Abschlussbericht zu GuT – Gesundheitskarte und Telematik-Infrastruktur

Arbeitsgruppe 3a II „Identitätsmanagement und PKI“

Datei	*Abschlussbericht-v.1.0.doc*
Version	*1.0*
Status	*Final*
Datum	*19.03.2004*

TeleTrusT Deutschland e.V.

Chamissostraße 11

99096 Erfurt

Inhaltsverzeichnis

Das vorliegende Papier wurde im Rahmen des Projektes GuT – Gesundheitskarte und Telematik-Infrastruktur im Arbeitspaket 3 „Kritische Elemente einer Infrastruktur“ von der durch TeleTrusT moderierten Arbeitsgruppe 3a II **„Identitätsmanagement und PKI“** unter der Mitwirkung folgender Firmen bzw. Institutionen und Autoren (alphabetische Reihenfolge) erstellt:

Bundesministerium für Gesundheit und Soziale Sicherung (BMGS)
www.bmgs.bund.de

Herr Benedikt Hoffmann
benedikt.Hoffmann@bmgs.bund.de

Herr Dr. H.-W. Eisermann
hans-werner.eisermann@bmgs.bund.de

IBM Deutschland

Herr Dr. Herbert Bunz
bunz@de.ibm.com

Intercard

Herr Kersten Trojanus
kersten.trojanus@intercard.de

Kassenärztliche Vereinung Bayerns
Arabellastrasse 30
D-81925 München
www.kvb.de

Herr Dr. Christoph Goetz
christoph.goetz@kvb.de

Kassenzahnärztliche Bundesvereinigung

Herr Dieter Reul
d.reul@kzbv.de

Microsoft Deutschland GmbH
Katharina Heinroth Ufer 1,
D-10787 Berlin
www.microsoft.com/germany

Herr Helge Schroda
helgesch@microsoft.com

Herr Michael Wise
mwise@microsoft.com

NetSys-IT GbR
Weimarer Straße 28
D-98693 Ilmenau
www.netsys-it.de

Herr Ralf Döring
rdoering@netsys-it.de

noventum consulting GmbH
Münsterstraße 111
D-48155 Münster
www.noventum.de

Herr Stephan Wappler
stephan.wappler@noventum.de

SIEMENS AG – ICN VD CCS
Völklinger Strasse 1
D-40219 Düsseldorf

Herr Volker Brunsiek
volker.brunsiek@siemens.com

SignCard GmbH & Co KG
Nürnberger Straße 1
D-90546 Stein
www.signcard.de

Herr Dr. Harald Ahrens
harald.ahrens@signcard.com

T-Systems

Herr Stephan Wollny
stephan.wollny@t-systems.com

TeleTrusT Deutschland e.V.
Chamissostraße 11
D-99096 Erfurt
www.teletrust.de

Herr Arno Fiedler
arno.fiedler@teletrust.de

Herr Peter Steiert
peter.steiert@teletrust.de

Herr Prof. Helmut Reimer
helmut.reimer@teletrust.de

1. Einleitung

Die vorläufige Projektgruppe GuT (Gesundheitskarte und Telematik-Infrastruktur) der Vertragspartner der Selbstverwaltung gem. § 291a SGB V einschließlich des Verbandes der privaten Krankenversicherungen hat in ihrer konstituierenden Sitzung am 27. November 2003 eine industrieoffene Arbeitsgruppe für das Arbeitspaket „Kritische Elemente einer Infrastruktur“ gebildet.

Auf der konstituierenden Sitzung der GuT-Arbeitsgruppe 3 „Kritische Elemente einer Infrastruktur“ am Freitag, 19. Dezember 2003, wurde die Unterarbeitsgruppe 3a II **„Identitätsmanagement und PKI“** unter der Federführung von TeleTrusT Deutschland e.V. vereinbart. Die Leitung der Unterarbeitsgruppe übernahm Herr Wappler im Namen von TeleTrusT Deutschland e.V..

1.1. Kritische Elemente einer Infrastruktur

Unter kritischen Elementen einer Infrastruktur werden solche Elemente verstanden, zu denen bisher wenig konzeptionelle Vorarbeit geleistet wurde oder bei denen anhand des Standes der Standardisierung oder des Lösungsangebotes im Vergleich zu den absehbaren Anforderungen erkennbar wird, dass die Bereitstellung geeigneter Lösungen für den Projektablauf zeitkritisch oder gar erfolgskritisch ist.

Hierzu zählen z.B. Elemente einer Kommunikations- und Sicherheitsinfrastruktur, die typischerweise außerhalb der Betrachtung einer konzeptionellen Architekturarbeit liegen mögen, wie beispielsweise der Einfluss der Möglichkeit des Versicherten, sich für seine Gesundheitskarte seinen PKI-Dienstleister selbst aussuchen zu können, oder die Möglichkeit für einen Arzt, Attribut-Zertifikate für sein Personal selbst signieren zu können. Weiterhin sind bestehende Lösungen im Markt und deren umfassende Interoperabilität zu nennen.

2. Arbeitsgruppe 3a II „Identitätsmanagement und PKI“

Die konstituierende Sitzung der Arbeitsgruppe fand am 08.01.2004 in Münster statt. Auf dieser Sitzung wurden die folgenden Unterarbeitspakete identifiziert und vereinbart:

- Unterarbeitspaket Szenarien
- Unterarbeitspaket Zertifikatsprofile
- Unterarbeitspaket Interoperabilität von PKI
- Unterarbeitspaket Identitätsmanagement

Insgesamt fanden 3 gemeinsame Sitzungen statt, in denen die Ergebnisse besprochen und diskutiert wurden:

- 08.01.2004, in Münster
- 02.02.2004, in Erfurt
- 01.03.2004, in Berlin

Ziel alle Unterarbeitspakete war es, kritische Punkte zu identifizieren, die bei der Nutzung verschiedener Infrastrukturen bzw. Lösungsarchitekturansätzen auftreten können und auf einen störungsfreien Betrieb negative Auswirkungen haben können. Ziel war es nicht, detaillierte Vorschläge zu erarbeiten oder Vorgaben für die zu entwickelnde Lösungsarchitektur zu machen.

2.1. Unterarbeitspaket „Szenarien“

Im Unterarbeitspaket Szenarien wurden die zwei verschiedenen PDC-Herausgabeszenarien und das Management der PDC betrachtet:

1. Ausgabe einer PDC, bei der der Versicherte gefragt wird, ob er eine Signaturfunktionalität haben möchte
2. Krankenkasse gibt generell Karte mit digitaler Signatur aus.

Ziel war es, die kritischen Punkte des jeweiligen Szenarios zu identifizieren.

2.2. Unterarbeitspaket „Zertifikatsprofile“

Ziel des Unterarbeitspakets war die Betrachtung verschiedener Zertifikatsprofile, die Interoperabilität auf Profilebene zwischen HPC und PDC zu untersuchen und Aussprache einer Empfehlung.

2.3. Unterarbeitspaket „Interoperabilität von PKI“

Das Unterarbeitspaket Interoperabilität von PKI beschäftigte sich mit den organisatorischen und technischen Rahmenbedingungen, die bei der Nutzung der Dienste verschiedener Public Key Infrastrukturen für die herauszugebenden PDC’s und HPC’s beachtet werden sollten.

Ziel war es nicht, Vorgaben für einzelne Public Key Infrastrukturen oder detaillierte Lösungsvorschläge zu erarbeiten.

2.4. Unterarbeitspaket „Identitätsmanagement“

Aufgrund der Zusammensetzung der Mitarbeit im Unterarbeitspaket Identitätsmanagement wurden vorrangig die juristischen Aspekte des Identitätsmanagements bzgl. Vertretungsregelung und Geschäftsfähigkeit betrachtet.

„Identitätsverwaltung“ ist im Zusammenhang mit der PDC die Summe aller Vorgänge technisch - organisatorischer Art, welche sicherstellen, dass eine bestimmte Handlung (nur) dem Inhaber der PDC zuzuordnen ist (und keinem anderen).

Die Prozesse der Benutzer- und Berechtigungsverwaltung bauen auf der Identitätsverwaltung auf und wurden nicht betrachtet.

3. Die Ausgangssituation

In Deutschland ist die Einführung der Patient Data Card (PDC), auch als elektronische Gesundheitskarte (eGK) bezeichnet, zum 01.01.2006 für die gesetzlich Krankenversicherten geplant. Parallel zur PDC wird der Heilberufeausweis, auch als Health Professional Card (HPC) bezeichnet, eingeführt. Voraussichtlich werden auch die privaten Krankenversicherer eine PDC für ihre Versicherten herausgeben und sich somit an der Gesamtlösung beteiligen.

Die HPC wird durch die im Gesetz verankerten Organisationen / Verbände (Ärztekammer, Zahnärztekammer, Apothekervereinigung) und durch auch im Gesetz noch nicht berücksichtige Organisationen / Verbände (z.B. Hebammen, Physiotherapeuten) ausgegeben werden. Die HPC wird unterschieden werden nach dem

- Heilberufeausweis für z.B. Ärzte und Apotheker
- Berufsausweis für Sprechstundenhilfe, Schwestern usw.

Der Heilberufeausweis wird eine qualifizierte Signatur einer vorab akkreditierten Einrichtung beinhalten. Die HPC wird voraussichtlich von den verschiedenen Landeskammern bzw. Vereinigungen ausgegeben werden. Es ist vorstellbar und in der Diskussion, dass alle in Deutschland HPC-ausgebende Instanzen sich unter einer Root-CA befinden werden.

Die PDC wird durch die gesetzliche Krankenkasse ausgegeben. Die Krankenkassen können dies selbst vornehmen oder einen Dienstleister (DL) mit der Erstellung und Herausgabe beauftragen. Es besteht auch die Möglichkeit eines gemeinsamen DL je Spitzenverband. Im Gesetz ist formuliert: ***„Sie muss technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen.“*** Jedoch steht noch nicht fest, ob die PDC im Umfeld des Gesundheitswesens Signaturen leisten können muss oder ob diese eine Option sein wird. .Zur Frage des Niveaus der Signatur sagt das Gesetz: ***“...im Falle des Absatzes 3 Satz 1 Nr. 5 können die Versicherten auch mittels einer eigenen Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt, zugreifen.“***

Für die Arbeitsgruppe ging aus den zur Verfügung stehenden Informationen nicht sicher hervor, ob die die Authentifizierungs- und Verschlüsselungsfunktionalität der PDC auf asymmetrischer Kryptografie basieren muss und somit der Einsatz von Public Key Infrastrukturen (PKI) erfordern wird.

Auf Basis der allgemeinen Erwartungshaltung an die Technik „vollständige technische Interoperabilität zwischen allen Karten und Zertifikaten“ und der Erwartung, dass innerhalb der Europäischen Union auf mittlerer Sicht auch eine Interoperabilität der Karten gewährleistet sein muss, wird der einer PKI empfohlen und bei den nachfolgenden Betrachtungen davon ausgegangen. Andernfalls ist die Entwicklung von proprietären Lösungen zu befürchten, die dann wiederum zu Interoperabilitätsproblemen führen können und somit zu deutlich erhöhten Kosten bei der Behebung dieser Probleme.

Wichtig für die Umsetzung ist, dass die Pflichtanwendungen ohne Mitwirkung des Versicherten realisiert werden können, d.h. nur durch Vorlage der PDC durch den Versicherten und anschließend ohne weitere Mitwirkung.

4. Identifizierte „Kritische Punkte“

4.1. Generelle „Kritische Punkte“

Generell wurden von der Arbeitsgruppe die folgenden allgemeinen Punkte als kritisch identifiziert:

- Die Erreichung einer vollständigen technischen Interoperabilität zwischen allen Karten und Zertifikaten bedarf eines hohen Abstimmungsbedarfes zwischen allen beteiligten Organisationen (Leistungserbringern, Krankenkassen, Kartenausstellern und Applikationsentwicklern) und ist der kritischste Punkt für eine erfolgreiche Einführung.

- Festlegung des kompletten Funktionsumfangs des künftigen Szenarios. Im Anschluss sind daraufhin die IST-Prozesse zu erfassen und das Delta zu den SOLL-Prozessen zu bilden. Darauf aufbauen kann einen Stufen-Migrationskonzept entwickelt und umgesetzt werden. Auf Basis des Migrationskonzeptes können weitere Planungen über Zeit, Ressourcen und Kosten entwickelt werden.

- Die Sicherstellung technischer und organisatorischer Interoperabilität innerhalb der Europäischen Union muss auf mittlere Sicht gewährleistet sein, bzw. mit geringem finanziellem und organisatorischem Aufwand erreicht werden können (Investitionssicherheit).

- In der Arbeitsgruppe wurde festgestellt, dass im Moment zeitgleich aus abstrakter Prozesssicht an vergleichbaren Lösungen für verschiedene Fachanwendungen gearbeitet wird. Dies geschieht sogar in parallelen Bundesprojekten (siehe GuT und JOBCARD). Eine Koordinierung/Zusammenarbeit zwischen den Projekten ist absolut empfehlenswert, um
    - Kosten für parallele Entwicklungen zu sparen,
    - die Interoperabiltität zwischen den verschiedenen Lösungen zu gewährleisten,
    - Infrastrukturen, wo möglich, gemeinsam zu nutzen,
    - bestimmte Nutzungen mit allen Karten zu ermöglichen.

- Wie wird das Lifecycle-Management der Karte gestaltet werden?
    - Ausgabe der Karte an den Inhaber
    - Betrieb der Karte
    - Sperren der Karte
    - Einzug der Karte vom Inhaber

- Als weiterer kritischer Punkt wurde die Schnittstelle zum Card-OS (z.B. PC/SC oder PKCS#11) identifiziert. Da nicht jeder existierende Standard alle benötigten Funktionalitäten abdeckt bzw. einige Funktionalitäten bisher noch gar nicht standardisiert sind, ist die Entwicklung einer entsprechenden Schnittstelle notwendig. Es wird empfohlen, die Übernahme der Signatur Bündnis-API zu prüfen, um Kosten für parallele Entwicklungen zu sparen und die Interoperabilität zwischen den verschiedenen Lösungen zu gewährleisten.

- Wenn eine optionale digitale Signatur auf die PDC aufgebracht werden soll, welche Stufe der Signatur muss/kann diese dann haben? (Fortgeschritten, Qualifiziert…?) Dies ist ein Thema das in Zusammenhang mit der Migrationsfähigkeit entschieden werden muss.

- Weiterhin sind die Fragen zu klären:
  - Muss/sollte jede Kommunikationsverbindung/Datenaustausch verschlüsselt erfolgen?
  - Welche Kommunikationsrichtungen möglich und zulässig und wie diese zu sichern sind?
    - Verbindung Arzt ← → Arzt
    - Verbindung Patient → Arzt
    - Verbindung Arzt → Patient
  - Wo beginnt der Verantwortungsbereich des Patienten für seine Daten?

- Klärung der Fragen ob Public Key Infrastrukturen (auch für die PDC) eingesetzt werden sollen oder nicht.
  - Definition von Profilen für
    - Zertifikate
    - Sperrlisten
  - Definition des Rahmens für die Policy
  - Festlegung und Überwachung von Teilnahmevoraussetzungen
  - Definition und Realisierung von Zertifikatsrollout und –renewal.

- Festlegung und Definition von Algorithmen und Verfahren und deren Einsatzgebiete:
  - Symmetrische Algorithmen
  - Asymmetrische Algorithmen
  - Hashwertverfahren

- Festlegung von Schlüssellängen bzw. Hashwerte, die als Mindestlänge einzuhalten sind.

- Wie werden die Interoperabilitätstests generell organisiert, durchgeführt und ausgewertet? Wer definiert das Testumfeld und wer führt die Tests durch?

- Wie kann die Überprüfung der Gültigkeit der Karte erfolgen?
  - Nutzung der unique Chip-ID der Karte?
    - White Lists für Offline Prüfung zum Download
  - X.509 Zertifikate?
    - Sichere Verteilung der Wurzelzertifikate, Erneuerung über quartalsmäßiges Update möglich
    - Download der CRL in regelmäßigen Abständen → Offline Prüfung möglich in Zusammenhang mit dem Wurzelzertifikat

4.2. „Kritische Punkte“ – Unterarbeitspaket Szenarien

4.2.1. Ausgabe der Karte

Von sehr großer Bedeutung bei der Herausgabe der Karten sind die folgenden Fragen, die direkten Einfluss auf die Kosten und die Produktionszeiten haben:

Produktion der Karte

- Werden die Karten beschlüsselt oder unbeschlüsselt im Trust Center produziert?

- Erfolgt die Generierung der Zertifikate im Trust Center?

- Wie kann der Zugriff auf Patientendaten der GKV erfolgen, um die Karte produzieren zu können durch einen Dienstleister?

- Wie lange ist die Karte, sind die aufgebrachten Daten und Zertifikate gültig?
- Wie kann eine Gültigkeitsverlängerung der Karte bzw. der aufgebrachten Daten und Zertifikate erfolgen? Unter welchen Voraussetzungen ist eine Verlängerung möglich?
    - Verlängerung beim Arzt
    - Verlängerung beim Apotheker
    - Verlängerung durch die GKV
    - Verlängerung online durch den Patienten

Sperrung der Karte:

- Wie kann die Sperrung der Karte erfolgen und welche Bedingungen müssen eingehalten werden, um eine Sperrung auszuführen?
    - Durch den Patienten (Hotline)?
    - Durch die GKV?
    - Durch einen HPC-Inhaber?

Gültigkeitsprüfung:

- Wie soll die Prüfung der Gültigkeit der Karte bzw. der Zertifikate erfolgen?
    - CRL ?
    - OCSP?
    - Gegen Kartendaten?

- Wann muss die Gültigkeitsprüfung erfolgen?
    - Bei jeder Vorlage
    - Einmal im Quartal

Weitere offene Fragen:

- Was passiert bei PIN- Falscheingabe?
    - Wird eine Ersatzkarte erstellt?
    - Gibt es einen alternativen Prozess ohne Karte?

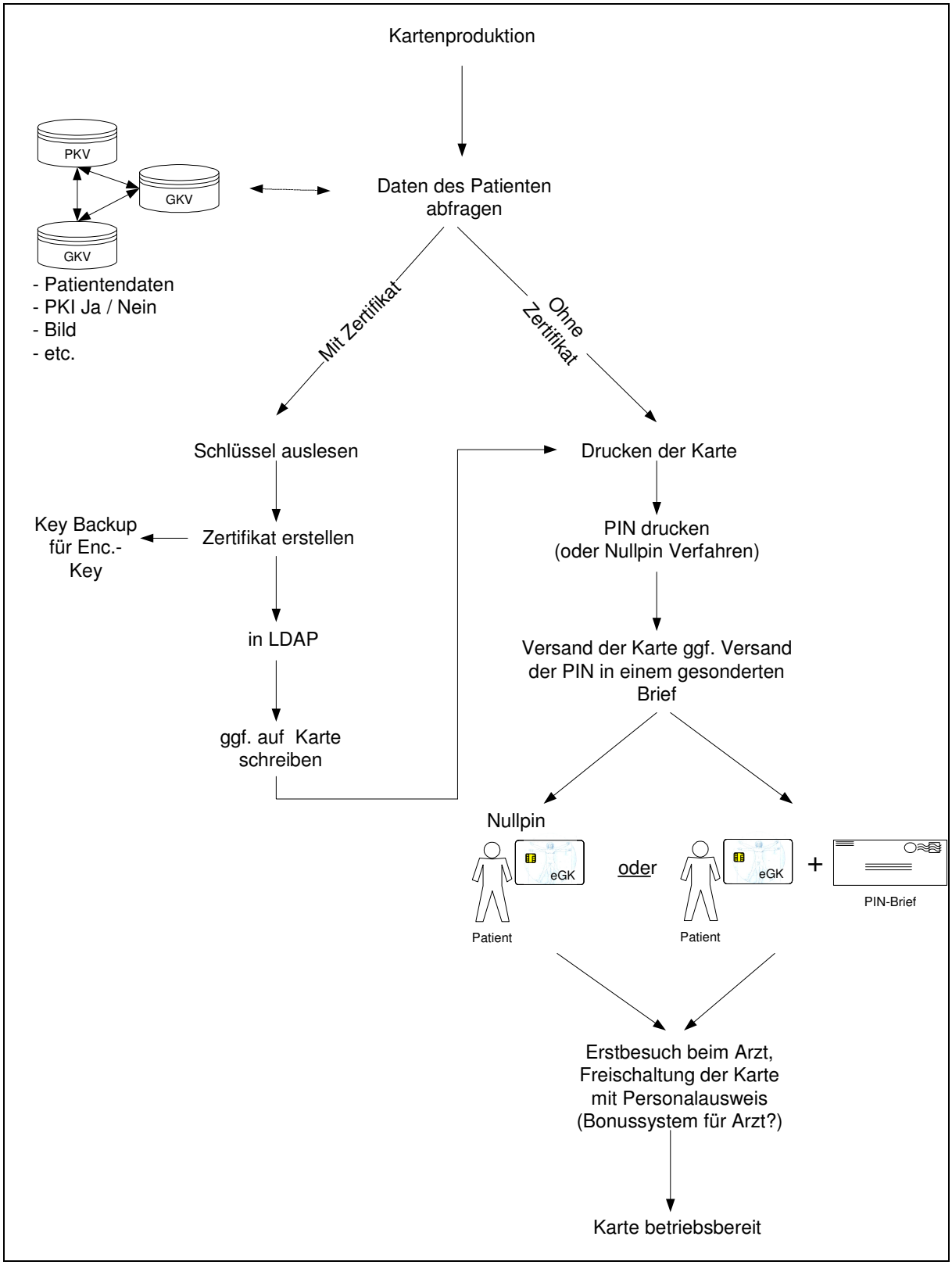
- Was passiert bei Verlust der Karte?

- Ist ein Bonusmodell für Tätigkeiten im Rahmen von Registrierung und Verwaltung (z.B. Freischaltung) für die HPC-Inhaber angedacht, wenn diese Mitwirkungspflichten erfüllen?

4.2.2. Ausgabe der Karten (Initial)

Wichtig ist die Klärung der Fragen:

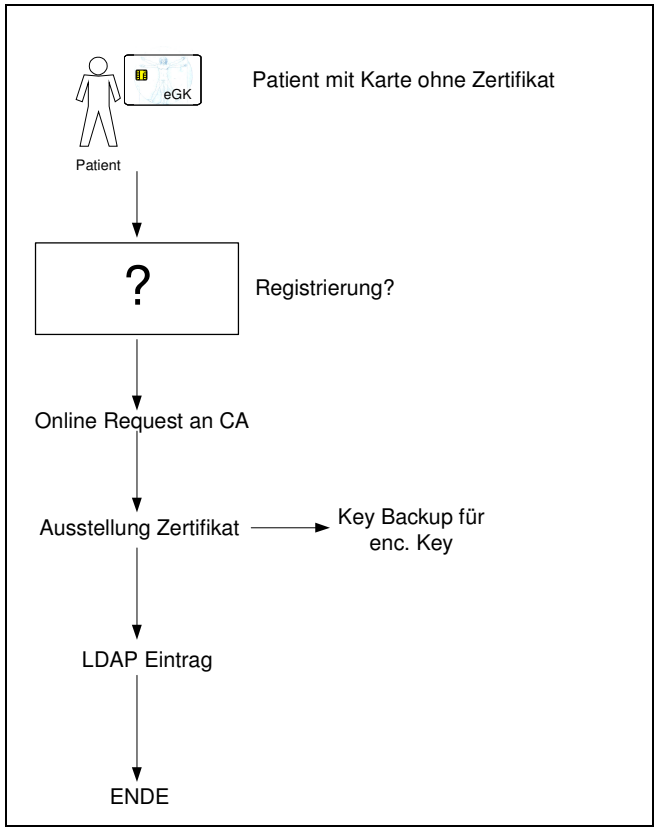
- Wer gibt die Karten aus und wie erhält er die Patientenspezifischen Daten?
- Welche Daten müssen bei der Ausgabe der Karte bereits aufgebracht sein?
- Werden die Karten + PIN-Brief oder mit Null-PIN ausgegeben?
  - Dies hat Auswirkung auf den weiteren Geschäftsprozessablauf der Aktivierung der Karte.
  - Eventuell muss der Patient noch einen Brief an die GKV senden, um den Erhalt des PIN-Briefes zu dokumentieren oder der Arzt muss die Aktivierung mit übernehmen, beim Erstbesuch mit der neuen Karte (Null-PIN-Verfahren).
  - Weiterhin hängt hiervon auch die Einstellung/Aktivierung der öffentlichen Schlüssel/Zertifikate im Verzeichnisdienst ab.


Kartenproduktion
PKV
GKV
GKV
- Patientendaten
- PKI Ja / Nein
- Bild
- etc.
Daten des Patienten abfragen
Mit Zertifikat
Ohne Zertifikat
Schlüssel auslesen
Drucken der Karte
Key Backup für Enc.-Key
Zertifikat erstellen
PIN drucken (oder Nullpin Verfahren)
in LDAP
Versand der Karte ggf. Versand der PIN in einem gesonderten Brief
ggf. auf Karte schreiben
Nullpin
eGK
oder
eGK
+
PIN-Brief
Patient
Patient
Erstbesuch beim Arzt, Freischaltung der Karte mit Personalausweis (Bonussystem für Arzt?)
Karte betriebsbereit

4.2.3. Ausgabe des Zertifikats bei vorhandener Karte (Nachpersonalisierung)

Wichtig ist die Klärung der Fragen:

- Wer führt die Registrierung durch?
- Wo wird registriert und wie sieht der Registrierungsprozess aus?
- Was sind die Vorgaben für die Registrierung?



4.2.4. Falscheingabe PIN / Kartensperre

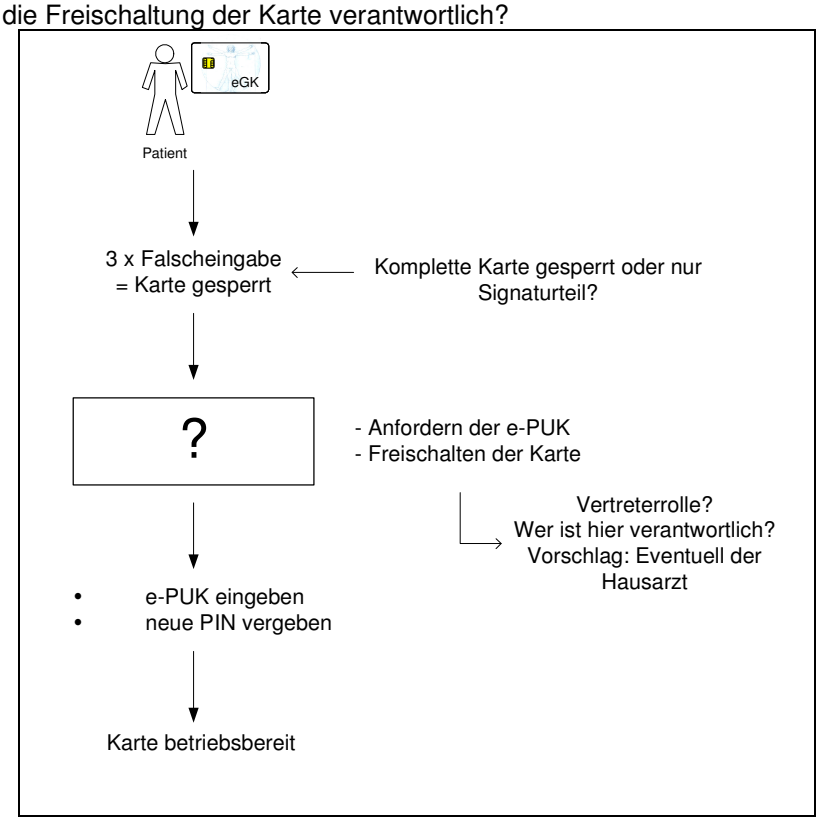
Grundsätzlich müssen die Fragen geklärt werden, ob und wofür eine PIN bei der PDC benötigt wird:

- Bei der Signatur sicherlich, diese ist aber optional.
- Beim Rezept?
- Beim Arztbesuch? Schützt diese PIN die freiwilligen Patientendaten?

Wichtig ist die Klärung der Fragen:

- Wird bei der Falscheingabe die komplette Karte mit all ihren Funktionen gesperrt oder nur Teile, wie zum Beispiel die Signatur?
- Wo kann die PUK angefordert werden?

- Wer verwaltet die PUK?
- Wer ist für die Freischaltung der Karte verantwortlich?



4.2.5. Auswahl des Typs der elektronische Signaturen auf einer PDC

Es muss festgelegt werden, welche Art von elektronischer Signatur für wann und bei welchen Anwendungen eingesetzt werden soll. Dies hat auch Auswirkung auf die Auswahl der Karten (z.B. Evaluierungsstufe) und gegebenenfalls auf die Dateistruktur auf der Karte.

4.2.5.1. Qualifizierte Signatur vs. fortgeschrittene Signatur vs. Einmalpasswort

Bezugnehmend auf die Formulierung im Gesetz ***„... im Falle des Absatzes 3 Satz 1 Nr. 5 können die Versicherten auch mittels einer eigenen Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt, zugreifen.“*** ist, falls Signaturen auf der PDC verwendet werden, die Frage zu beantworten, ob qualifizierte oder fortgeschrittene Signaturen zum Einsatz kommen. Die Beantwortung der Frage beinhaltet die Themen wie Kosten, Beweiswert und Nutzbarkeit. Diese Themen werden zurzeit im Signaturbündnis behandelt. Die dort gefundenen Regelungen sollten berücksichtigt werden.

Auch der Einsatz von Einmalpasswörtern wird gegenwärtig diskutiert.

4.2.6. Das PIN-Management

Bezugnehmend auf die Formulierung im Gesetz (§ 291a Abs 5 Satz 2) "Durch technische Vorkehrungen ist zu gewährleisten, dass in den Fällen des Absatzes 3 Satz 1 Nr. 2 bis 6 der Zugriff nur durch Autorisierung der Versicherten möglich ist." bzw. (§291a Abs 5 Satz 4) "Der Zugriff auf Daten nach Absatz 2 Satz 1 Nr 1 mittels der elektronischen Gesundheitskarte kann abweichend von den Sätzen 3 und 4 auch erfol-

gen, wenn die Versicherten den jeweiligen Zugriff durch ein geeignetes technisches Verfahren autorisieren." kann dies mittels PIN erfolgen.

Es bedarf der Definition und Festlegung:

- Anforderungen an die PIN-Länge in Abhängigkeit des Sicherheitsniveaus und der zu schützenden Objekte (Schlüssel, Files)
- Regelungen für Retry-Counter und Resetting Codes
- Regelungen zur Änderbarkeit von PINs.

Darüber hinaus sind auch Angaben zum Transport-PIN-Mechanismus erforderlich.

4.3. „Kritische Punkte“ – Unterarbeitspaket Zertifikatsprofile

Die Interoperabilität der Zertifikatsprofile ist der wichtigste Punkt im Umgang und der Verarbeitung der Zertifikate in den Applikationen. Auch beim internationalen Einsatz der Karten (sowohl HPC als auch PDC) sind die Zertifikate und da insbesondere die Profile der Hauptberührungspunkt für die Applikationen. Aus diesem Grund ist es unbedingt notwendig, international anerkannte Standards zu unterstützen bzw. interoperabel zu diesen zu sein.

Zusätzlich sind noch die folgenden Fragen zu klären:

- Gibt es eine Notwendigkeit für generische HPC Daten, im PDC Zertifikat speziell Daten, wie zum Beispiel Name des Versicherers oder Patienten Identifikationsnummer, als Zertifikatserweiterung mit aufzunehmen?

- Werden Richtlinien für Kartenemittent spezifische Erweiterungen benötigt?

- Sind diese Daten allgemein lesbar oder müssen sie verschlüsselt werden, damit sie nur in einer „berechtigten“ Umgebung lesbar sind? Wenn sie im Zertifikat stehen, sind sie nach heutiger Praxis nach Einstecken der Karte lesbar, Wenn sie verschlüsselt wären, wie erfolgt der Zugang: mit PIN des Patienten? Über Entschlüsselung mit „Gesundheitsschlüssel“ durch die Geräte in Praxis und Apotheke?

Empfohlen wird, die Erfahrungen aus dem Signaturbündnis mit einzubeziehen (ISIS-MTT).

4.4. „Kritische Punkte“ – Unterarbeitspaket Interoperabilität von PKI

Bei einer organisationsübergreifenden Kommunikation muss Interoperabilität auf allen 4 Ebenen der Interoperabilität geschaffen werden:

- Infrastruktur
- Organisation
- Produkte
- Zertifikatsprofile

Die Basis für automatisierte Geschäftsprozesse und organisationsübergreifende Kommunikation sind definierte Schnittstellen und deren Einhaltung in Anwendungen und Diensten. Ein reibungsloser Ablauf zwischen den einzelnen Anwendungen und Diensten kann nur durch den Einsatz interoperabler Protokolle und Schnittstellen sichergestellt werden.

Um eine organisationsübergreifende, vertrauenswürdige Kommunikation zu ermöglichen, bedarf es neben der Festlegung von Protokollen und Schnittstellen auch der Klärung der folgenden Punkte:

- Vertrauenswürdiger Austausch von Wurzelzertifikaten,
- Zugriff auf Verzeichnisdienste und Verzeichnisdienstinformationen
- Validierungsmöglichkeit von Zertifikaten,
- Festlegung des organisatorischen und rechtlichen Rahmens
- Prüfung der Policies und Überwachung der Einhaltung

4.4.1. Organisatorische Interoperabilität

Für die organisatorische Interoperabilität ist die Beantwortung der folgenden Fragen von entscheidender Bedeutung für den Erfolg der Lösung:

- Wie können organisatorische Vertrauensbeziehungen zwischen den verschiedenen Teilnehmern/Organisationen geschaffen werden?
  - Klärung der Haftung für den jeweiligen Geschäftsprozeß?
  - Vertragswerk?
- Wie wird das organisatorische Vertrauen auf lange Sicht etabliert?

- Wird es in Deutschland eine Root-Instanz für die HPC oder mehrere Root-Instanzen geben?
- Wird es in Deutschland eine Root-Instanz für die PDC oder mehrere Root-Instanzen geben?
- Wie wird die Entwicklung innerhalb der Europäischen Union weitergehen?

- Wie können organisatorische Vertrauensbeziehungen zwischen den verschiedenen Root-Instanzen geschaffen werden?
- Wer darf unter welchen Voraussetzungen an der Architektur teilnehmen?
- Wer legt die Voraussetzungen für eine Teilnahme fest? (Governance?)
- Wer überprüft die Policies und führt das Mapping aus? (Governance?)
- Wer überprüft in welchen Abständen, ob die Teilnahmevoraussetzungen eingehalten werden?
- Wer ist der Ansprechpartner bei Problemen?

4.4.2. Technische Interoperabilität

Zur Interoperabilität zwischen verschiedenen PKI Strukturen müssen die folgenden Aufgaben über die einzelnen PKI-Grenzen hinweg gelöst werden:

- Sicherer Austausch und Verteilung von Wurzelzertifikaten
- Automatische Verteilung von Sub-CA Zertifikaten bzw. Cross-Zertifikaten
- Automatische Verteilung der Zertifikate bzw. Zugriffsinformationen
- Automatische Validierung von Zertifikaten bzw. Validierungszugangsinformationen

4.4.2.1. Interoperabilität von Certification Authorities

Um auf der Zertifikatsebene ist der Verteilung der Root-Zertifikate der verschiedenen Teilnehmer Public Key Infrastrukturen (HPC und PDC) an die einzelnen Teilnehmer und von dort in die Applikationen notwendig. Der Verteilungsvorgang ist kein einmaliger Prozess, sondern muss zeitnah und unkompliziert möglich sein. Dies ist die Voraussetzung für die Aufnahme neuer Teilnehmer-PKI's bzw. den schnellen Austausch von Root-Zertifikaten bei vermuteter oder erkannter Diskreditierung.

Weiterhin kann eine Cross-Zertifizierung auf Sub-CA-Ebene notwendig sein. Eine Cross-Zertifizierung ist dann erforderlich, wenn nicht der Gesamten PKI-Struktur des Teilnehmers, sondern nur einem Zweig das Vertrauen ausgesprochen werden soll. Hierbei ist festzulegen, ob eine einseitige oder eine zweiseitige Cross-Zertifizierung durchzuführen ist.

Die Verteilung, der Austausch und das Management der Root-Zertifikate bzw. Cross-Zertifikate in den Applikationen ist ein wichtiger Bestandteil der Interoperabilität.

Zusammenfassung:

- Austausch Wurzelzertifikate
- Wenn Cross Zertifizierung, dann muss auch die Art festgelegt werden (einseitig oder zweiseitig)

4.4.2.2. Interoperabilität von Verzeichnisdiensten

Für die Interoperabilität von Verzeichnisdiensten ist die Beantwortung der folgenden Fragen bzw. Festlegung von Vorgabe von entscheidender Bedeutung für den Erfolg der Lösung:

- Erarbeitung eines Rahmens für den Directory Information Tree (DIT) für den gesamten Verbund, soweit dies möglich ist (siehe Europäische Aktivitäten).

- Normierung und Formalisierung von Namensräumen und –konventionen über dem gesamten Directory Verbund.

- Vorgaben für den Zugriff auf die verschiedenen Verzeichnisdienste und das Management dieser Informationen:
  - Zugriff als Anonymus?
  - Zugriff per Username / Passwort?
  - Zugriff per Zertifikatsauthentifizierung und Autorisierung?
  - Absicherung der Datenübertragung durch SSL-Verbindungen?

- Wie erfolgen die Verteilung und das Management der Zugangsinformationen zu den Verzeichnisdiensten an die Applikationen? Der Verteilungsvorgang ist kein einmaliger Prozess, sondern muss zeitnah und unkompliziert jederzeit möglich sein.

- Wie erfolgt die Zugriffskontrolle auf diese Verzeichnisdienste?

- Welche Daten werden in den Verzeichnisdiensten bereitgestellt?

- Wer stellt die Daten für die Verzeichnisdienste bereit?

- Wie kann verhindert werden, dass andere Nutzer (eventuell Internetnutzer) der Infrastruktur Einblicke in die Verzeichnisstrukturen und deren Aufbau erhalten?

- Wie können Daten aus verschiedenen sicheren internen Netzwerkverzeichnissen über das Netzwerk (z.B. Internet) abgefragt werden, ohne dass unkalkulierbare Sicherheitsrisiken entstehen?

4.4.2.3. Interoperabilität von Validierungsdiensten

Für die Interoperabilität von Validierungsdiensten ist die Beantwortung der folgenden Fragen bzw. Festlegung von Vorgabe von entscheidender Bedeutung für den Erfolg der Lösung:

- Wie erfolgen die Verteilung und das Management der Zugangsinformationen zu den Validierungsdiensten an die Applikationen? Der Verteilungsvorgang ist kein einmaliger Prozess, sondern muss zeitnah und unkompliziert jederzeit möglich sein.

- Normierung und Formalisierung von Namensräumen und –konventionen über dem gesamten Validierungsverbund / Directory-Verbund.

- Wie soll die Validierung von Zertifikaten erfolgen?
  - Per OCSP?
  - Per CRL?

- Fallunterscheidung: Es gibt zwei verschiedene Modelle für die Bereitstellung von Certificate Revocation Informationen in Listenform mit ihren Besonderheiten:
  - Gesamt-CRL
    - Die Größe der Files kann beträchtliches Ausmaße annehmen und zu Handling-Problemen führen. Er existieren bereits erste CRL's im Internet mit einer Größe von ca. 80 MB.
  - Delta-CRL
    - Da es eine Vielzahl von Delta-CRL's geben kann, sind eine Reihe von Fragen zu klären:
      - Sollen alle Delta-CRL's geladen werden? (Sortierung, Reihenfolge?)
      - Wenn nicht, wie soll die Selektion erfolgen?
      - Wie erfolgt der Import auf dem Client?
      - Was geschieht bei der Neuinstallation eines Clients (Historie)?

- Wie erfolgt die Langzeitarchivierung von den notwendigen Validierungsinformationen?
- Wie lang müssen die Validierungsinformationen online verfügbar sein?
- Wie lang müssen die Validierungsinformationen offline verfügbar sein?

4.5. „Kritische Punkte" – Unterarbeitspaket Identitätsmanagement

Die nachfolgenden Themen wurden durch Vertreter des BMGS und biT4Health bearbeitet und Antworten auf die aufgeworfenen Fragen erarbeitet:

- Betreuungsverhältnis und Delegation der Willenserklärung
  - Dürfen unter Betreuung stehende Personen eine Karte mit Signaturfunktion erhalten?
  - Wie sieht es mit den verschiedenen Stufen der Betreuung aus?
  - Herausgabe der PIN erst nach der Volljährigkeit?

- Identifikationsmerkmale auf der Karte und Prüfung des Lichtbild
  - Reicht ein Foto auf der Karte als eindeutige Identifizierung aus?
  - Können Fotos bis zu einem bestimmten Alter weggelassen werden?
  - Wie kann der Arzt prüfen, ob die Karten im richtigen Kontext eingesetzt werden?
    - Weitergabe von Karten
    - Zuordnung Karte - Patient

1. Auch - gleich aus welchen Gründen - unter Betreuung stehende Versicherte dürfen und müssen eine PDC (mit/ohne Signaturfunktion) erhalten (zur „alten“ KVK: § 15 Abs. 6 Satz 1 SGB V). Einige der Krankenkassen verfahren gegenwärtig so, dass sie die PDC (KVK) bei nicht nach § 36 SGB I handlungsfähigen Versicherten, in der Regel also, wer das fünfzehnte Lebensjahr noch nicht vollendet hat oder unter Betreuungsvorbehalt nach § 1903 BGB steht, an den Ort oder Wohnsitz des gesetzlichen Vertreters übersenden.

2. Der Erhalt der PDC ist nicht von irgendeiner „Stufe der Betreuung“ abhängig. Der Grund, aus dem die Betreuung angeordnet worden ist (z. B. körperliche Gebrechlichkeit oder geistige Verwirrung, geistige Unreife als Kleinkind usw.) ist dabei unerheblich.

3. Die Ausgabe der PIN kann und sollte vor Erreichen der Volljährigkeit erfolgen.

4. Ein Lichtbild des Versicherten ist auf der PDC aufzubringen. Zusätzliche Anforderungen werden nicht zum Nachweis der Versicherteneigenschaft - von Gesetzes wegen – gefordert.

5. Neben der Prüfung des Lichtbildes sollte die Aktualität der Versichertenstatus geprüft werden (Online bzw. aktuelles Update auf der PDC).

5. Empfehlungen der Arbeitsgruppe

Empfehlung Migrationsfähigkeit

Es wird empfohlen, mit einer pragmatischen und robusten Lösung zu starten, die ein hohes Einsparpotential ermöglicht. Es muss jedoch eine Migration zu neueren Techniken und die Einbindung weiterer Funktionalitäten bzw. Applikationen mit geringem finanziellem und organisatorischem Aufwand möglich sein. Eine Harmonisierung in Europa sollte unter den gleichen Aspekten möglich sein.

Die Gesamtlösung sollte auf einheitlichen und anerkannten Standards und auf einer europaweit akzeptierten Infrastruktur basieren.

Empfehlung Einsatz von PKI

Die Arbeitsgruppe empfiehlt auf Basis der allgemeinen Erwartungshaltung an die Technik „Vollständige technische Interoperabilität zwischen allen Karten und Zertifikaten“ und der Erwartung, dass innerhalb der Europäischen Union auf mittlerer Sicht auch eine Interoperabilität der Karten gewährleistet sein muss, den Einsatz einer PKI. Andernfalls ist die Entwicklung von proprietären Lösungen zu befürchten, die dann wiederum zu Interoperabilitätsproblemen führen können und somit zu deutlich erhöhten Kosten bei der Behebung dieser Probleme.

Empfehlung ISIS-MTT

Für die Zertifikats- und Sperrlistenprofile empfiehlt die Arbeitsgruppe, die ISIS-MTT Spezifikation als Basis zu nutzen. Diese Spezifikation ist international anerkannt und es existiert bereits ein Testbed, gegen das getestet werden kann.

Empfehlung Policy

Es wird empfohlen innerhalb von Deutschland eine zentrale Stelle (eventuell Projektbüro der Selbstverwaltung?) einzurichten, die Vorgabe zu den Mindestniveaus festlegt und überwacht, an die sich die Teilnehmer an der Gesamtarchitektur zu halten haben. Innerhalb der Europäischen Union könnte diese Stelle das Policy Mapping zu den anderen EU-Mitgliedsstaaten und deren Lösungen vornehmen und so zu einer Harmonisierung beitragen.

Empfehlung European Bridge-CA

Da die Verzeichnisdienst- und Validierungsdienstzugangsinformationen von den verschiedenen Public Key Infrastrukturen der HPC ausgebenden Stellen und der PDC ausgebenden Stellen bei den Teilnehmern (Ärzte, Apotheker, Hebammen, …) über eine Vielzahl von stationären oder mobilen PCs in die Applikationen verteilt und ständig aktuell gehalten werden müssen, ist der Einsatz einer kostengünstigen und möglichst zentral administrierbaren Lösung absolut zu empfehlen, wie sie bereits bei der European Bridge-CA implementiert und umgesetzt ist. Aus diesem Grund empfiehlt die Arbeitsgruppe die Architektur der European Bridge-CA (auf Basis ETSI TSL 220) als Basis für die zentrale Verwaltung der verschiedenen Informationen und für den Austausch der Root-Zertifikate bzw. Cross-Zertifikate zu nutzen.

Empfehlung Validierung: OCSP und CRL

Für die Validierung wird ein zweistufiges Vorgehen empfohlen:

- Bereitstellung von OCSP zur Validierung von End Entity-Zertifikaten,
- Bereitstellung von CRLs für CA-Zertifikate.

Für die Validierung bei fehlender Online-Fähigkeit wird empfohlen, die anwendungsspezifische Prüfung manuell deaktivieren zu können.

Empfehlung Verwendung Signaturfunktion (Derzeit OPTIONAL)

Bezugnehmend auf die Formulierung im Gesetz ***„... im Falle des Absatzes 3 Satz 1 Nr. 5 können die Versicherten auch mittels einer eigenen Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt, zugreifen.“*** Wird empfohlen, falls Signaturen auf der PDC verwendet werden, qualifizierte Signaturen zu verwenden, da das Gesetz eine qualifizierte Signatur für den Zugriff auf die Karte erfordert.

6. Abkürzungsverzeichnis

BGB	Bürgerliches Gesetzbuch
CA	Certification Authority
CRL	Certificate Revocation List
DIT	Directory Information Tree
DL	Dienstleister
eGK	elektronische Gesundheitskarte
GKV	Gesetzliche Krankenversicherung
HBA	Heilberufeausweis
HPC	Health Professional Card
KVK	Krankenversichertenkarte
LDAP	Leightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PDC	Patient Data Card
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
SGB	Sozialgesetzbuch
SSL	Secure Socket Layer
TC	Trust Center