

Reporting a problem with a certificate issued according to CA/Browser Forum requirements

Do you want to inform us of a problem with a TLS/SSL or S/MIME certificate issued by D-Trust GmbH?

It is not a technical problem, such as faulty installation *

This certificate does not comply with the BR/EV or S/MIME requirements of the CA/B Forum.*

Select one of the following options depending on which certificate is concerned.

TLS/SSL certificate

Report of a problem with a TLS/SSL certificate (end entity certificate) issued by D-Trust GmbH for my organisation or for a domain belonging to my organisation.

Report of a problem with a TLS/SSL certificate (end entity certificate) issued by D-Trust GmbH.

S/MIME certificate

Report of a problem with an S/MIME certificate (end entity certificate) issued by D-Trust GmbH for my organisation or for a domain belonging to my organisation.

Report of a problem with an S/MIME certificate (end entity certificate) issued by D-Trust GmbH.

CA certificate

Report of a problem with a CA certificate issued by D-Trust GmbH.

1. Reason for revocation

Please let us know why the certificate should be revoked. *

2. When did you detect the problem?

Date: *

Time: *

3. Which certificate is concerned?

Certificate serial number (Hex) *

Please enter in 32 digit hex format with colons as separators

URL under which the TLS certificate is used

crt.sh URL (optional)

Mandatory field in case of a problem with the TLS/SSL certificate type

4. Contact details

First name *

Family name *

E-mail-address *

Phone

Please note: Enter with international dialling code without "0" in the area code and without spaces.

Please send us the completed form to the following e mail address with the subject:
"Reporting a certificate problem": certificate-issue@d-trust.net.

Privacy policy in the event of security incidents

Why do we collect data within the scope of this process?

As the certificate issuer, D-Trust GmbH must provide a way to report suspected certificate misuse. The following data will be collected in connection: first and family name, e-mail (mandatory) and telephone number (optional). D-Trust GmbH is obliged to contact both, the person reporting the security incident and the subscriber. Please refer to the Baseline Requirements of the CA/B Forum (<https://cabforum.org/baseline-requirements-documents/>) for more information. The legitimate interest of D-Trust GmbH is to protect our products and the general public from insecure online communication (using TLS-secured connections).

How do we process the data and how long is the data stored?

In the Support area of D-Trust's website you can report a security problem with TLS and/ or S/MIME certificates. Also for CA certificates issued according to the specifications of the CA/Browser Forum. Simply complete the form provided and send it to the e-mail address shown there. The report will then be handled according to a defined process in the IT systems of Bundesdruckerei GmbH and D-Trust GmbH. Any personal data from the report will be kept in the IT systems of Bundesdruckerei GmbH and D-Trust GmbH until the entire incident was clarified. If neither the reporter nor the subscriber provides further feedback within a period of 12 weeks, the data will be deleted at the end of the following year.

Who will be informed about the incident?

In order to process the case or connected to audits, both Bundesdruckerei GmbH and D-Trust GmbH and, if applicable, the respective conformity assessment body will receive the contents of the report including the personal data of the reporter.

Who is responsible according to the General Data Protection Regulation?

The responsible representative for data processing and the rights of the persons concerned and the right of appeal to a supervisory authority for data protection can be found in the following data protection information: <https://www.d-trust.net/en/privacy-policy>