

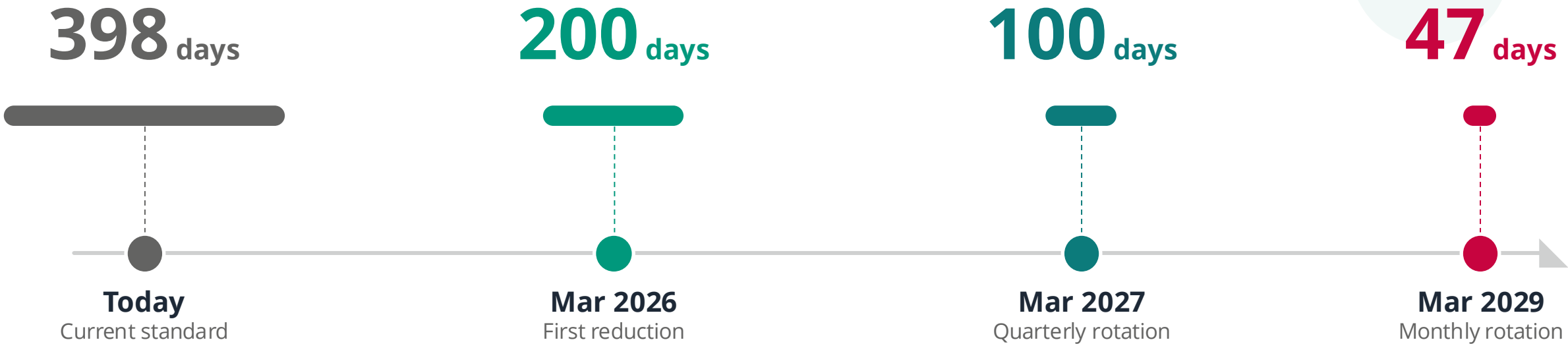
SSL/TLS Certificate Lifecycle Changes

Preparing for shorter certificate validity periods

SSL/TLS Certificate Lifecycle Changes

Industry-wide timeline for shorter certificate validity periods

CA/Browser Forum (Ballot SC-081) mandates a phased reduction of maximum SSL/TLS certificate validity



Why it matters: Manual certificate management becomes impractical. Without automation, organizations face repeated service disruptions — including with CDQ integrations.

How to Address This Challenge

Recommended approaches for certificate lifecycle management



Trust Root / Intermediate Certificates

Configure trust at the root or intermediate CA level instead of pinning leaf certificates. Avoids breakage on every renewal cycle.



Automate via ACME Protocol

Use ACME-based automation (RFC 8555) with Certbot, acme.sh, or enterprise CLM platforms. Automation is the only sustainable path at 47-day lifetimes.



Centralize Certificate Inventory

Maintain a single inventory using discovery tools and CT log monitoring. No automation without full visibility.



Integrate into CI/CD and Infrastructure-as-Code

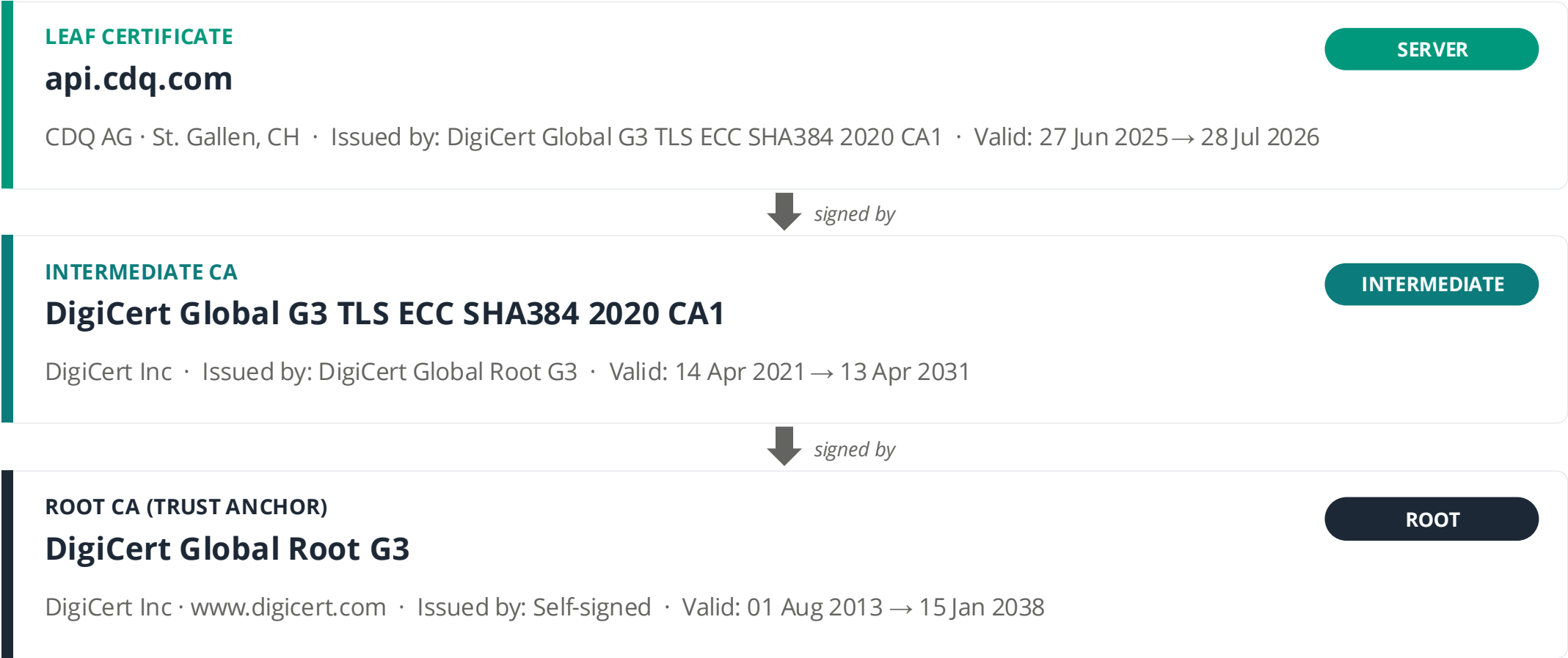
Embed cert provisioning into pipelines (Terraform, Ansible, K8s cert-manager) or use cloud-native solutions (AWS ACM, Azure Key Vault).

CDQ Contact

Dr. Martin Ofner
Head of Software Dev & Ops
martin.ofner@cdq.com

Appendix: Certificate Chain for api.cdq.com

Live chain as presented by the server — leaf, intermediate CA, and trust root



Pin trust at the root: The leaf rotates yearly today (and far more often soon) — the DigiCert Global Root G3 is valid until 2038 and is stable.