PKI der Dataport AöR

Zertifikatsrichtlinie
Certificate Policy (CP)
&
Erklärung zum Zertifizierungsbetrieb
Certification Practice Statement (CPS)

Regelungsverantwortlich:	Holger Kraft; TZ 61		
Version:	2.1.9	vom:	08.07.2022
Status:	Gültig		
Dokumenttyp:	Richtlinie		
Schutzstufe:	keine Schutzstufe		
Zielgruppe:	Dataport, Kunden		
gültig ab:	09.12.2013	bis:	TT.MM.JJJJ
beschlossen durch:	Vorstand	am:	21.01.2016

Inhaltsverzeichnis

1 Einleitung

Der Begriff „Certificate Policy (CP)“, definiert im X.509 Standard, steht für die Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer Certificate Policy wird im RFC 3647 („Certificate Policy and Certification Practices Framework“) ausführlich diskutiert. Die CP ist eine Entscheidungshilfe für den Zertifikatsnutzer, ob einem bestimmten Zertifikat und Anwendung vertraut werden kann.
Insbesondere sollte eine CP darlegen:

- welche technischen und organisatorischen Anforderungen die bei der Ausstellung der Zertifikate eingesetzten Systeme und Prozesse erfüllen,
- welche Vorgaben für die Anwendung der Zertifikate, sowie im Umgang mit den zugehörigen Schlüsseln und Signaturerstellungseinheiten (z.B. Chipkarten) gelten,
- welche Bedeutung den Zertifikaten und zugehörigen Anwendungen zukommt, d.h. welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Ciphertexte bzw. Signaturen besitzen.

Das Konzept eines “Certification Practice Statement (CPS)” wurde von der American Bar Association (ABA) entwickelt und ist in deren Digital Signature Guidelines (ABA Guidelines) aufgeführt. Das CPS ist eine detaillierte Beschreibung des Zertifizierungsbetriebes der Organisation. Aus diesem Grund stellen Organisationen, die eine oder mehrere Zertifizierungsstellen betreiben, in der Regel auch ein CPS zur Verfügung. Im Rahmen einer organisationsweiten PKI ist das CPS für Organisationen ein adäquates Mittel um sich selbst zu schützen, sowie Geschäftsvorfälle zu Zertifikatsnehmern und vertrauenden Parteien darzustellen.
Ein zentraler Aspekt der CP/CPS ist die Bestimmung der Vertrauenswürdigkeit auszugebender Zertifikate und des Zertifizierungsdienstes, der durch das Dataport Rechenzentrum betrieben wird. Mit Teilnahme an den Dataport Zertifizierungsdiensten akzeptieren die Dataport Kunden und vertrauende Parteien die im CP/CPS aufgeführten Bedingungen und Regularien.
Die Dokumentenstruktur orientiert sich an den im RFC 3647 angegebenen Empfehlungen. Entsprechend den Vorgaben des RFC 3647 legt die Dataport CP/CPS die Vorgehensweise dar, die der Zertifizierungsdienst bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate anwendet.
Aufgrund der Anforderung einer vereinfachten Dokumentenverwaltung wurden die CP (Certficate Policy) und das CPS (Certification Practice Statement) in einem zentralen Dokument zusammengefasst. Dieses Dokument beschreibt die **Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der PKI der Dataport AöR**. Das Dokument ist kostenfrei und öffentlich zugänglich.

1.1 Überblick

Dataport stellt für seine Kunden Zertifikate auf Smartcards, Token und anderen Zertifikatsspeichern für verschiedene Verwendungszwecke aus.
In diesem Dokument werden keine technischen Details der Umsetzung beschrieben. Die Leistungen werden von folgenden Prozessbeteiligten erbracht:

Dataport AöR

Dataport betreibt und entwickelt die für die Ausstellung der Zertifikate benötigte Infrastruktur, setzt die in dieser Richtlinie beschriebenen Prozesse und Maßnahmen durch und ist zentraler Ansprechpartner für die Kunden.

Kunden

Dataport liefert Zertifikate an Kunden. Dataport übernimmt hier die Aufgabe der Registration Authority oder Registrierungsstelle, kurz RA genannt.
Dataport bietet den Kunden über Schnittstellen die Möglichkeit eigenständig Zertifikate zu verwalten:

Die Kunden übernehmen in dieser Variante die Funktion von Registrierungsstellen(RA) und die mit dieser Funktion verbundenen Aufgaben. Im Prozess der Ausstellung von Zertifikaten liefern sie die für die Ausstellung benötigten Informationen und übernehmen die Prüfung der Identität der Antragsteller.

1.1.1 Architektur

Die Dataport AöR betreibt Zertifizierungsdienste für die Erzeugung, Ausgabe und Verwaltung von Zertifikaten. Die Dataport PKI erlaubt auch die automatisierte und kontrollierte Ausgabe von Zertifikaten bzw. Smartcards.
Die automatisierte Ausgabe von Zertifikaten steht nur in von Dataport verwalteten Verzeichnisdiensten zur Verfügung. Zertifikate auf Smartcards werden durch ein Zertifikats- und Smartcardmanagementsystem. kontrolliert ausgegeben und verwaltet.
Darüber hinaus werden Cerification Authority (CA) Zertifikate zur Zertifizierung der Stammzertifizierungsstelle Dataport Root CA 02 selbst und zur Zertifizierung der untergeordneten Zertifizierungsstellen Dataport CA 03, Dataport CA 04, Dataport CA 05 und Dataport CA 06 ausgestellt.
Ein Netzwerk Hardware Security Module (HSM) übernimmt die Schlüsselgenerierung und –verwaltung für die Dataport Zertifizierungsstellen und auch für das Zertifikatsmanagementsystem (CM).

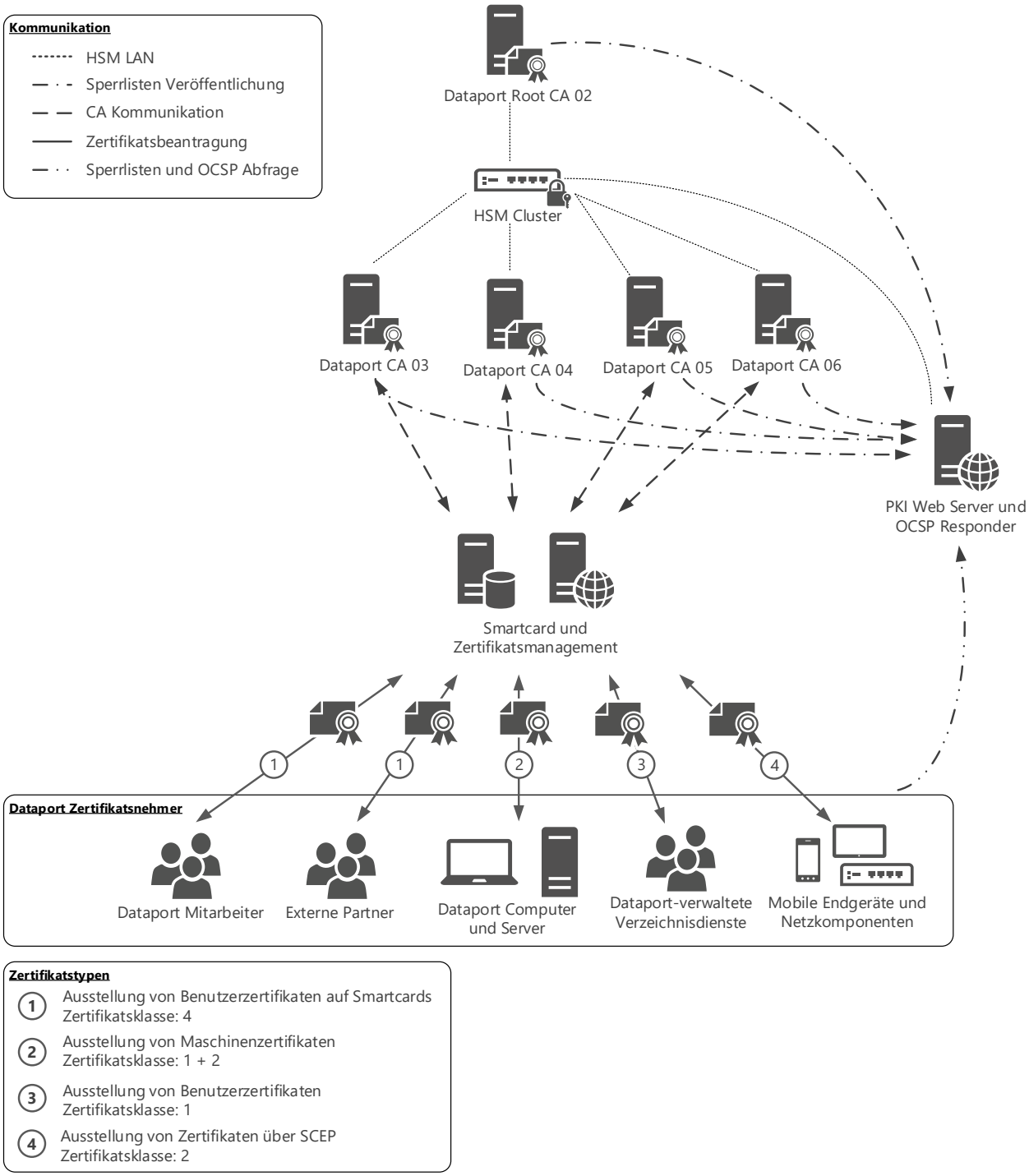

Abbildung 1 - Dataport PKI

Die Dataport Zertifizierungsinfrastruktur ist hierarchisch aufgebaut und terminiert an der Dataport ROOT CA 02. Die Dataport PKI ist zweistufig aufgebaut.
Die derzeitige Implementierung umfasst eine Dataport Root CA 02 und drei Zwischenzertifizierungsstellen. Die Dataport CA 03 ist für die Ausgabe von Benutzerzertifikaten, die Dataport CA 04 für die Ausgabe von Maschinenzertifikaten, die Dataport CA 05 für die automatisierte Ausgabe von Benutzerzertifikaten vorgesehen sowie die Dataport CA 06 für die automatisierte Ausgabe von Maschinenzertifikate.

Alle an der PKI beteiligten Komponenten sind durch ausfallsichere Netzwerk Hardware Security Modules (HSMs) abgesichert. Die Schlüsselgenerierung und –verwaltung für die Komponenten erfolgt auf diesen Appliances.
Die PKI betreffende Informationen werden über einen Web - Dienst veröffentlicht. Dazu zählen die Statusinformationen der Zertifikate (CRLs), die Zertifikate der CAs, die CP/CPS sowie ergänzende Dokumente (Anleitungen etc.). Alternativ zur Veröffentlichung der Statusinformationen der Zertifikate via Web werden diese Informationen über Online Certificate Status Protocol (OCSP) Responder bereitgestellt.
Die Ausgabe von Zertifikaten wird über Autoenrollment für Clients und Domänencontroller und für alle anderen über ein Zertifikatsmanagement Tool umgesetzt. Eine Web-basierte Ausgabe von Zertifikaten, direkt auf den CAs, ist nicht vorgesehen.

1.2 Dokumentenidentifikation

Die Bezeichnung des Dokumentes lautet:

„Dataport PKI, Zertifikatsrichtlinie Certificate Policy (CP) & Erklärung zum Zertifizierungsbetrieb Certification Practice Statement (CPS)“

Version 2.1.6 vom 23.09.2020

Ein eindeutiger ASN.1 Object Identifier (OID) ist diesem Dokument zugewiesen.
Die Dataport OID ist bei der iana.org registriert, siehe auch:

http://www.iana.org/assignments/enterprise-numbers

Kontaktperson: Holger Kraft
Leiter Zertifikatsdienste

Dataport AöR
Niederlassung Hamburg
Billstr. 82, 20539 Hamburg
Telefon: +49 (40) 4 28 46 2892
Telefax: +49 (40) 4 279 46 892
E-Mail: Holger.Kraft@dataport.de
Internet: www.dataport.de

Der OID [OID] ist wie folgt zusammengesetzt:

Object Identifier						Beschreibung
1.3.6.1.4.1						IANA registrierter „Private Enterprise Number“ Namensraum
	.38103					IANA PEN Dataport
		.509				Allgemeiner Dataport PKI Nummernkreis
			.1			Dataport SHA1 PKI Issuance Policy Reference
			.10			Dataport SHA1 PKI Dokumenten Nummernkreis
				.1		CP/CPS Dokumentbezeichner
					.X	Dokument Version 1…n
			.100			Dataport SHA1 PKI Zertifikatsklassen Nummernkreis
				.X		Dataport SHA1 PKI Zertifikatsklassen 1…4
			.2			Dataport SHA2 PKI Issuance Policy Reference
			.20			Dataport SHA2 PKI Dokumenten Nummernkreis
				.1		CP/CPS Dokumentbezeichner

					.X	Dokument Version 1…n
			.200			Dataport SHA2 PKI Zertifikatsklassen Nummernkreis
				.X		Dataport SHA2 PKI Zertifikatsklassen 1…4

Der CP/CPS Titel lautet: „PKI der Dataport AöR Zertifikatsrichtlinie Certificate Policy (CP) & Erklärung zum Zertifizierungsbetrieb Certification Practice Statement (CPS)“
Die CP/CPS OID lautet: 1.3.6.1.4.1.38103.509.20.1.2

1.3 Teilnehmer und Instanzen

1.3.1 Zertifizierungsdienst und -instanzen

Der Zertifizierungsdienst im Sinne dieser Richtlinie sind alle technischen und organisatorischen Einrichtungen mit denen Dataport Zertifikate ausstellt.
Der Zertifizierungsdienst nutzt für die verschiedenen Zertifikatstypen unterschiedliche Zertifizierungsinstanzen.
Zertifizierungsinstanzen sind logische Einheiten für die Signierung von Zertifikaten.
Durch die Zertifizierungsinstanzen des Zertifizierungsdienstes, und die von ihnen ausgestellten Zertifikate, wird die in der Abbildung 1 - Dataport PKI dargestellte zweistufige Zertifizierungshierarchie definiert. Es wird eine getrennte Infrastruktur von Zertifikaten für Benutzer und Maschinen betrieben um den unterschiedlichen Anforderungen Rechnung zu tragen.
Auf der obersten Hierarchieebene befindet sich die ROOT CA 02. Die Eindeutigkeit der Zertifizierungsstellen wird durch den „Distinguished Name“ (DN) der Zertifizierungsstelle gewährleistet.
Der vollständige DN der Dataport ROOT CA 02 lautet:

CN = Dataport ROOT CA 02

O=Dataport AöR

C=DE

Diese CA basiert auf einem selbst-signierten CA Zertifikat. Sie wird offline betrieben und unterhält eine dedizierte Verbindung zum Netzwerk HSM. Alle kryptographischen Operationen der Dataport ROOT CA 02 werden durch das HSM ausgeführt. Die Dataport ROOT CA 02 stellt CA Zertifikate und Sperrlisten für untergeordnete Zertifizierungsstelleninstanzen (SUB CAs), wie auch für sich selbst aus. Verantwortlich für den Betrieb ist

Dataport Anstalt öffentlichen Rechts
Zertifikatsdienste
Altenholzer Straße 10 - 14
24161 Altenholz
Tel. +49 (431) 4 2846 – 1994

www.dataport.de

Auf der zweiten Hierarchieebene befinden sich Zertifizierungsinstanzen für die Ausstellung von Benutzer- und Maschinenzertifikaten. Sie sind mit dem Produktionsnetz verbunden und unterhalten ebenso, wie die Dataport Root CA 02, eine dedizierte Verbindung zum Netzwerk HSM. Alle kryptographischen Operationen der Zertifizierungsstellen werden durch das HSM ausgeführt.

Der vollständige DN der Dataport CA 03 lautet:

CN = Dataport CA 03

O=Dataport AöR

C=DE

Der vollständige DN der Dataport CA 04 lautet:

CN = Dataport CA 04

O=Dataport AöR

C=DE

Der vollständige DN der Dataport CA 05 lautet:

CN = Dataport CA 05

O=Dataport AöR

C=DE

Der vollständige DN der Dataport CA 06 lautet:

CN = Dataport CA 06

O=Dataport AöR

C=DE

Für die Dataport Zertifizierungsstellen sind folgende Lebensdauern von Zertifikaten festgelegt:

Dataport ROOT CA 02

- ROOT CA 02 Zertifikat: 12 Jahre
- ROOT CA 02 CRLs: 9 Monate (6 Monate Publikationsintervall und 3 Monate Überlappungszeitraum)

Dataport CA 03

- DATAPORT CA 03 Zertifikat: 6 Jahre
- DATAPORT CA 03 CRLs: 2 Tage (1 Tag Publikationsintervall und 1 Tag Überlappungszeitraum)
- DATAPORT CA 03 Delta CRLs: 4 Stunden (2 Stunden Publikationsintervall und 2 Stunden Überlappung)

Dataport CA 04

- DATAPORT CA 04 Zertifikat: 6 Jahre
- DATAPORT CA 04 CRLs: 10 Tage (8 Tage Publikationsintervall und 2 Tage Überlappungszeitraum)
- DATAPORT CA 04 Delta CRLs: 12 Stunden (6 Stunden Publikationsintervall und 6 Stunden Überlappung)

Dataport CA 05

- DATAPORT CA 05 Zertifikat: 6 Jahre
- DATAPORT CA 05 CRLs: 2 Tage (1 Tag Publikationsintervall und 1 Tage Überlappungszeitraum)
- DATAPORT CA 05 Delta CRLs: 4 Stunden (2 Stunden Publikationsintervall und 2 Stunden Überlappung)

Dataport CA 06

- DATAPORT CA 06 Zertifikat: 6 Jahre
- DATAPORT CA 06 CRLs: 2 Tage (2 Tag Publikationsintervall und 5 Tage Überlappungszeitraum)

- DATAPORT CA 06 Delta CRLs: 12 Stunden (6 Stunden Publikationsintervall und 6 Stunden Überlappung)

Die ausgegebenen Delta CRLs werden nicht in der Basis CRL referenziert und dienen bei allen Zertifizierungsstellen nur zur Überprüfung durch den Online Responder.

1.3.2 Registrierungsstellen

Die Registrierungsstellen im Sinne dieser Certificate Policy sind Instanzen, welche die Zertifikatsnehmer und Antragssteller erfassen, identifizieren und für Zertifikatsnehmer Zertifikate beantragen. Für die unterschiedlichen Zertifikatstypen gibt es unterschiedliche Registrierungsstellen. Für personenbezogene Zertifikate (Benutzerzertifikate zur Authentifizierung, Verschlüsselung und Signierung) sind diese durch den Kunden zu bestimmen (in der Regel die zugehörige Personalstelle).

1.3.2.1 Zertifikatsnehmer

Zertifikatsnehmer sind End-Entitäten, denen ein Zertifikat durch die SUB CAs zugewiesen wird. Schlüsselgenerierung und Zertifikatsausgabe unterstehen nicht der Kontrolle des Zertifikatsnehmers, sondern obliegen der Dataport PKI.
End-Entitäten als Zertifikatsnehmer im Rahmen dieser PKI stellen Dataport Vollzeit-Mitarbeiter, Teilzeitbeschäftigte, technische Systeme (wie z.B.: Domänen Maschinen), Geschäftspartner und auch externe Mitarbeiter dar.

1.3.2.2 Vertrauende Parteien

Vertrauende Parteien im Sinne der vorliegenden Richtlinie sind alle Personen und Systeme, die mit Hilfe eines Zertifikates mit dessen Zertifikatsnehmer sicher kommunizieren wollen.

1.3.2.3 Sonstige Teilnehmer

nicht anwendbar

1.4 Zertifikatsnutzung

Zertifikate werden für die Signierung und/oder Verschlüsselung von Daten als auch für die Authentifizierung verwendet. Die Verwendung von Schlüsseln und Zertifikaten obliegt der Verantwortung des Zertifikatsinhabers.
Zertifikate können auch für weitere, hier nicht genannte Zwecke, eingesetzt werden, solange die Verwendung nicht gegen diese Richtlinie oder gesetzliche Regelungen verstößt.

1.4.1 Zulässige Verwendung von Zertifikaten

Dataport Root CA 02
Die von der Dataport Root CA 02 ausgestellten Zertifikate werden ausschließlich auf den Dataport Zwischenzertifizierungsstellen verwendet.

Dataport CA 03
Die von der Dataport CA 03 stellt personenbezogene Zertifikate aus, die auf sicheren Trägermedien ausgegeben werden und für folgende Zwecke zulässig sind:

- Authentifizierung an elektronischen Systemen (z.B. Benutzeranmeldung)
- Signierung und Verschlüsselung von Daten (z.B. S/MIME)

Dataport CA 04
Die von der Dataport CA 04 stellt Maschinenzertifikate aus, für folgende Zwecke zulässig sind:

- Authentifizierung von Maschinen (z.B. für Computer, Netzwerkkomponenten und mobile Endgeräte)
- Verschlüsselung von Kommunikation (z.B. VPN, TLS)

Dataport CA 05
Die von der Dataport CA 05 stellt personenbezogene Zertifikate aus, die für folgende Zwecke zulässig sind:

- Signierung und Verschlüsselung von Daten (z.B. S/MIME)

Dataport CA 06
Die von der Dataport CA 06 stellt Maschinenzertifikate aus, die für folgende Zwecke zulässig sind:

- Authentifizierung von Maschinen (z.B. für Computer)
- Verschlüsselung von Kommunikation (z.B. TLS)

1.4.2 Unzulässige Verwendung von Zertifikaten

Die Nutzung der Zertifikate ist für andere, nicht unter 1.4.1 beschriebene Anwendungszwecke und für private Zwecke untersagt. Zertifizierungsstellenzertifikate für untergeordnete Zertifizierungsstellen dürfen ausschließlich durch die Dataport ROOT CA 02 ausgestellt werden.
Die Sicherheit der verwendeten Zertifikate darf durch deren Anwendung nicht kompromittiert werden.
Zum Schutz der Dataport-CP/CPS-Konformität ist jegliche Änderung oder Erweiterung der Zertifikatsanwendung unverzüglich der Dataport PKI Administration anzuzeigen.

1.5 Richtlinienverwaltung

1.5.1 Organisation

Für die Verwaltung der CP/ CPS sind die unter 1.5.2 genannten Kontaktpersonen von Dataport AöR verantwortlich.

1.5.2 Kontaktperson

Holger Kraft
Leiter Zertifikatsdienste

Dataport AöR
Niederlassung Hamburg
Billstr. 82, 20539 Hamburg
Telefon: +49 (40) 4 28 46 2892
Telefax: +49 (40) 4 279 46 892
E-Mail: Holger.Kraft@dataport.de

Dataport Anstalt öffentlichen Rechts
Zertifikatsdienste
Altenholzer Straße 10 - 14
24161 Altenholz
Tel. +49 (431) 4 2846 – 1994
Dataport-pki@dataport.de

1.5.3 Verantwortlichkeit für das CP/ CPS

Dataport ist für die Einhaltung des Zertifizierungsbetriebes und der -richtlinie gemäß der CP/CPS und ergänzender Dokumente verantwortlich. Kontaktpersonen sind die unter 1.5.2 aufgeführten Personen.

1.5.4 Freigabe des CP/ CPS

Die Richtlinie ist durch einen Beschluss des Vorstandes genehmigt.

1.6 Definitionen und Abkürzungen

Abkürzung	Erläuterung
ABA	American Bar Association – Verband der amerikanischen Revisoren
ASN.1	Abstract Syntax Notation – Abstrakte Syntaxnotation Nummer 1, Datenbeschreibungssprache
BLOB	Binary Large Object – Datentyp in einer Datenbank
C	Country – Landesobjekt (Teil des X.500 Distinguished Name), für Deutschland C=DE
CA	Certification Authority – Zertifizierungsstelle
CN	Common Name – Namensobjekt (Teil des X.500 Distinguished Name)
CP	Certificate Policy – Zertifikatsrichtlinie
CPS	Certification Practice Statement – Zertifizierungsbetrieb
CRL	Certificate Revocation List – Liste, in der eine Zertifizierungsstelle die von ihr ausgestellten Zertifikate, die gesperrt aber noch nicht abgelaufenen sind, veröffentlicht
CSR	Certificate Signing Request – Signierte Zertifikatsanforderung
DN	Distinguished name – Eindeutiger Name basiert auf der X.500 Namensbildung. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Die wichtigsten Attribute in diesem DN sind CommonName (CN), Organization (O) und Country (C)
DNS	Domain Name System – Standard für Internet Namen
FIPS	Federal Information Processing Standard – Kryptographiestandard der US Behörden
GRP	Kennzeichen im CN: Personen- bzw. Funktionsgruppen
HSM	Hardware Security Module – Hardwarekomponente, die sicherheitsrelevante Informationen wie Daten und kryptographische Schlüssel sicher erzeugt, speichert und verarbeitet
IETF	Internet Engineering Task Force – Projektgruppe für die technische Weiterentwicklung des Internets. Spezifiziert Quasistandards in Form von RFCs
IP	Internet Protocol – Internetprotokoll
ISO	International Organization for Standardization – Internationale Normungsstelle
ITU	International Telecommunications Union – Standardisierungsgremium, hat auch X.509 spezifiziert
LDAP	Lightweight Directory Access Protocol – Zugriffsprotokoll für Verzeichnisdienste
NIST	National Institute of Standards and Technology – Normungsstelle der Vereinigten Staaten
O	Organization – Objekt für die Organisation (Teil des X.500 Distinguished Name)
OCSP	Online Certificate Status Protocol – Protokoll mit dem online der Status (ob eine Sperrung vorliegt) von Zertifikaten abgefragt werden kann
OCSP-Responder	Online Certificate Status Protocol Responder – Server der über OCSP Auskünfte zum Status von Zertifikaten erteilt

OID	Object Identifier – Object Identifikator, eindeutige Refrenz zu Objekten im OID Namensraum, der von der IANA verwaltet wird
OU	Organizational Unit – Objekt für die Organisationseinheit (Teil des X.500 Distinguished Name)
PIN	Personal Identification Number – Geheimzahl zur Authentisierung eines Individuums z.B. gegenüber einer Chipkarte
PKCS	Public Key Cryptographic Standard – Serie von Quasistandards für kryptographische Operationen spezifiziert durch RSA
PKI	Public Key Infrastructure – Beschreibung von Technologien, Prozessen und Teilnehmern im Rahmen der asymmetrischen Kryptographie
PKIX	Public Key Infrastructure eXchange – eine Serie von Spezifikationen der IETF im Umfeld von digitalen Zertifikaten nach X.509 Spezifikation
RA	Registration Authority – Registrierungsstelle
RFC	Request For Comment – Quasi Internet Standard ausgegeben durch die IETF
RSA	Asymmetrisches Kryptografieverfahren für Verschlüsselung und elektronische Signierung, benannt nach Rivest, Shamir, Adleman.
TSS	Time Stamp Service – Zeitstempel wird für die elektronische Signierung von Software benötigt um die Gültigkeit von Zertifikaten zum Zeitpunkt der Erstellung nachzuweisen
SN	Subject Name – wird für die Identifikation des Zertifikatsinhabers genutzt
SAN	Subject Alternate Name – wird für ergänzende Informationen des SN genutzt
SSL	Secure Socket Layer – Protokoll zur sicheren Kommunikation z.B. über das Internet
UPN	User Principal Name – ist ein Attribut eines Benutzerkontos und wird für die Anmeldung an einem Verzeichnisdienst genutzt
URL	Uniform Resource Locator – Ressourcen Lokation im Internet
X.500	Protokolle und Dienste für ISO konforme Verzeichnisse
X.509	Authentifikationsmethode für X.500 Verzeichnisse
X.509v3	Aktuell gültiger PKI Zertifikatsstandard

2 Publikationen und Informationsdienste

2.1 Verzeichnisdienst und Informationsdienste

Die Zertifikate der CAs werden in den Gesamtstrukturen der an der PKI beteiligten Kunden veröffentlicht. Zertifikatsinformationen können im Bedarfsfall in den zugewiesenen Verzeichnisdiensten veröffentlicht werden. Für die Veröffentlichung der CP/CPS und ergänzender Informationen wird aus Gründen der Erreichbarkeit ein Webdienst genutzt. Dieser ist intern wie extern unter http://pki.servicedpaor.de/ zu erreichen.

2.2 Publikation für Zertifikatsinformationen

Die Informationen zum Status der Zertifikate werden durch die jeweilige SUB CA automatisch auf dem internen Webserver für die Veröffentlichung der CRL hinterlegt. Die CRL der Dataport ROOT CA 02 wird durch Mitarbeiter des Bereiches Zertifikatsdienste von Dataport manuell auf demselben Webserver hinterlegt. Eine automatisierte Veröffentlichung ist aufgrund der Netztrennung dieser CA nicht möglich. Zusätzlich kann der Status eines Zertifikats über OCSP abgefragt werden.
Die CA Zertifikate und die CP/CPS Dokumentation werden durch die Mitarbeiter der Dataport Zertifikatsdienste auf dem internen Webserver veröffentlicht, auf dem auch die Sperrlisten publiziert werden.
Eine Weiterverteilung alle dieser Daten auf den externen Webserver erfolgt automatisiert unter derselben URL.

Folgende Pfade werden für die Veröffentlichung genutzt:

- Dataport CP/CPS http://pki.servicedpaor.de/cps
- Dataport CRLs http://pki.servicedpaor.de/crl/Dataport ROOT CA 02.crl
  http://pki.servicedpaor.de/crl/Dataport CA 03.crl
  http://pki.servicedpaor.de/crl/Dataport CA 03+.crl
  http://pki.servicedpaor.de/crl/Dataport CA 04.crl
  http://pki.servicedpaor.de/crl/Dataport CA 04+.crl
  http://pki.servicedpaor.de/crl/Dataport CA 05.crl
  http://pki.servicedpaor.de/crl/Dataport CA 05+.crl
  http://pki.servicedpaor.de/crl/Dataport CA 06.crl
  http://pki.servicedpaor.de/crl/Dataport CA 06+.crl
- Dataport CA Zertifikate http://pki.servicedpaor.de/ca/Dataport ROOT CA 02.crt
  http://pki.servicedpaor.de/ca/Dataport Root CA 02(1).crt
  http://pki.servicedpaor.de/ca/Dataport CA 03(1).crt
  http://pki.servicedpaor.de/ca/Dataport CA 03(2).crt
  http://pki.servicedpaor.de/ca/Dataport CA 04(1).crt
  http://pki.servicedpaor.de/ca/Dataport CA 04(2).crt
  http://pki.servicedpaor.de/ca/Dataport CA 05.crt
  http://pki.servicedpaor.de/ca/Dataport CA 05(1).crt

http://pki.servicedpaor.de/ca/Dataport CA 06.crt

- Dataport OCSP Dienst http://pki.servicedpaor.de/ocsp

2.3 Veröffentlichungsintervalle

Die Veröffentlichung der CPs und CPS erfolgt umgehend nach deren Erstellung bzw. Änderung.
Eine Veröffentlichung der CA Zertifikate erfolgt einmalig nach deren Erzeugung. Eine erneute Veröffentlichung erfolgt nur nach deren Ablauf bzw. nach einer Zertifikatserneuerung.
Die CRLs werden in einem definierten Intervall erzeugt und sofort auf den dafür vorgesehenen Webdiensten zur Verfügung gestellt.

Dataport ROOT CA 02

- ROOT CA 02 CRLs: 9 Monate (6 Monate Publikationsintervall und 3 Monate Überlappungszeitraum)

Dataport CA 03

- DATAPORT CA 03 CRLs: 2 Tage (1 Tag Publikationsintervall und 1 Tag Überlappungszeitraum)
- DATAPORT CA 03 Delta CRLs: 4 Stunden (2 Stunden Publikationsintervall und 2 Stunden Überlappung)

Dataport CA 04

- DATAPORT CA 04 CRLs: 10 Tage (8 Tage Publikationsintervall und 2 Tage Überlappungszeitraum)
- DATAPORT CA 04 Delta CRLs: 12 Stunden (6 Stunden Publikationsintervall und 6 Stunden Überlappung)

Dataport CA 05

- DATAPORT CA 05 CRLs: 2 Tage (1 Tag Publikationsintervall und 1 Tage Überlappungszeitraum)
- DATAPORT CA 05 Delta CRLs: 4 Stunden (2 Stunden Publikationsintervall und 2 Stunden Überlappung)

Dataport CA 06

- DATAPORT CA 06 CRLs: 10 Tage (5 Tag Publikationsintervall und 5 Tage Überlappungszeitraum)
- DATAPORT CA 06 Delta CRLs: 12 Stunden (6 Stunden Publikationsintervall und 6 Stunden Überlappung)

2.4 Zugang zu den Informationsdiensten

Der Zugriff auf die Dataport CA Zertifikate, Sperrlisteninformationen mittels CRLs oder OCSP und der CP/CPS Dokumentation ist nicht eingeschränkt und daher öffentlich. Siehe auch Veröffentlichungsorte in 2.2.

3 Identifikation und Authentifikation

3.1 Namen

3.1.1 Namensformen

In der Dataport PKI wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der Dataport PKI ausgestellten Zertifikate enthalten eindeutige Namen (DN) gemäß der Normenserie X.500. Ein DN enthält eine Folge von eindeutig kennzeichnenden Attributen, durch die jeder Zertifikatnehmer eindeutig referenziert wird. Abweichungen sind mit dem Bereich Zertifikatsdienste abzustimmen und müssen im CPS erläutert werden.
Ein DN entspricht grundsätzlich folgendem Schema, dabei sind optionale Attribute in eckige Klammern gesetzt, Attribute in spitzen Klammern müssen durch die jeweiligen Werte ersetzt werden. Die Reihenfolge der Attribute muss eingehalten werden.

[emailAddress=<E-Mail Adresse>]

CN=<Eindeutiger Name>

[OU=<Organisationseinheit>]

O= Dataport AöR

[L=<Ort>]

[ST=<Bundesland>]

C=DE

In der tatsächlichen Umsetzung der Zertifizierungsstelleninfrastruktur werden nicht alle (Namens-) Attribute festgelegt. In den nachfolgenden Tabellen werden die Namensformen in den einzelnen Ausprägungen dargestellt.

3.1.1.1 Dataport ROOT CA 02

Der X.500 Distinguished Name der selbst-signierten Dataport ROOT CA 02 lautet:

Attribute	Werte
Common Name (CN)	Dataport ROOT CA 02
Organization (O)	Dataport AöR
Country (C)	DE

3.1.1.2 Dataport SUB CAs

Der X.500 Distinguished Name in den Zertifikaten der Dataport SUB CAs, welche durch die Dataport ROOT CA 02 ausgestellt werden, lautet:

Attribute	Werte
Common Name (CN)	Dataport CA <Nummer>
Organization (O)	Dataport AöR
Country (C)	DE

3.1.1.3 Personenbezogene Zertifikate

Der X.500 Distinguished Name im Zertifikat für die End-Entitäten, welches durch die Dataport CA 03 oder Dataport CA 05 ausgestellt wird, lautet:

Attribute	Werte	Pflicht
emailAddress (E)	< E-Mail Adresse des Benutzers>	Nein
Common Name (CN)	<Common Name des Benutzers>	Ja
Organization Unit (OU)	<Behörde>	Ja
Organization (O)	Dataport AöR	Ja
Country (C)	DE	ja

3.1.2 Anforderungen und Regelungen für Namen

Der Distinguished Name muss den Zertifikatsinhaber eindeutig identifizieren. Ist der DN nicht ausreichend, können zur Einhaltung der Eindeutigkeit eines Namens auch weitere Attribute wie die E-Mail-Adresse der Subject Alternative Name herangezogen werden. Bei der Namensvergabe sind folgenden Regelungen wirksam:

- Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden.
  - Bei Authentisierungszertifikaten für Benutzer wird der Common Name für Benutzer aus dem Vor- und Zunamen des Zertifikatsinhabers gebildet. Der Subject Alternative Name (SAN) wird aus dem User Principal Name (UPN) des Zertifikatsnehmers in der Form Anmeldename@<Anmeldedomain>.de gebildet.
  - Bei Verschlüsselungs- und Signaturzertifikaten für Benutzer wird der Common Name für Benutzer aus dem Vor- und Zunamen des Zertifikatsinhabers gebildet und der SAN in der Form von „Vorname.Nachname@<eMaildomain>.de“ gebildet.
  - Bei Signaturzertifikaten für Code und Dokumente wird der Common Name aus der „Behörde/Firma/Institution + CodeSigning“ gebildet (z.B. „Dataport CodeSigning“).
  - Bei den Authentisierungszertifikaten für Endgeräte bzw. Web Sites wird der Common Name entweder aus dem DNS Namen oder GeräteID des Endgerätes oder der URL der Webseite gebildet. Der Subject Alternative Name kann aus dem DNS Namen des Servers, der URL der

Webseite beziehungsweise des Dienstes oder dem Netbios Namen des Servers gebildet werden. Der alternative Name in den Authentifikationszertifikaten für Maschinen enthält den DNS Namen der Maschine beziehungsweise die Web Server URL in der Form MachineName.<Anmeldedomain>.de

- Der DN der Dataport Zertifizierungsstellen wird durch die Namens-Objekte Common Name, Organisation, und Country gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.
- Der DN der Authentisierungszertifikate wird durch die Namens-Objekte emailAddress (optional), Common Name, Organisation Unit, Organisation und Country gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten und im SAN der UPN zu gewährleisten.
- Der DN der Verschlüsselungs- und Signaturzertifikate wird durch die Namens-Objekte emailAddress, Common Name, Organisation Unit, Organisation und Country des Benutzers gebildet. Eine Eindeutigkeit des DNs ist mit diesen zur Verfügung stehenden Namensobjekten zu gewährleisten. Im Subject Alternative Name ist die E–Mail-Adresse des Inhabers in der Form Vorname.Nachname@%maildomain des Kunden%.de enthalten.
- Der DN der Signaturzertifikate für Code und Dokumenten wird durch die Namens-Objekte Common Name, Organisation Unit, Organisation und Country des Benutzers oder einer Gruppe (Organisationseinheit) gebildet. Im Common Name ist bei einer Gruppen dem Namen das Kennzeichen „GRP:“ voranzustellen. Eine Eindeutigkeit des DNs ist mit diesen zur Verfügung stehenden Namensobjekten zu gewährleisten. Eine Verwechslung mit existierenden Namen muss ausgeschlossen sein. Dabei dürfen keine Domänen-Namen oder IP-Adressen verwendet werden.
- Jedem Zertifikat wird eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.

3.1.3 Anonymität und Pseudonyme von Zertifikatsinhabern

Abgesehen von technischen Konten (Service Zertifikate für das Managementsystem) sind Zertifikatsinhaber (natürliche Personen und Maschinen) nicht anonym noch werden zur Kennung von Zertifikatsinhabern Pseudonyme verwendet. Jedem Zertifikatsinhaber (Personen und Maschinen) können daher die Zertifikate eindeutig zugeordnet werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Die ausgewiesenen Distinguished Names im Zertifikatsprofil folgen dem X.500 Standard.
Die E-Mail Adressen und UPN Einträge im Zertifikatsprofil folgen dem RFC 822 Regelwerk. UPN Namensinformationen müssen UTF-8 encodiert vorliegen.

3.1.5 Eindeutigkeit von Namen

Der komplette Distinguished Name in den von Dataport ausgestellten Zertifikaten erlaubt die Eindeutigkeit von Namen, sowohl der Dataport Zertifizierungsstellen als auch der Namen für die Zertifikatsnehmer.
Eine zusätzliche Kennung im alternativen Namensfeld, nämlich die eindeutige E-Mail Adresse, UPN Namen und Maschinen DNS Namen sowie eine eindeutige Seriennummer in den Zertifikaten, berücksichtigen diesen Aspekt.

3.1.6 Erkennen, Authentifizierung und Rolle von Warenzeichen

In der Regel beschränkt sich der DN auf natürliche Personen und Maschinen und hat somit keine Relevanz in der Anerkennung von Warenzeichen. Grundsätzlich ist der Zertifikatsnehmer und auch der

Zertifizierungsstellenbetreiber verpflichtet, aufgrund der automatisierten Ausstellung von End-Entitäten Zertifikaten, den Schutz von Warenzeichen zu gewährleisten.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Überprüfung des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Zertifikatsinhaber werden auf der beantragenden Maschine oder auf Smartcards für Benutzerzertifikate generiert. Der Besitznachweis für die privaten Schlüssel erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der Certificate Signing Request (CSR) ist die Basis der Überprüfung von privaten Schlüsseln.
Die Schlüsselpaare der Dataport Zertifizierungsstellen werden durch das HSM generiert. Der Besitznachweis für die privaten Schlüssel zu den CA Zertifikaten erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der CSR ist die Basis der Überprüfung von privaten Schlüsseln.

3.2.2 Authentifikation von Organisationen

Die Vergabe der Prüfung von Identitäten kann durch Dataport auf der Basis von rechtlichen Vorgaben an Kunden delegiert werden.

Die Prüfung externer Zertifikatsinhaber, die nicht bei Kunden von Dataport bzw. bei Dataport selbst angestellt sind, unterliegt den gleichen Anforderungen und Regelungen wie unter 3.2.3 beschrieben.

3.2.3 Authentifikation von Zertifikatsnehmern

Für die Erstausstattung von Zertifikaten für Benutzer findet eine Identitätsprüfung durch die Registrierungsstelle statt. Sie kann sich hierzu auch eines externen Dienstleisters (z.B. PostIdent) bedienen. Bei der Prüfung werden die notwendigen Maßnahmen ergriffen um die Identität eines Antragsstellers eindeutig festzustellen. Die Detailverfahren zur Identitätsprüfung können aus den Prozessabläufen für die Ausgabe der entsprechenden Zertifikate entnommen werden. Die Prozessabläufe sind durch den jeweiligen Kunden selbst festzulegen, zu beschreiben und zu dokumentieren.
Für teilnehmende Benutzer und Maschinen wird im Falle einer automatisierten Ausgabe von Zertifikaten die Authentifikation durch ein valides Konto in einem Dataport Verzeichnisdienst mittels Kerberos durchgeführt. Für teilnehmende Maschinen wird im Falle einer kontrollierten Ausgabe von Zertifikaten die Authentifikation durch ein valides Benutzer-Konto in einem Dataport Verzeichnisdienst mittels Kerberos durchgeführt. Hierbei beantragt ein Benutzer das Zertifikat für die Maschine, z. B. für Web Server. Eine Beantragung von diesen Zertifikaten kann nur nach erfolgreicher Benutzerauthentifizierung erfolgen.

3.2.4 Nicht überprüfte Informationen des Zertifikatsnehmers

Es werden nur die Informationen des Zertifikatsnehmers überprüft, welche im Rahmen der Authentifikation und Identifikation des Zertifikatsnehmers notwendig sind. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt

3.2.5 Prüfung zur Berechtigung der Antragstellung

Für die Ausgabe von Benutzerzertifikaten findet eine Überprüfung der Berechtigung zur Antragsstellung statt. Die Detailverfahren zur Prüfung der Berechtigung können aus den Prozessabläufen für die Ausgabe der entsprechenden Zertifikate entnommen werden
Für automatisiert erstellte Maschinenzertifikate sind einzig die Zugehörigkeit in der zulässigen Dataport Domäne und ein valides Kerberoskonto ausschlaggebend und dienen als Berechtigungsnachweis.

3.2.6 Kriterien für Cross-Zertifizierung und Interoperation

Zurzeit nicht zutreffend, da keine Cross-Zertifizierung mit anderen Organisationen geplant bzw. implementiert ist.

3.3 Identitätsprüfung und Authentifikation bei Zertifikatserneuerung

Für die Identifizierung und Authentifizierung bei einer routinemäßigen Zertifikatserneuerung mit Schlüsselwechsel (d.h. bei der Ausstellung eines neuen Zertifikates zu einem neuen Schlüssel kurz vor dem regulären Ablauf des alten Zertifikates) ist eine erfolgreiche Anmeldung mit dem persönlichen Kennwort oder im Falle von Smartcards die Anmeldung mittels Smartcard und zusätzlich einem „Einmal“ Kennwort für Benutzer ausreichend.

3.3.1 Prüfung bei routinemäßiger Erneuerung

Die Erneuerung von Benutzerzertifikaten erfolgt automatisiert durch die Dataport PKI und die zugehörigen Managementsysteme. Betroffene Zertifikatsnehmer werden über die anstehende Erneuerung informiert oder ihr Zertifikat erneuert sich automatisch. Zur Erneuerung von Zertifikate auf sicheren Trägermedien wird eine Authentifikation am Zertifikatsmanagementsystem mittels dieses Mediums und einem Einmal Kennwort erzwungen.
Für teilnehmende Maschinen wird im Falle einer automatisierten Erneuerung von Zertifikaten die Authentifikation durch ein valides Maschinen-Kerberoskonto in der Dataport Active Directory Domäne durchgeführt.
Für teilnehmende Maschinen wird im Falle einer kontrollierten Erneuerung von Zertifikaten die Authentifikation durch ein valides Benutzer-Kerberoskonto in der Dataport Active Directory Domäne durchgeführt. Der zugehörige Antragsteller für die Maschine wird vor Ablauf der Zertifikatslebensdauer mittels E-Mail informiert. Hierbei beantragt ein Benutzer das Zertifikat für die Maschine, z. B. für Web Server. Eine Beantragung von diesen Zertifikaten kann nur nach erfolgreicher Benutzerauthentifizierung erfolgen.

3.3.2 Prüfung bei Zertifikatserneuerung nach erfolgtem Zertifikatsrückruf

Die Identifizierung und Authentifizierung bei einer Zertifikatserneuerung nach einer Sperrung entspricht den unter 3.2.3 beschriebenen Kriterien der initialen Registrierung.

3.4 Identitätsprüfung und Authentifikation bei Zertifikatsrückruf

Für Benutzerzertifikate existiert ein Antragswesen. Die Prozesse für die Identifikation und Authentifikation beim Zertifikatsrückruf sind im Antragswesen beschrieben und niedergelegt. Grundsätzlich kann das Zurückziehen von Zertifikaten durch den Vorgesetzten des Zertifikatsinhabers beauftragt werden. Die Detailverfahren zum Zertifikatsrückruf können aus den Prozessabläufen für die Ausgabe der entsprechenden Zertifikate entnommen werden.
Der Zertifikatsrückruf von verwalteten Maschinenzertifikaten erfolgt durch Informationen an den Bereich Zertifikatsdienste. Weitergehende Informationen zum Einsatzbereich der Dataport PKI können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.
Zertifikate für Dataport verwaltete Maschinen, die automatisch mit Zertifikaten versehen wurden, werden ebenso zurückgezogen. Weitergehende Informationen zum Einsatzbereich der Dataport PKI können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.

4 Betriebliche Anforderungen an den Zertifikatslebenszyklus

Im folgenden Abschnitt werden die grundsätzlichen Parameter der Dataport PKI aufgezeigt. Die Dataport PKI dient der Ausgabe und Verwaltung von Benutzer- als auch Maschinenzertifikaten.
Für die Abbildung der Prozesse der Ausgabe und Verwaltung von Benutzerzertifikaten wird durch Dataport ein Management Tool genutzt, das Dataport für seine Kunden betreibt und verwaltet.
Dataport ist somit in der Lage auf rechtliche Rahmenbedingungen seiner Kunden reagieren zu können und die Identitätsprüfung sowie die Beantragung von Benutzerzertifikaten an Dritte zu delegieren.

Nutzung von Dataport Benutzerzertifikaten auf sicheren Trägermedien:

Die Nutzung von Dataport Benutzerzertifikaten auf Smartcards dient zur Windows Netzwerkanmeldung und zur Authentifikation auf Web Servern. Des Weiteren werden Zertifikate für Benutzer ausgegeben, die neben der Authentifikation auch zur Verschlüsselung und zum Erstellen einer digitalen Signatur herangezogen werden können.
Detaillierte Anwendungsfälle können aus den Dataport Zertifikatsprofilen entnommen werden.
Folgende technische Rahmenbedingungen sind hervorzuheben:

- Benutzerzertifikate liegen auf der Smartcard/Token vor.
- Die Verwaltung und Ausgabe von Dataport Benutzerzertifikaten obliegt der Kontrolle durch das zentrale Zertifikatsmanagementtool.
- Zugehörige CPS, CRL und CA-Zertifikate sind intern und extern veröffentlicht. Dies ermöglicht eine problemlose interne und externe Kommunikation.
- Für Smartcard Logon in Windows Netzwerken ist die Verfügbarkeit von Sperrlisteninformationen zwingend erforderlich.
- S/MIME Zertifikate können in den für das entsprechende Verfahren relevanten von Dataport verwalteten Verzeichnisdiensten veröffentlicht werden.
- Eine Schlüsselarchivierung von Verschlüsselungsschlüsseln ist etabliert.

Nutzung von Dataport Benutzerzertifikaten ohne sichere Trägermedien:

Die Nutzung von Dataport Benutzerzertifikaten dient zur Verschlüsselung und zum Erstellen digitaler Signaturen.
Detaillierte Anwendungsfälle können aus den Dataport Zertifikatsprofilen entnommen werden.
Folgende technische Rahmenbedingungen sind hervorzuheben:

- Zugehörige CPS, CRL und CA-Zertifikate sind intern und extern veröffentlicht. Dies ermöglicht eine problemlose interne und externe Kommunikation.
- S/MIME Zertifikate können in den, für das entsprechende Verfahren relevante, von Dataport verwalteten Verzeichnisdiensten veröffentlicht werden.
- Eine Schlüsselarchivierung von Verschlüsselungsschlüsseln ist etabliert.

Nutzung von Dataport Maschinenzertifikaten:

Die Nutzung von Dataport Maschinenzertifikaten dient ausschließlich der Authentifikation von Maschinen.
Folgende technische Rahmenbedingungen sind hervorzuheben:

- Eine CRL Überprüfung von Maschinen ist nicht applikationsübergreifend konfiguriert. Diese ist applikationsabhängig durchzuführen.
- Zugehörige CPS, CRL und CA-Zertifikate sind intern und extern veröffentlicht. Dies ermöglicht eine problemlose interne und externe Kommunikation.

- Als Verschlüsselung von Kommunikationsbeziehungen zwischen Maschinen kommen TLS oder IPSec zum Einsatz.

Weitergehende Informationen zum Einsatzbereich der Dataport PKI können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.

4.1 Zertifikatsantrag

Zertifikatsantrag für Dataport CA 03:

Die Erstbeantragung und die Verlängerung von Benutzerzertifikaten erfolgt kontrolliert durch ein Zertifikats- und Smartcard-Managementtool. Benutzerbezogene Zertifikate werden auf einer Smartcard provisioniert. Hierbei untersteht die Zertifikatslebenszyklusverwaltung und respektive die Smartcardverwaltung der Kontrolle des Managamentsystems.

Zertifikatsantrag für Dataport CA 04:

Zertifikatsantrag nicht-Domänenintegrierter Endgeräte:

Die Erst-Beantragung und die Verlängerung eines Maschinenzertifikats für von Dataport betreuten Endgeräten erfolgt kontrolliert durch entsprechende Managementtools.

Zertifikatsantrag domänenintegrierter Endgeräte:

Die Erstbeantragung und die Verlängerung eines Maschinenzertifikats für Dataport domänenintegrierte Endgeräte erfolgt automatisiert über Gruppenrichtlinien. Dies bezieht sich auf alle domänenintegrierten Endgeräten mit einem validen Kerberoskonto in der Dataport Domäne. Eine Unterscheidung erfolgt anhand der Rolle der Maschine. Den Domänencontrollern werden hierbei angepasste Zertifikate zur Verfügung gestellt.

Zertifikatsantrag für Dataport CA 05:

Die Erstbeantragung und die Verlängerung eines Benutzerzertifikats erfolgt automatisiert über Gruppenrichtlinien. Die Ausstellung ist abhängig von einem validen Benutzer- und Maschinenkontos in der entsprechenden Domäne.

Zertifikatsantrag für Dataport CA 06:

Die Erstbeantragung und die Verlängerung eines Maschinenzertifikats erfolgt automatisiert über Gruppenrichtlinien. Die Ausstellung ist abhängig von einem validen Maschinenkonto in der entsprechenden Domäne.

Weitergehende Informationen zum Einsatzbereich der PKI, sowie zum Zertifikatsantrag, können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden. Die Detailverfahren zum Zertifikatsantrag von Benutzerzertifikaten sind aus den Prozessabläufen für die Ausgabe von Smartcards zu entnehmen.

4.1.1 Antragsberechtigt für Zertifikate

Antragsberechtigt für ein Benutzerzertifikat aus der Dataport PKI sind

- Alle Mitarbeiter von Dataport
- Alle Mitarbeiter der öffentlichen Verwaltung eines Kunden von Dataport
- Externe Mitarbeiter, die bei Dataport oder einer öffentlichen Verwaltung eines Kunden von Dataport beschäftigt bzw. für diese tätig sind
- von Dataport betriebene Maschinen/Computer
    - Dataport Maschinen, die in von Dataport betreuten Domänen integriert sind

- Dataport Maschinen, die nicht in von Dataport betreuten Domänen integriert sind
- Dataport Web Server

4.1.2 Ausgabeprozess und Verantwortlichkeiten

Die Ausgabe der Benutzerzertifikate erfolgt durch die ausgebende Dataport CA 03 oder Dataport CA 05. Die technische Verantwortlichkeit für den Ausgabeprozess obliegt dem Bereich Zertifikatsdienste bei Dataport. Die organisatorische Verantwortung des jeweiligen Ausgabeprozesses obliegt den teilnehmenden Kunden selbst. Eine detaillierte Beschreibung des Ausgabeprozesses und der technischen Umsetzung kann bei Bedarf vom Bereich Zertifikatsdienste erfragt werden. Die Detailverfahren zum Ausgabeprozess von Benutzerzertifikaten sind aus den jeweiligen Prozessabläufen zu entnehmen.

Die Ausgabe von Maschinenzertifikaten erfolgt durch die Dataport CA 04 und Dataport CA 06.

4.2 Prozess der Antragsbearbeitung

Der Prozess der Bearbeitung der Anträge - wie auch die Beantragung selbst – werden sofern möglich durch ein Management Tool unterstützt.

Detailinformationen zur Antragsbearbeitung können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.

4.2.1 Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung des Antragsstellers erfolgt auf Basis der bestehenden validen AD Domänenkonten in den von Dataport betreuten und betriebenen Verzeichnisdiensten. Dies gilt sowohl für Benutzer als auch für Maschinen. Bei der manuellen Antragsbearbeitung von Zertifikaten muss ein valides Benutzerkonto zur Authentifikation existieren.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Annahme oder Ablehnung des Antragsstellers erfolgt auf Basis etablierter Beantragungsprozesse und Prüfung des Zertifikatsantrags. So findet eine Überprüfung der Antragsberechtigung wie in 4.1.1 beschrieben statt. Dies gilt sowohl für Benutzer als auch für Maschinen.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitung der Zertifikatsanträge ergibt sich aus den jeweils mit dem Kunden abgestimmten Prozessen.

4.3 Zertifikatsausgabe

Die Ausgabe von manuell beantragten Benutzer- und Maschinenzertifikaten ist ein kontrollierter Prozess durch das Zertifikatsmanagementsystem.
Bei Zertifikaten, die nicht durch das Zertifikatsmanagementsystem ausgegeben werden, stellt die Zertifikatsausgabe einen automatischen Prozess dar.

Weitergehende Informationen zur Zertifikatsausgabe können bei Bedarf erfragt werden. Die Detailverfahren zum Ausgabeprozess von Benutzerzertifikaten sind aus den jeweiligen Prozessabläufen zu entnehmen.

4.4 Zertifikatsannahme

Zertifikate, die durch die Dataport PKI signiert wurden, gelten als gültig und benötigen keine Annahme durch den Antragsteller.

Die Detailverfahren zum Ausgabeprozess von Benutzerzertifikaten sind aus den jeweiligen Prozessabläufen zu entnehmen.

4.4.1 Publikation der Zertifikate

Im Falle von S/MIME Verschlüsselungszertifikaten kann die Publikation der End-Entitäten-Zertifikate automatisiert durch die PKI im Verzeichnisdienst des jeweiligen Trägerlandes erfolgen. Ein Eingreifen durch den Nutzer ist hierzu nicht notwendig.

Die Publikation der Dataport CA Zertifikate wird manuell durch den Bereich Zertifikatsdienste ausgeführt.

4.4.2 Ausgabebenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Dataport CAs findet nicht statt.

4.5 Schlüsselpaar- und Zertifikatsverwendung

Grundsätzlich ist der Gebrauch des Schlüsselpaares für die unter 1.4 genannten Verwendungszwecke zulässig.

4.5.1 Nutzung des privaten Schlüssels und Zertifikats durch den Zertifikatsnehmer

Die Nutzung der Zertifikate durch den Zertifikatsinhaber hat den Dataport Zertifikatsrichtlinien zu folgen. In Kapitel 1.4 Zertifikatsnutzung sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Außerdem muss der Zertifikatsnehmer bei der Nutzung der privaten Schlüssel seine in der Dataport Policy für Smartcards definierten Pflichten erfüllen.
In Ergänzung dessen sind der Zertifikatsnehmer bei Benutzerzertifikaten und der Antragssteller bei Maschinenzertifikaten verpflichtet:

- Den privaten Schlüssel zu schützen
- Ein unautorisiertes Duplizieren der Schlüsselpaare zu verhindern
- Wann immer möglich eine Prüfung der CRL und der Zertifikatskette durchzuführen

Im Fall der vermuteten oder tatsächlichen Kompromittierung des Schlüsselpaares ist sofort der Helpdesk oder die Mitarbeiter der RA zu informieren, die Zertifikate zu sperren und die Nutzung der Zertifikate einzustellen.

4.5.2 Nutzung des privaten Schlüssels und Zertifikats durch vertrauende Parteien

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien seiner Organisation zu folgen. Dort sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt.

4.6 Zertifikatserneuerung ohne Schlüsselwechsel

In Rahmen der Dataport PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Zertifikatserneuerung mit gleichen Schlüsselpaaren, sprich ohne Schlüsselwechsel, ist nicht vorgesehen. Daher sind alle nachfolgenden Punkte unter 4.6. für die Dataport PKI nicht zutreffend.

4.6.1 Umstände für eine Zertifikatserneuerung

nicht zutreffend.

4.6.2 Antragsberechtigte für eine Zertifikatserneuerung

nicht zutreffend.

4.6.3 Durchführen einer Zertifikatserneuerung

nicht zutreffend.

4.6.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

nicht zutreffend.

4.6.5 Verfahren zur Annahme der Zertifikatserneuerung

nicht zutreffend.

4.6.6 Publikation des erneuerten Zertifikats durch die CA

nicht zutreffend.

4.6.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

nicht zutreffend.

4.7 Zertifikatserneuerung mit Schlüsselwechsel

In Rahmen der Dataport PKI findet die Zertifikatserneuerung für bestimmte Zertifikatstypen mit Schlüsselwechsel und ohne Datenanpassung statt.

4.7.1 Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel

Die Zertifikatserneuerung mit Schlüsselwechsel und ohne Datenanpassung kann beantragt werden, wenn die folgenden Voraussetzungen erfüllt sind:

- die Gültigkeitsdauer des aktuellen Zertifikats ist abgelaufen oder steht kurz vor Ablauf
- der alte Schlüssel kann oder darf nicht mehr verwendet werden, weil er verloren oder (möglicherweise) kompromittiert wurde
- die eingesetzten kryptographischen Algorithmen bieten keine ausreichende Sicherheit mehr
- die im Zertifikat enthaltenen Daten sind nicht korrekt

4.7.2 Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Siehe 4.1.1 wie Erstantrag.

4.7.3 Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.7.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Eine Erneuerungsbenachrichtigung ist bei automatisiert ausgegebenen Zertifikaten nicht erforderlich. Vor Ablauf der Zertifikatsgültigkeitsdauer wird ein automatisierter Erneuerungsprozess durch die Dataport PKI angestoßen.

Bei der kontrollierten Ausgabe- und Erneuerung durch das Zertifikatsmanagementsystem wird eine Erneuerungsbenachrichtigung an den Antragssteller per E-Mail versendet.

4.7.5 Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.7.6 Publikation des erneuerten Zertifikats durch die CA

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.7.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Endentitäten findet nicht statt.

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

In Rahmen der Dataport PKI findet die Zertifikatserneuerung für bestimmte Zertifikatstypen mit Schlüsselwechsel und mit Datenanpassung statt. Eine Anpassung der Zertifikatsinhalte (Datenanpassung) ist vorgesehen, da sich Personendaten wie E-Mail Adresse und Namen über die Laufzeit hin verändern können. Technisch betrachtet handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel (respektive auch neuem privaten Schlüssel) und möglicher Anpassung von Inhaltsdaten.

4.8.1 Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Die Zertifikatserneuerung mit Schlüsselwechsel und mit Datenanpassung muss beantragt werden, wenn sich die maschinen- oder personen-bezogenen Daten geändert haben.

4.8.2 Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Siehe auch 4.1.1 wie Erstantrag.

4.8.3 Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.8.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Eine Erneuerungsbenachrichtigung ist bei automatisiert ausgegebenen Zertifikaten für Maschinen nicht erforderlich. Vor Ablauf der Zertifikatsgültigkeitsdauer wird ein automatisierter Erneuerungsprozess durch die Dataport PKI angestoßen.
Bei der kontrollierten Ausgabe- und Erneuerung durch das Zertifikats- und Smartcard-Managementsystem wird eine Erneuerungsbenachrichtigung an den Antragssteller per E-Mail versendet.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.8.6 Publikation des erneuerten Zertifikats durch die CA

Der Prozess erfolgt analog der Erst-Antragsstellung.

4.8.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten (Benutzer und Maschinen) durch die Dataport CAs findet nicht statt.

4.9 Zertifikatssperrung und -suspendierung

Im Folgenden werden die Umstände für eine Sperrung eines Zertifikates erläutert. Eine Suspendierung von Zertifikaten ist nur im Rahmen der Ausgabe von temporären Smartcards vorgesehen.

4.9.1 Umstände für die Sperrung

Ein Zertifikat ist in den folgenden Fällen zu sperren:

- Wenn eine Smartcard entwendet, beschädigt oder verloren wurde, d.h. eine permanente Ersatzkarte mit neuen Zertifikaten ausgestellt wird.
- Wenn der berechtigte Verdacht besteht, dass der private Schlüssel kompromittiert wurde.
- Wenn der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptographischen Algorithmen oder Geräte die Fälschungssicherheit der erzeugten Signaturen nicht mehr gewährleisten.
- Wenn zum Zertifikat, eine Zertifikatserneuerung mit Schlüsselwechsel beantragt wurde.
- Wenn Dataport die Zertifizierungsdienste einstellt. In diesem Fall werden sämtliche von den Zertifizierungsdiensten ausgestellten Zertifikate gesperrt.
- Wenn der Zertifikatseigentümer die Voraussetzungen nicht mehr erfüllt, die zur Ausstellung des Zertifikats geführt haben, z.B. weil der Mitarbeiter aus dem Dienst ausscheidet oder gegen die bestehende Zertifikatsrichtlinie verstoßen wird.

4.9.2 Antragsberechtigte für eine Sperrung

Folgende Personenkreise und Instanzen sind berechtigt Zertifikate zu sperren:

- die Sperrung eines Zertifikats kann durch
  - den Zertifikatsnehmer selbst (Zertifikatsinhaber),
  - seinen Vorgesetzten oder
  - durch einen Mitarbeiter der RA beantragt werden
- Die Sperrung von CA Zertifikaten kann durch die Leitung des Dataport Zertifizierungsdienstes veranlasst werden.

4.9.3 Durchführung einer Zertifikatssperrung

Die Zertifikatssperrung erfolgt durch einen Mitarbeiter der entsprechenden RA. Die Identifikation des Antragsberechtigten wird mit geeigneten Mitteln ausgeführt. Nähere Informationen dazu können vom Bereich Zertifikatsdienste erfragt werden. Die Sperrung hat endgültig zu erfolgen.

4.9.4 Meldefrist von Sperranträgen für Zertifikatsnehmer

Es sind keine vorgeschriebenen Fristen festgelegt. Grundsätzlich soll eine Meldung von Sperranträgen direkt und unverzüglich erfolgen.

4.9.5 Bearbeitungsdauer von Sperranträgen durch die CA

Sobald ein Sperrantrag vorliegt, muss die Sperrung unverzüglich innerhalb eines Tages erfolgen.

4.9.6 Prüfung des Zertifikatsstatus durch vertrauende Parteien

Eine Überprüfung des Zertifikatsstatus durch vertrauende Parteien ist erforderlich. Der Sperrstatus von Dataport Zertifikaten und von Dataport Zertifizierungsstellen Zertifikaten können über die entsprechenden Sperrlisten und OCSP geprüft werden. Die aktuellen Zertifikatssperrlisten können durch die in den Zertifikat enthaltenen CDPs (CRL Distribution Points) und OCSP heruntergeladen bzw. geprüft werden.

4.9.7 Ausstellungszeiträume für CRLs

Folgende Ausgabeschemata sind für die Dataport PKI gültig:
Dataport ROOT CA 02:

- CRL Veröffentlichungsperiode: 6 Monate
- CRL Veröffentlichung Überlappungsperiode: 3 Monate

Dataport CA 03:

- CRL Veröffentlichungsperiode: 1 Tag
- CRL Veröffentlichung Überlappungsperiode: 1 Tag
- Delta CRL Veröffentlichungsperiode: 2 Stunden
- Delta CRL Veröffentlichung Überlappungsperiode: 2 Stunden

Dataport CA 04:

- CRL Veröffentlichungsperiode: 8 Tage
- CRL Veröffentlichung Überlappungsperiode: 2 Tage
- Delta CRL Veröffentlichungsperiode: 6 Stunden
- Delta CRL Veröffentlichung Überlappungsperiode: 6 Stunden

Dataport CA 05:

- CRL Veröffentlichungsperiode: 1 Tag
- CRL Veröffentlichung Überlappungsperiode: 1 Tag
- Delta CRL Veröffentlichungsperiode: 2 Stunden
- Delta CRL Veröffentlichung Überlappungsperiode: 2 Stunden

Dataport CA 06:

- CRL Veröffentlichungsperiode: 5 Tage
- CRL Veröffentlichung Überlappungsperiode: 5 Tage
- Delta CRL Veröffentlichungsperiode: 6 Stunden
- Delta CRL Veröffentlichung Überlappungsperiode: 6 Stunden

4.9.8 Maximale Latenz von CRLs

Die CRLs stehen sofort nach Veröffentlichung auf den Dataport Sperrlistenveröffentlichungspunkten zur Verfügung. Eine Verzögerung in der Prüfung kann sich durch clientseitige Mechanismen ergeben.

4.9.9 Online Sperrung und Statusprüfung von Zertifikaten

Online Sperrung und Statusprüfung ist für die Dataport PKI mittels OCSP implementiert.

4.9.10 Anforderung für die Online Prüfung des Sperrstatus

Die Online Prüfung des Sperrstatus ist jederzeit aus dem internen und externen Netz bereitgestellt. Für die Verwendung der Online Sperrprüfung muss ein RFC6960 kompatibler OCSP-Resolver verwendet werden.

4.9.11 Weitere Arten zur Bekanntmachung von Zertifikatsstatus

Es sind keine weiteren Arten zur Bekanntmachung des Zertifikatsstatus vorgesehen. Die Sperrlisten werden auf ausfallsicheren Webservern veröffentlicht, welche im Zertifikat über die CDP Einträge bekannt gemacht werden.

4.9.12 Spezielle Maßnahmen bei Schlüsselkompromittierung

Bei einem Hinweis einer Schlüsselkompromittierung wird eine entsprechende Untersuchung durchgeführt. Sollte die Kompromittierung sich als stichhaltig erweisen, ist ein Sperrvorgang gemäß 4.9.3 einzuleiten.

4.9.13 Umstände für eine Suspendierung

Die Suspendierung (temporäre Sperrung) von Zertifikaten ist bei der Ausgabe von temporären Smartcards vorgesehen.

4.9.14 Berechtigte für eine Suspendierung

Da sich die Prozesse für die Smartcard-Verwaltung je nach Bedarfsträger unterscheiden können, sind Detailinformationen aus den jeweiligen Prozessbeschreibungen für Smartcards der beteiligten Bedarfsträger zu entnehmen.

4.9.15 Durchführung einer Suspendierung

Da sich die Prozesse für die Smartcard-Verwaltung je nach Bedarfsträger unterscheiden können, sind Detailinformationen aus den jeweiligen Prozessbeschreibungen für Smartcards der beteiligten Bedarfsträger zu entnehmen.

4.9.16 Dauer einer Suspendierung

Da sich die Prozesse für die Smartcard-Verwaltung je nach Bedarfsträger unterscheiden können, sind Detailinformationen aus den jeweiligen Prozessbeschreibungen für Smartcards der beteiligten Bedarfsträger zu entnehmen.

4.10 Auskunftsdienste für den Zertifikatsstatus

Dataport betreibt Auskunftsdienste über den Zertifikatsstatus. Dieser Auskunftsdienst ist web-basiert.
Alternativ zur Publikation von Zertifikatssperrlisten wird ein OCSP (Online Certificate Status Protocol) Responder Dienst für die Zertifikatsvalidierung bereitgestellt. Dieser Dienst kann von allen Systemen angesprochen werden, die über eine OCSP Client Komponente verfügen.

4.10.1 Betriebliche Ausprägung

Der Auskunftsdienst ist webbasierend und verwendet als Übertragungsprotokoll http.
Die Informationen können unter den URLs aus 2.2 abgerufen werden.
Die CRLs und zu sperrenden Zertifikate müssen von der gleichen Zertifizierungsstelle ausgegeben worden sein. Eine Unterstützung von „indirekten CRLs“ ist in der jetzigen Implementierung nicht gegeben.
Das ausgegebene CRL Profil ist RFC 5280 konform und entspricht dem X.509 Version 2 Standard.

4.10.2 Verfügbarkeit des Auskunftsdienstes

Die Verfügbarkeit der Dataport PKI Web-Server ist für einen 7 x 24h Betrieb ausgelegt.

4.10.3 Optionale Funktionen

Keine.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Ein Eigentümer oder Zertifikatsnehmer eines Dataport Zertifikats scheidet aus den Zertifizierungsdiensten aus, wenn er aus dem Arbeitsverhältnis der öffentlichen Verwaltung eines Kunden von Dataport oder von Dataport selbst ausscheidet bzw. sein Arbeitsverhältnis als externer Mitarbeiter endet.
Im Falle von Dataport Maschinen scheiden zugehörige Zertifikate aus, wenn die Maschinen nicht mehr durch Dataport betrieben werden oder ihnen neue Rollen zugewiesen werden.

4.12 Schlüsselhinterlegung und -wiederherstellung

Für die von Dataport betriebenen Zertifizierungsstellen werden die Schlüsselpaare auf einem Hardware Security Module (HSM) hinterlegt und in sicherer Umgebung abgelegt.
Im Falle von benutzerbezogenen Verschlüsselungszertifikaten wird eine Schlüsselhinterlegung und –wiederherstellung praktiziert. Für die Wiederherstellung von Benutzerschlüsseln wird auf eine Sicherungskopie der Schlüssel zurückgegriffen. Eine Detailbeschreibung dieses Prozesses kann vom Bereich Zertifikatsdienste erfragt werden.

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Im Rahmen der Dataport PKI wurde eine Wiederherstellungsrichtlinie erarbeitet. Eine Detailbeschreibung dieses Prozesses kann vom Bereich Zertifikatsdienste erfragt werden.

4.12.2 Richtlinien und Praktiken zur Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (symmetrischen Schlüsseln)

Nicht zutreffend. Sitzungsschlüssel werden DVGO konform nicht archiviert.

5 Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische- und Umgebungssicherheit

Die infrastrukturellen Sicherheitsmaßnahmen der Dataport PKI sind in den Rechenzentrumsbetrieb von Dataport eingebettet und unterliegen den dort geltenden Richtlinien. Die für die physikalische- und Umgebungssicherheit umgesetzten technischen und organisatorischen Maßnahmen gehen über die Standardmaßnahmen von IT-Grundschutz hinaus. Ein detaillierter Sicherheitsnachweis ist beim IT-Sicherheitsmanagement von Dataport verfügbar. Nachfolgende Vorkehrungen und physikalische Schutzmaßnahmen sind integraler Bestandteil der durch Dataport betriebenen Rechenzentren.
Der physikalische Zugang zur Hardware und Software der CAs, den HSMs und die Nutzung der auf den CAs betriebenen Dienste wird durch sicherheitstechnische Maßnahmen beschränkt.
Es haben nur vertrauenswürdige Personen entsprechend ihrer Rolle Zugang zur Hardware und Software der CAs.
Alle Komponenten der CAs werden in einer sicheren Umgebung betrieben.
Die Komponenten der RAs sind entsprechend der Vorgaben von Dataport durch die Kunden zu betreiben und unterliegen den generellen Richtlinien von Dataport.

5.1.1 Lage und Konstruktion

Die Systeme der Dataport PKI befinden sich in den Räumlichkeiten des Dataport Rechenzentrums. Die Räume bieten hinsichtlich der physikalischen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.
Das Rechenzentrum entspricht den Richtlinien für den sicheren Betrieb von Rechenzentren bei Dataport, in denen die Vorgaben des IT-Grundschutzes berücksichtigt sind. Weitergehende Informationen sind bei Bedarf nach Absprache erhältlich.

5.1.2 Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen gesichert. Ein Zutritt zu den Betriebsräumen der Zertifizierungsstelle wird nur Mitarbeitern gestattet, die die entsprechende Freigabestufe besitzen. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt.

5.1.3 Stromversorgung und Klimatisierung

Die Installation zur Stromversorgung entspricht den erforderlichen Normen, eine Klimatisierung der Räume für die technische Infrastruktur ist vorhanden.

5.1.4 Wasserschäden

Die Räume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Prävention und Schutz vor Feuer

Die bestehenden Brandschutzvorschriften werden eingehalten, eine Löschanlage sowie Handfeuerlöscher sind vorhanden.

5.1.6 Datenträger

Datenträger mit sensiblen Daten, wie z. B. HSM Hardware Tokens, werden in der Sicherheitszentrale aufbewahrt. Siehe 5.1.1.

5.1.7 Abfallentsorgung

Informationen auf elektronischen Datenträgern werden sachgemäß und sicher gelöscht und anschließend sachgerecht entsorgt. Papierdatenträger werden mittels vorhandenen Aktenvernichtern zerstört oder durch zertifizierte Dienstleister sachgerecht entsorgt.

5.1.8 Off-Site Backup

Der Dataport Rechenzentrumsbetrieb regelt die Anlage von Off-Site Sicherungen.

5.2 Organisatorische Sicherheitskontrollen

5.2.1 Sicherheitskritische Rollen

Sicherheitskritische Aufgaben werden für den Betrieb der Dataport PKI in Rollen zusammengefasst. Ein PKI Rollenkonzept ist verfügbar und wird für den organisatorischen Prozess und auch für den HSM Betrieb umgesetzt.
Mechanismen der sicheren Identifikation, Authentifikation und Autorisierung werden so weit wie möglich umgesetzt.
Eine Beschreibung der Rollendefinition kann bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.

5.2.2 Zugewiesene Zahl von Personen bei sicherheitskritischen Aufgaben

Das Vier-Augen-Prinzip gilt bei folgenden Operationen:

- Wiederherstellen des Schlüsselmaterials der Dataport Zertifizierungsstellen
- Wiederherstellen der Dataport Zertifizierungsstellen
- Zugriff auf die Hardware Security Module der Dataport Zertifizierungsstellen

5.2.3 Identifikation und Authentifikation der Rollen

Die Identifikation und Authentisierung der Benutzer erfolgt beim Zutritt zu sicherheitsrelevanten Räumen und beim Zugriff auf sicherheitsrelevante Systeme mit Hilfe von eToken, Smartcards, Hardware Tokens und/oder Benutzername und Passwort.
Bei besonders sicherheitskritischen Operationen wird das Vier-Augen-Prinzip angewendet.

5.2.4 Trennung von Rollen und Aufgaben

Das Rollenkonzept regelt, welche Zuordnungen von Personen zu Rollen sich gegenseitig ausschließen. Detailinformationen zur Rollen- und Aufgabentrennung können beim Bereich Zertifikatsdienste erfragt werden. Dabei gelten die folgenden Grundregeln:

- Leitende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Administrative Rollen dürfen keine operativen Aufgaben übernehmen

Daneben gelten weitere Ausschlüsse zur Trennung der folgenden sicherheitskritischen Verantwortlichkeiten:

- Einhaltung der Sicherheitsvorschriften und die Prüfung durch Audits
- Zutritt zu den Räumlichkeiten der Zertifizierungsstellen und Zugriff auf die internen Systeme

5.3 Sicherheitsmaßnahmen für das Personal

Dataport stellt im Rahmen der PKI erfahrenes Personal zur Verfügung. Notwendige Qualifikation, Wissenstand und Erfahrungswerte des Personals sind für den sicheren PKI Regelbetrieb vorhanden.

5.3.1 Anforderung an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Das zuständige Personal verfügt über die erforderlichen spezifischen Kenntnisse und Erfahrungen aus dem Bereich der PKI. Ebenso sind grundlegende IT Kenntnisse vorhanden um auch systemnahe Operationen auszuführen.
Das zuständige Personal ist sicherheitsüberprüft.

5.3.2 Prozess zur Sicherheitsüberprüfung von Mitarbeitern

Es gelten die allgemeinen Personaleinstellungsrichtlinien von Dataport. Vorzusehende Sicherheitsüberprüfungen sind rechtlich im Staatsvertrag von Dataport und in den Sicherheits-überprüfungsfeststellungsverordnungen der Trägerländer geregelt.

5.3.3 Trainingsanforderung

Das für den Zertifizierungsdienst eingesetzte Personal wird vor Aufnahme der Tätigkeit ausreichend geschult. Das Training beinhaltet auch eine Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit und potenzieller Bedrohungen.

5.3.4 Trainingsfrequenz

Die Frequenz der Trainings orientiert sich an den Anforderungen der Dataport PKI. Trainings werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Frequenz und Abfolge von Job Rotation

Eine Job Rotation ist nicht vorgesehen.

5.3.6 Sanktionen bei unzulässigen Handlungen

Die allgemeinen Sanktionsmöglichkeiten von Dataport werden bei unzulässigen Handlungen angewandt.

5.3.7 Vertragsbedingungen für das Personal

Das Dataport PKI Betriebspersonal verpflichtet sich auf die die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.
Diese Regelungen gelten auch für bei Dataport nicht direkt, sondern als Dienstleister, unter Vertrag stehendes Personal.

5.3.8 An das Personal ausgehändigte Dokumente

Folgende Dokumente werden dem Dataport Personal zum ordnungsgemäßen Betrieb der PKI zur Verfügung gestellt:

- Erklärung zum Zertifizierungsbetrieb oder Certification Practice Statement (CPS)
- Betriebskonzept und Sicherheitskonzept der PKI
- Handlungsanweisungen
- Betriebshandbücher der Systeme und Software

5.4 Überwachung von sicherheitskritischen Ereignissen

5.4.1 Protokollierte Ereignisse

Zu jedem Ereignis werden folgenden Daten erfasst:

- Zeitpunkt (Datum und Uhrzeit)
- Log ID des Eintrages
- Art des Ereignisses
- Ursprung des Ereignisses

Zusätzlich werden alle administrativen Tätigkeiten über die bei Dataport standardisierten Log- Mechanismen dokumentiert.

Die folgenden Ereignisse werden elektronisch protokolliert:

- Ereignisse im Lebenszyklus von Zertifikaten/Smartcards und Schlüsselpaaren:
  - Erstmalige Registrierung für Mitarbeiterzertifikate
  - Ausstellung von Zertifikaten
  - Veröffentlichung von Zertifikaten
  - Registrierung für eine Erneuerung von Zertifikaten
  - Sperranfragen an die CA durch die RA
  - Sperrungen
  - Erstellung von Sperrlisten
- Zusätzliche Ereignisse im Lebenszyklus von Smartcards:
  - Smartcard PIN Wechsel
  - Ausgabe von Ersatzkarten bei Verlust oder Diebstahl
  - Entsperrung von Smartcards
  - Temporäre Ausgabe von Smartcards
- Ereignisse im Lebenszyklus der Verschlüsselungsschlüsselpaare:
  - Generierung von Verschlüsselungsschlüsselpaaren
  - Archivierung (Backup) von privaten Verschlüsselungsschlüsseln
  - Wiederherstellung von privaten Verschlüsselungsschlüsseln

- Ereignisse im Lebenszyklus der HSMs:
  - Initialisierung eines HSM
  - Änderung der Konfiguration eines HSM
  - An- und Abmeldung an einem HSM
  - Generierung von Schlüsseln in einem HSM
  - Backup und Wiederherstellung von Schlüsseln in einem HSM
  - Löschen von Schlüsseln in einem HSM
- Systemereignisse und Fehlermeldungen der sicherheitskritischen Systeme:
  - Versuche zur An- und Abmeldung
  - Vergabe und Entzug von Zugriffsberechtigungen
  - Zugriffe und Zugriffsversuche per Netzwerk
- Ereignisse der Zutrittskontrollanlagen:
  - Betreten und Verlassen von gesicherten Räumen
  - Fehlgeschlagene Zutrittsversuche und Alarme
  - Vergabe und Entzug von Zutrittsberechtigungen
  - Beantragung, Ausgabe und Sperrung von Zutrittskarten

Ergänzend zu den elektronischen Log-Dateien werden auch Änderungen der Richtlinien und des Betriebshandbuchs erfasst:

- Rollendefinitionen
- Prozessbeschreibungen
- Wechsel der Verantwortlichkeiten

5.4.2 Überprüfungshäufigkeit von Log-Daten

In regelmäßigen Abständen wird eine Überprüfung der Log-Daten vorgenommen. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.[1]

5.4.3 Aufbewahrungsfristen von Audit Log-Daten

Sicherheitsrelevante Protokolldaten werden entsprechend den gesetzlichen Regelungen aufbewahrt.[2]

5.4.4 Schutzmaßnahmen von Audit Log-Daten

Elektronische Log-Dateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.

[1] Siehe „Revisionskonzept SV3“
[2] Siehe „Protokollierungskonzept SV3“

5.4.5 Audit Log-Daten Backup-Verfahren

Die Protokolldaten werden zusammen mit anderen relevanten Daten einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

5.4.6 Audit Collection System (Protokollierungssystem intern oder extern)

Alle Protokoll-Dateien werden regelmäßig gesichert.

5.4.7 Benachrichtigung bei Auslösen eines sicherheitskritischen Ereignisses

Eine Benachrichtigung des PKI Bedienerpersonals findet bei Auftreten von Produktionsproblemen statt.

5.4.8 Schwachstellenanalyse

Erfolgt regelmäßig durch Dataport und die Hersteller der Soft- und Hardware.

5.5 Archivierung von Protokolldaten

Dataport archiviert in Rahmen des PKI Betriebes die notwendigen Protokolldaten.

5.5.1 Archivierte Protokolldatentypen

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- Zertifikatanträge, diese enthalten persönliche Daten des Zertifikatnehmers
- Alle von der Zertifizierungsstelle ausgestellten Zertifikate
- Sperranträge für Zertifikate und für Zertifizierungsstellen Zertifikate
- Vor einer Modifikation eines Systems gesicherte Systemdaten
- Datensicherungen der Produktivsysteme
- Administrative Tätigkeiten auf den an der PKI beteiligten Systemen
- Dokumentation der personellen Sicherheitsmaßnahmen (z.B. Dokumentation der Sicherheitsüberprüfungen)
- Dokumentationen von Prozeduren und Systemen (z.B. Handlungsanweisungen, Notfallpläne, Systemhandbücher)
- Protokolle von sicherheitsrelevanten PKI Prozeduren und Prozessen:
  - Prozeduren der Schlüsselzeremonie
  - Prozeduren bei Installation und Konfiguration der Zertifizierungsstellen
  - Prozeduren bei Installation und Konfiguration der Personen PKI
  - Notfallprozeduren
  - Changemanagement-Prozeduren
  - Zugang zu den geschützten Räumlichkeiten durch externes Personal
  - Prüfung, Installation und Administration der HSMs
  - Ausgabe von Zutrittskarten zu geschützten Räumlichkeiten
  - Änderung, Kenntnisnahme oder Übergabe von PINs und Passwörtern für HSMs

- Änderungen in den Zuweisungen von Rollen

5.5.2 Archivierungsfristen

Zu archivierende Daten werden gemäß den gesetzlichen Anforderungen der Teilnehmer der Dataport PKI aufbewahrt.

5.5.3 Schutzmaßnahmen für das Archiv

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Sind in den Archiven personenbezogene Daten enthalten, wird darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.
Die Schutzmaßnahmen für elektronische Datenträger entsprechen den für den Rechenzentrumsbetrieb von Dataport vorgesehenen Prozessen.

5.5.4 Backup-Verfahren für das Archiv

Die Verfahren und Prozesse für das Archiv Backup folgt der für den Rechenzentrumsbetrieb von Dataport vorgesehenen Umsetzung.

5.5.5 Zeitstempelanforderungen für archivierte Daten

Audit Logs, protokollierte Ereignisse, archivierte Daten, Zertifikate, Zertifikatssperrlisten und andere Eintragungen enthalten jeweils eine eindeutige Zeit- und Datumsangabe. Datums- und Zeitangaben von Online-Systemen werden in regelmäßigen Abständen gegen eine vertrauenswürdige Zeitquelle synchronisiert.

5.5.6 Archivierungssystem (intern oder extern)

Ein Archivierungssystem wird im Rahmen der Dataport PKI eingesetzt.

5.5.7 Verfahren zur Beschaffung und Verifizierung von Archivdaten

Das Dataport PKI Betriebskonzept beschreibt die Prozesse für die Beantragung und Verifikation von Archivdaten. Eine Detailbeschreibung dieses Prozesses kann vom Bereich Zertifikatsdienste erfragt werden.

5.6 Schlüsselwechsel der Zertifizierungsstellen

Bei einem Schlüsselwechsel der Dataport ROOT CA 02 wird ein neues selbst-signiertes Zertifikat ausgestellt und veröffentlicht. Eine Sperrung des selbstsignierten ROOT CA 02 Zertifikats ist technisch auf der CA Seite nicht machbar.
Bei einem Schlüsselwechsel der Zwischenzertifizierungsstellen werden deren Zertifikate von der Dataport ROOT CA 02 ausgestellt und veröffentlicht. Die Beantragung selbst erfolgt durch die Dataport SUB CAs.
Die CA Zertifikatserneuerung mit Schlüsselwechsel folgt dem unten aufgeführtem Schema:

- Dataport ROOT CA 02 Zertifikat: 12 Jahre Lebenszyklus
- Erneuerungsperiode Dataport ROOT CA 02 Zertifikat 6 Jahre vor Ablauf

Dataport CA 03

- DATAPORT CA 03 Zertifikat: 6 Jahre Lebenszyklus
- Erneuerungsperiode Dataport CA 03 Zertifikat 3 Jahre

Dataport CA 04

- DATAPORT CA 04 Zertifikat: 6 Jahre Lebenszyklus
- Erneuerungsperiode Dataport CA 04 Zertifikat 3 Jahre vor Ablauf

Dataport CA 05

- DATAPORT CA 05 Zertifikat: 6 Jahre Lebenszyklus
- Erneuerungsperiode Dataport CA 05 Zertifikat 3 Jahre vor Ablauf

Dataport CA 06

- DATAPORT CA 06 Zertifikat: 6 Jahre Lebenszyklus
- Erneuerungsperiode Dataport CA 06 Zertifikat 3 Jahre vor Ablauf

Die Erneuerung von CA Zertifikaten unterliegt folgenden Rahmenbedingungen:

- Es ist jederzeit garantiert, dass alle von der CA ausgestellten, gültigen Zertifikate im Gültigkeitszeitraum des CA Zertifikates liegen
- Ein neues CA Schlüsselpaar ist generiert, bevor das Ablaufdatum der von der CA ausgestellten Zertifikate erreicht wurde
- Alle neuen Zertifikate werden mit dem neuen Schlüsselpaar signiert
- Mit dem alten Schlüsselpaar wird die entsprechende Sperrliste solange signiert, bis das letzte mit diesem Schlüsselpaar generierte Zertifikat abgelaufen ist

5.7 Kompromittierung und Wiederanlauf nach Katastrophen

5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Es existieren Notfallpläne von Dataport, in denen die Prozesse, Prozeduren und Verantwortlichkeiten bei IT-Sicherheitsvorfällen, Notfällen und Katastrophen geregelt sind. Zielsetzung dieser Notfallprozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit. Die Notfall-Prozeduren sehen bei Sicherheitsvorfällen insbesondere die folgenden Maßnahmen vor:

- Öffnung eines Sicherheitsvorfalls in dem bei Dataport dafür vorgesehenen Tool
- Analyse und Bewertung der Funktionseinschränkung und Sicherheitsprobleme der betroffenen Dienste und Systeme der Zertifizierungsstelle
- Festlegung von Sofortmaßnahmen, die den Funktionseinschränkungen und Sicherheitsproblemen entgegenwirken
- Regelung der Verantwortlichkeiten und Rollen
- Falls erforderlich, Benachrichtigung betroffener Stellen und Personen, z.B. der Zertifikatsnehmer, über die Problematik und gegebenenfalls notwendige Gegenmaßnahmen
- Analyse und Dokumentation der Ursachen des Vorfalles
- Gegebenenfalls Erstellung, Prüfung und Genehmigung eines Change Requests zur Modifikation der Systemkonfiguration mit dem Ziel, Vorfälle dieser Art in Zukunft zu verhindern. Überwachung der Umsetzung des Change Requests
- Protokollierung der einzelnen Maßnahmen und Tätigkeiten

5.7.2 Kompromittierung bei IT Ressourcen

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben,

- wird der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt.
- Das IT-System wird neu aufgesetzt unter Wiederherstellung der Software und der Daten aus der Datensicherung, überprüft und in einem sicheren Zustand in Betrieb genommen.
- Anschließend wird das fehlerhafte oder modifizierte IT-System analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.
- Falls sich in einem Zertifikat fehlerhafte Angaben befinden, wird der Zertifikatnehmer unverzüglich informiert und das Zertifikat widerrufen.

5.7.3 Wiederanlauf bei Kompromittierung von privaten Schlüsselmaterial

Die Kompromittierung von privatem Schlüsselmaterial stellt einen ernstzunehmenden Zwischenfall dar und wird daher besonders gehandhabt.

- Bei Kompromittierung von privatem Schlüsselmaterial der Zertifizierungsstellen wird das jeweilige Zertifikat sofort gesperrt. Gleichzeitig werden alle mit Hilfe dieses Zertifikats ausgestellten Zertifikate gesperrt.
- Bei Kompromittierung von privatem Schlüsselmaterial des Dataport Benutzerzertifikats für Smartcards wird das jeweilige Zertifikat sofort gesperrt.
- Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.
- Alle betroffenen Zertifikatsnehmer und vertrauenden Parteien werden umgehend benachrichtigt.

5.7.4 Notfallbetrieb nach einem Katastrophenfall

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe bei Verlust ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist.

5.7.5 Einstellung des Betriebs der Zertifizierungs- und/oder Registrierungsstelle

Im Falle der Einstellung des Betriebes der Dataport Zertifizierungsstellen oder der Registrierungsstellen sind folgende Maßnahmen festgelegt:

- Alle Zertifikatsnehmer und vertrauende Parteien werden von der Einstellung des Zertifizierungsdienstes informiert. Eine zeitliche Frist wurde noch nicht festgelegt.
- Alle Benutzerzertifikate, sowie die Zertifikate der Zertifizierungsstellen werden gesperrt.
- Alle privaten Schlüssel der Zertifizierungsstellen und Benutzerzertifikate für Smartcards der Zertifikatsnehmer werden vernichtet.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselpaarerzeugung und Installation

6.1.1 Schlüsselpaarerzeugung

Die Schlüsselerzeugung und die Auswahl der kryptographischen Algorithmen für die Dataport PKI erfolgt nach FIPS 140-2 Level 2 (Federal Information Processing Standards).
Die Generierung der Schlüsselpaare wird von Hard- und Softwarekomponenten ausgeführt und unterscheidet sich je nach Entität:

Schlüsselpaargenerierung für die Dataport Zertifizierungsstellen:

Alle Schlüsselpaare für die Dataport Zertifizierungsstellen werden durch das Netzwerk HSM (Hardware Security Modul) generiert. Die generierten CA Schlüssel werden auch durch das Netzwerk HSM kryptographisch geschützt. In jeden Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden. Die Dataport Netzwerk HSM wird im Fips 140-2 Level 2 Modus betrieben.

Schlüsselpaargenerierung für die Dataport Zertifikatsmanagement Agenten und OCSP:

Alle Schlüsselpaare für die Dataport Zertifikatsmanagement Agenten und OCSP Response Signing Zertifikate werden durch das Netzwerk HSM generiert. Die generierten Agenten Schlüssel /OCSP Schlüssel werden auch durch das Netzwerk HSM kryptographisch geschützt. In jedem Prozess, der den Zugriff auf die privaten Schlüssel für Agentenzertifikate und OCSP Response Signing Zertifikate erforderlich macht, ist das HSM zwingend eingebunden. Das Dataport Netzwerk HSM wird im FIPS 140-2 Level 2 Modus betrieben.

Schlüsselpaargenerierung für Dataport Benutzerzertifikate auf sicheren Trägermedien:

Das Authentifikationsschlüsselpaar für Benutzerzertifikate auf Smartcards wird durch die eingesetzte Smartcard für den Dataport Zertifikatsnehmer generiert. Die Generierung des Schlüsselmaterials erfolgt in diesem Fall durch Hardware. Die Hardware Krypto-Komponenten auf der Smartcard sind nach FIPS 140-2 Level 3 zertifiziert.

Schlüsselpaargenerierung für softwaregenerierte Zertifikate:

Die Authentifikationsschlüsselpaare werden selbst auf den beantragenden Maschinen generiert. Die Generierung des Schlüsselmaterials erfolgt in diesem Fall durch Softwarekomponenten. Die Software Krypto-Komponenten sind nach FIPS 140 Level 1 zertifiziert.

6.1.2 Auslieferung der privaten Schlüssel an Zertifikatsnehmer

Private Schlüssel der Dataport Zertifizierungsstellen:

In jeden Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden; alle privaten CA Schlüssel liegen nur in dem HSM selbst vor.
Eine Auslieferung des privaten Schlüsselmaterials von CA Schlüsseln ist nicht notwendig, da die HSM für die Schlüsselerzeugung und als sichere Ablage für private Schlüssel dient. Zur Sicherung des privaten Schlüsselmaterials auf dem HSM dienen HSM Backup Token.

Private Schlüssel für Dataport Benutzerzertifikate auf Smartcards:

Die Smartcard wird an den Dataport Zertifikatsnehmer ausgeliefert. Im Auslieferungszustand ist die Smartcard ohne Schlüsselpaare und Zertifikate. Im Rahmen der Smartcard Provisionierung werden die Schlüsselpaare für Benutzerzertifikate auf der eingesetzten Smartcard generiert.
Der Zugriff auf den privaten Schlüssel wird erst nach erfolgreicher Freischaltung durch einen Benutzer PIN gewährt.

Private Schlüssel für Dataport Benutzerzertifikate als Softzertifikate:

Die Authentifikationsschlüsselpaare werden selbst auf den beantragenden Endgeräten der Benutzer generiert, wenn diese sich in einen Verzeichnisdienst von Dataport befinden und automatisiert ausgerollt werden.
Eine Auslieferung ist nur dann notwendig, wenn entweder das Endgerät des Benutzers (Dataport Zertifikatsnehmer) sich nicht in einem Verzeichnisdienst von Dataport befindet oder aus sicherheitstechnischen Anforderungen heraus Bereitstellung manuell erfolgt. In diesen Fällen erfolgt die Auslieferung des privaten Schlüssels an die Benutzer (Dataport Zertifikatsnehmer) über geeignete sichere Verfahren, wie PKCS#12 und der Verschlüsselung des Schlüsselmaterials mittels eines Transport PINs. Sind Zielmaschine und beantragende Maschine identisch, so ist eine Auslieferung nicht notwendig.

Private Schlüssel der Dataport Zertifikatsmanagement Agenten und OCSP:

In jeden Prozess, der den Zugriff auf den privaten Schlüssel der Zertifikatsmanagement Agenten und OCSP Response Signing erforderlich macht, ist das HSM zwingend eingebunden; alle privaten Agenten Schlüssel liegen nur in der HSM selbst vor.
Eine Auslieferung des privaten Schlüsselmaterials von Agenten Schlüsseln ist nicht notwendig, da die HSM für die Schlüsselerzeugung und als sichere Ablage für private Schlüssel dient.

Private Schlüssel der Dataport Maschinen (Authentisierung):

Die Authentisierungschlüsselpaare werden selbst auf den beantragenden Maschinen generiert.
Eine Auslieferung ist nur dann notwendig, wenn die Zielmaschine (Dataport Zertifikatsnehmer) nicht identisch ist mit der beantragenden Maschine. In diesem Fall erfolgt die Auslieferung des privaten Schlüssels an die Zielmaschine (Dataport Zertifikatsnehmer) über geeignete sichere Verfahren, wie PKCS#12 und der Verschlüsselung des Schlüsselmaterials mittels eines Transport PINs. Sind Zielmaschine und beantragende Maschine identisch, so ist eine Auslieferung nicht notwendig.

6.1.3 Auslieferung der öffentlichen Schlüssel an Zertifikatsaussteller

Der Certificate Signing Request (CSR) des Zertifikatnehmers wird durch die PKI an die Zertifizierungsstelle zum Zwecke der Zertifizierung im PKCS#10 Format übermittelt. Der gesamte Prozess findet automatisiert statt.
Der Certificate Signing Request der Dataport CA 03, der DATAPORT CA 04, der Dataport CA 05 und der Dataport CA 06 erfolgt auch im PKCS#10 Format. Allerdings findet dieser Prozess, aufgrund der Offline-Mimik der Dataport ROOT CA 02, rein manuell statt.

6.1.4 Auslieferung der öffentlichen CA Schlüssel an vertrauende Parteien

Die Auslieferung der öffentlichen CA Schlüsseln erfolgt manuell. Des Weiteren sind die öffentlichen Schlüssel der Dataport Zertifizierungsstellen auf dafür vorgesehenen Web-URLs publiziert:

- Dataport ROOT CA 02: http://pki.servicedpaor.de/ca/Dataport ROOT CA 02.crt
- Dataport ROOT CA 02 (2021): http://pki.servicedpaor.de/ca/Dataport Root CA 02(1).crt
- Dataport CA 03 (2018): http://pki.servicedpaor.de/ca/Dataport CA 03(1).crt
- Dataport CA 03 (2021): http://pki.servicedpaor.de/ca/Dataport CA 03(2).crt
- Dataport CA 04 (2018): http://pki.servicedpaor.de/ca/Dataport CA 04(1).crt
- Dataport CA 04 (2021): http://pki.servicedpaor.de/ca/Dataport%20CA%2004(2).crt
- Dataport CA 05: http://pki.servicedpaor.de/ca/Dataport CA 05.crt
- Dataport CA 05 (2019): http://pki.servicedpaor.de/ca/Dataport CA 05(1).crt

- Dataport CA 06: http://pki.servicedpaor.de/ca/Dataport CA 06.crt

6.1.5 Schlüssellängen

Dataport CA Schlüssellänge:

- Dataport ROOT CA 02 – 4096bit (HSM) – RSA Algorithmus
- Dataport CA 03 – 4096bit (HSM) – RSA Algorithmus
- Dataport CA 04 – 4096bit (HSM) – RSA Algorithmus
- Dataport CA 05 – 4096bit (HSM) – RSA Algorithmus
- Dataport CA 06 – 4096bit (HSM) – RSA Algorithmus

6.1.6 Erzeugung und Prüfung der Schlüsselparameter

Für den RSA Algorithmus nicht zutreffend.

6.1.7 Schlüsselverwendungszweck (wie im X.509 Version 3 Key Usage Feld)

Siehe 7.1
Dataport CA Schlüsselverwendung:

- Dataport ROOT CA 02 – Certificate Signing, Off-line CRL Signing, CRL Signing (06)
- Dataport CA 03 – Certificate Signing, Off-line CRL Signing, CRL Signing (06)
- Dataport CA 04 – Certificate Signing, Off-line CRL Signing, CRL Signing (06)
- Dataport CA 05 – Certificate Signing, Off-line CRL Signing, CRL Signing (06)
- Dataport CA 06 – Certificate Signing, Off-line CRL Signing, CRL Signing (06)

6.2 Schutz des privaten Schlüssels und kryptographische Module

In der Dataport PKI wird privates Schlüsselmaterial durch kryptographische Module in der Ausprägung als Hardware oder Software geschützt.
Der Schutz des privaten Schlüsselmaterials von Dataport Zertifizierungsstellen wird durch das Hardware Security Modul umgesetzt. Das private Schlüsselmaterial von Dataport Zertifikatsnehmern wird abhängig von der Zertifikatsklasse durch Software oder Hardware Implementierung einer Krypto-Schnittstelle umgesetzt.

6.2.1 Standards und Sicherheitsmaßnahmen von kryptographischen Modulen

- Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 und Level 3 evaluiert.
- Die eingesetzten Smartcards sind nach FIPS 140-2, Level 3 evaluiert.
- Die eingesetzten Software Krypto-Module sind nach FIPS 140-2, Level 1 evaluiert.

6.2.2 Mehr-Personenkontrolle von privaten Schlüsseln (n von m Verfahren)

Eine Schlüsselteilung von privaten Schlüsseln findet nicht statt. Ausnahme bildet der Betrieb der Netzwerk HSM. Ein n-von-m Verfahren für die Netzwerk HSM Verwaltung wurde eingerichtet.

6.2.3 Hinterlegung von privaten Schlüsseln

Nicht erforderlich

6.2.4 Backup von privaten Schlüsseln

Privates Schlüsselmaterial der Dataport Zertifizierungsstellen wird durch das Netzwerk HSM und zugehörigen HSM Backup Token und Prozesse gesichert. Archiviertes privates Schlüsselmaterial der Dataport Zertifikatsnehmer wird durch verfügbare Backup Methoden gesichert.

6.2.5 Archivierung von privaten Schlüsseln

Privates Schlüsselmaterial welches durch Zertifikatsnehmer zur Datenverschlüsselung verwendet wird muss archiviert werden. Die Archivierung von privatem Schlüsselmaterial für Signatur oder Authentifizierung ist verboten.

6.2.6 Transfer von privaten Schlüsseln in oder aus einem kryptographischen Modul

Nicht zutreffend. Ein Transfer von privaten Schlüsseln ist nicht vorgesehen, da alle privaten Schlüssel in der Komponente verbleiben, die diese auch erzeugt haben.

6.2.7 Ablage von privaten Schlüsseln im kryptographischen Modul

Die privaten Schlüssel der Dataport Zertifizierungsstellen werden durch das Netzwerk HSM verwaltet und geschützt. Darüber hinaus wird ein Backup der CA Schlüssel durch das Netzwerk HSM ausgeführt, dieses wiederum ist in einer physisch geschützten Umgebung abgelegt.

6.2.8 Aktivierung der privaten Schlüssel

Eine Aktivierung von privaten Schlüsseln ist nur für Dataport Benutzerschlüssel auf Smartcards vorgesehen. Die Aktivierung und damit auch der Zugriff auf den privaten Schlüssel erfolgt durch Festlegung einer Smartcard PIN durch den Benutzer.

6.2.9 Deaktivierung der privaten Schlüssel

Nicht zutreffend. Eine Deaktivierung von privaten Schlüsseln ist für die Dataport PKI nicht vorgesehen.

6.2.10 Vernichtung der privaten Schlüssel

Die Methoden zur Vernichtung privater Schlüssel durch den Zertifizierungsdienstanbieter hängen von der kryptographischen Hardware und/oder der kryptographischen Software ab, in der die Schlüssel gespeichert werden:

- Die Vernichtung des gesamten privaten Schlüsselmaterials erfolgt in der Regel durch das Löschen des privaten Schlüsselspeichers. Eine individuelle Löschung von privaten Schlüsseln muss manuell umgesetzt werden.
- Private Schlüssel, die auf HSMs gespeichert sind, werden durch das Löschen des Schlüssels im HSM vernichtet.
- Private Schlüssel, die auf Smartcards vorliegen, werden durch eine Initialisierung bzw. Formatierung gelöscht.

6.2.11 Bewertung des kryptographischen Moduls

- Das eingesetzte Netzwerk HSM kann nach FIPS 140-2, Level 2 betrieben werden.
- Die eingesetzten Smartcards werden nach FIPS 140-2, Level 3 betrieben.
- Die eingesetzten Software Krypto-Module werden nach FIPS 140-2, Level 1 betrieben.

6.3 Weitere Aspekte für die Verwaltung von Schlüsselpaaren

6.3.1 Archivierung der öffentlichen Schlüssel

Alle von den Zertifizierungsdiensten ausgestellten Zertifikate werden in der Zertifizierungsstellen-datenbank archiviert. Darüber hinaus findet keine Archivierung öffentlicher Schlüssel statt.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren.

Für die Dataport Zertifizierungsstellen sind folgende Lebensdauern festgelegt:

Dataport ROOT CA 02

- ROOT CA 02 Zertifikat: 12 Jahre
- ROOT CA 02 CRLs: 9 Monate
- Zertifikatserneuerung mit Schlüsselwechsel

Dataport CA 03

- DATAPORT CA 03 Zertifikat: 6 Jahre
- DATAPORT CA 03 CRLs: 2 Tage
- Zertifikatserneuerung mit Schlüsselwechsel

Dataport CA 04

- DATAPORT CA 04 Zertifikat: 6 Jahre
- DATAPORT CA 04 CRL: 10 Tage
- Zertifikatserneuerung mit Schlüsselwechsel

Dataport CA 05

- DATAPORT CA 05 Zertifikat: 6 Jahre
- DATAPORT CA 05 CRL: 2 Tage
- Zertifikatserneuerung mit Schlüsselwechsel

Dataport CA 06

- DATAPORT CA 06 Zertifikat: 6 Jahre
- DATAPORT CA 06 CRL: 10 Tage
- Zertifikatserneuerung mit Schlüsselwechsel

Endentitätenzertifikate

- Maximal drei Jahre Laufzeit

6.4 Aktivierungsdaten

In Rahmen der Dataport PKI Implementierung fallen Aktivierungsdaten an, welche den Zugriff auf das private Schlüsselmaterial kontrollieren.
Bei der Ausgabe von Smartcards werden Aktivierungsdaten in Form einer Benutzer PIN und PUK individualisiert.

6.4.1 Erzeugung der Aktivierungsdaten und Installation

Die zufallsgenerierte Erzeugung der Aktivierungsdaten (PUK) erfolgt durch das Zertifikats- und Smartcard-Managementsystem.

6.4.2 Schutz der Aktivierungsdaten

Aktivierungsdaten (PUK) werden durch das Zertifikats- und Smartcard-Managementsystem geschützt. Hierzu werden diese Daten verschlüsselt auf der zugehörigen Zertifikatsmanagementdatenbank abgelegt. Der Zugriff auf diese erfolgt exklusiv nur für das Managementsystem.

6.4.3 Weitere Aspekte von Aktivierungsdaten

Nicht zutreffend.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische technische Anforderungen von Sicherheitsmaßnahmen für Computer

Für Server, die zentrale Funktionen der Zertifizierungsdienste implementieren, sowie alle Rechner, die dem Schutz der Einrichtungen der Zertifizierungsdienste dienen, wurden die Standard Sicherheitsmaßnahmen von IT-Grundschutz umgesetzt. Diese beinhalten:

- Auf dem Server ist nur die für die jeweilige Funktion notwendige Software installiert.
- Der Server besitzt nur die für die jeweilige Funktion notwendigen Kommunikationsschnittstellen. Insbesondere sind die Rechner nur in die für ihre Funktion notwendigen Teilnetzwerke integriert.
- Unnötige Funktionen des Betriebssystems und der installierten Software werden – sofern möglich – deaktiviert.
- Falls Sicherheitsrisiken in der verwendeten Software bekannt werden, ergreifen die Systemadministratoren zeitnah die vom Hersteller bzw. von unabhängigen Experten empfohlenen Gegenmaßnahmen. Insbesondere werden beim Betriebssystem und der Software stets die aktuellen Patches gegen bekannte Sicherheitslücken eingespielt.
- Der Zugriff auf die Server ist auf das für den Betrieb der Zertifizierungsdienste notwendige Maß beschränkt. Insbesondere werden die Server nur durch die verantwortlichen Systemadministratoren verwaltet.
- Sicherheitskritische Ereignisse auf den Rechnern werden protokolliert.
- Systeme mit hohen Verfügbarkeitsanforderungen sind hochverfügbar ausgelegt, so dass bei Ausfall eines Rechners die Funktion erhalten bleibt.
- Mittels unterbrechungsfreier Stromversorgungen und mittels Aggregaten werden Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von mehreren Stunden überbrückt.

- Auf den Systemen dürfen nur nach Viren geprüfte Datenträger verwendet werden.

6.5.2 Bewertung der Computersicherheit

Die Dataport PKI baut auf Zertifizierungsdiensten auf, die nach Common Criteria EAL (Evaluation Assurance Level) 4+ (FLR – augmented with Flow Remediation) evaluiert sind.
Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 und Level 3 evaluiert.
Die eingesetzten Smartcards sind nach FIPS 140-2, Level 3 evaluiert.
Die eingesetzten Software Krypto-Module sind nach FIPS 140-2, Level 1 evaluiert.

6.6 Technische Kontrollen für den gesamten Lebenszyklus

6.6.1 Sicherheitsmaßnahmen bei der Systementwicklung

Nicht zutreffend.

6.6.2 Sicherheitsmanagement

Dataport betreibt ein IT-Sicherheitsmanagementsystem (ISMS) nach ISO 27001 auf Basis von IT-Grundschutz. Die PKI ist in dieses Sicherheitsmanagementsystem integriert.

6.6.3 Sicherheitsmaßnahmen für den gesamten Lebenszyklus

In Rahmen des Sicherheitskonzeptes für das Dataport PKI und die zugehörigen Zertifizierungsstellen werden die notwendigen Sicherheitsmaßnahmen beleuchtet. Detailinformation zum Sicherheitskonzept können bei Bedarf vom Bereich Zertifikatsdienste erfragt werden.

6.7 Sicherheitsmaßnahmen im Netz

Die Zertifizierungsdienste implementieren die folgenden Maßnahmen zur Netzwerksicherheit:

- Die produktiven Systeme und Netzwerke sind durch Firewalls vom Internet getrennt.
- Die internen Netzwerke der Zertifizierungsdienste sind soweit möglich nach dem Schutzbedarf der Systeme aufgeteilt. Die Trennung in Teilnetze erfolgt durch Firewalls.
- Firewalls beschränken den Datenverkehr auf das für den Betrieb notwendige Maß.
- Die Firewall des Betriebssystems ist aktiviert, konfiguriert und dokumentiert.

6.8 Zeitstempel

Die Dataport Zertifizierungsstellen nutzen Zeitstempel bei der Ausgabe von Zertifikaten und Zertifikatssperrlisten. Die verwendete Zeitquelle ist hierbei die lokale Systemuhr des verwendeten Computersystems. Die lokale Systemuhr der Online Server wird regelmäßig mit einer externen Zeitquelle automatisch synchronisiert.
Der Einsatz einer vertrauenswürdigen und evaluierten Zeitstempelkomponente ist für die PKI Lösung nicht notwendig.

7 Profil der Zertifikate und Sperrlisten

In Rahmen der PKI sind Zertifikats- und CRL Profile für die Dataport ROOT CA 02 definiert. Diese Profile folgen den PKIX Vorgaben nach RFC 5280 und haben insbesondere Interoperabilitätsaspekte im Fokus. Erweiterungen für die Zertifikats- und CRL Profile sind vorgesehen, soweit diese zum Zwecke der Unterscheidung von Zertifikatstypen genutzt werden können.

7.1 Zertifikatsprofil

Dataport Zertifikate entsprechen:

- ITU-T Empfehlung X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997.

Dataport Zertifikatsprofile sind konform:

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- RFC 5280 (Ablösung von RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

Die Basisbeschreibung von Dataport Zertifikaten enthält:

Feld	Wert
Version	Die X.509-Versionsnummer. Siehe 7.1.1
Seriennummer (Serial Number)	Die eindeutige Seriennummer, die dem Zertifikat von der ausstellenden Zertifizierungsstelle (Certification Authority, CA) zugewiesen wird. Allen von einer bestimmten Zertifizierungsstelle ausgestellten Zertifikaten wird eine eindeutige Seriennummer zugewiesen.
Signaturalgorithmus (Signature Algorithm)	Der Hashalgorithmus, der von der Zertifizierungsstelle zum digitalen Signieren des Zertifikats verwendet wird. Siehe 7.1.3
Aussteller (Issuer)	Informationen zur Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Siehe 7.1.4
Gültig (Validity)	Zeigt das Anfangs- und Enddatum der Gültigkeitsdauer des Zertifikats an (von, bis).
Antragsteller (Subject Name)	siehe 7.1.4
Öffentlicher Schlüssel (Public Key)	Der Typ und die Länge des öffentlichen Schlüssels, der dem Zertifikat zugeordnet ist.
Signaturwert (Signature Value)	Signatur der ausstellenden CA

Dataport CA Zertifikate

Dataport ROOT CA 02 (2015)	
Version	V3
Seriennummer (Serial Number)	422d96c7e332018845134de5757603aa
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Dienstag, 12. Mai 2015 14:39:32
Gültig bis (Valid to)	Mittwoch, 12. Mai 2027 14:49:29
Antragsteller (Subject Name)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=1
Stellenschlüsselkennung (Authority Key Identifier)	Keine
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	Keine
Zugriff auf Stelleninformation (Authority Information Access)	Keine
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	3f6bc66348f24044f409b45d6a5a27a2b1c8e769

Dataport ROOT CA 02 (2021)	
Version	V3
Seriennummer (Serial Number)	729773b9d11503874b05146e7617c5b8
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE

Gültig ab (Valid from)	Dienstag, 12. Mai 2015 14:39:32
Gültig bis (Valid to)	Mittwoch, 27. April 2033 19:09:03
Antragsteller (Subject Name)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=1
Stellenschlüsselkennung (Authority Key Identifier)	Keine
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	Keine
Zugriff auf Stelleninformation (Authority Information Access)	Keine
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	4f09d027d3f8dd8553e22809e1a97d2ae9985f73

Dataport CA 03 (Erneuert 2018)	
Version	V3
Seriennummer (Serial Number)	6e00000008fcda03b34b9f365a000000000008
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Mittwoch, 2. Mai 2018 15:54:36
Gültig bis (Valid to)	Donnerstag, 2. Mai 2024 16:04:36
Antragsteller (Subject Name)	CN = Dataport CA 03 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	68b6cf120d4c7bc6e8afd5f918be3ac167b76bb8
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps

	Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 03.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	9bd17c51b59972b5df4daba35047dd2496c01687

Dataport CA 03 (Original 2021)	
Version	V3
Seriennummer (Serial Number)	6e0000000e8fa422e643c95edd00010000000e
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Dienstag, 27. April 2021 19:28:33
Gültig bis (Valid to)	Dienstag, 27. April 2027 19:38:33
Antragsteller (Subject Name)	CN = Dataport CA 03 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	68b6cf120d4c7bc6e8afd5f918be3ac167b76bb8
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 03.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)

Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	2767d955b08f97b80f17c5f188e83f2ae930bbc4

Dataport CA 04 (Erneuert 2018)	
Version	V3
Seriennummer (Serial Number)	6e0000000929b77ab9def7e691000000000009
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Mittwoch, 2. Mai 2018 16:06:00
Gültig bis (Valid to)	Donnerstag, 2. Mai 2024 16:16:00
Antragsteller (Subject Name)	CN = Dataport CA 04 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	b1e2a6dbfc89e537e8efa2cb3a8c98d0f44924df
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 04.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	80c3384cfc9f4e68bef04155f40b83308d11b879

Dataport CA 04 (Original 2021)

Version	V3
Seriennummer (Serial Number)	6e0000000f404baad6316521b300010000000f
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Dienstag, 27. April 2021 19:29:23
Gültig bis (Valid to)	Dienstag, 27. April 2027 19:39:23
Antragsteller (Subject Name)	CN = Dataport CA 04 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	b1e2a6dbfc89e537e8efa2cb3a8c98d0f44924df
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 04.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	dffb6de55af71bbb497946bc24a204717e5c0fc0

Dataport CA 05 (Original 2016)	
Version	V3
Seriennummer (Serial Number)	6e0000000630fff68877b65c91000000000006
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Dienstag, 27. September 2016 19:23:49
Gültig bis (Valid to)	Dienstag, 27. September 2022 19:33:49
Antragsteller (Subject Name)	CN = Dataport CA 05 O = Dataport AöR

	C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	15c5cc1ee8fcdf4847abf00779e642e1757eec9d
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 05.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	58b45ecbd7fa85b77860bb9b87bdfe729721a311

Dataport CA 05 (Erneuert 2019)	
Version	V3
Seriennummer (Serial Number)	6e0000000ad10f2e02efbe5dbc00000000000a
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Dienstag, 17. September 2019 09:35:10
Gültig bis (Valid to)	Mittwoch, 17. September 2025 09:45:10
Antragsteller (Subject Name)	CN = Dataport CA 05 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	21289f9f3af22bb4271324b7878a6b2287a43ac7
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab

Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 05.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0
Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	9be9f23bf3f4c63e61595bd787fd01c314eca8c1

Dataport CA 06 (Orginal 2020)	
Version	V3
Seriennummer (Serial Number)	6e0000000bdd5d5c0e93fdbe8200000000000b
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Signaturhashalgorithmus (Signatur Hashalgorithm)	sha256
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	Donnerstag, 3. September 2020 14:52:54
Gültig bis (Valid to)	Donnerstag, 3. September 2026 15:02:54
Antragsteller (Subject Name)	CN = Dataport CA 06 O = Dataport AöR C = DE
Öffentlicher Schlüssel (Public Key)	RSA (4096 Bits)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	2743c22002a8b67c0f509a5da65da7b444f69c21
Zertifikatsrichtlinien	Richtlinienkennzeichnerinformation http://pki.servicedpaor.de/cps Zertifikatsklassen 1-4 http://pki.servicedpaor.de/certclass
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	http://pki.servicedpaor.de/crl/Dataport Root CA 02.crl
Zugriff auf Stelleninformation (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 06.crt
Schlüsselverwendung (Key Usage)	Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Offline CRL Signing), Signieren der Zertifikatsperrliste (CRL Signing) (06)
Basiseinschränkungen (Basic Constraints)	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0

Alternativer Antragstellername (Subject Alternate Name)	Keine
Erweiterte Schlüsselverwendung (Extended Key Usage)	Keine
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	f864a1893bef8d61f1305cc9c45df2675f5403d8

Detaillierte Informationen zu weiteren Dataport Zertifikatsprofilen sind der aktuellen Zertifikatsprofiltabelle zu entnehmen[3].

7.1.1 Versionsnummern

Die Dataport Zertifizierungsstellen stellen X.509 Version 3 Zertifikate aus.

7.1.2 Zertifikatserweiterungen

Folgende Zertifikatserweiterungen werden in den von der Dataport bereitgestellten Zertifikaten berücksichtigt:

Erweiterung	Wert	Kritisch
Schlüsselverwendung (Key Usage)	Digitale Signatur (Digital Signature), Zertifikatsignatur (Certificate Signing), Offline Signieren der Zertifikatsperrliste (Certificate Trust List Signing (offline)), Signieren der Zertifikatsperrliste (Certificate Trust List Signing), Schlüsselverschlüsselung (Key Encipherment), Zugelassen (Non Repudiation)	Ja
Basiseinschränkungen (Basic Constraints)	Typ des Antragsstellers (Subject Type): Zertifizierungsstelle (CA), Endeinheit (End Entitiy) Einschränkung der Pfadlänge (Path Length Constraint): 0, 1, keine (none)	Ja
Schlüsselkennung des Antragstellers (Subject Key Identifier)	Eindeutige Nummer, die mit dem öffentlichen Schlüssel des Antragstellers korrespondiert. Die Methode Key Identifier wird verwendet.	Nein
Stellenschlüsselkennung (Authority Key Identifier)	Eindeutige Nummer, die mit dem öffentlichen Schlüssel des Ausstellers korrespondiert. Die Methode Key Identifier wird verwendet.	Nein
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	Enthält Informationen, wo die aktuelle Sperrliste abgerufen werden kann.	Nein
Zugriff auf Stelleninformationen (Authority Information Access)	Enthält einen Link, unter dem weitere Informationen zur ausstellenden Zertifizierungsstelle gefunden werden können (CA Issuers Method).	Nein
Erweiterte Schlüsselverwendung (Extended Key Usage)	Enthält Anwendungsspezifische Attribute/OIDs.	Nein
Alternativer Antragstellername	Enthält alternative Antragstellernamen, wie E-Mail oder Prinzipalnamen (UPN).	Nein

[3] Nähere Infomationen dazu können durch den Bereich Zertifikatsdienste zur Verfügung gestellt werden

(Subject Alternate Name)		
Zertifikatsausgabe Richtlinien (Certificate Issuance Policies)	1.3.6.1.4.1.38103.509.2 (Dataport CP/CPS OID Referenz)	Nein

Folgende private Zertifikatserweiterungen kommen zur Anwendung:

Erweiterung	OID	Kritisch
Zertifikatsrichtlinie (Certificate Template Information)	1.3.6.1.4.1.311.21.7	Nein
Anwendungsrichtlinien (Application Policies)	1.3.6.1.4.1.311.21.10	Nein

7.1.3 OIDs der Algorithmen

- Die Dataport Zertifizierungsstellen erstellen RSA Schlüsselpaare (OID: 1.2.840.113549.1.1.1) gemäß RFC 5280.
- Die Dataport Zertifizierungsstellen erstellen Signaturen mit sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) gemäß RFC 5280.

7.1.4 Namenskonventionen

Die von der Dataport ROOT CA 02 ausgestellten CA Zertifikate enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld. Der Aufbau des DNs erfolgt gemäß X.500 und enthält die Komponenten in folgender Reihenfolge:

CN = [Common Name],

O = [Organization],

C = [Country]

Weiteres zu den verwendeten Namen ist in 3.1 nachzulesen.

7.1.5 Namenseinschränkungen

nicht zutreffend. Es existieren keine Beschränkungen bezogen auf Namen.

7.1.6 Zertifikatsrichtlinie

Die Dataport Certificate Policy OID lautet:

- 1.3.6.1.4.1.38103.509.2

7.1.7 Richtlinieneinschränkungen-Erweiterung

nicht zutreffend.

7.1.8 Policy Qualifiers Syntax und Semantik

Die Dataport Certificate Policy Qualifier ID ist: CPS.
Dataport PKI OID:

- 1.3.6.1.4.1.38103.509.2

Die Dataport CPS Lokation wird durch eine URL bereitgestellt:

- http://pki.servicedpaor.de/cps/Dataport_CPS.pdf

7.1.9 Zertifikatsklassen

Zur Differenzierung der Dataport Ausgabeverfahren von Zertifikaten, der Methode der Schlüsselerzeugung als auch den etablierten Schutzbedarf der Schlüsselpaare werden Zertifikatsklassen eingeführt.
Dataport Zertifikate werden wie folgt in 4 Zertifikatsklassen eingeteilt:

Zertifikatsklasse 1 - Basis Schutzbedarf

Zertifikate dieser Klasse werden automatisch ausgegeben. Voraussetzung für den Erhalt eines Zertifikates ist, dass der Client Mitglied einer Domäne ist, die ein beidseitiges Vertrauen mit der Gesamtstruktur dpaor.de hat, und ein gültiges Kerberos Ticket besitzt. Die Erneuerung der Zertifikate erfolgt auch automatisch. Die Zertifikate besitzen eine maximale Gültigkeit von drei Jahren. Die Schlüsselgenerierung erfolgt durch eine Software Kryptokomponente.

Dataport Zertifikatsklasse 1 OID: 1.3.6.1.4.1.38103.509.200.1

Zertifikatsklasse 2 - Mittlerer Schutzbedarf

Diese Zertifikatsklasse umfasst Maschinenzertifikate, die durch einen manuellen Ausgabeprozess verteilt wurden. Der Ausgabeprozess wird durch ein Zertifikatsmanagementtool unterstützt. Die Erneuerung der Zertifikate unterliegt ebenfalls einem Ausgabeprozess, der abhängig von den Anforderungen vom initialen Ausgabeprozess abweichen kann. Die Zertifikate besitzen eine maximale Gültigkeit von drei Jahren. Die Schlüsselgenerierung erfolgt durch eine Software Kryptokomponente.

Dataport Zertifikatsklasse 2 OID: 1.3.6.1.4.1.38103.509.200.2

Zertifikatsklasse 3 - Hoher Schutzbedarf

Zertifikate dieser Klasse sind ausschließlich solche, welche über einen manuellen Antragsprozess bei der Zertifizierungsstelle beantragt werden. Die Zertifikate besitzen eine maximale Gültigkeit von drei Jahren. Die Schlüsselgenerierung erfolgt durch eine Software Kryptokomponente.

Dataport Zertifikatsklasse 3 OID: 1.3.6.1.4.1.38103.509.200.3

Zertifikatsklasse 4 - Höchster Schutzbedarf

Zertifikate dieser Klasse sind ausschließlich solche, bei den das Schlüsselpaar auf einem sicheren Trägermedium (z.B. Smartcard, HSM) erzeugt wurde und gespeichert ist. Die Zertifikate besitzen eine maximale Gültigkeit von drei Jahren.

Dataport Zertifikatsklasse 4 OID: 1.3.6.1.4.1.38103.509.200.4

7.1.10 Processing Semantics für kritische Certificate Policies Extension

nicht zutreffend.

7.2 CRL Profil

CRLs werden in Rahmen der Dataport PKI ausgegeben.

Dataport CRL Profile entsprechen:

- ITU-T Empfehlung X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Juni 1997.

Dataport CRL Profile sind konform:

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- RFC 5280 (Ablösung von RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

Die Basis CRL Felder sind wie folgt festgelegt:

Feld	Wert
Version	Die X.509-Versionsnummer. Siehe 7.2.1
Aussteller (Issuer)	Informationen zur Zertifizierungsstelle, die die Sperrliste ausgestellt hat.
Gülitg ab (Valid from)	Zeigt das Anfangsdatum der Gültigkeitsdauer der Sperrliste an.
Nächste Aktualisierung (Next update)	Zeigt das Datum der nächsten Aktualisierung der Sperrliste an.
Signaturalgorithmus (Signature Algorithm)	Der Hashalgorithmus, der von der Zertifizierungsstelle zum digitalen Signieren der Sperrliste verwendet wird. Siehe 7.1.3
Signaturwert (Signature Value)	Signatur der ausstellenden CA

Dataport ROOT CA 02 – CRL Profil

Feld	Wert
Version	V2
Aussteller (Issuer)	CN = Dataport ROOT CA 02 O = Dataport AöR C = DE
Gültig ab (Valid from)	<Datum/Zeit>
Nächste Aktualisierung (Next update)	<Datum/Zeit>
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Stellenschlüsselkennung (Authority Key Identifier)	bcc64b2d8d90ecbd260c20b0737edcee05554bab
Sperrlistennummer (CRL Number)	<Eindeutige steigende Nummer pro CRL>
Version der Zertifizierungsstelle (CA Version)	Beginnt mit: V0.0
Nächste Sperrlistenveröffentlichung (Next CRL Publish)	<Datum/Zeit>
Sperrliste	**Wert**
Seriennummer (Certificate Serial Number)	<Seriennummer der gesperrten Zertifikate>
Sperrdatum (Revocation Date)	<Datum/Zeit>
Sperrlistengrundcode (Reason Code)	Sperrgrund: Nicht angegeben (Unspecified), Schlüsselkompromiss (Key Compromise), Stellenkompromiss (CA Compromise), Zugehörigkeit geändert (Affiliation Changed), Abgelöst (Superseded), Vorgangsende (Cessation of Operation), Zertifikat blockiert (Certificate Hold), Entfernung aus Zertifikatssperrliste (RemoveFromCRL)

Dataport SUB CAs – CRL Profil

Feld	Wert
Version	V2
Aussteller (Issuer)	CN = Dataport CA <Nummer> O = Dataport AöR C = DE
Gültig ab (Valid from)	<Datum/Zeit>
Nächste Aktualisierung (Next update)	<Datum/Zeit>
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Stellenschlüsselkennung (Authority Key Identifier)	<Dataport SUB CA <Nummer> Schlüsselkennungshash>
Sperrlistennummer (CRL Number)	<Eindeutige steigende Nummer pro CRL>
Version der Zertifizierungsstelle (CA Version)	Beginnt mit: V0.0
Nächste Sperrlistenveröffentlichung (Next CRL Publish)	<Datum/Zeit>
Sperrliste	**Wert**
Seriennummer (Certificate Serial Number)	<Seriennummer der gesperrten Zertifikate>
Sperrdatum (Revocation Date)	<Datum/Zeit>
Sperrlistengrundcode (Reason Code)	Sperrgrund: Nicht angegeben (Unspecified), Schlüsselkompromiss (Key Compromise), Stellenkompromiss (CA Compromise), Zugehörigkeit geändert (Affiliation Changed), Abgelöst (Superseded), Vorgangsende (Cessation of Operation), Zertifikat blockiert (Certificate Hold), Entfernung aus Zertifikatssperrliste (RemoveFromCRL)

7.2.1 Versionsnummern

Die Dataport Zertifizierungsstellen stellen CRLs auf Basis X.509 Version 2 aus.

7.2.2 CRL und CRL Entry Extensions

CRL Extensions (Erweiterungen) können aus dem aktuell geltenden CRL Profil entnommen werden. Siehe 7.2.

7.3 OCSP Profil

Das Profil für das OCSP Response Signing Zertifikat ist in untenstehender Tabelle aufgeführt:

Dataport OCSP Response Signing	
Version	V3
Seriennummer (Serial Number)	<Zertifikatsseriennummer>
Signaturalgorithmus (Signature Algorithm)	sha256RSA
Aussteller (Issuer)	CN = Dataport CA 03 / CN = Dataport CA 04 / Dataport CA 05/ Dataport CA 06 O = Dataport AöR C = DE
Gültig ab (Valid from)	<Datum/Zeit>
Valid to	<Datum/Zeit>
Antragsteller (Subject Name)	CN = <OCSP Server FQDN>
Öffentlicher Schlüssel (Public Key)	RSA (2048 Bits)
Schlüsselverwendung (Key Usage)	Digitale Signatur (Digital Signature)
Schlüsselkennung des Antragstellers (Subject Key Identifier)	<Antragsteller Schlüsselkennungshash>
Stellenschlüsselkennung (Authority Key Identifier)	<Schlüsselkennung der ausgebenden Zertifizierungsstelle>
Sperrlisten-Verteilungspunkte (CRL Distribution Points)	Keine
Zugriff auf Stelleninformationen (Authority Information Access)	http://pki.servicedpaor.de/ca/Dataport CA 03.crt http://pki.servicedpaor.de/ca/Dataport CA 04.crt http://pki.servicedpaor.de/ca/Dataport CA 05.crt http://pki.servicedpaor.de/ca/Dataport CA 06.crt
Alternativer Antragstellername (Subject Alternative Name)	<OCSP Server FQDN>
Erweiterte Schlüsselverwendung (Extended Key Usage)	OCSP-Signatur (OCSP Signing) (1.3.6.1.5.5.7.3.9)
OCSP-Prüfung der Nichtsperrung (OCSP No Revocation Checking)	05 00
Fingerabdruckalgorithmus (Thumbprint Algorithm)	sha1
Fingerabdruck (Thumbprint)	<Zertifikatshash>

7.3.1 Versionsnummern

Das OCSP Response Signing Zertifikat entspricht dem X.509 Version 3 Zertifikatsprofil.

7.3.2 OCSP Erweiterungen

Die URL für den OCSP Zugang ist im End-Entitäten Zertifikat hinterlegt.
Dies ist im Authority Information Access (AIA) Attribut aufgeführt:

- http://pki.servicedpaor.de/ocsp

8 Auditierung und Überprüfung der Konformität

In Rahmen der Dataport PKI werden interne Audits durchgeführt, um Abweichungen vom Regelbetrieb der Dataport PKI zu den Ausführungen in der Dataport Certificate Policy bzw. Certification Practice Statement (CP/CPS) zu identifizieren, und bei aufgedeckten Abweichungen der Konformität notwendige korrektive Maßnahmen zu ergreifen.

8.1 Frequenz und Umstand der Überprüfung

Grundsätzlich sind interne Audits und Überprüfungen in regelmäßigen Abständen, mindestens einmal jährlich, geplant. Frequenz und Umstände, die zu einer Überprüfung führen können, werden durch die Dataport Revision im „Informationssicherheit Managementhandbuch“[4] festgelegt.

8.2 Identität und Qualifikation des Prüfers/Auditors

Es wird vorgesehen, dass interne Dataport Mitarbeiter oder Dritte (z.B. qualifizierte Unternehmen wie TÜV IT) die Konformitätsüberprüfung durchführen. Das Auditierungspersonal muss über Knowhow aus der Auditierung im Sicherheitsumfeld besitzen, insbesondere die notwendigen Kenntnisse aus dem Bereich der Public Key Infrastructure (PKI) und aus dem Bereich des Rechenzentrumsbetriebes (ITIL-Zertifizierung) sind erforderlich.

8.3 Verhältnis des Prüfers zur überprüften Entität

Der zugewiesen Auditor für die Überprüfung der Konformität ist zur überprüften Entität, nämlich der Dataport PKI (Technologie und Prozesse) organisatorisch unabhängig.

8.4 Von der Überprüfung abgedeckte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die Dataport Revision festgelegt und decken alle fünf Schichten des IT-Grundschutzes ab. Für Umstände, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche von vornherein festgelegt werden.
Dazu gehören unter anderem:

- Key Management Operations
- Certificate Lifecycle Processes
- Data Processing Security and Operations

8.5 Maßnahmen bei Nichterfüllung oder Abweichen von der Konformität

Werden Abweichungen zur Konformität festgestellt, so müssen diese zeitnah korrigiert werden. Die hierzu notwendigen Maßnahmen um die notwendigen Korrekturen auszuführen sind im „Informationssicherheit Managementhandbuch“ von Dataport beschrieben.
Nach Umsetzung des Aktionsplans gilt es zu überprüfen, ob die ausgeführten Maßnahmen zu einer Korrektur der Mängel geführt haben. Das Dataport IT Management und die Dataport Revision wird über die erzielten Ergebnisse informiert.

[4] Nähere Informationen dazu können durch den Bereich Zertifikatsdienste zur Verfügung gestellt werden

8.6 Kommunikation der Prüfergebnisse

Die Ergebnisse der Auditierung bzw. Prüfung werden im Bericht des Basissicherheitschecks beschrieben und können den Kunden (so beauftragt) im Rahmen des Sicherheitskonzeptes Ihrer Verfahren zur Verfügung gestellt werden.

9 Weitere rechtliche und geschäftliche Regelungen

Dieser Abschnitt bezieht sich auf die geschäftlichen-, rechtlichen- und Datenschutz-Aspekte der Dataport PKI.

9.1 Entgelte

Die Entgelte für Dienstleistungen, die durch die von Dataport betriebenen Zertifizierungsstellen erbracht werden, sind der internen Verrechnungstabelle zu entnehmen. Diese kann bei der in 1.5.2 angegebenen Kontaktpersonen abgerufen werden.

9.1.1 Entgelte für die Ausstellung und Erneuerung von Zertifikaten

Detailinformationen sind der internen Verrechnungstabelle von Dataport für den PKI Dienst zu entnehmen.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Detailinformationen sind der internen Verrechnungstabelle von Dataport für den PKI Dienst zu entnehmen.

9.1.3 Entgelte für den Zugriff auf Speerlisten- oder Status-Information

Detailinformationen sind der internen Verrechnungstabelle von Dataport für den PKI Dienst zu entnehmen.

9.1.4 Entgelte für weitere Dienste

Detailinformationen sind der internen Verrechnungstabelle von Dataport für den PKI Dienst zu entnehmen.

9.1.5 Richtlinie für die Erstattung von Entgelte

Detailinformationen sind der internen Verrechnungstabelle von Dataport für den PKI Dienst zu entnehmen.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Ein Versicherungsschutz ist nicht gegeben.

9.2.2 Vermögenswerte

Vermögenswerte werden nicht abgedeckt.

9.2.3 Versicherungsschutz oder Gewährleistung für Zertifikatsnehmer

Ein Versicherungsschutz für Zertifikatnehmer ist nicht gegeben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertrauliche Informationen berücksichtigt

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen unter anderem Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die beim Registrierungsprozess zur Kenntnis gekommen sind.

9.3.2 Vertrauliche Informationen nicht berücksichtigt

Jegliche Informationen, die in den herausgegebenen Zertifikaten und Widerrufslisten explizit (z.B. E-Mail Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der Dataport PKI operierende Zertifizierungsstelle trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Datenschutz (personenbezogen)

9.4.1 Datenschutzrichtlinie/-plan

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen des Landes Schleswig-Holstein.

9.4.2 Vertraulich zu behandelnde Informationen

Jegliche Informationen über Zertifikatsnehmer und Antragsteller sind vertraulich zu behandeln.

9.4.3 Nicht vertraulich zu behandelnde Informationen

Nicht vertraulich sind Informationen die in den öffentlichen Zertifikaten, wie im Dataport Zertifikat oder im Zertifizierungsstellen-Zertifikat, enthalten sind. Ebenfalls gilt es für Informationen, die in den öffentlichen Zertifikatssperrlisten (CRLs) enthalten sind.

9.4.4 Verantwortung zum Schutz personenbezogener Information

Der Dataport PKI Betrieb ist verantwortlich für den Schutz vertraulicher Informationen. Eine Offenlegung von vertraulichen Informationen kann nur in Abstimmung mit den verantwortlichen Stellen geschehen. Näheres hierzu kann vom Bereich Zertifikatsdienste erfragt werden.

9.4.5 Benachrichtigung bei Nutzung personenbezogener Information

Der Zertifikatnehmer stimmt der Nutzung von personenbezogenen Daten durch eine Zertifizierungsstelle zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder in Rahmen einer gerichtlichen Beweisführung

Die Dataport richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet nur gegenüber staatlichen Instanzen statt, wenn entsprechende Anordnungen ausgegeben wurden.

9.4.7 Andere Umstände einer Veröffentlichung

Keine.

9.5 Urheberrechte

Die Dataport besitzt die Urheberrechte für ausgegebene Dokumentationen im Rahmen der PKI.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Die Dataport Zertifizierungsstellen verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.2 Verpflichtung der Registrierungsstellen

Die Registrierungsstellen verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.3 Verpflichtung des Zertifikatsnehmers

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den „Dataport Richtlinien für den Gebrauch von Zertifikaten“ zu folgen. In 1.4 sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Außerdem muss der Zertifikatsnehmer bei der Nutzung der privaten Schlüssel seine in der Zertifikatsrichtlinie definierten Pflichten erfüllen.

9.6.4 Verpflichtung der vertrauenden Partei

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien seiner Organisation zu folgen. Dort sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt.

9.6.5 Verpflichtung anderer Teilnehmer

Nicht zutreffend, da keine anderen Teilnehmer vorgesehen sind.

9.7 Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Dataport stellt die notwendigen IT Ressourcen für den Betrieb der PKI zur Verfügung, aber ohne eine garantierte Verfügbarkeit.

9.8 Haftungsbeschränkung

Dataport übernimmt keinerlei Haftung für Sach- und Vermögensschäden. Insbesondere bei einer unsachgemäßen oder einer grob fahrlässigen Nutzung der Dataport PKI erlischt jegliche Haftung gegenüber Dritten.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zu Grunde liegenden privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung, ist Dataport von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Nach Veröffentlichung der aktuellen Dataport CP/CPS Dokumentation tritt diese auch in Kraft. Änderungen treten ebenfalls mit der Veröffentlichung auf der öffentlichen Webseite (siehe Kapitel 2.2) in Kraft.

9.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der Dataport Zertifizierungsstellen eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Keine.

9.11 Individuelle Benachrichtigung und Kommunikation mit Teilenehmern

Die individuelle Benachrichtigung der Dataport PKI Teilnehmer erfolgt durch die Verteilung und Zustimmung der „Dataport Richtlinien für den Gebrauch von Zertifikaten“.

9.12 Ergänzungen der Richtlinie

Die Ergänzung und Modifikation der CP bzw. CPS Dokumentation obliegt dem Bereich Zertifikatsdienste. In 1.5. sind entsprechende Kontaktdaten veröffentlicht.

9.12.1 Prozess für die Ergänzung der Richtlinie

Nicht zutreffend.

9.12.2 Benachrichtigungsmethode und –zeitraum

Nicht zutreffend.

9.12.3 Bedingungen für die Änderung einer OID

Nicht zutreffend.

9.13 Schiedsverfahren

Nicht zutreffend.

9.14 Gerichtsstand

Der Betrieb der Dataport PKI unterliegt den Gesetzen der Bundesrepublik Deutschland. Der Gerichtsstand ist Kiel, Bundesrepublik Deutschland. Dieser Gerichtsstand gilt auch für Parteien deren Wohnsitz oder deren gewöhnlicher Aufenthaltsort ins Ausland verlegt wird oder unbekannt ist.

9.15 Konformität zum geltenden Recht

Die von der Dataport PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten. Die Vorgaben und Richtlinien für qualifizierte Signaturen nach eIDAS sind daher nicht bindend für den Betrieb der Dataport PKI.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle im CPS für das PKI beschriebenen Regelungen gelten zwischen den von Dataport betriebenen Zertifizierungsstellen und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Übertragung der Rechte

Eine Übertragung der Rechte ist nicht vorgesehen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CP & CPS Regelwerkes unwirksam sein oder dieses Regelwerk Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.
Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht. Im Falle von Lücken, gilt dasjenige als vereinbart, was nach Sinn und Zweck dieses Vertrages vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.
Es wird ausdrücklich vereinbart, dass sämtliche Bestimmungen dieser CP & CPS, die eine Haftungsbeschränkung, den Ausschluss oder die Beschränkung von Gewährleistungen oder sonstigen Verpflichtungen oder den Ausschluss von Schadensersatz vorsehen, als eigenständige Regelungen und unabhängig von anderen Bestimmungen bestehen und als solche durchzusetzen sind.

9.16.4 Erzwingungsklausel

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer von Dataport betriebenen Zertifizierungsstelle herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.
Erfüllungsort und ausschließlicher Gerichtsstand ist Kiel, Bundesrepublik Deutschland.

9.16.5 Höhere Gewalt

Dataport übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieses CPS, sofern dies aus Ereignissen außerhalb ihrer Kontrolle, wie z.B. höhere Gewalt, Kriegshandlungen, Epidemien, Netzausfälle, Brände, Erdbeben und andere Katastrophen, resultiert.

9.16.6 Andere Regelung

Keine

10 Änderungsverzeichnis

Version	Änderungs-datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
0.0.1	15.05.2012		Erstellung	Holger Kraft
0.0.3	16.09.2012		Erstes Review, Zusammenführung der Kapitel und Ergänzungen: 1. OCSP Responder 2. Zertifikatsklassen CPS Erweiterung für Maschinen	Jung-Uh Yang
0.0.4	30.11.2012		Haftungs- und Versicherungsfragen	Achim Koch
0.0.6	11.03.2013		Zweites Review	Arne Karsten
0.0.8	20.03.2013		Kommentare eingearbeitet	Holger Kraft
0.0.9	19.08.2013		Kommentare eingearbeitet und aktualisiert	Holger Kraft
1.0.0	09.12.2013		Abnahme durch Vorstand	Vorstand
1.1.0	07.04.2015		Aktualisiert für sha 2 PKI	Manfred Schäfer
1.2.0	29.12.2015	3.1.1; 3.1.2, 4.	Aufnahme von Gruppenzertifikaten	Holger Kraft
2.0.0	29.12.2015		Kommentare aktualisiert	Sven Makiola
2.1.0	21.11.2016	alle	Komplette Überarbeitung im Rahmen des Aufbaus von Dataport CA 05	Arne Karsten
2.1.1	04.05.2016	7	Ergänzung CA Daten	Arne Karsten
2.1.2	25.08.2017	7	Korrektur CA Daten	Arne Karsten
2.1.3	09.10.2017	3	Anpassung CodeSigning	Sven Makiola
2.1.4	31.01.2019	1.5.2; 7.	Anpassung Kontakt und URL der Dataport CA 05	Holger Kraft
2.1.5	10.02.2020	alle	Jährliche Überprüfung	Sven Makiola
2.1.6	22.09.2020	Alles	Dataport CA 06 ergänzt	Holger Kraft
2.1.7	28.04.2021	Alle	Dataport Root CA, CA 03 und 04 aktualisiert	Holger Kraft
2.1.8	20.12.2021	Alle	Links aktualisiert	Holger Kraft
2.1.9	08.07.2022	5.5.1	Schreibweise Changemanagement aktualisiert	Nando Krog