

Trust, but Verify: When CAs Reuse Domain Validation at Scale

FRANCESCO PRISCO*, SIMON PIETRO ROMANO*,
ANTONIA AFFINITO^, RAFFAELE SOMMESE^

* UNIVERSITY OF NAPLES, FEDERICO II,
^ UNIVERSITY OF TWENTE

TO APPEAR AT: WTMC 2026 (ACM CCS WORKSHOP)

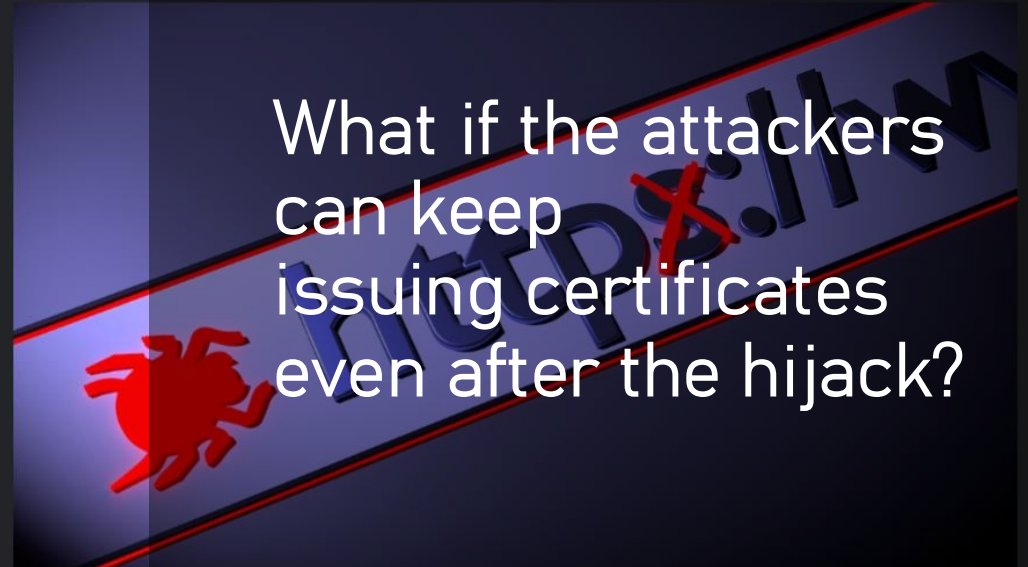


CRYPTOGRAPHIC IMPERSONATION

Hackers obtain counterfeit TLS certificates for Google and other large services

Compromise of 3 domain registries allows hackers to walk off with unauthorized certs.

DAN GOODIN - 6 OCT 2026 21:21 | 48



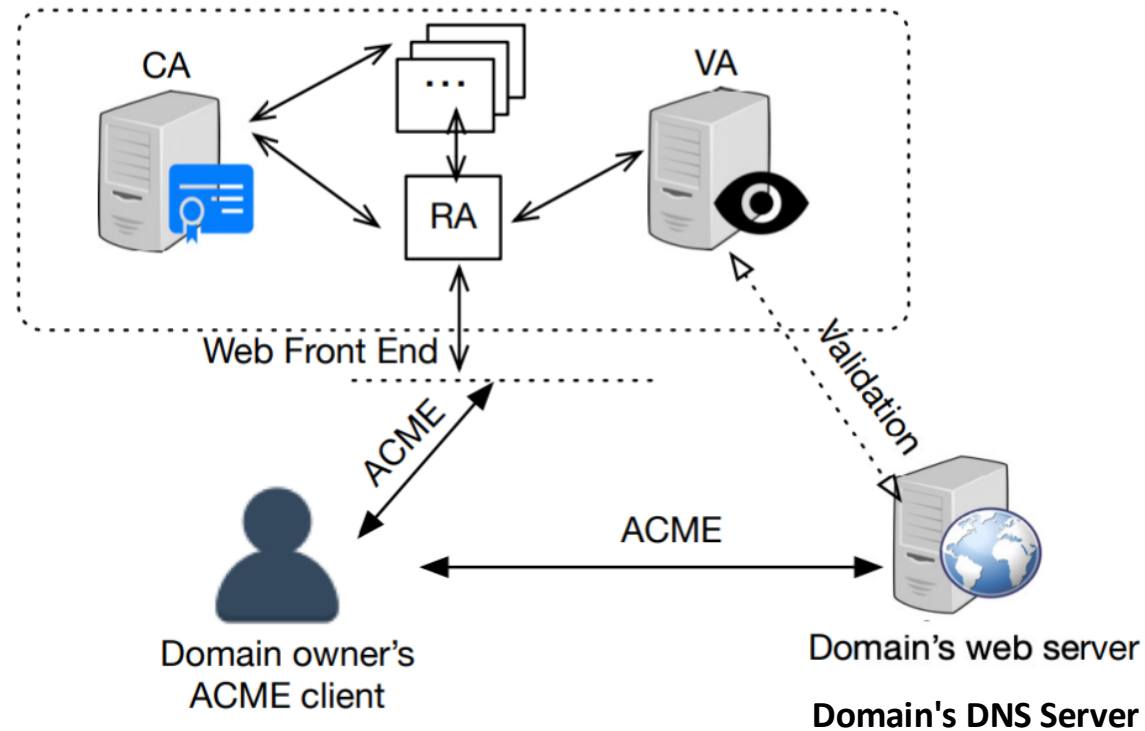
Credit: Getty Images



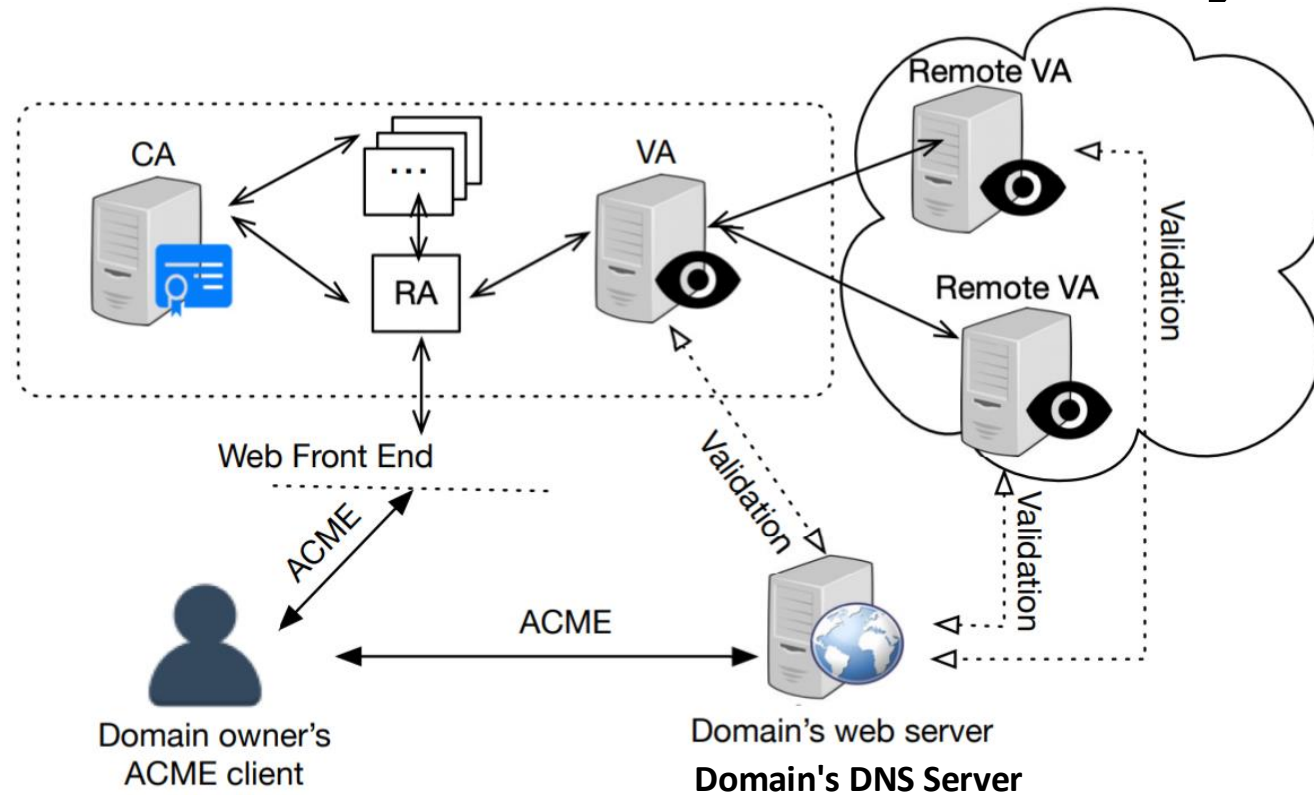
Attackers hijacked three top-level domains and used their control to mint counterfeit TLS certificates for Google and other large organizations, Google said Tuesday.

The attackers launched a series of attacks on the .gh, .sl, and .as country code top-level domains (ccTLDs) and then modified authoritative DNS records for selected domains within those namespaces. By controlling those DNS records, the attackers were able to pass automated domain control validation checks and obtain unauthorized certificates for “several Google domains” and “several leading global brands and widely used online services.” Google said it updated Chrome to block all certificates it identified as unauthorized, and worked with the issuing certification authorities to ensure the

Certs are issued in this way, right?



Actually, certs are issued in this way, right?

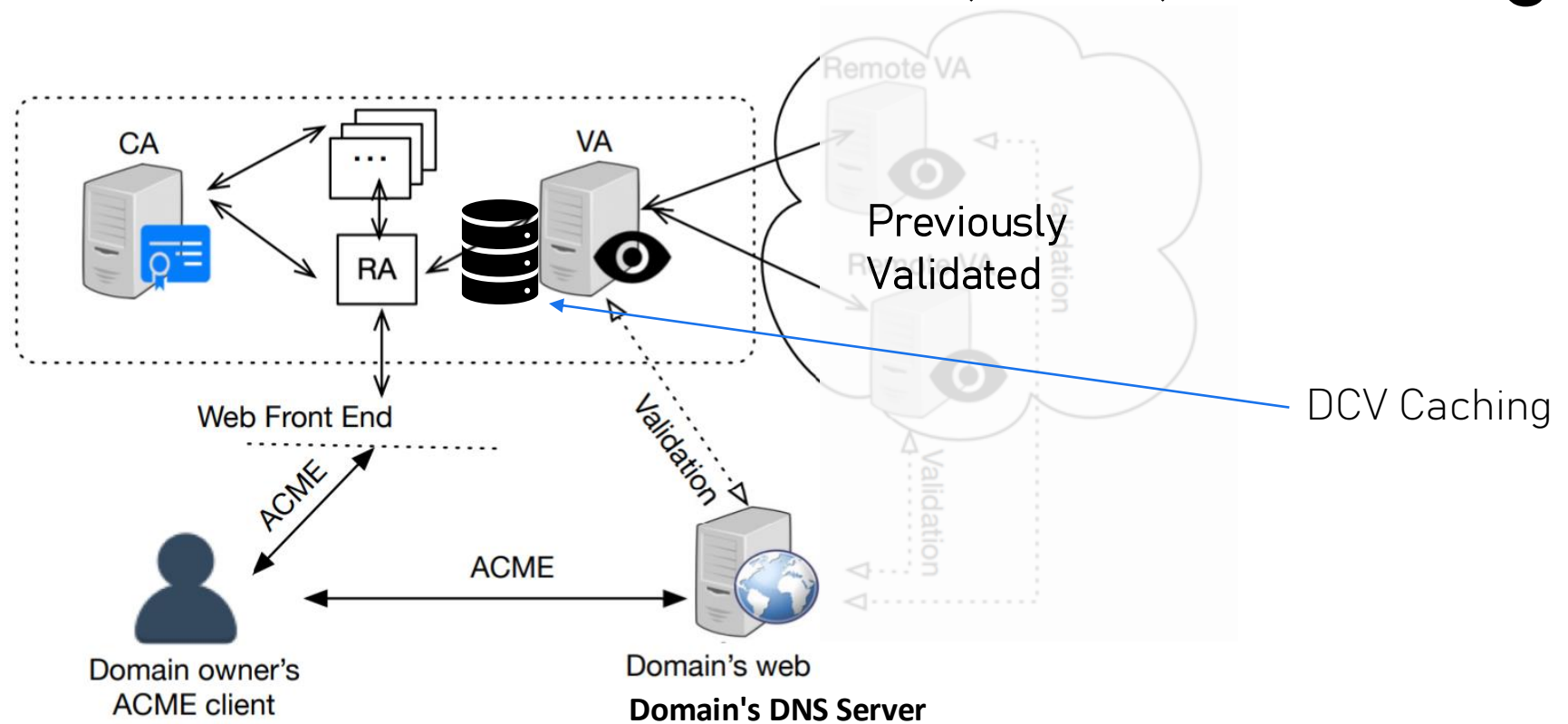




Meet Domain Control Validation (DCV) Caching

- Repeated domain-control validation may overload domain infrastructure and CA validation servers, with **catastrophic consequences**
- Two common mitigations are **rate limiting** (PSL-based?) and **domain control validation caching**.
- We focus on **caching**, and on the security, risks introduced by **reusing validation results**.

Meet Domain Control Validation (DCV) Caching



Web PKI & Domain Validation Reuse



96.4% Domain-Validated (DV)

Publicly trusted TLS certificates rely on proof of control over domain names.



398-Day Validation Reuse Window

CA/Browser Forum rules allowed validation data to be reused for up to 398 days.



A Gradual Reduction

The reuse period is being shortened, with a target of 10 days in 2029.



Stale Validation Caching & Ownership Risks



Domain Expiration

When domain expires or is deleted, its registration and DNS delegation disappear.



Stale Validation Reuse

As in that case or if a domain changes ownership, previously cached validation data may no longer reflect the current controller.

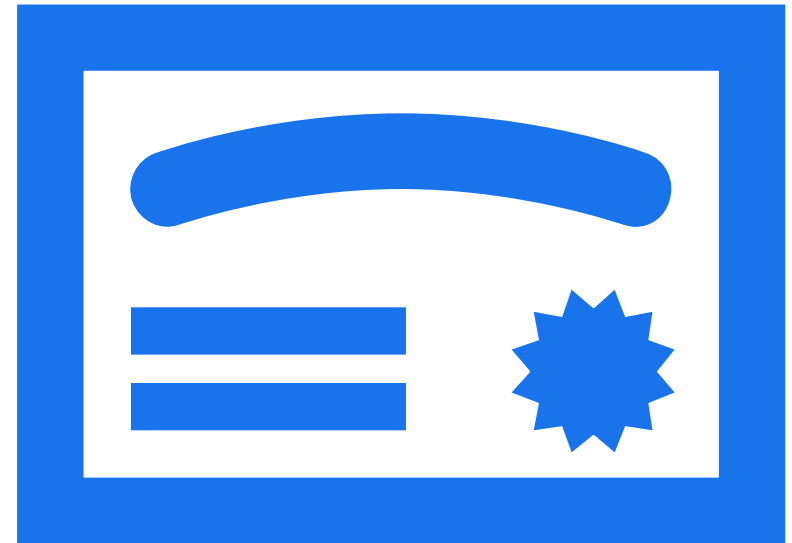


Potential MitM Risk

Combined with BGP traffic redirection, this could enable an attacker to obtain a browser-trusted certificate and intercept traffic without the usual certificate warnings.

How do we find DCV caching cases?

- How often do CT logs contain certificates for domains with no contemporaneous registration or DNS evidence?
- How many cases have historical evidence consistent with validation reuse?
- How do these cases vary across CAs and individual issuers?





Measurement Pipeline & Data Sources

- 1. Detection
 - OpenINTEL Zonestream matches CT precertificates against daily gTLDs zone files.
- 2. Verification
 - Newly detected domains are checked via RDAP and monitored with DNS queries for 48 hours.
- 3. Historical cross-check
 - DNS Coffee checks a ± 3 -day window around certificate issuance for evidence of prior domain delegation (accounting for MMD).
- **Caveat:** CT log timing and historical data availability can affect what we observe.
 - We check that the first DNS measurement we issue is within 5 min from the certificate issuance request.

Measurement Results Across 2025

Pipeline Stage	Certificates	Unique Domains
Potential new domains / certs observed	46,887,049	40,994,309
RDAP 404 responses (registry non-existent)	1,340,137	811,932
Consistent NXDOMAIN for 48 hours	490,233	284,880
CT-to-measurement gap $\leq$ 5 minutes	190,337	169,030
Absent from historical zones ($\pm$ 3 days) [Final]	142,848	121,091

Subsequent Domain Lifecycle

- 121,091 unique domains had certificates issued without contemporaneous DNS evidence.
- 111,899 domains did not reappear in zone files after issuance.
- 9,192 domains were subsequently re-registered, raising the possibility of ownership transfer while prior validation data remained reusable.
 - We could not determine if the registrant was different due to lack of registrant data in RDAP.



Are These Cases Explained by DCV caching?

- 91.88% had a predecessor certificate from the same issuer within the 398-day reuse window.
- 92.82% of these cases had evidence of active delegation when the historical same-issuer certificate was issued.
- This historical evidence is consistent with prior validation, but does not completely establish that a cached token was reused.

Top Issuers & Normalized Radar Rates

Certificate Issuer	Affected Domains	Radar CT Volume	Aff. / 100K Radar
GoDaddy G2	23,567	305.3M	7.72
GTS WE1 (Google)	23,413	716.3M	3.27
DigiCert Enc. Everywhere G2	16,682	114.3M	14.60
ZeroSSL ECC	8,396	239.1M	3.51
Sectigo DV E36	6,861	125.4M	5.47

Why Does This Problem Exist?

CAs long-lived trust in DNS

CAs may reuse domain-validation evidence long after the original check.

Limited historical visibility

DNS is queried on demand, and temporary zone changes or short-lived validation records may leave no durable public evidence.

Operating on private evidence of domain registration?

Some CAs also operate as registrars and may have access to internal registry information not visible through public RDAP.

Shall CAs trust DNS at all?

We should reconsider the transitive trust the CA ecosystem places in DNS evidence.



Meanwhile on the CAs side

- In March 2026, the maximum domain-validation reuse period was reduced to 200 days under Ballot SC-081.
- Further reductions are planned to bring validation reuse closer to certificate lifetimes (that are also getting shortened).
- The target is 10 days by March 2029.



Questions?

Historical validation
evidence is not
necessarily evidence of
current domain control.

r.sommese@utwente.nl

Full Paper:



https://academia.r4ffy.info/paper/WTMC_prisco.pdf

