JUMBO BLOCK CERT

Eigene Zertifizierungsstelle und TLS-Zertifikate



Handbuch · Version 1.0.0

Oktober 2026

ZANNI GROUP · Andreas Zanni e.K. · Brauhof 12 · 44866 Bochum · jumboblock.org

Inhalt

1. Überblick
2. Grundbegriffe
3. Arbeitsablauf
4. Zertifizierungsstelle anlegen
5. CA-Datei, Entsperren und Sicherung
6. CA-Zertifikat auf den Geräten einrichten
7. Zertifikat ausstellen
8. Dateien und Formate
9. FRITZ!Box
10. CSR signieren
11. Register und Sperrliste
12. Zertifikat prüfen
13. Sicherheit und Technik
14. Fehlerbehebung

1. Überblick

CERT ist das Zertifikatswerkzeug der JUMBO BLOCK Engineering Suite. Es erstellt eine eigene Zertifizierungsstelle (CA) und stellt damit TLS-Zertifikate für Router, FRITZ!Box, NAS, Server, Kameras und Webanwendungen aus. Geräte, auf denen das CA-Zertifikat einmal als vertrauenswürdig eingerichtet ist, erkennen alle Zertifikate dieser CA ohne Warnung an.

Viele Router und Rechner arbeiten mit selbst erzeugten oder abgelaufenen Zertifikaten. Browser zeigen dann Warnungen, und die Echtheit der Gegenstelle lässt sich nicht mehr sicher feststellen. Mit CERT entstehen gültige Zertifikate in wenigen Minuten – auch im Krisenfall, ohne Internet und ohne externe Dienste.

- **Vollständig offline:** CERT läuft im Browser, auch direkt vom USB-Stick (`file://`). Es gibt keine Server-Verbindung, kein Konto und keine Cloud.
- **Ohne Fremdcode:** Zertifikate, Anforderungen, Sperrlisten und PKCS#12 sind eigener Programmcode. Schlüssel, Signaturen und Verschlüsselung nutzen die eingebaute Web Crypto API des Browsers.
- **Eine Datei pro CA:** Zertifikat, verschlüsselter Schlüssel, Ausstellungsregister und Sperrlisten-Stand liegen in einer CA-Datei (`.dbm`).
- **Prüfen inklusive:** Vorhandene Zertifikate lassen sich auf Laufzeit, Algorithmen und die Anforderungen aktueller Browser untersuchen.



Abb. 1: Die sechs Bereiche von CERT

Bereich	Aufgabe
Zertifizierungsstelle	CA anlegen, CA-Datei öffnen, speichern, entsperren und sichern, CA-Zertifikat für die Geräte herunterladen
Zertifikat ausstellen	Schlüsselpaar und Zertifikat für ein Gerät erzeugen und in allen benötigten Formaten herunterladen
CSR signieren	Zertifikatsanforderungen von Geräten mit eigener Schlüsselerzeugung signieren
Register & Sperrliste	Übersicht aller ausgestellten Zertifikate, Sperren und Erstellen der Sperrliste (CRL)
Zertifikat prüfen	Zertifikate, Ketten, Anforderungen, Sperrlisten und Schlüssel untersuchen
Einrichten	Anleitungen zum Import des CA-Zertifikats auf allen gängigen Systemen

2. Grundbegriffe

Begriff	Bedeutung
Zertifizierungsstelle (CA)	Stelle, die Zertifikate ausstellt und mit ihrem privaten Schlüssel signiert. Ihr eigenes Zertifikat (Stammzertifikat) wird auf den Geräten als vertrauenswürdig eingerichtet.
Zertifikat	Elektronischer Ausweis eines Geräts: Name, Adressen, öffentlicher Schlüssel, Laufzeit und die Signatur der CA. Ein Zertifikat ist öffentlich und darf weitergegeben werden.
Privater Schlüssel	Geheimer Gegenpart zum Zertifikat. Nur das Gerät darf ihn kennen. Wer ihn besitzt, kann sich als dieses Gerät ausgeben.
SAN (Subject Alternative Name)	Liste der Hostnamen und IP-Adressen, für die das Zertifikat gilt. Browser prüfen ausschließlich diese Liste.
Common Name (CN)	Anzeigename im Zertifikat. Für die Adressprüfung wird er von Browsern nicht mehr verwendet.
CSR	Zertifikatsanforderung (Certificate Signing Request). Ein Gerät erzeugt seinen Schlüssel selbst und schickt nur den öffentlichen Teil mit Namen zur Signatur.
Sperrliste (CRL)	Von der CA signierte Liste vorzeitig gesperrter Zertifikate.
PEM / DER	Dateiformate für Zertifikate und Schlüssel: PEM ist Text mit `-----BEGIN …-----`, DER ist die gleiche Information in binärer Form.
PKCS#12 (.p12 / .pfx)	Passwortgeschützter Container mit privatem Schlüssel, Zertifikat und Zertifikatskette – üblich bei Windows, IIS, NAS und vielen Routern.

Das Zwei-Stufen-Prinzip

CERT arbeitet mit einer eigenen Stammzertifizierungsstelle. Deren Zertifikat wird **einmal** auf jedem Rechner, Telefon und Browser eingerichtet. Danach werden alle Gerätezertifikate dieser CA automatisch anerkannt. Neue oder ersetzte Gerätezertifikate erfordern keine Änderung an den Endgeräten.

> Einzelne selbstsignierte Zertifikate pro Gerät müssten auf jedem Endgerät einzeln eingerichtet und nach jedem Austausch erneut importiert werden. Die eigene CA vermeidet diesen Aufwand.

3. Arbeitsablauf

1. **Zertifizierungsstelle anlegen** – Name, Schlüssel, Laufzeit, optional Namensbeschränkung und Passwort festlegen (Kapitel 4).
2. **CA-Datei speichern und sichern** – auf mindestens zwei getrennten Datenträgern, Passwort getrennt davon (Kapitel 5).
3. **CA-Zertifikat herunterladen** und auf allen Endgeräten als vertrauenswürdige Stammzertifizierungsstelle einrichten (Kapitel 6).
4. **Gerätezertifikate ausstellen** – für Geräte, die Zertifikat und Schlüssel importieren können (Kapitel 7 bis 9), oder **CSR signieren** für Geräte mit eigener Schlüsselerzeugung (Kapitel 10).
5. **Dateien auf den Geräten einspielen** und die Verbindung im Browser prüfen.
6. **CA-Datei speichern** – das Register enthält danach alle ausgestellten Zertifikate.
7. **Laufzeiten im Register überwachen**, Zertifikate rechtzeitig erneuern und bei Bedarf sperren (Kapitel 11).

Private Schlüssel ausgestellter Gerätezertifikate werden nicht gespeichert. Die benötigten Dateien müssen direkt nach dem Ausstellen heruntergeladen werden.

4. Zertifizierungsstelle anlegen

Im Bereich *Zertifizierungsstelle* wird eine neue CA angelegt. Pflichtangaben sind der Name der CA und das Passwort.

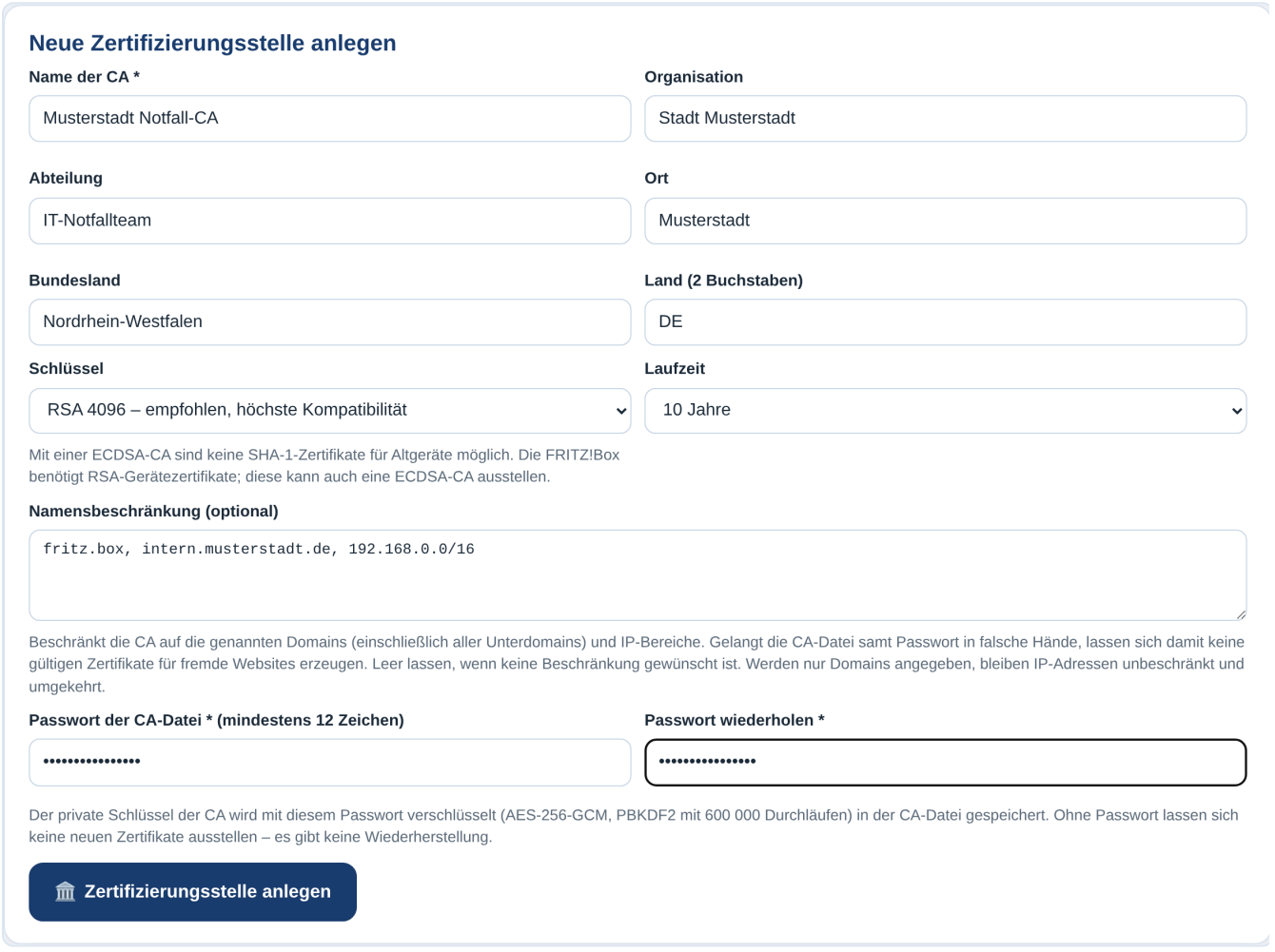


Abb. 2: Neue Zertifizierungsstelle anlegen

Feld	Bedeutung
Name der CA *	Erscheint auf allen Geräten als Name der Stammzertifizierungsstelle, z. B. „Musterstadt Notfall-CA“.
Organisation, Abteilung, Ort, Bundesland	Optionale Angaben zur Herkunft der CA.
Land	Ländercode mit zwei Buchstaben, Voreinstellung DE.
Schlüssel	RSA 4096 (empfohlen, höchste Kompatibilität), RSA 3072, RSA 2048, ECDSA P-384 oder ECDSA P-256.
Laufzeit	5, 10, 15 oder 20 Jahre, Voreinstellung 10 Jahre. Gerätezertifikate enden spätestens mit der CA.
Namensbeschränkung	Optional: Domains und IP-Bereiche, für die die CA ausschließlich Zertifikate ausstellen darf.
Passwort *	Mindestens 12 Zeichen. Verschlüsselt den privaten Schlüssel der CA in der CA-Datei.

Schlüsselwahl

RSA 4096 wird von praktisch allen Systemen verstanden, auch von älteren Geräten. ECDSA-Schlüssel sind kürzer und schneller, werden aber von sehr alten Geräten nicht unterstützt. Mit einer ECDSA-CA sind keine SHA-1-Zertifikate für Altgeräte möglich. RSA-Gerätezertifikate für die FRITZ!Box kann auch eine ECDSA-CA ausstellen.

Namensbeschränkung

Die Namensbeschränkung begrenzt die CA auf die eingetragenen Domains (einschließlich aller Unterdomains) und IP-Bereiche, z. B. `fritz.box, intern.musterstadt.de, 192.168.0.0/16`. Gelangen CA-Datei und Passwort in falsche Hände, lassen sich damit keine Zertifikate erzeugen, die für fremde Websites gültig sind.

- Domains gelten mit allen Unterdomains: `intern.musterstadt.de` umfasst auch `nas.intern.musterstadt.de`.
- IP-Bereiche werden in CIDR-Schreibweise angegeben (`192.168.0.0/16`, `fd00::/8`). Eine einzelne Adresse ohne Bereich gilt nur für sich selbst.
- Werden nur Domains angegeben, bleiben IP-Adressen unbeschränkt – und umgekehrt.

> Die Namensbeschränkung ist fester Bestandteil des CA-Zertifikats und kann später nicht geändert werden. Zertifikate für Namen außerhalb der Beschränkung werden von Browsern abgelehnt.

Nach *Zertifizierungsstelle anlegen* erzeugt CERT das Schlüsselpaar (bei RSA 4096 einige Sekunden) und verschlüsselt den Schlüssel. Anschließend sollte die CA-Datei sofort gespeichert werden.

5. CA-Datei, Entsperren und Sicherung

Nach dem Anlegen oder Öffnen zeigt der Bereich *Zertifizierungsstelle* die Daten der CA.



Abb. 3: Geöffnete Zertifizierungsstelle

Schaltfläche	Funktion
CA-Zertifikat (.crt, PEM)	Öffentliches CA-Zertifikat für macOS, Linux, Firefox, Android und iOS.
CA-Zertifikat (.cer, DER – Windows)	Dasselbe Zertifikat im Binärformat, per Doppelklick unter Windows installierbar.
CA-Datei speichern	Speichert Zertifikat, verschlüsselten Schlüssel, Register und Einstellungen als `.dbm`.
Entsperren / Sperren	Entschlüsselt den CA-Schlüssel mit dem Passwort bzw. entfernt ihn wieder aus dem Arbeitsspeicher.
Passwort ändern	Verschlüsselt den CA-Schlüssel mit einem neuen Passwort. Danach die CA-Datei speichern.
Schließen	Schließt die CA. Bei ungespeicherten Änderungen fragt CERT nach.

Öffnen und Entsperren

Über *Vorhandene CA-Datei öffnen* oder durch Ziehen der `.dbm`-Datei in das Fenster wird eine CA geladen. CERT prüft dabei die SHA-256-Prüfsumme der Datei. Stimmt sie nicht, wurde die Datei außerhalb von CERT verändert; CERT öffnet sie trotzdem und weist darauf hin.

Anschließend fragt CERT nach dem Passwort. Nach dem Entschlüsseln wird zusätzlich geprüft, ob der Schlüssel zum CA-Zertifikat passt. Das Register lässt sich auch im gesperrten Zustand ansehen; zum Ausstellen, Signieren und Erstellen von Sperrlisten muss die CA entsperrt sein.

Speichern

Jede Ausstellung, Sperrung und Einstellungsänderung ändert das Register. Ungespeicherte Änderungen zeigt CERT oberhalb der CA-Daten an; beim Schließen des Browserfensters erscheint eine Warnung. Der Dateiname lautet standardmäßig `CA_<Name>.dbm`.

Aufbau der CA-Datei

Die CA-Datei folgt der gemeinsamen DBM-Hülle der Suite mit `_hashAlgorithm` und `_hash`. Die Programmversion geht in die Prüfsumme ein. Eigene Daten stehen unter den Schlüsseln `cert_ca`, `cert_register` und `cert_crl`; unbekannte Schlüssel anderer Programme bleiben beim Speichern unverändert erhalten.

Sicherung: Die CA-Datei auf mindestens zwei getrennten Datenträgern aufbewahren (z. B. USB-Stick im Notfallordner und verschlüsseltes Backup), das Passwort getrennt davon. Ohne Passwort lassen sich keine neuen Zertifikate ausstellen – eine Wiederherstellung ist nicht möglich.

6. CA-Zertifikat auf den Geräten einrichten

Das CA-Zertifikat wird einmal pro Endgerät als vertrauenswürdige Stammzertifizierungsstelle importiert. Es enthält nur den öffentlichen Schlüssel. Der private Schlüssel der CA und die CA-Datei werden nie auf Endgeräte übertragen. Die Anleitungen stehen auch im Bereich *Einrichten* des Programms.

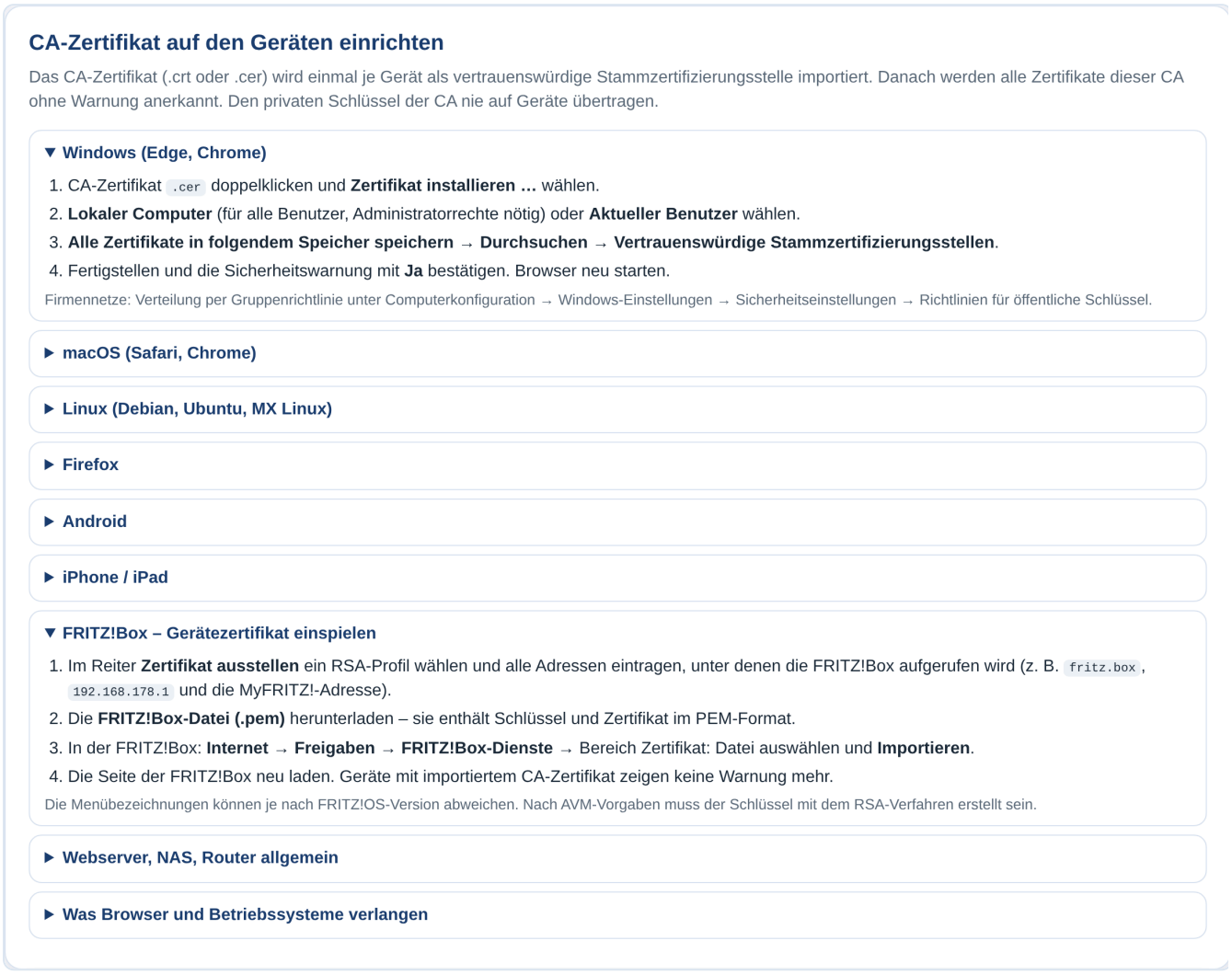


Abb. 4: Bereich Einrichten mit Anleitungen

Windows (Edge, Chrome)

1. CA-Zertifikat `.cer` doppelklicken und *Zertifikat installieren …* wählen.
2. *Lokaler Computer* (alle Benutzer, Administratorrechte nötig) oder *Aktueller Benutzer* wählen.
3. *Alle Zertifikate in folgendem Speicher speichern → Durchsuchen → Vertrauenswürdige Stammzertifizierungsstellen*.
4. Fertigstellen, die Sicherheitswarnung mit *Ja* bestätigen und den Browser neu starten.

In Firmennetzen lässt sich das Zertifikat per Gruppenrichtlinie verteilen: Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Richtlinien für öffentliche Schlüssel.

macOS (Safari, Chrome)

1. CA-Zertifikat `.crt` doppelklicken; in der Schlüsselbundverwaltung den Schlüsselbund *System* wählen.
2. Das Zertifikat doppelklicken und *Vertrauen* aufklappen.
3. *Bei Verwendung dieses Zertifikats* auf *Immer vertrauen* stellen und mit dem Passwort bestätigen.

Linux (Debian, Ubuntu, MX Linux)

```
sudo cp ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

Die Dateiendung `.crt` ist dabei Pflicht. Das gilt für Programme, die den Systemspeicher nutzen.

Chrome und Chromium verwenden unter Linux einen eigenen Zertifikatsspeicher (`~/.pki/nssdb`) und übernehmen die systemweiten Zertifikate nicht. Zuverlässig ist der Import per Terminal; danach Chrome neu starten:

```
sudo apt install libnss3-tools
certutil -d sql:$HOME/.pki/nssdb -A -t "C,," -n "Meine CA" -i ca.crt
```

Alternativ die Zertifikatsverwaltung über `chrome://certificate-manager` öffnen und das CA-Zertifikat bei den selbst installierten, vertrauenswürdigen Zertifikaten importieren – nicht unter den eigenen Zertifikaten, diese erwarten PKCS#12-Dateien.

Firefox

1. Einstellungen → *Datenschutz & Sicherheit* → *Zertifikate anzeigen …*
2. Reiter *Zertifizierungsstellen* → *Importieren …* → CA-Zertifikat wählen (nicht im Reiter *Ihre Zertifikate*).
3. *Dieser CA vertrauen, um Websites zu identifizieren* anhaken und bestätigen.

Firefox nutzt einen eigenen Zertifikatsspeicher. Unter Windows und macOS übernimmt Firefox die Systemzertifikate, wenn in `about:config` der Wert `security.enterprise_roots.enabled` auf `true` steht.

Android

1. CA-Zertifikat `.crt` auf das Telefon übertragen.
2. Einstellungen → Sicherheit (je nach Hersteller: Sicherheit und Datenschutz → Weitere Sicherheitseinstellungen) → *Verschlüsselung und Anmeldedaten* → *Zertifikat installieren* → *CA-Zertifikat*.
3. Warnhinweis bestätigen und die Datei wählen.

Chrome und Firefox erkennen vom Benutzer installierte CAs an. Manche Apps vertrauen ausschließlich den vorinstallierten Zertifizierungsstellen.

iPhone und iPad

1. CA-Zertifikat `.crt` per Safari, Mail oder AirDrop öffnen – es wird als Profil geladen.
2. Einstellungen → *Profil geladen* → *Installieren*.
3. Einstellungen → Allgemein → Info → *Zertifikatsvertrauenseinstellungen* → das Zertifikat bei *Vollständiges Vertrauen für Root-Zertifikate* einschalten.

7. Zertifikat ausstellen

Im Bereich *Zertifikat ausstellen* entstehen Schlüsselpaar und Zertifikat für ein Gerät direkt im Browser. Das eignet sich für alle Geräte, die ein eigenes Zertifikat samt Schlüssel importieren können: FRITZ!Box, NAS, Router, Firewalls, Webserver und Webanwendungen.

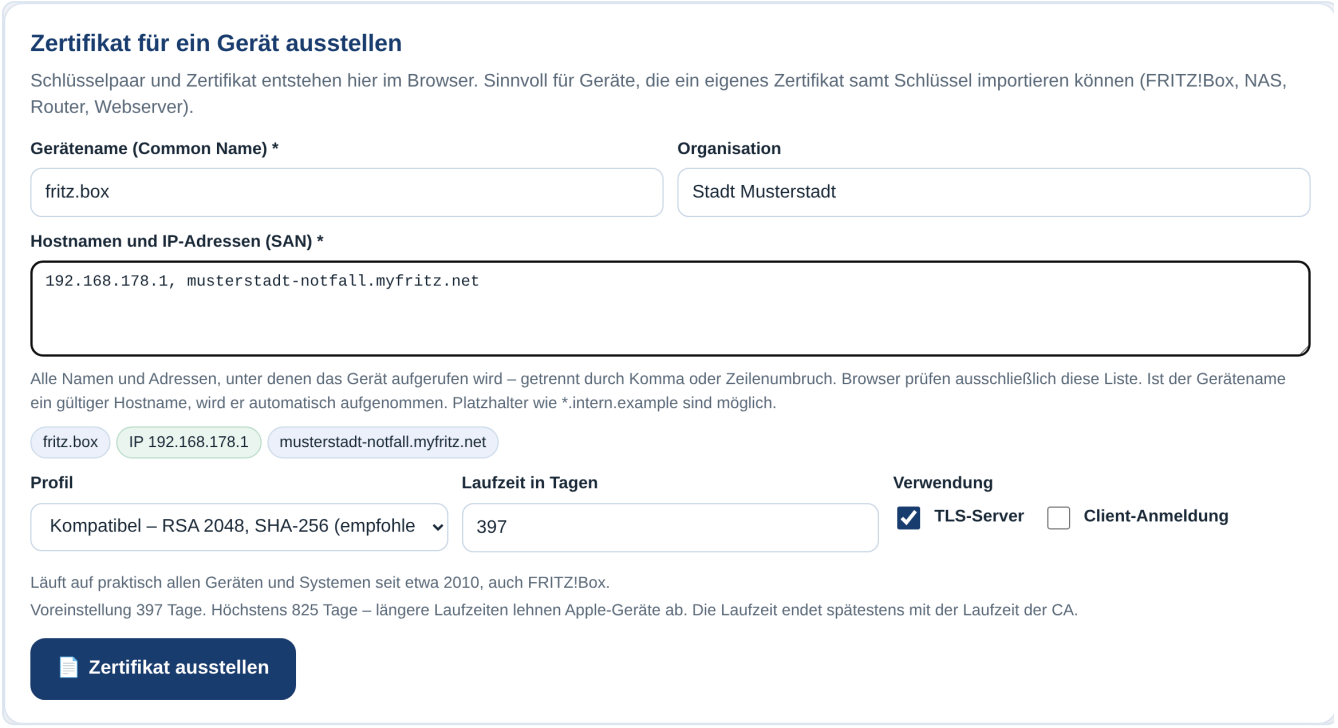


Abb. 5: Zertifikat für ein Gerät ausstellen

Feld	Bedeutung
Gerätename (Common Name) *	Anzeigename des Zertifikats, z. B. `fritz.box`. Ist er ein gültiger Hostname, wird er automatisch in die Adressliste übernommen.
Organisation	Optionale Angabe im Zertifikat.
Hostnamen und IP-Adressen (SAN) *	Alle Namen und Adressen, unter denen das Gerät aufgerufen wird, getrennt durch Komma oder Zeilenumbruch.
Profil	Schlüsseltyp und Signaturverfahren (siehe Tabelle unten).
Laufzeit in Tagen	1 bis 825 Tage, Voreinstellung 397 Tage.
Verwendung	*TLS-Server* für Web- und Geräteoberflächen (Voreinstellung), *Client-Anmeldung* für Zertifikate, mit denen sich ein Gerät oder Benutzer anmeldet (z. B. VPN).

Adressen (SAN)

Unter dem Eingabefeld zeigt CERT jede erkannte Adresse als Feld an: Hostnamen blau, IP-Adressen grün, ungültige Einträge rot. Möglich sind:

- Hostnamen wie `fritz.box` oder `nas.intern.musterstadt.de`, auch mit Umlauten (werden automatisch in die internationale Schreibweise umgewandelt),
- Platzhalter für genau eine Ebene, z. B. `*.intern.musterstadt.de`,
- IPv4-Adressen wie `192.168.178.1` und IPv6-Adressen wie `fd00::1`.

Das Zertifikat gilt nur für die eingetragenen Adressen. Wird ein Gerät auch per IP-Adresse oder über einen weiteren Namen (z. B. die MyFRITZ!-Adresse) aufgerufen, müssen diese ebenfalls eingetragen sein.

Profile

Profil	Schlüssel / Signatur	Einsatz
Kompatibel (Voreinstellung)	RSA 2048 / SHA-256	Praktisch alle Geräte und Systeme seit etwa 2010, auch FRITZ!Box
Stark	RSA 3072 / SHA-256	Längerer Schlüssel, etwas langsamer beim Verbindungsaufbau, FRITZ!Box-tauglich
Modern	ECDSA P-256 / SHA-256	Aktuelle Systeme; nicht für FRITZ!Box und sehr alte Geräte
Altgeräte	RSA 2048 / SHA-1	Nur für Geräte, die kein SHA-256 beherrschen; nur mit RSA-CA verfügbar

Zertifikate mit SHA-1 werden von aktuellen Browsern und Apple-Systemen abgelehnt. Das Profil *Altgeräte* ist ausschließlich für alte Geräte gedacht, die kein anderes Verfahren verstehen.

Laufzeit

Die Voreinstellung von 397 Tagen entspricht der Höchstlaufzeit öffentlicher Zertifikate. Mehr als 825 Tage sind nicht möglich, da Apple-Geräte längere Serverzertifikate ablehnen. Reicht die Laufzeit über das Ablaufdatum der CA hinaus, kürzt CERT sie auf dieses Datum und weist darauf hin. Der Gültigkeitsbeginn liegt eine Stunde vor dem Ausstellungszeitpunkt, damit kleine Uhrabweichungen der Geräte nicht stören.

Nach *Zertifikat ausstellen* wird das Zertifikat ins Register eingetragen und das Ergebnis mit allen Download-Möglichkeiten angezeigt (Kapitel 8).

8. Dateien und Formate

Nach dem Ausstellen zeigt CERT die Daten des Zertifikats und alle Download-Möglichkeiten.

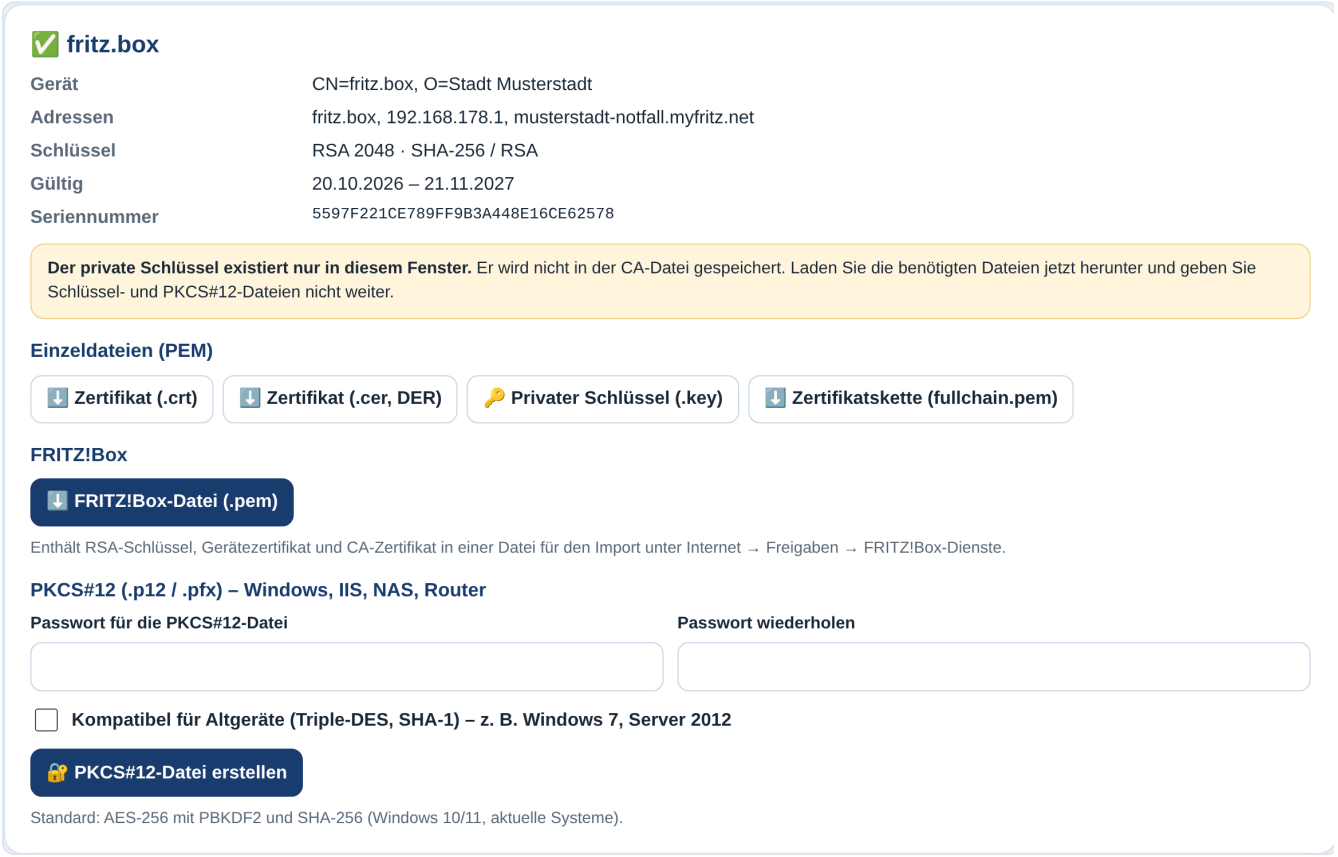


Abb. 6: Ergebnis mit allen Download-Möglichkeiten

Datei	Inhalt	Verwendung
Zertifikat (.crt)	Gerätezertifikat, PEM	Server und Geräte, die Zertifikat und Schlüssel getrennt erwarten
Zertifikat (.cer, DER)	Gerätezertifikat, binär	Windows und Geräte mit DER-Import
Privater Schlüssel (.key)	Schlüssel, PEM (PKCS#8), unverschlüsselt	nginx, Apache, Geräte mit getrenntem Schlüssel-Import
Zertifikatskette (fullchain.pem)	Gerätezertifikat und CA-Zertifikat	Webserver, damit Clients die Kette vollständig erhalten
FRITZ!Box-Datei (.pem)	RSA-Schlüssel, Gerätezertifikat und CA-Zertifikat in einer Datei	Import in die FRITZ!Box (nur bei RSA-Profilen)
PKCS#12 (.p12)	Schlüssel, Zertifikat und CA-Zertifikat, passwortgeschützt	Windows, IIS, viele NAS und Router

PKCS#12

Für die PKCS#12-Datei wird ein eigenes Passwort mit mindestens 8 Zeichen vergeben. Es wird beim Import auf dem Zielgerät abgefragt.

- **Standard:** AES-256 mit PBKDF2 und SHA-256 – für Windows 10/11 und aktuelle Systeme.
- **Kompatibel für Altgeräte:** Triple-DES mit SHA-1 – für Windows 7, Windows Server 2012 und ältere Geräte, die das moderne Verfahren nicht lesen können.

Der private Schlüssel existiert nur in diesem Fenster. Er wird nicht in der CA-Datei gespeichert. Schlüssel-, FRITZ!Box- und PKCS#12-Dateien geheim halten, nicht per E-Mail verschicken und nach dem Einspielen vom Arbeitsrechner löschen. Geht der Schlüssel verloren, wird einfach ein neues Zertifikat ausgestellt.

Einbindung in Webserver

System	Zertifikat	Schlüssel
nginx	`ssl_certificate` → fullchain.pem	`ssl_certificate_key` → .key
Apache	`SSLCertificateFile` → fullchain.pem	`SSLCertificateKeyFile` → .key
Windows / IIS	PKCS#12-Datei importieren	in der PKCS#12-Datei enthalten

9. FRITZ!Box

Die FRITZ!Box erzeugt ab Werk ein eigenes, selbstsigniertes Zertifikat. Mit einem Zertifikat der eigenen CA entfallen die Browser-Warnungen auf allen Geräten, auf denen das CA-Zertifikat eingerichtet ist.

1. Im Bereich *Zertifikat ausstellen* als Gerätename `fritz.box` eintragen.
2. Unter *Hostnamen und IP-Adressen* alle Adressen der FRITZ!Box eintragen, z. B. `192.168.178.1` und die MyFRITZ!-Adresse.
3. Ein RSA-Profil wählen (*Kompatibel* oder *Stark*) und das Zertifikat ausstellen.
4. **FRITZ!Box-Datei (.pem)** herunterladen.
5. In der FRITZ!Box: *Internet* → *Freigaben* → *FRITZ!Box-Dienste* → Bereich Zertifikat: Datei auswählen und *Importieren*.
6. Die Seite der FRITZ!Box neu laden.

> Nach den Vorgaben von AVM müssen Zertifikat und privater Schlüssel im PEM-Format vorliegen und der Schlüssel mit dem RSA-Verfahren erstellt sein. Die FRITZ!Box-Datei von CERT erfüllt beides. Die Menübezeichnungen können je nach FRITZ!OS-Version abweichen.

Bei ECDSA-Profilen bietet CERT keine FRITZ!Box-Datei an, da die FRITZ!Box solche Schlüssel nicht annimmt.

10. CSR signieren

Viele Geräte – Server, NAS, Kameras, Firewalls – erzeugen ihren Schlüssel selbst und liefern nur eine Zertifikatsanforderung (CSR, Datei meist `.csr` oder `.req`). CERT signiert sie mit der eigenen CA. Der private Schlüssel verlässt das Gerät dabei nie.

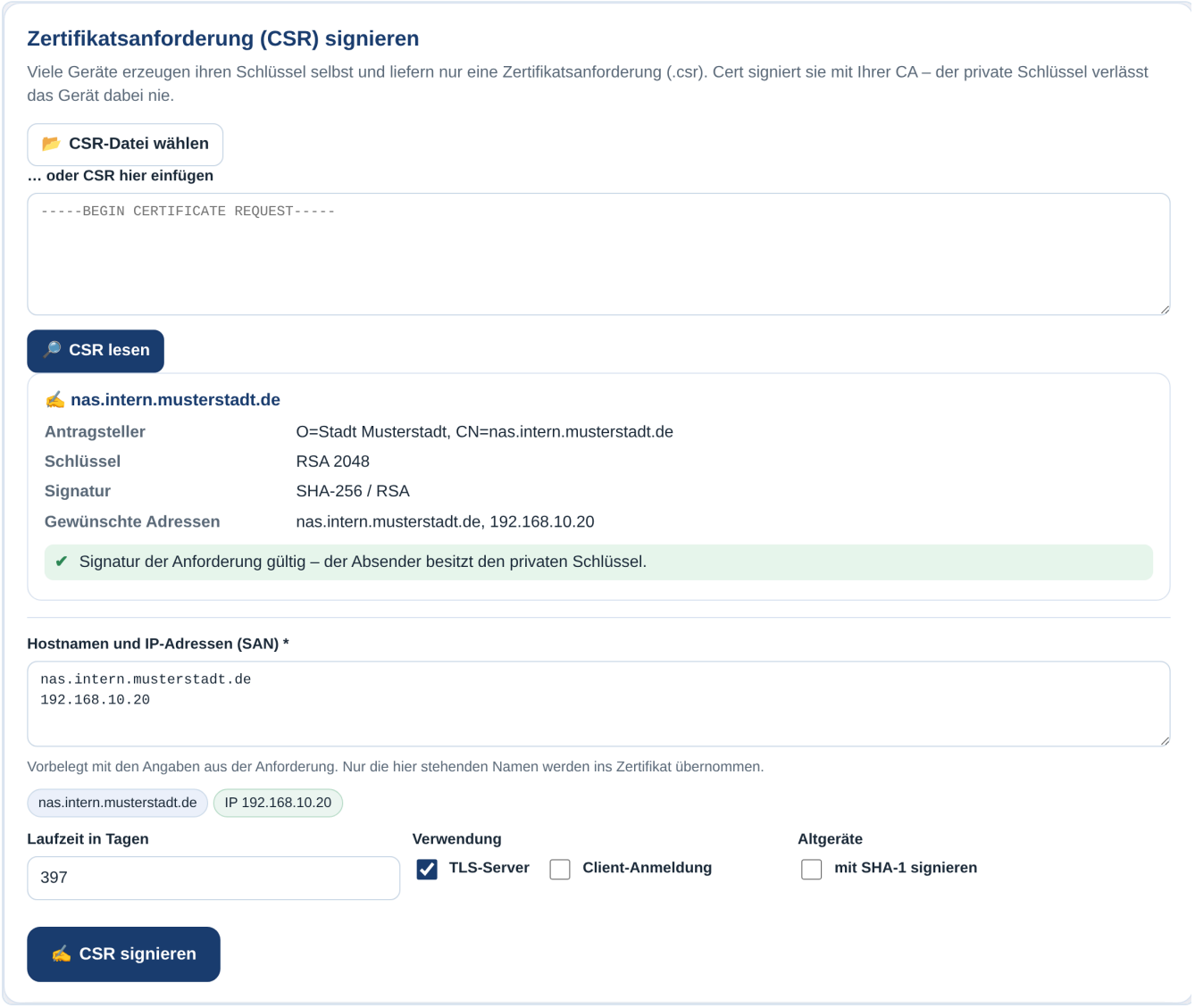


Abb. 7: Gelesene Zertifikatsanforderung mit Optionen

1. CSR auf dem Gerät erzeugen und exportieren.
2. In CERT über *CSR-Datei wählen*, durch Einfügen des PEM-Texts oder durch Ziehen der Datei in das Fenster laden und *CSR lesen*.
3. CERT zeigt Antragsteller, Schlüssel, Signaturverfahren und die gewünschten Adressen und prüft die Signatur der Anforderung.
4. Adressen kontrollieren und bei Bedarf ergänzen, Laufzeit und Verwendung festlegen.
5. *CSR signieren* und das Zertifikat bzw. die Zertifikatskette herunterladen.
6. Das Zertifikat auf dem Gerät einspielen, das die Anforderung erzeugt hat.

Prüfung	Bedeutung
Signatur der Anforderung gültig	Der Absender besitzt den zugehörigen privaten Schlüssel. Nur dann lässt sich die CSR signieren.
Signatur ungültig	Die Anforderung wurde verändert oder ist beschädigt und wird nicht signiert.
RSA unter 2048 Bit	CERT fragt vor dem Signieren nach, da Browser und Apple-Systeme solche Schlüssel ablehnen.
Verfahren nicht unterstützt	Unterstützt werden RSA und ECDSA (P-256, P-384, P-521) mit SHA-1 oder SHA-2.

Ins Zertifikat übernimmt CERT den Antragsteller aus der Anforderung und ausschließlich die im Feld *Hostnamen und IP-Adressen* stehenden Adressen. Ist die CA eine RSA-CA, kann für Altgeräte zusätzlich *mit SHA-1 signieren* gewählt werden.

11. Register und Sperrliste

Ausstellungsregister

Das Register enthält alle mit der CA ausgestellten Zertifikate – auch signierte CSRs – mit Gerätename, Seriennummer, Schlüssel, Adressen, Laufzeit und Status. Es wird in der CA-Datei gespeichert.



Abb. 8: Ausstellungsregister

Status	Bedeutung
gültig	Zertifikat läuft noch mindestens 30 Tage
läuft bald ab	Weniger als 30 Tage Restlaufzeit – rechtzeitig neu ausstellen
abgelaufen	Laufzeit überschritten
gesperrt	Vorzeitig gesperrt, mit Datum

Das Suchfeld filtert nach Name, Adresse oder Seriennummer. Über *.crt* lässt sich jedes Zertifikat erneut herunterladen; private Schlüssel sind im Register nicht enthalten.

Zertifikat sperren

Über *Sperren* wird ein Zertifikat vorzeitig für ungültig erklärt, z. B. wenn ein Gerät verloren ging, ausgemustert oder ein Schlüssel bekannt geworden ist. Als Grund stehen *Ohne Angabe*, *Schlüssel kompromittiert*, *Zugehörigkeit geändert*, *Ersetzt* und *Betrieb eingestellt* zur Wahl. Die Sperrung ist endgültig. Sperren ist auch im gesperrten Zustand der CA möglich; für die Sperrliste muss die CA entsperrt sein.

Sperrliste (CRL)



Abb. 9: Sperrliste erstellen

Sperrliste erstellen (.crl) erzeugt eine von der CA signierte Liste aller gesperrten Zertifikate mit fortlaufender Nummer und lädt sie im DER-Format herunter; eine PEM-Fassung steht zusätzlich bereit. Die Gültigkeit der Sperrliste beträgt 7, 30, 90, 180 oder 365 Tage. Vor Ablauf muss eine neue Sperrliste erstellt werden.

Die Sperrliste wird in Server, VPN-Gateways oder Firewalls eingespielt, die eine CRL prüfen, oder unter einer festen Adresse bereitgestellt.

Abrufadresse der Sperrliste

Optional kann eine HTTP-Adresse eingetragen werden, unter der die Sperrliste dauerhaft abrufbar ist, z. B. `http://192.168.178.10/ca.crl`. Sie wird in alle danach ausgestellten Zertifikate geschrieben.

> Die Abrufadresse nur eintragen, wenn die Datei dort dauerhaft erreichbar ist. Eine unerreichbare Adresse kann manche Windows-Anwendungen verzögern oder blockieren – gerade im Krisenfall. Ohne Eintrag bleibt das Feld in den Zertifikaten leer.

12. Zertifikat prüfen

Der Bereich *Zertifikat prüfen* untersucht vorhandene Dateien: Zertifikate, Zertifikatsketten, Zertifikatsanforderungen, Sperrlisten, private Schlüssel und PKCS#12-Container, im PEM- oder DER-Format. Dateien werden gewählt, in das Fenster gezogen oder als PEM-Text eingefügt. Eine Datei mit mehreren Zertifikaten wird vollständig ausgewertet.



Abb. 10: Eingabe der zu prüfenden Daten

Für jedes Zertifikat zeigt CERT Antragsteller, Aussteller, Laufzeit, Seriennummer, Schlüssel, Signaturverfahren, Adressen, Verwendungen sowie die Fingerabdrücke SHA-256 und SHA-1. Darunter folgt die Bewertung.



Abb. 11: Bewertung eines Gerätezertifikats

Kennzeichen	Bedeutung
✔ grün	In Ordnung
! gelb	Hinweis, der Probleme verursachen kann (z. B. Ablauf in weniger als 30 Tagen, fehlende Verwendung serverAuth, selbstsigniert)
✖ rot	Wird von Browsern oder Betriebssystemen abgelehnt (z. B. abgelaufen, SHA-1 oder MD5, RSA unter 2048 Bit, keine Adressen im SAN, mehr als 825 Tage Laufzeit)
i blau	Information (z. B. CA mit Pfadlänge, Namensbeschränkung)

Weitere Prüfungen

- **Gegen Adresse prüfen:** Mit einer eingetragenen Adresse (z. B. `fritz.box` oder `192.168.178.1`) prüft CERT, ob das Zertifikat dafür gilt – einschließlich Platzhaltern.
- **Ketten:** Liegt das ausstellende Zertifikat in derselben Prüfung vor, wird die Signatur dagegen geprüft. Stammzertifikate werden auf ihre Selbstsignatur geprüft.
- **Geöffnete CA:** Ist eine CA geöffnet, prüft CERT, ob sie das Zertifikat ausgestellt hat und ob es im Register gesperrt ist. Sperrlisten werden gegen die geöffnete CA geprüft.
- **Noch nicht gültig:** Liegt der Gültigkeitsbeginn in der Zukunft, sind meist Datum und Uhrzeit des Geräts falsch eingestellt.

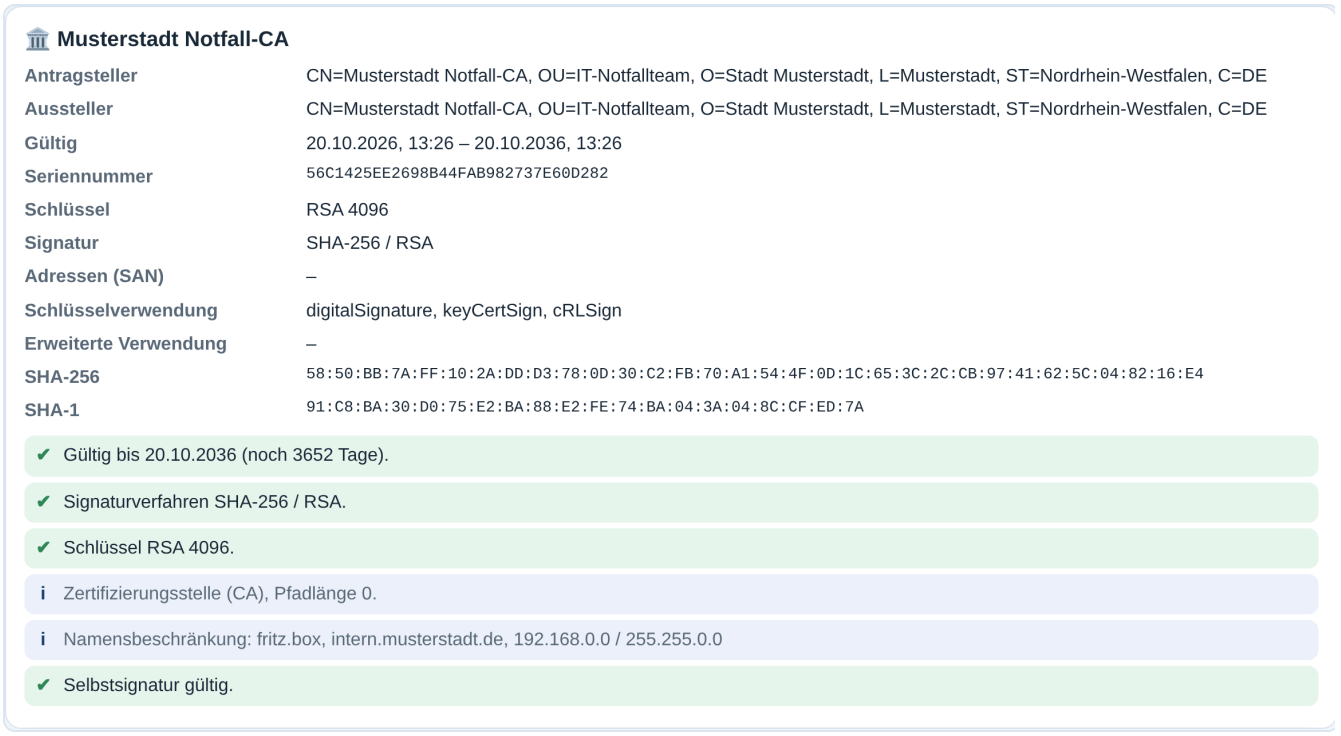


Abb. 12: Bewertung eines CA-Zertifikats mit Namensbeschränkung

13. Sicherheit und Technik

Bereich	Umsetzung
Verarbeitung	Vollständig lokal im Browser, keine Netzwerkverbindung (Content Security Policy mit `connect-src 'none'`)
Schlüsselerzeugung und Signatur	Web Crypto API des Browsers: RSA (PKCS#1 v1.5) und ECDSA
Schutz des CA-Schlüssels	AES-256-GCM, Schlüsselableitung PBKDF2-SHA-256 mit 600 000 Durchläufen, zufälliges Salz und IV
Integrität der CA-Datei	SHA-256-Prüfsumme über den gesamten Inhalt einschließlich Programmversion
Seriennummern	128 Bit, zufällig
CA-Zertifikat	X.509 v3, BasicConstraints CA mit Pfadlänge 0, KeyUsage keyCertSign und cRLSign, Schlüsselkennungen, optional NameConstraints
Gerätezertifikat	X.509 v3, SAN, KeyUsage, ExtendedKeyUsage serverAuth/clientAuth, Schlüsselkennungen, optional Abrufadresse der Sperrliste
PKCS#12	Standard: PBES2 mit AES-256-CBC und PBKDF2/HMAC-SHA-256, MAC SHA-256 · Altgeräte: Triple-DES und MAC SHA-1
Sperrliste	X.509 CRL v2 mit CRL-Nummer, Schlüsselkennung und Sperrgrund
Programmcode	ASN.1/DER, X.509, PKCS#8, PKCS#10, PKCS#12 und Triple-DES als eigener Code der ZANNI GROUP, keine Fremdbibliotheken

Grenzen

- CERT ersetzt keine öffentliche Zertifizierungsstelle: Zertifikate der eigenen CA werden nur auf Geräten anerkannt, auf denen das CA-Zertifikat eingerichtet ist.
- Die Sicherheit hängt vom Schutz der CA-Datei und des Passworts ab. Der Rechner, auf dem CERT entsperrt wird, sollte vertrauenswürdig sein.
- OCSP-Abfragen und Zwischenzertifizierungsstellen sind nicht Bestandteil von CERT. Für den Einsatz im eigenen Netz und im Krisenfall genügt die direkte Ausstellung durch die Stamm-CA.
- Bei Aufruf über das Netzwerk stellt der Browser die Web Crypto API nur über HTTPS bereit. Vom USB-Stick (`file://`) und über jumboblock.org funktioniert CERT ohne Einschränkung.

14. Fehlerbehebung

Problem	Ursache und Lösung
Browser warnt trotz Zertifikat	Das CA-Zertifikat ist auf diesem Gerät nicht als vertrauenswürdige Stammzertifizierungsstelle eingerichtet (Kapitel 6), oder der Browser wurde nach dem Import nicht neu gestartet. Firefox nutzt einen eigenen Speicher.
Browser meldet beim Import des CA-Zertifikats „Datei beschädigt“	Das CA-Zertifikat wurde im Bereich *Ihre Zertifikate* importiert. Dieser erwartet PKCS#12-Dateien mit privatem Schlüssel. Das CA-Zertifikat gehört zu den Zertifizierungsstellen bzw. vertrauenswürdigen Zertifikaten; Chrome unter Linux siehe Kapitel 6.
Warnung „Name stimmt nicht überein“	Die aufgerufene Adresse fehlt im SAN. Zertifikat mit allen Namen und IP-Adressen neu ausstellen und im Bereich *Zertifikat prüfen* mit *Gegen Adresse prüfen* kontrollieren.
Zertifikat „noch nicht gültig“ oder „abgelaufen“	Datum und Uhrzeit des Geräts prüfen. Geräte ohne Uhrbatterie starten nach Stromausfall mit falschem Datum.
iPhone/iPad oder Mac lehnt ab	CA-Zertifikat unter *Zertifikatsvertrauenseinstellungen* vollständig vertrauen. Laufzeit höchstens 825 Tage, Verwendung TLS-Server, kein SHA-1 – mit Profil *Kompatibel*, *Stark* oder *Modern* erfüllt.
FRITZ!Box nimmt die Datei nicht an	RSA-Profil verwenden und die *FRITZ!Box-Datei (.pem)* importieren, nicht das einzelne Zertifikat.
Windows importiert die PKCS#12-Datei nicht	Bei Windows 7, Server 2012 oder älter die Option *Kompatibel für Altgeräte* wählen.
„Das Passwort ist falsch“ beim Entsperren	Groß-/Kleinschreibung und Tastaturbelegung prüfen. Ohne das richtige Passwort ist der CA-Schlüssel nicht wiederherstellbar.
„Prüfsumme stimmt nicht“ beim Öffnen	Die CA-Datei wurde außerhalb von CERT verändert. Register und Einstellungen kontrollieren und auf eine Sicherung zurückgreifen, wenn Einträge fehlen.
Zertifikat wird trotz Namensbeschränkung abgelehnt	Name oder IP-Adresse liegt außerhalb der Beschränkung der CA. Die Beschränkung ist im Bereich *Zertifizierungsstelle* angezeigt.
Privater Schlüssel verloren	Ein neues Zertifikat ausstellen und das alte im Register sperren.
Web Crypto API nicht verfügbar	Aktuellen Browser verwenden; bei Aufruf über das Netzwerk HTTPS nutzen.