Verisign's Path to RPKI

ROW12

Mike Hollyman

June 20th 2023

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.

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
  - 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

AS396757
AS396649
AS396557
AS396618
AS396551
AS396619
AS397197
AS396663
AS396691
AS396711

60+ Countries   **240+** Global Sites   **230+** Billion Transactions Daily

powered by **VERISIGN**

Verisign's global footprint (Cont'd)

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

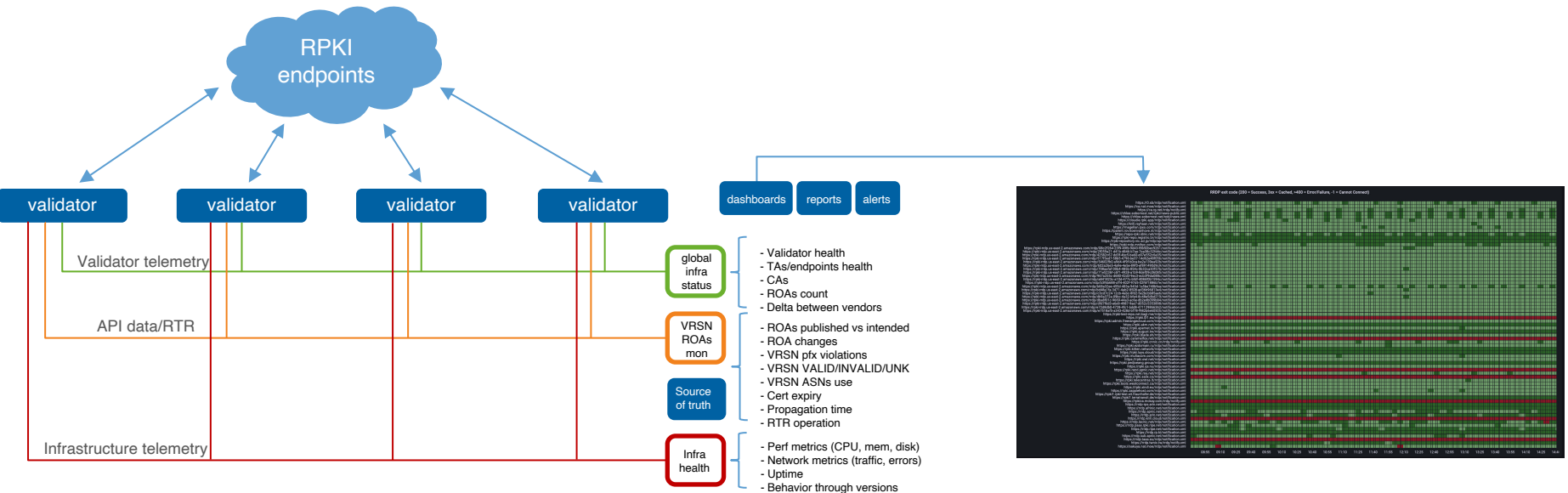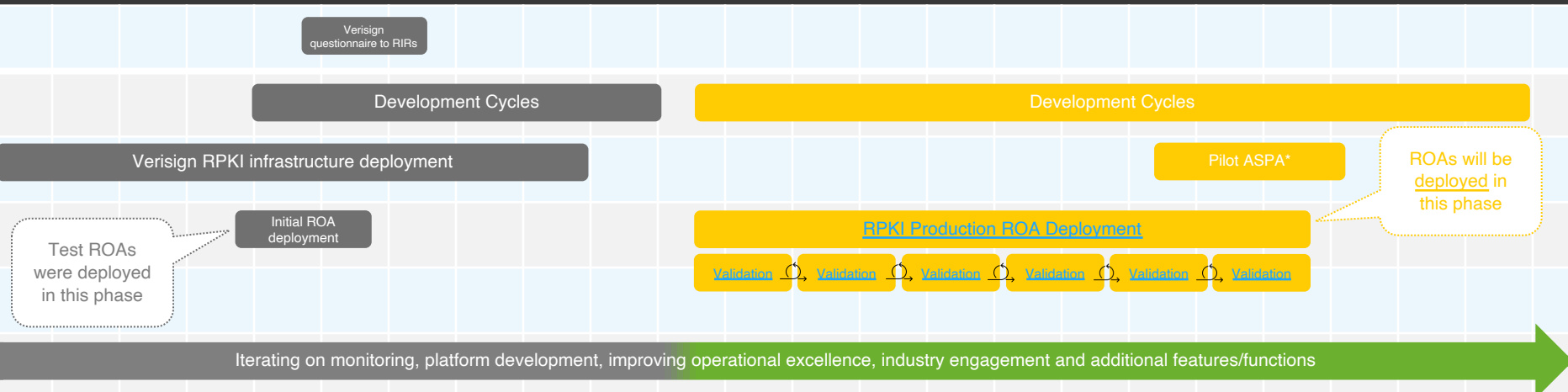| Secondary |
| --- |
| Overclaiming by RIR CAs |
| Opt-in: Even if you don't sign a ROA, one could be maliciously signed for you |
| Transparency with operator policies "/.well-known/rpki.txt" ? |
| Avoiding polarized anycast traffic |
| Future scale of RPKI |
| RPKI adds safety, not security |

RPKI infrastructure and monitoring

- **Global monitoring as a priority for running RPKI**

  o Heavy investment in management and monitoring dev efforts

  o Detected and reported multiple incidents with service availability and integrity

  o Resource appropriately

- **Intent based pipeline for IRR and RPKI**

  o Verisign routes are published to IRR and same dataset to RPKI

  o Lifecycle management of data-set is automated and monitoring identifies undesirable data drift

Verisign's RPKI plan

Verisign questionnaire to RIRs

Development Cycles

Development Cycles

Verisign RPKI infrastructure deployment

Pilot ASPA*

ROAs will be deployed in this phase

Initial ROA deployment

RPKI Production ROA Deployment

Validation | Validation | Validation | Validation | Validation | Validation

Test ROAs were deployed in this phase

Iterating on monitoring, platform development, improving operational excellence, industry engagement and additional features/functions

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

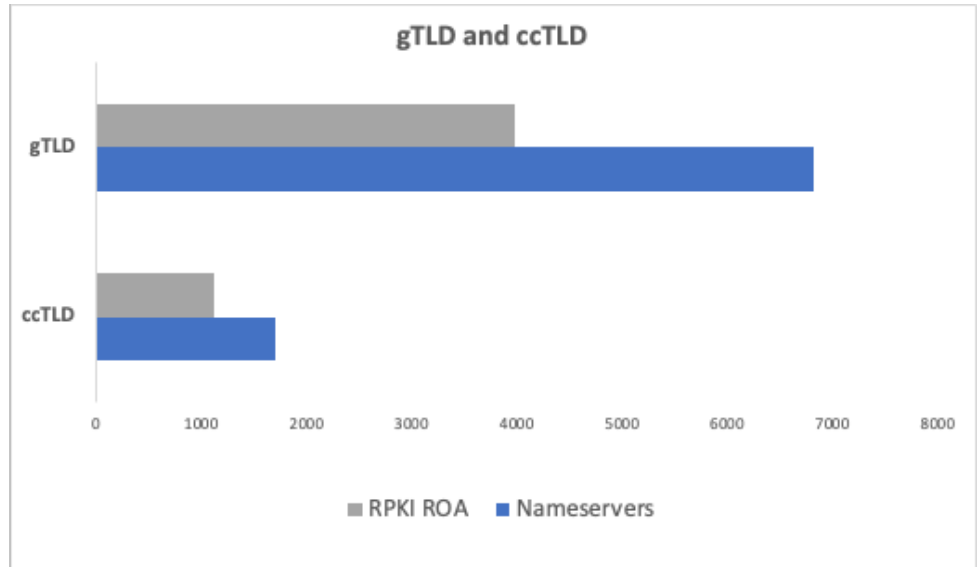Evaluate and advise how future route security initiatives will impact Verisign services

powered by **VERISIGN**

*Autonomous System Provider Authorization (ASPA) – for path validation with the IETF currently

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

A view of TLD RPKI

TLD Group	Nameservers	RPKI ROA	Percent (%)
Legacy	80	6	8
ccTLD	1712	1128	66
gTLD	6823	1059	15

TLD	IPv4 RPKI	IPv6 RPKI
.com	no	no
.net	no	no
.org	no	no
.gov	no	no
.mil	no	no
.biz	3 of 6	3 of 4
.info	no	no

gTLD and ccTLD

■ RPKI ROA ■ Nameservers

powered by

VERISIGN®