Gemeinsam
IT gestalten.

IT.Niedersachsen

Anleitung
zur Beantragung von Zertifikaten aus der DOI-CA/Niedersachsen für das EGVP-Backend, beBPo, Digitalpakt und weitere Fachverfahren

INHALT **SEITE**

Wichtige Hinweise:
Die Zertifikate sind so ausgelegt, dass diese auch für das Verfahren „beBPo“, "Online-Erhebung für den (kommunalen) Finanzausgleich (OLEFA)", „Digitalpakt“ und ggf. weitere Verfahren verwendet werden können. Dadurch soll die Anzahl der für die Fachverfahren benötigten Zertifikate eingeschränkt und somit Kosten und Aufwände eingespart werden.

Die nachfolgende Anleitung führt Sie durch das Antragsverfahren und enthält Informationen für die weitere Vorgehensweise.

1. ZUGANG ZUM PORTAL DER DOI-CA/NIEDERSACHSEN

Schritt 1
Bitte aktivieren Sie Javascript und Cookies in Ihrem Browser oder fügen die folgende Webseite den vertrauenswürdigen Seiten hinzu (notwendig zum Download der Antragsformulare und Zertifikate):

https://doi.telesec.de

Rufen Sie dann zunächst bitte folgende Internetadresse im Browser auf (beachten Sie bitte Groß-/Kleinschreibung; dieser Link steht Ihnen auch auf den Webseiten des SignaturCard Service zur Verfügung (Kontaktdaten des SignaturCard Service siehe Kapitel 5):

https://doi.telesec.de/doi/ee/itn/login/displayLogin.html

Schritt 2
Das abgebildete Anmeldefenster wird geöffnet:

Geben Sie hier bitte die folgenden Zugangsdaten ein:

<Login:> **#######**
<Passwort:>**#######**

Bestätigen Sie mit <*Anmelden*>

(s. nebenstehende Abbildung).

Nach Eingabe der Kennungsdaten steht Ihnen die Startseite des Portals der DOI-CA/Niedersachsen zur Verfügung (s. nebenstehende Abbildung).

2. BEANTRAGUNG VON SOFTWARE-BASIERTEN GRUPPENZERTIFIKATEN

Schritt 1

Wählen Sie bitte zunächst den Menüpunkt

„*Software-Zertifikate*“

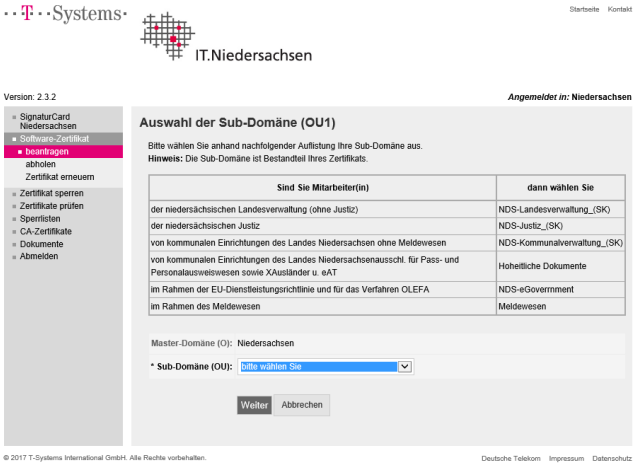
und dann den darin befindlichen Unterpunkt

„*beantragen*“

(s. nebenstehende Abbildung).

Schritt 2

Die menügeführte Eingabe Ihrer Antragsdaten wird zunächst mit der Aufforderung zur Auswahl der Sub-Domäne gestartet. Wählen Sie bitte die Sub-Domäne „NDS-eGovernment“ im Auswahlfeld aus und betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).



Schritt 3

Die Auswahl "Gruppen-/Funktions-Zertifikat" ist bereits aktiviert.

Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).

Hinweis:
Über die Schaltfläche "Zurück" gelangen Sie jederzeit zum vorhergehenden Eingabefenster um hier evtl. Änderungen Ihrer gewählten Eingabedaten vornehmen zu können (s. nebenstehende Abbildung).

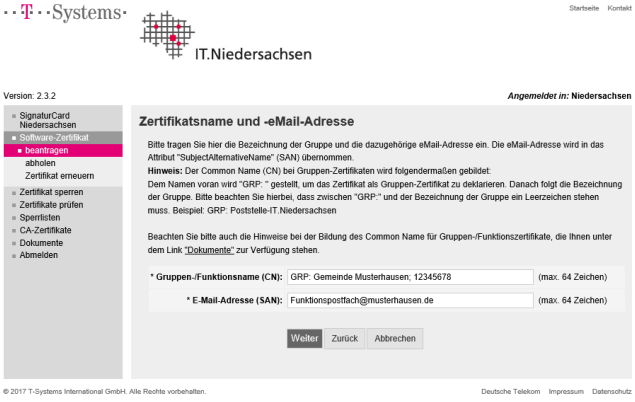
Schritt 4

Tragen Sie als Schlüsselverantwortlicher in die entsprechenden Formularfelder bitte Ihre dienstliche Anschrift und Ihre Kontaktdaten ein. Die Rolle des Schlüsselverantwortlichen sollte nach Möglichkeit die Person übernehmen, die auch bereits mit der Rolle des Postfachverantwortlichen betraut ist.

Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).

Schritt 5

Innerhalb des Feldes "Gruppen-/Funktionsname (CN)" tragen Sie bitte GRP: [Name/Bezeichnung der Kommune]; [8stelliger AGS] z. B.: "GRP: Stadt Musterhausen; 12345678". Behörden tragen hier nach dem Semikolon bitte die 5stellige Dienststellennummer (NLBV) ein.
Soll das Zertifikat für eine „FITKO“-Anwendung für die von der Föderalen IT-Kooperation (FITKO) im Auftrag des IT-Planungsrates betriebene FIT-Connect-Infrastruktur eingesetzt werden, tragen sie den GRP-Namen wie folgt ein: GRP: [Name/Bezeichnung der Kommune_FitKo]
➔ "GRP:" muss dem Gruppennamen vorangestellt sein und darf deshalb nicht gelöscht werden
Sofern in begründeten Ausnahmefällen mehr als ein EGVP/ beBPo eingerichtet werden muss, muss aus dem Namen des Zertifikats durch Zusatz z. B. der Abteilung eindeutig eine Unterscheidung möglich sein (z. B. Stadt Musterhausen – Vollstreckung) .
Der Name/Bezeichnung der Kommune/Behörde sollte mit dem Eintrag im Feld Name der EGVP-/ beBPo-Visitenkarte übereinstimmen. Das Feld "E-Mail-Adresse (SAN)" befüllen Sie bitte mit der E-Mail-Adresse des Funktions-Postfachs für diese Gruppe.



Ist bereits ein geeignetes Zertifikat vorhanden, aber für eine Fachanwendung (z. B. für „Digitalpakt“) soll ein extra Zertifikat beantragt werden, muss dieses ebenfalls durch einen Zusatz (sie-

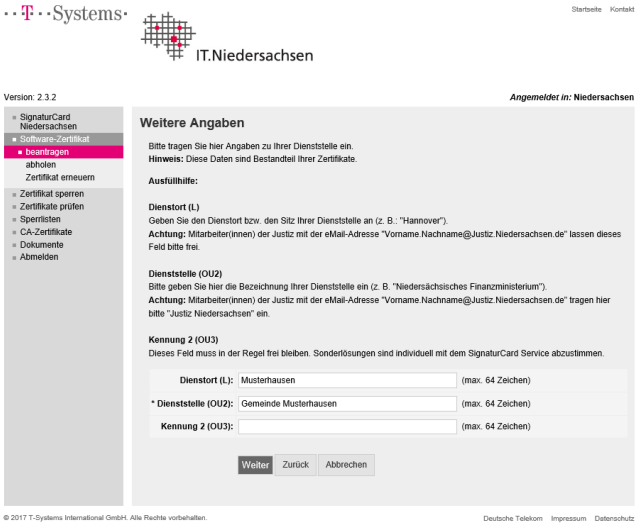
he oben) gekennzeichnet werden.
Beachten Sie bitte auch die aufgeführten Hinweise über den Eingabefeldern.

Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).

Schritt 6

Geben Sie im Feld "Dienstort (L)" bitte den Dienstort Ihrer Behörde/Organisation ein. Die Bezeichnung sollte mit dem Feld „Ort“ der EGVP-/ beBPo-Visitenkarte übereinstimmen. Im Feld "Dienststelle (OU2)" tragen Sie bitte die Bezeichnung Ihrer Dienststelle ein (z. B. Gemeinde Wennigsen). Die Bezeichnung sollte mit dem Eintrag im Feld „Name“ der EGVP-/ beBPo-Visitenkarte übereinstimmen. Innerhalb des Feldes "Kennung 2 (OU3)" sind bitte keine Eintragungen vorzunehmen.

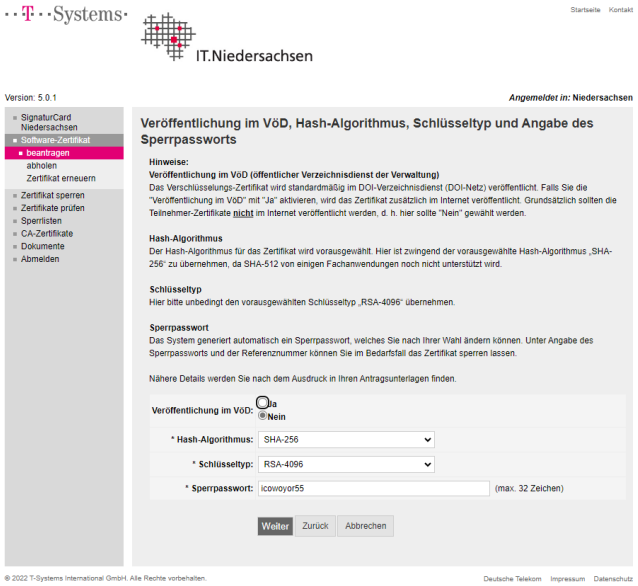
Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).



Schritt 7

Der VöD ist der Verzeichnisdienst der öffentlichen Verwaltung im Internet. Die Voreinstellung der Auswahl ist hier "Nein". Falls das Zertifikat im Internet veröffentlicht werden soll, aktivieren Sie hier bitte die Auswahl "Ja". Das Feld „Hash-Algorithmus:“ ist bereits mit dem Eintrag „SHA-256“ vorausgewählt und darf nur für „FITKO“-Anwendungen verändert werden.
Soll das Zertifikat für eine „FITKO“-Anwendung für die von der Föderalen IT-Kooperation (FITKO) im Auftrag des IT-Planungsrates betriebene FIT-Connect-Infrastruktur eingesetzt werden, wählen sie hier bitte unbedingt den Hash-Algorithmus „SHA-512“ aus.
Für den Eintrag im Feld „Schlüsseltyp:“ wählen sie bitte unbedingt „RSA-4096“ aus.
Das im Feld "Sperrpasswort:" eingetragene Passwort wurde vom System automatisch vergeben, kann aber mit einem von Ihnen selbst gewählten überschrieben werden.

Betätigen Sie anschließend die Schaltfläche „Weiter“ (s. nebenstehende Abbildung).



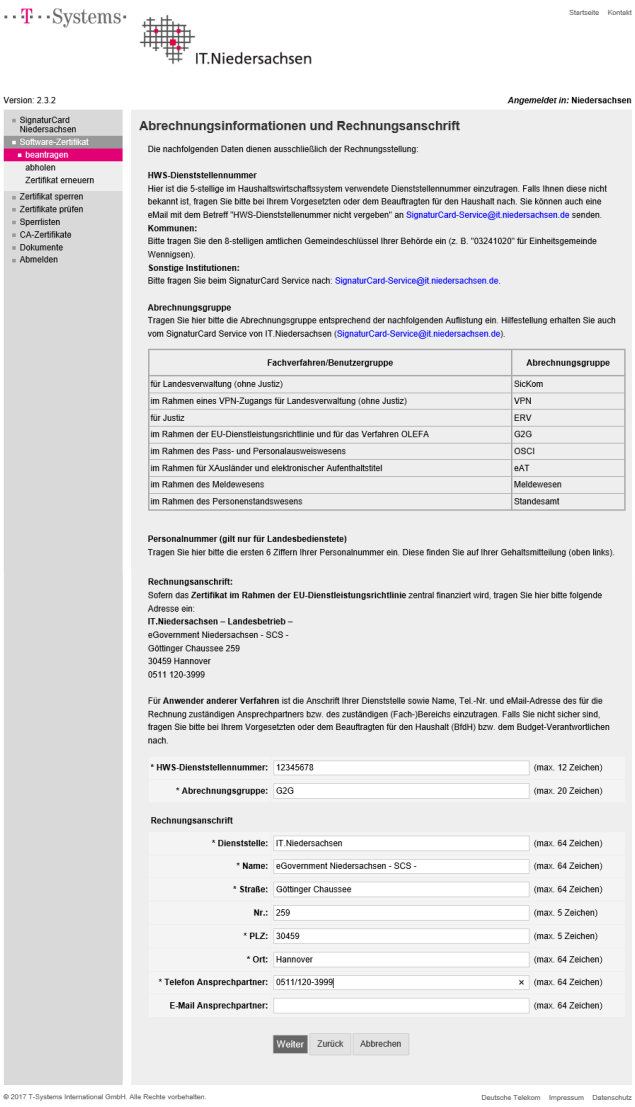
Schritt 8
In das Feld "HWS-Dienststellennummer" tragen Sie bitte folgendes ein:
Dienststellen des Landes Niedersachsen:
Bitte die HWS-Dienststellennummer eintragen.
Kommunen:
Bitte den 8-stelligen amtlichen Gemeindeschlüssel (AGS) Ihrer Behörde eintragen
Kammern:
Eine Zuordnungsnummer ist vom SignaturCard Service IT.N vergeben worden. Diese können Sie per eMail über folgende Adresse erfragen: SignaturCard-Service@it.niedersachsen.de

In das Feld "Abrechnungsgruppe" tragen Sie bitte „G2G“ ein. Tragen Sie in die Felder unter der Rubrik "Rechnungsanschrift" bitte die Rechnungsanschrift ein wie nachfolgend beschrieben:

Sollten Sie das neue Zertifikat nicht für ein bereits bestehendes Postfach, mit der Funktion „Einheitliche Ansprechpartner“/ „Zuständige Stellen“ im Rahmen einer Zertifikatserneuerung einsetzen wollen, ist dieses in jedem Fall kostenpflichtig. In diesem Fall (z. B. bei einem Zertifikats-Neuantrag für ein beantragtes beBPo- Postfach) müssen in die Felder der Rechnungsanschrift unbedingt die Daten der beantragenden Dienststelle eingetragen werden.

Nur für Zertifikatserneuerungen für bereits bestehende Postfächer im Rahmen der EU-Dienstleistungsrichtlinie EGVP/ beBPo **(betrifft die Funktionen„Einheitliche Ansprechpartner“/ „Zuständige Stellen“) darf die folgende Rechnungsanschrift angegeben werden:**
Dienststelle: IT.Niedersachsen
Name: eGovernment Niedersachsen – SCS -
Straße: Göttinger Chaussee
Nr.: 259
PLZ: 30459
Ort: Hannover
Telefon Ansprechpartner: 0511/120-3999

Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).



Schritt 9

Innerhalb des Feldes "Mitteilungen an die RA" können Sie bei Bedarf eine Mitteilung an die Registrierungsstelle (SignaturCard Service IT.N) formulieren.

Betätigen Sie anschließend die Schaltfläche "Weiter" (s. nebenstehende Abbildung).

Schritt 10

Die menügeführte Eingabe Ihrer Antragsdaten ist nun beendet. Abschließend wird Ihnen eine Übersicht aller von Ihnen getätigten Eingaben zur Verfügung gestellt. Bitte kontrollieren Sie noch einmal den Inhalt Ihrer Eingaben auf Richtigkeit. Sollten Sie noch Änderungswünsche feststellen, können Sie über die ggf. mehrfache Betätigung der Schaltfläche "Zurück" das gewünschte Eingabefeld auswählen und die Eingabe korrigieren. Mittels ggf. mehrfacher Betätigung der Schaltfläche "Weiter" gelangen Sie wieder zur Zusammenfassung Ihrer Antragsdaten.

Wenn alle Einträge korrekt angezeigt werden, betätigen Sie bitte die Schaltfläche "Absenden" (s. nebenstehende Abbildung).

Schritt 11

Der Zertifikatsantrag wurde mit einer eindeutigen Referenznummer im System der CA gespeichert und wird Ihnen über die Schaltfläche "Zertifikatsantrag herunterladen" zum Download angeboten (s. nebenstehende Abbildung). Bitte speichern Sie diesen auf Ihrer Festplatte oder einem sonstigen Datenträger.

Schritt 12

1. Nach dem Herunterladen des Dokuments sind folgende weitere Schritte auszuführen:
   - Ausdruck
   - Unterschrift des Schlüsselverantwortlichen (Antragsteller)
   - Unterschrift der "Vollmacht gebenden Stelle" (z.B. Behörden-/Dienststellenleiter, Abteilungsleiter)
   - Bestätigung der Identität des Antragstellers durch Unterschrift sowie Dienstsiegel einer Siegel führenden Stelle
   - Versand der 3. Ausfertigung des Antrags an den SignaturCard Service von IT.N (Kontaktdaten siehe Kapitel 5).

   ⇒ Weitere Hinweise finden Sie auf dem Deckblatt des Ausdrucks.

Das Antragsverfahren ist hier abgeschlossen.
Nach dem Eingang des Antrags beim SignaturCard Service wird dieser geprüft und in der Regel genehmigt. Sie erhalten dann per eMail eine Benachrichtigung an die oben unter "Zertifikatsdaten" angegebene eMail Adresse. Bitte beachten Sie, dass nicht die eMail-Adresse des Schlüsselverantwortlichen adressiert wird. Eine Kurzanleitung zum Download des Zertifikats bzw. der PSE erhalten Sie zusammen mit der genannten eMail. Außerdem wird das Verfahren im Kapitel 3 beschrieben.

3. DOWNLOAD VON SOFTWARE-ZERTIFIKATEN

Schritt 1
Gehen Sie mit Ihrem Browser auf das Portal der DOI-CA Niedersachsen wie im Kap. 1 beschrieben.

Schritt 2
Wählen Sie bitte zunächst den Menüpunkt

*"*Software-*Zertifikate"*

und dann den Unterpunkt

"abholen".

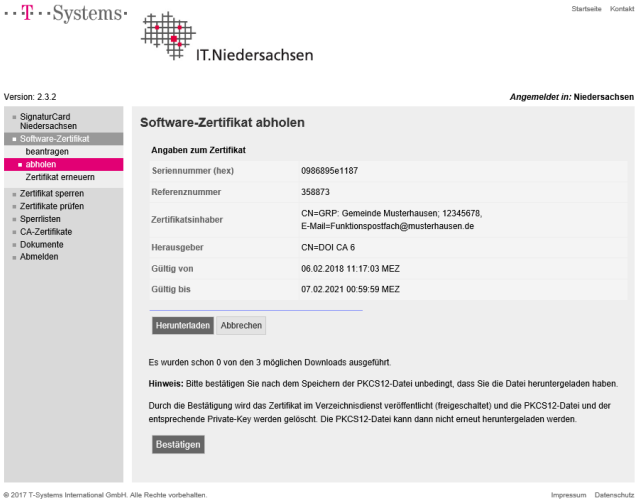
(s. nebenstehende Abbildung)

Schritt 3
Geben Sie bitte in die entsprechenden Formularfelder die "Referenznummer" und das "Download-Passwort" ein. Diese Informationen entnehmen Sie bitte ihrem Zertifikatsantrag.

Betätigen Sie anschließend die Schaltfläche "Suchen" (s. nebenstehende Abbildung).

Schritt 4
Die Zertifikatsdaten werden Ihnen zusammengefasst angezeigt. Bitte prüfen Sie diese.

Betätigen Sie bitte die Schaltfläche "Herunterladen" (s. nebenstehende Abbildung).



Schritt 5
Die Datei mit dem PSE-Container (Zertifikat + privater Schlüssel) wird Ihnen zum Download

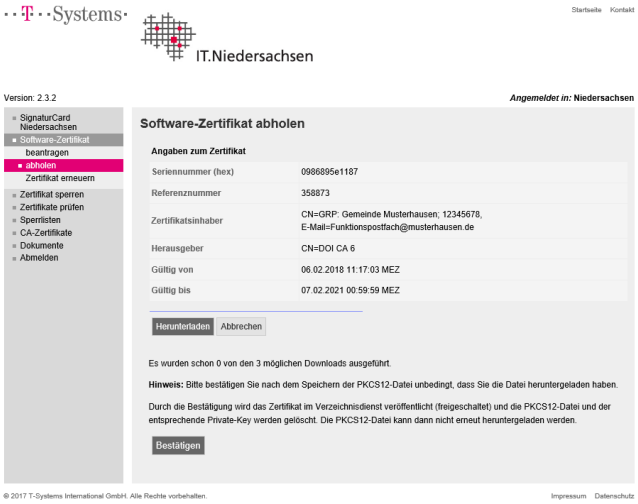
angeboten.

Betätigen Sie bitte die Schaltfläche "Speichern" um die Datei in Ihrem Filesystem zu speichern (s. nebenstehende Abbildung). Die Datei wird daraufhin im Ordner „Downloads“ gespeichert. Möchten Sie einen anderen Speicherort bestimmen, wählen Sie bitte über den Auswahl-Schalter (kleines Dreieck) „Speichern unter“.

Achtung: Der Download der P12-Datei ist mit einem Zähler behaftet und kann lediglich 3 x durchgeführt werden.

Schritt 6

Stellen Sie sicher, dass die P12-Datei (Zertifikat + Schlüsselpaar) in Ihrem Filesystem gespeichert wurde. Falls etwas nicht funktioniert haben sollte, wählen Sie die Schaltfläche "Herunterladen" erneut; sonst wählen Sie für die Freischaltung des Zertifikats unbedingt die Schaltfläche "Bestätigen" (s. nebenstehende Abbildung).



Hinweis:

Nachdem der Download über den Button „Bestätigen“ quittiert wurde, wird das Zertifikat für den Verzeichnisdienst frei geschaltet und kann nicht erneut heruntergeladen werden. Die P12-Datei und der Private-Key werden automatisch auf dem Server gelöscht.

Das Zertifikat kann erst genutzt werden, nachdem dies bestätigt wurden (s. o.) und dadurch das Zertifikat freigeschaltet ist.

Mittels Betätigung der Schaltfläche "Zertifikat herunterladen" haben Sie optional die Möglichkeit, nur den öffentlichen Schlüssel dieses Zertifikats herunterzuladen (s. nebenstehende Abbildung).

Bewahren Sie das heruntergeladene Zertifikat (bzw. den PSE-Container/P12-Datei) und den Antrag mit dem PSE-Passwort sicher auf, so dass Sie diese jederzeit wiederverwenden können.

4. ERLÄUTERUNGEN ZU GRUPPENZERTIFIKATEN AUS DER DOI-CA

Ausführliche Informationen können dem Dokument "DOI-CA / Niedersachsen: Erläuterungen zum Antrag für Gruppen-Zertifikate" (s. Webseite des SignaturCard Service) in der jeweils aktuellen Version entnommen werden. Nachfolgend werden in Kurzform die Funktionen des Schlüsselverantwortlichen und der *Vollmacht gebenden Stelle* erläutert. Nach der Policy der Verwaltungs-PKI (BSI) müssen bei der Vergabe von Gruppen-Zertifikaten ein Schlüsselverantwortlicher und eine *Vollmacht gebenden Stelle* eingesetzt werden**.**

Der Schlüsselverantwortliche

Das BSI stellt in [BSI2003-1] folgende Anforderungen an die Vergabe von Gruppen-Zertifikaten: Für jedes Gruppenzertifikat ist eine natürliche Person als Schlüsselverantwortlicher zu benennen. Diese Person muss ein entsprechendes Zertifikat beantragen und die geforderten Identitäts- und Authentisierungsnachweise erbringen. Die Person muss die Berechtigung zur Beantragung des Gruppenschlüssels nachweisen. Der Schlüsselverantwortliche nimmt die entsprechenden Schlüssel und Zertifikate in Empfang und verpflichtet sich gegenüber der Zertifizierungsstelle zur Einhaltung der Regelungen für Gruppenzertifikate [BSI2002-3] und [DOI110]. Wird die Verantwortung an einen neuen Schlüsselverantwortlichen übergeben, muss dieser ebenfalls die geforderten Nachweise zur Identifizierung erbringen und sich gegenüber der Zertifizierungsstelle zur Einhaltung der Regelungen für Gruppenzertifikate verpflichten.
Grundsätzlich gelten für den Schlüsselverantwortlichen die Vorgaben des BSI [BSI2002-3] bzw. [DOI110], die teilweise auch in den ausführlichen Erläuterungen (s.o.) aufgelistet sind.

Die *Vollmacht gebende Stelle (VgS)*

Die Berechtigung zur Beantragung eines Gruppenschlüssels muss von der VgS vergeben werden. Die VgS wird durch die Policy in [BSI2002-3] als diejenige Stelle bezeichnet, die für den Einsatz der Gruppenzertifikate verantwortlich ist.
Die Funktion der VgS wird im Rahmen der DOI-CA/Niedersachsen durch den Dienststellen-/Behördenleiter und bei größeren Organisationen auch durch Abteilungsleiter wahrgenommen, für dessen Behörde/ Dienststelle das jeweilige Gruppenzertifikat ausgestellt wird. Dieser kann die Funktion delegieren (z.B. an den IT-Verantwortlichen oder Sicherheitsbeauftragten). Die Funktion der VgS darf nicht auf den Schlüsselverantwortlichen übertragen werden. Die VgS genehmigt den Zertifikatsantrag durch Unterschrift. Durch diese Maßnahme ist gewährleistet, dass der Schlüsselverantwortliche den zuständigen Stellen bekannt und in die Abläufe eingebunden ist. Die VgS kann das Zertifikat sperren lassen. Dazu wird ihr über den Zertifikatsantrag das Sperrpasswort bekannt gemacht (für telefonische Sperrung, weitere Informationen zur Sperrung finden Sie auf den Seiten des SignaturCard Service; Kontaktdaten im Kap. 5). Der Schlüsselverantwortliche muss den Anforderungen entsprechend qualifiziert sein und entsprechende Befugnisse besitzen. Die diesbezügliche Verantwortung trägt die VgS. Ferner ist es Aufgabe der VgS, im Falle von Personalwechseln die Informationen über erteilte Berechtigungen für Gruppenschlüssel und die Sperrmodalitäten an den neuen Schlüsselverantwortlichen weiter zu geben. Ein Wechsel des Schlüsselverantwortlichen muss der zuständigen Registrierungsstelle (SignaturCard Service) mitgeteilt werden.

Hinweise zu den Zertifikatsdaten

Die Zertifikatsdaten beinhalten wesentliche Angaben zur Identifizierung der Gruppe bzw. der Funktion des Zertifikats. Die genauen Regeln für die Bildung entnehmen Sie bitte den entsprechenden Dokumenten der T-Systems/DOI [DOI110] bzw. des BSI [BSI 2002-2], grundsätzlich ist aber zu beachten:

- Aus dem Gruppennamen muss eindeutig hervorgehen, dass es sich um ein Gruppenzertifikat handelt, deshalb muss der Name (CN) mit der Kennzeichnung "GRP:" beginnen.
- Die Verwendung von Personennamen als Gruppennamen sollte vermieden werden.
- Grundsätzlich sollten Gruppenzertifikate nur für Gruppen, Dienste oder Server ausgestellt werden, die Teil der ausstellenden Behörde sind oder zum Verantwortungsbereich der Behörde gehören.

Literaturhinweise

[BSI2003-1] Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung; Version 3.2 vom 09.01.2003; Bonn.

[BSI 2002-2] Bundesamt für Sicherheit in der Informationstechnik: Zertifizierungsinfrastruktur für die PKI-1-Verwaltung; Namensregeln und –formate; Version 1.3 vom 25.11.2002

[BSI2002-3] Bundesamt für Sicherheit in der Informationstechnik (BSI): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung; Regelungen für Gruppenzertifikate, Version 1.3 vom 10.12.2002

[DOI 110] Deutschland Online Infrastruktur / T-Systems: DOI-CA; Hinweise zur Nutzung von Gruppen- und Pseudonym-Zertifikaten; Stand 30.09.2009, Version 1.0

Online-Quellen:

Landesintranet: http:/intra.it.niedersachsen.de
Internet: https://doi.telesec.de/doi/ee/itn/login/displayLogin.html

5. KONTAKTDATEN

5.1 SIGNATURCARD SERVICE

Für Fragen zur SignaturCard Niedersachsen und zu Software-Zertifikaten steht Ihnen der SignaturCard Service von IT.N zur Verfügung:

Postanschrift	IT.Niedersachsen - SignaturCard Service - Göttinger Chaussee 259 30459 Hannover
Intranet	http://intra.it.niedersachsen.de
eMail	SignaturCard-Service@it.niedersachsen.de
Telefon	0511/120-3990