Antrag zum Sperren eines Zertifikats der SEN.CA

Mit der beantragten Sperrung des Zertifikats durch den Antragsteller wird das Zertifikat aus dem LDAP gelöscht und in die Sperrliste eingetragen.

Name des Antragstellers:	
S/MIME E-Mail Adresse des Antragstellers:	
Zertifikatstyp:	
Ausgestellt für[1]:	
Zertifikatsnummern[2]:	
ENC	
SIGN	
TLS	
Ausstellende Sub-CA[3]:	
Sperrgrund[4]:	

1 Zu finden in den allgemeinen Zertifikatsinformationen „ausgestellt für“
2 Zu finden in den Zertifikatsdetails unter „Seriennummer“
3 Zu finden in den allgemeinen Zertifikatsinformationen „ausgestellt von“
4 Für Sub-CA, GWA, GWH und EMT zwingend, für SMGw optional. Sperrgründe: Unspezifiziert, Schlüssel kompromittiert, CA kompromittiert, Zugehörigkeit geändert, Zertifikat wurde ersetzt, Betrieb eingestellt, Zertifikat zurückgehalten, aus der CRL gelöscht, Rechte entzogen, Root Zertifikat kompromittiert

Wenn der Sperrgrund „Schlüssel kompromittiert“ lautet, müssen die folgenden Fragen beantwortet werden:

Was wurde kompromittiert bzw. was wurde betroffen?

Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt?

Wer hat das Vorkommnis festgestellt?

Ort des Vorkommnisses

Wie ist das Vorkommnis vermutlich abgelaufen?

Wenn bereits eine Maßnahme durchgeführt wurde: Welche Maßnahmen wurden eingeleitet

Ort, Datum, Vorname, Name, Unterschrift des Antragstellers

Hinweis zur Übermittlung:

Bitte senden Sie uns Ihren Sperrantrag per signierter E-Mail an trustcenter@sen-pki.de .

Wir setzen uns mit Ihnen in Verbindung.