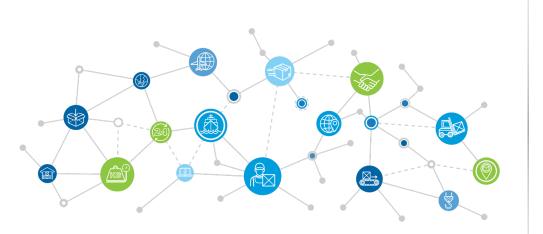
### **Critical Internet Services:**

- Globally distributed, proprietary DNS registration and resolution infrastructure purpose-built for dependability in an ever-increasing cyberthreat environment
- Registry services for several well-known TLDs including .COM and .NET, operate 2 of the 13 internet root servers, and perform the root zone maintainer function on behalf of ICANN
- Research, develop, and deploy new technologies to make the internet more stable and secure
- Comprehensive security program aligned with NIST cybersecurity framework and CIS controls
- Securing Verisign-operated critical infrastructure benefits the global internet ecosystem, including RPKI
  - Systemic and circular dependencies are minimized and/or carefully managed

### Commitment to security, stability and resiliency.



## Similarities between the global supply chain and the internet





"Supply chain isn't a single process but rather a complex system of interconnected and interdependent relationships. As such, disruptive events resulting from systemic risks — droughts, bankruptcies, and cyberattacks included — can trigger a domino effect up and down the supply chain, even causing adjacent industry failures. Systemic risks don't take turns; they often trigger one another and can materialize all at once. To 'fix the problem,' businesses must understand the top systemic risks shaping global supply networks."\*



The Internet is a loosely interconnected network of networks, computers and servers globally that enables the exchange of data and information between devices

\*https://www.forrester.com/press-newsroom/forrester-supply-chain-disruptions-have-become-the-new-normals-new-normal/



## Verisign's global footprint



## Verisign's global footprint

- Heavy anycast for global services
- Adoption of BCP-169
- Over ~270 different ASNs
  - Larger ROA dataset
- Automation investment as a must have
  Full ROA lifecycle is automated
- Significant internal investments in monitoring
  - o End-to-end monitoring and alerting
- Manage critical operations of root and top-level domains (TLD)
  - Conservative deployment rollout
  - Availability and data integrity are critical





## **RPKI** Potential Issues

### Primary

Maturity

DNS and RPKI dependencies

Commercial support

Additional complexity / new external dependencies

Shared fate dependency

Operational integration

Monitoring requirements

Public perception

Operational & security maturity of RIRs

### Secondary

Overclaiming by RIR CAs

Opt-in: Even if you don't sign a ROA, one could be maliciously signed for you

Transparency with operator policies "/.well-known/rpki.txt" ?

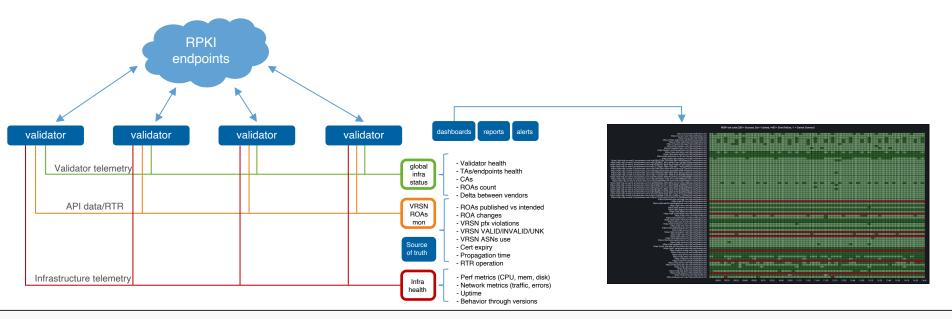
Avoiding polarized anycast traffic

Future scale of RPKI

RPKI adds safety, not security



## **RPKI** infrastructure and monitoring

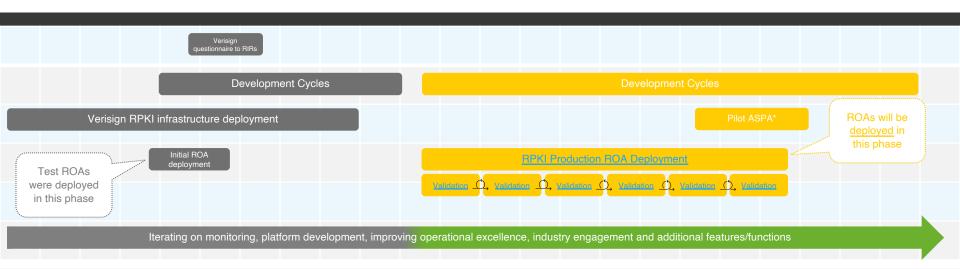


- Global monitoring as a priority for running RPKI
  - Heavy investment in management and monitoring dev efforts
  - Detected and reported multiple incidents with service availability and integrity
  - Resource appropriately

- Intent based pipeline for IRR and RPKI
  - Verisign routes are published to IRR and same dataset to RPKI
  - Lifecycle management of data-set is automated and monitoring identifies undesirable data drift



## Verisign's RPKI plan



#### Level 0 - (maturity index)

#### **Performing Fundamentals**

Teams are gaining familiarity with systems, monitoring is best effort and process are immature and manual

#### Level 1 - (maturity index)

#### Management & Maintenance

Teams are spending engineering cycles converting best effort systems to production grade Processes have reached an acceptable level of maturity. Foundations enable growth

#### Level 2 - (maturity index)

#### Modernizing Infrastructure

Compliance dashboards will drive alerts to automatically manage critical data needed for RPKI management

Infrastructure will continue to be hardened and roadmaps will be defined for features and functions based on stakeholder engagement

#### Level 3 - (maturity index)

#### **Advanced Automation**

Introduce automated correlation between systems like RPKI and error conditions specific to Verisign for rapid observation and action

Significant reduction in manual work related to RPKI data governance

Evaluate and advise how future route security protocols will impact Verisign services



### Lessons Learned

- Be deliberate in plans for RPKI to prevent any related outages to the DNS
- Significant net-new complexity comes with RPKI engineering and operational prioritization are key
- RPKI isn't free. There are costs to the Relying Parties, the RIRs and networks doing ROV. Financial support of the ecosystem components is critical (e.g., RIR funding to enhance operational and security posture)
- Organizations must invest heavily in tools to better manage and maintain critical aspects of the RPKI ecosystem for their specific organization – why not more open-sourced solutions here, and when do commercial solutions emerge?
- Overclaiming by RIRs puts the onus on the Relying Parties to know if they have bad data or resolve conflicts, increases attack surface substantially
- Technical side is complex, there are also organizational aspects of RPKI that implementors need to consider
- Shared security models like RPKI / ASPA highlight the need to prioritize collaboration within the industry



# powered by



# **VERISIGN**<sup>®</sup>

© 2023 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

# Appendix

## Examples of RPSLAS-SET objects for Geolocation



## Verisign AS-VRSN-ANYCAST

- RPSL objects published for Geolocation
- AS-GTLD remains as-is with ASN only
- AS-VRSN-ANYCAST contains Geolocated objects
  - whois –m AS-VRSN-ANYCAST
- Two-letter ISO codes for each country
  - AS-GTLD-[XX]
  - whois -m AS-GTLD-US



## Verisign AS-VRSN-ANYCAST

	-VRSN-ANYCAST
as-set:	AS-VRSN-ANYCAST
descr:	Verisign Per Node Global Anycast Service ASNs
remarks:	Verisign Global Registry Services
remarks:	ISO Country Code discriminators
remarks:	for per node global anycast
remarks:	in accordance with RFC6382.
remarks:	For non critical questions, contact radb@verisign.com.
members:	AS16838
members:	AS7342
members:	AS26415
members:	AS-GTLD-NL
members:	AS-GTLD-US
members:	AS-GTLD-AR
members:	AS-GTLD-GR
members:	AS-GTLD-IN
members:	AS-GTLD-ES
members:	AS-GTLD-RS
members:	AS-GTLD-LB

## Verisign AS-VRSN-ANYCAST

whois -m AS-GTLD-NL	
as-set:	AS-GTLD-NL
descr:	VeriSign Unique Origin Anycast Country Catchment – Netherlands
source:	RADB
members:	AS396613
members:	AS396614
members:	AS40647
members:	AS396615
members:	AS396616
members:	AS396617
members:	AS396587
members:	AS32651
members:	AS396588
members:	AS396589
members:	AS396590
members:	AS396566
members:	AS396567
members:	AS27544
remarks:	Verisign Global Registry Services
remarks:	This AS-Set indicates geographic country routing
remarks:	discriminators for Verisign anycasted prefixes as
remarks:	documented in RFC6382.