

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

Post Mortem - User PKI Incident

Stephan Mößler, E.ON Digital Technology GmbH

Post Mortem - User PKI Incident

Rebuilding a house while its on fire



Who I'am

Stephan Mößler

Lead Solution Architect

Security & Crisis Management

E.ON Digital Technology GmbH

M +491623343638 stephan.moessler@eon.com

e-on



User PKI @ E.ON Group

- End user certificates
 - **Public Trusted: Encryption, Signature**
 - Internal trusted: Authentication
- Certificates stored on smart cards, approx. 60k smart cards issued
- 2nd generation smart card introduced in 2025 (BSI requirements)
- designed more than a decade ago, with minor adaption, sized for approx. 500 users/day
- heavily used and integrated into nearly all business processes across E.ON Group since the mid-2000s.

Requirements - Compliance, Compliance, Compliance!

- **CA/Browser Forum (CAB Forum):**
 - global industry standards group (roughly CAs + Browser vendors).
 - publishes baseline requirements e.g. S/MIME Baseline Requirements
- **Publicly trusted**
 - a cert chains to a root in major browser/OS trust stores (Apple, Mozilla, Microsoft, Google, etc.).
 - Root store programs even more stricter than CA/B requirements.

If a CA breaks rules, root stores can distrust that CA/root

How it started – Compliance violation.

- violation of section 4.3.1.2 of the S/MIME Baseline Requirements.

[...]

*Effective March 15, 2025 the CA SHOULD implement a **Linting process testing compliance** with these Requirements for S/MIME Certificates.*

[...]

*The CA ... SHALL revoke a Certificate **within 5 days** ...*

source: https://bugzilla.mozilla.org/show_bug.cgi?id=2037000#c5

How it started – Compliance Audit @ D-Trust



2026-05-04 07:00 (UTC) Start internal Review of S/MIME CAs

2026-05-04 08:30 (UTC) Violation of S/MIME Baseline Requirements,

2026-05-04 09:17 (UTC) D-Trust stopped issuance from the affected part of its PKI

...

2026-05-04 12:40 (UTC) Start External communication

...

2026-05-08 15:00 (UTC) Start of mass revocation of certificates.

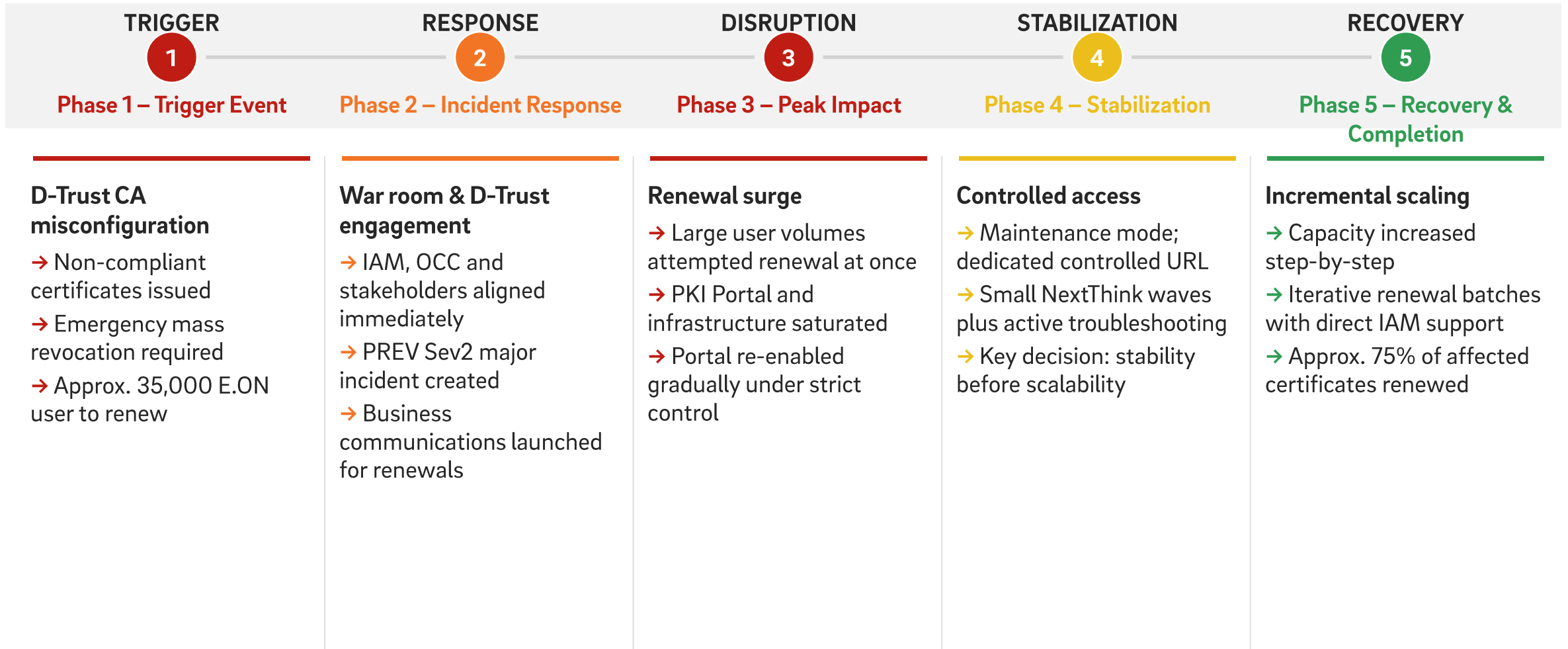


Mass revocation - Impact.

- Total number of certificates: **165,972**
- Affected issuing CAs:
 - **E.ON CA 2 2013 XXI,**
 - **E.ON CA 2 2013 XXIII,**
 - D-Trust Application Certificates CA 3-1 2013
- Affected certificate types: S/MIME
- Approx. 40% of all affected certificates are for E.ON Group

Incident Timeline – Certificate Mass Revocation

Executive incident overview



Key Lesson: Large-scale certificate replacement requires controlled onboarding, staged communication, scalability validation, and prioritizing stability before accelerated adoption.



CORE PRINCIPLE Control rollout behaviour before accelerating adoption.

1 Communication & Prioritization

- Avoid messaging that can trigger panic reactions
- Maintain constant communication and availability
- Prioritize correctly when pressure peaks

2 Release Discipline

- Keep lower test environments at production parity
- No production implementation without lower-environment validation

3 Scalability & Automation

- Include backend interface capacity when scaling frontends
- Treat automation as a requirement, not a demand

4 Team & Crisis Readiness

- Never underestimate the power of teamwork
- Run periodic drills for crisis management

Bottom line: Crisis response improves when communication, testing discipline, scalability planning, automation, and team readiness are designed before the next incident.



What Really Went Well – Incident Response

Success factors from recovery execution

HEADLINE

A concentrated response unlocked improvements that would normally take much longer.

2 weeks focus

1 Team mobilization

- Exemplary teamwork under pressure
- Multiple advocates and support across teams

2 User & stakeholder support

- Personalised support for users
- Periodic, transparent communications
- Crisis management reporting kept stakeholders aligned

3 Operational acceleration

- Swift scale-up of capacity and support
- Enterprise-wide cleanup of legacy Microsoft VSC
- Approver step removed, simplifying renewals and reducing cycle time

Overall result: Many enhancements were delivered within two weeks, compressing work that would otherwise have taken significantly longer.



GOOD NEWS

The incident update became a must-read — and the meme engine switched on.

Compass article traction

98,474

views on the Compass article

- Awareness reached far beyond the core incident team
- Colleagues stayed engaged — and kept the mood human
- A serious recovery still made room for shared humor

Meme fest: officially started



From helpful
comments...

...to memes.

Engagement metric:
highly visible,
surprisingly
entertaining.

Thank you: for renewing certificates, supporting users — and proving that even a certificate crisis can become internal internet culture.



Q&A

e-on