3.1.5 Datenschutz und Informationssicherheit

Der AN erstellt ein Datenschutz- und Datensicherheitskonzept einschließlich einer Datenschutzfolgeabschatzung und stimmt diese mit dem AG und den zuständigen Aufsichtsbehörden und insbesondere dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ab. Weiterhin führt der AN eine externe Begutachtung der IT-Sicherheit aller Komponenten und eine Durchführung von Penetrationstests durch. Diese Aufgaben können durch eine externe Firma oder eine unabhängige Geschäftseinheit den AN durchgeführt werden.

3.1.6 Support Dokumentationen

Der AN erstellt eine Benutzerdokumentation in elektronischer Form zur Installation, Integration und Nutzung zum Gesamtsystem elektronischer Impfnachweis. Adressaten zur Installation und Integration sind die IT-Dienstleister der Impfzentren und Praxen. Adressant für die Nutzung ist das medizinische Fachpersonal, welches mit der Ausstellung der Impfzertifikate betraut ist.

Für die Impfnachweis-App und die Prüf-App erstellt der AN eine Onlinefassung der Benutzerdokumentation zur Nutzung der Apps, welche in die Apps integriert und/oder Online aus der App heraus verlinkt ist. Da für die Apps kein Support vorgesehen ist, muss die Nutzerdokumentation eine hohe Qualität aufweisen. Weiterhin soll die Nutzerdokumentation FAQs mit Fragen und Antworten enthalten.

3.1.7 Veröffentlichung Schnittstellen und Quellcode

Der AN veröffentlicht den vollständigen und dokumentierten Quellcode für Impfnachweis-App, Prüf-App und das Frontend des Impfzertifikatsservices und gibt seine Zustimmung zur kostenfreien Nutzung durch Dritte. Der Quellcode wird in einem öffentlich zugänglich Repository (z. B. github) abgelegt und während der Projektlaufzeit im Zuge von Weiterentwicklungen und Fehlerkorrekturen aktualisiert. Neben dem Quellcode werden ebenfalls Build-Konfigurationsdateien und eine Dokumentation hierzu veröffentlicht, damit Dritte in die Lage versetzt werden, die Programmanteile zu erzeugen.

Der AN stellt ebenfalls eine Dokumentation zur Struktur des Impf- und Prüfzertifikats und deren Kodierung, sowie zum verwendeten 2D-Code bereit. Weiterhin erstellt der AN eine Dokumentation der Schnittstelle zum Backend des Impfzertifikatsservice. Die Dokumentation muss einerseits App-Entwickler von Impfnachweis-Apps bzw. Prüf-Apps in die Lage versetzten, Impfzertifikate und Prüfzertifikate zu verarbeiten, Prüfzertifikate durch das Backend erstellen zu lassen, und das kryptographische Rootmaterial für Impf- und Prüfzertifikate zu aktualisieren. Die Dokumentation muss es PVS-Herstellern ermöglichen, die Funktionen des Frondend selbst umzusetzen und direkt mit dem Backend bei der Erstellung der Impfzertifikate zu kommunizieren.

Weiterhin erstellt der AN Beispiel-Code für PVS-Hersteller zur Integration der Backend-Schnittstelle in den Sprachen Java und C++ bereit. Optional kann der AN ein SDK zur Integration bereitstellen.

3.1.8 Entwicklungsprozess

3.1.8.1 MS1 - Planungsabschluss

2 Wochen nach Projektstart sollen alle in dieser Leistungsbeschreibung genannten Abstimmungspunkte zwischen AN und AG, die auf den agilen Entwicklungsprozess der Gesamtlösung wirken, geklärt sein. Dies sind insbesondere:

- Der AN legt die Struktur des Impfzertifikats und des Prüfzertifikats im Sinne einer Schnittstelle fest und stimmt diese mit dem AG ab (Kapitel 3.1.1).
- Spätestens bis MS1 legt der AG das Format für das Feld UVCI fest (Kapitel 3.1.1).
- Zur Darstellung des Impfzertifikats auf dem Papierausdruck bzw. Bildschirm im Impfzentrum/Praxis verwendet der AN ein geeignetes 2D-Code-Format und stimmt das Format mit dem AG ab (Kapitel 3.1.1).

- Zur Darstellung des Prüfzertifikats in der Impfnachweis-App bzw. geeignetes 2D-Code-Format und stimmt das Format mit dem AG ab
- Der AN legt das „Trust Framework" zur kryptographischen Absich und stimmt dies mit dem AG ab (Kapitel 3.1.1).
- Abstimmung zur Berücksichtigung weiterer Regelungen der EU Struktur und Darstellung des Impfzertifikats als 2D-Code (Kapitel 3.
- Abstimmung mit dem AG zu weiteren Funktionen der Impfnachwei

Sofern der AN in der Lösungsskizze zusätzliche optionale Vorschläge zur Au Impf- und Prüfzertifikate unterbreitet hat, erfolgt spätestens zu MS1, in Al Festlegung durch den AG zu deren Berücksichtigung im Projektverlauf.

Nach erfolgreicher Abstimmung und einer Aktualisierung von Projektplan erklärt.

3.1.8.2 *MS2 - Betriebsbereitschaft*

Die Entwicklung der Gesamtlösung erfolgt in einer agilen Arbeitsweise. Mind den AN ein ablauffähiger Zwischenstand erstellt und dem AG präsentiert wer

Der AG hat hierbei die Möglichkeit durch frühzeitige Rückmeldungen Ein nehmen (z. B. beim UX-Design). Gleichzeit vereinfacht sich die spätere Ab Projektplan muss erkennbar sein, wie sich die Zwischenstände bis z Gesamtsystem entwickeln. An dem Termin nehmen neben den Projektl Experten auf Seiten des AN und AG teil.

8 Wochen nach Projektstart ist das Gesamtsystem fertig gestellt un Gesamtsystem wird durch den AN dem AG präsentiert.

Weiterhin müssen spatestens 8 Wochen nach Projektstart alle weiteren in genannten Abstimmungspunkte zwischen AN und AG, die auf den agi Gesamtlosung wirken, geklart sein. Dies sind insbesondere:

- Erstellung eines Datenschutz- und Datensicherheitskonz Datenschutzfolgeabschätzung durch den AN und Abstimmung hier

Nach Präsentation des Gesamtsystems, der Klärung der offenen Abstimmun

Im Rahmen des Projektabschlusses führt der AN eine strukturierte Erfassung der Projekterfahrungen im Rahmen eines „Lessons Learned"-Workshops mit dem AG durch.

3.2 Betriebsphase

3.2.1 Betrieb der Lösung

Mit Erreichung des MS2 beginnt der produktive Betrieb der Gesamtlösung. Der produktive Betrieb beginnt mit zwei kurzen Pilotierungsphasen die parallel und unabhängig voneinander starten können.

Die erste Pilotierung (Abschluss mit MS3a) betrachtet eine Pilotierung der Gesamtlösung in einem Impfzentrum in Deutschland und dauert bis zu einer Woche. Während der Pilotierung muss – nach Einwilligung der Bürger – für 10 verschiedene geimpfte Bürger ein Impfzertifikat erstellt werden. Für mindestens 5 Bürger muss – nach Aufklärung und Einwilligung – das Impfzertifikat mit der Impfnachweis-App eingelesen und das Prüfzertifikat mittels der Prüf-App geprüft werden.

Die zweite Pilotierung (Abschluss mit MS3b) betrachtet eine Pilotierung der Gesamtlösung in einer Arztpraxis in Deutschland und dauert bis zu einer Woche. Während der Pilotierung muss – nach Einwilligung der Bürger – für 6 verschiedene geimpfte Bürger ein Impfzertifikat erstellt werden. Für mindestens 3 Bürger muss – nach Aufklärung und Einwilligung – das Impfzertifikat mit der Impfnachweis-App eingelesen und das Prüfzertifikat mittels der Prüf-App geprüft werden.

Der AN dokumentiert die Ergebnisse aus beiden Pilotierungen in einem Pilotierungsbericht. Insbesondere sind aufgetretene Probleme zu beschreiben und zu adressieren. Die Ergebnisse werden mit dem AG besprochen, um zu entscheiden, ob ein Flächenrollout der Gesamtlösung starten kann.

3.2.2 Service und Support

Für die IT-Dienstleister der Impfzentren und für die Dienstleister-vor-Ort (DVO) der Praxen betreibt der AN einen Support für die dort vorhandenen und genutzten Systembestandteile der Gesamtlösung zum elektronischen Impfnachweis. Support erfolgt hierbei über Telefon, E-Mail und optional über eine Portallösung.

Jede Support-Anfrage bzw. diesbezügliche Kontaktaufnahme wird im Ticketsystem den AN mit mindestens folgenden Informationen erfasst:

- Erfassung als Interaction oder Sub-Interaction mit Zuordnung/Verlinkung zur übergeordneten Interaction-ID,
- Daten des Support-Anfragenden (Rufnummer, E-Mail, Firma etc. – sofern möglich und erforderlich),
- Status der Support-Anfrage (abgebrochen, angenommen, ...),
- Zeitstempel der vorgenommenen Bearbeitungsschritte (Eingang, Warteschleife, Annahme, Weiterleitung, ...),
- Zuordnung zu einem oder mehreren Kriterien als Basis für die Call-Klassifikation (Art der Anfrage, Nutzergruppe).

Alle Support-bezogenen Outbound-Aktivitäten werden ebenfalls im Ticketsystem zur betreffenden Interaction-ID dokumentiert. Dies können Rückrufe via Telefon oder gesendete E-Mails sein. Diese müssen entsprechend im Ticketsystem klassifiziert und dokumentiert werden.

Für den Support gelten folgende Service Zeiten und Service-Level:

- Servicezeit (Hauptzeit):
  Montag bis Freitag 08:00 bis 17:00 Uhr,
  ausgenommen bundeseinheitliche Feiertage

- Reaktionszeit nach Eingang der Support-Anfrage: 1 Stunde
- Erreichbarkeit Telefon-Support:
  - Annahme 75 % in 60 Sekunden
  - Annahme 95 % in 120 Sekunden

- Eingeschränkte Servicezeit (Nebenzeit):
  alle anderen Zeiten
  - Reaktionszeit nach Eingang der Support-Anfrage: 4 Stunde

3.2.3 Reporting gegenüber dem AG

Mit Beginn der Betriebsphase informiert der AN den AG regelmäßig alle zwei Wochen über folgende Kennzahlen:

- Anzahl der ausgestatteten Impfzentren und Praxen
- Anzahl der ausgestellten Impfzertifikate und Prüfzertifikate
- Anzahl der Support-Anfragen in Impfzentren und Arztpraxen
- Übersicht über erkannte Fehler im Gesamtsystem und Behandlung dieser
- Geplante und ungeplante Ausfallzeiten des Systems

Auf Anforderung des AG können weitere Kennzahlen in den Report aufgenommen werden.

Bei besonderen Vorkommnissen wie bspw. ungeplanten Systemausfällen, Einschränkungen der Verfügbarkeit, Sicherheits- und Datenschutzvorfälle informiert der AN den AG unaufgefordert und unverzüglich.

Besprechungen in der Betriebsphase werden nur bei Bedarf durch den AG oder AN einberufen.

4 Projektablauf

4.1 Phasen und Meilensteine

Das Projekt ist in folgende Phasen untergliedert:

- Aufbauphase,
- Projektphase und
- Betriebsphase.

Den Projektphasen sind Meilensteine (MS) zugeordnet, zu denen jeweils bestimmte Lieferungen bzw. Leistungen seitens des AN erfolgt sein müssen:

- MS1 – Planungsabschluss,
- MS2 – Betriebsbereitschaft,
- MS3a – Abschluss Pilotierung Impfzentrum,
- MS3b – Abschluss Pilotierung Arztpraxis,
- MS4 –Projektabschluss und Abnahme,
- MS5 – Ende Wirkbetrieb

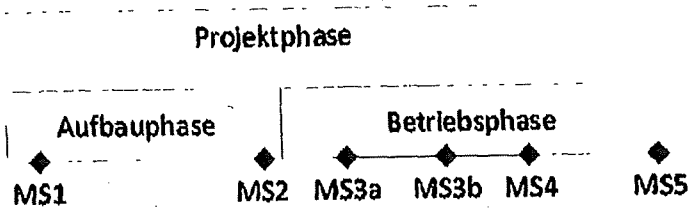


Abbildung 5: Projektphasen und Meilensteine

Die zeitliche Abfolge – ausgenommen der Abfolge vom MS3a und MS3b - der Meilensteine ist einzuhalten. Es gelten folgende Termine:

- MS1: spätestens 1 Wochen nach Projektbeginn
- MS2: spätestens 8 Wochen nach Projektbeginn
- MS3a: spätestens 9 Wochen nach Projektbeginn
- MS3b: spätestens 9 Wochen nach Projektbeginn
- MS4: spätestens 13 Wochen nach Projektbeginn
- MS5: Ende Betriebsphase ist der 31.12.2021

Für diese sechs Meilensteine sind die vom AN in seinem Angebot getätigten Angaben verbindlich, soweit diese strengere Fristen oder Termine vorsehen. Die den Meilensteinen zugeordneten Leistungen sind in Kapitel 3 beschrieben.

Der AG erwartet, dass sich aufgrund der sich verändernden Anforderungslage (u.a. zur Berücksichtigung der EU Vorgaben) regelmäßig Änderungen im Projekt ergeben, die über das Change-Verfahren (siehe Kapitel

5.6) adressiert werden. Die Projektphase wird in diesem Fall entsprechend verlängert, dass geänderte Vorgehen zur Abnahme wird im Change-Verfahren geregelt.

5 Zusammenarbeit

5.1 Projektmanagement

5.1.1 Allgemeines

Das Vorhaben erfordert eine sehr strukturierte und zielgerichtete Planung und Steuerung durch ein vom AN aufzusetzendes Projektmanagement.

An dieses Projektmanagement werden folgende übergreifende Anforderungen gestellt:

- Der AN stellt ein geeignetes Projektmanagement zur effizienten vertragsgerechten Umsetzung seiner Leistungen bereit.
- Der AN ergreift geeignete Maßnahmen und Methoden um Projektrisiken – etwa technischer, organisatorischer, zeitlicher oder kommerzieller Art – zu vermeiden bzw. frühzeitig zu erkennen und ihnen in effizienter Weise entgegenzuwirken.
- Der AN muss ein kontinuierlich begleitendes Qualitätsmanagement in seine Projektplanungen einbeziehen (siehe Kapitel 5.3).
- Der AN sorgt dem AG gegenüber stets für Transparenz über den Projektfortschritt.
- Der AN stimmt sich bei allen Umsetzungstätigkeiten eng mit dem AG ab.

5.1.2 Projektorganisation

Der AN hat eine geeignete Projektorganisation aufzubauen, die eng mit dem AG zusammenarbeitet. Hierzu hat er für die Dauer der Projektabwicklung unter anderem die Mitglieder der Projektorganisation und konkrete Ansprechpartner zu benennen für:

- Projektleitung
- Kernteam (wichtigste Ansprechpartner für bestimmte Rollen und Funktionen (kaufmännisch, vertraglich, fachlich) und für bestimmte Leistungen bzw. Phasen der Umsetzung)

Die Erreichbarkeit dieser Ansprechpartner für den geplanten Projektzeitraum ist durch den AN zu gewährleisten. Ein Austausch von benannten Mitgliedern der Projektorganisation ist nur nach Zustimmung des AG möglich.

Der AN gewährleistet, dass die Ansprechpartner verbindliche Auskünfte/Entscheidungen innerhalb ihres Verantwortungsbereiches erteilen/treffen können oder jederzeit durch verbindliche Aussagen des Projektleiters unterstützt werden.

Spätestens zum Start des Projektes hat der AN seine organisatorische Vorbereitung abzuschließen. Hierbei werden zwischen AG und AN auch erforderliche Organisations- und Steuerungsmittel, Regelmeetings, Kommunikationsformen und -formate, Berichtswege und -intervalle, Änderungs- und Eskalationsverfahren sowie weitere Aspekte der Organisation des Projektes abgestimmt und bestätigt.

Weiterhin gelten folgende Anforderungen:

- Aufgrund der kurzen Abbauphase findet ein Projektstatus-Meeting einmal pro Woche (im Bedarfsfall auch häufiger) statt.
- Die Entwicklung der Lösung erfolgt in einer agilen Arbeitsweise unter Einbeziehung des AG (siehe Kapitel 3.1.8.2).
- Der AN übernimmt für die gesamte Projektdauer die Projektplanung. Der AG kann nach Zuschlagserteilung jederzeit Anpassungen in Abstimmung mit dem AN aus sachlichen Gründen verlangen.

- Relevante Änderungen müssen durch den AG genehmigt werden.

5.2 Kick-off-Workshop

AN und AG führen innerhalb von 3 Arbeitstagen nach Projektstart einen Kick-off-Workshop durch. Die Einladung und Organisation erfolgen durch den AN. Der AG bestimmt, ob der Termin in den Räumen des AG oder als Videokonferenz stattfindet. Teilnehmer sind die Projektleiter beider Häuser sowie mit wesentlichen Aufgaben betraute Projektteilnehmer.

Die Agenda umfasst mindestens

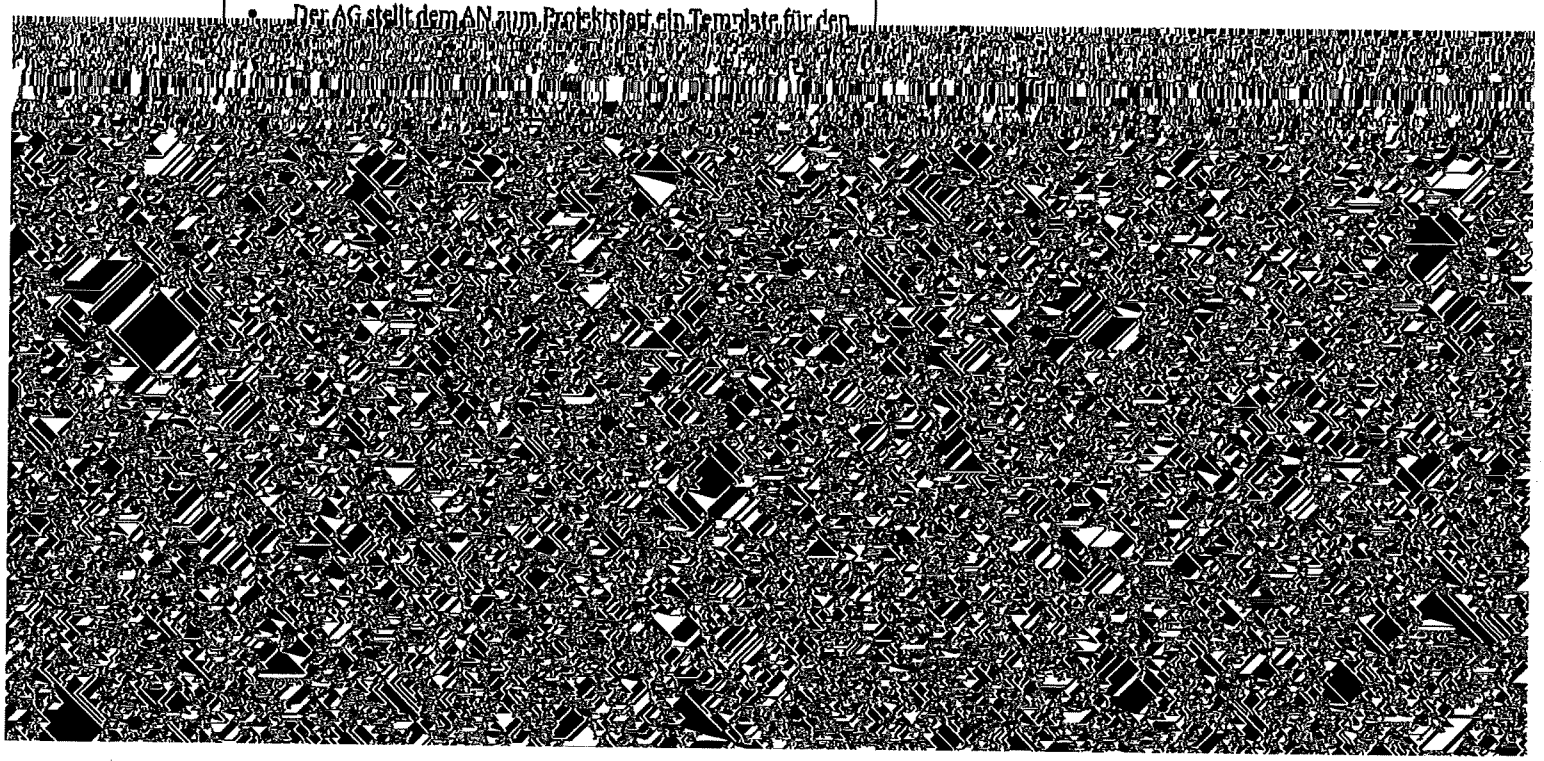
- die Konkretisierung der organisatorischen Zusammenarbeit (Berichtswesen, Datenaustausch, Vorlagen u. ä.),
- die Besprechung der Systemlösung und des Projektplans des AN,
- Klärung bzw. Dokumentation offener Fragestellungen und
- zeitliche Planung zur Abstimmung der in dieser Leistungsbeschreibung festgelegten Abstimmungsthemen zwischen AN und AG.

5.2.1 Berichtswesen und Reporting

Der AN muss innerhalb des Projektmanagements in den Projektphasen die folgenden Aufzeichnungen führen und dem AG zur Verfügung stellen.

Tabelle 1: Dokumente des Projektmanagements

Projektaufzeichnung
Projektplan (Gantt-Diagramm) • Aktivitäten, Abhängigkeiten, Soll- und Ist-Aufwand, Soll- und Ist-Termine, Liefergegenstände und Meilensteine, kritischer Pfad etc.
Statusbericht (Frequenz wöchentlich) • Erfüllungsgrad der Aktivitäten des Projektplans, detaillierter Forecast der Liefergegenstände, ggf. Aufzeigen von Abweichungen, Abstimmungs- und Entscheidungsbedarfe, Risiken, Liste der offenen Punkte etc. • Der AG stellt dem AN zum Projektstart ein Template für den



Räumen des AG oder als Videokonferenz stattfindet. Der AG kann für einzelne Themen oder permanent weitere Teilnehmer – bspw. der gematik, anderer betroffener Ministerien und ggf. beauftragter IT-Dienstleister des Bundes – hinzuziehen.

5.4 Qualitätsmanagement

5.4.1 Grundlagen des Qualitätsmanagements

Um die einwandfreie Qualität seiner Services und Dienstleistungen gewährleisten zu können, muss der AN über ein geeignetes Qualitätsmanagementsystem (z. B. nach ISO 9001:2015 oder gleichwertig) bei Vertragsschluss verfügen, danach verfahren und dies umfassend dokumentieren sowie über die Vertragsdauer aufrechterhalten.

Der AN muss alle notwendigen Prozesse seines Qualitätsmanagementsystems auf den Vertragsgegenstand anwenden. Dies bedeutet, dass das Qualitätsmanagementsystem des Unternehmens die für den jeweiligen Liefergegenstand geeigneten Qualitätsplanungs-, Qualitätslenkungs-, Qualitätssicherungs- und Qualitätsverbesserungstätigkeiten umfassen muss.

Der AN wird mit seinem Qualitätsmanagementsystem sicherstellen, dass die von ihm oder einem Unterauftragnehmer erbrachten Leistungen den vertraglichen Anforderungen entsprechen.

5.4.2 Qualitätssicherung

Der AN muss sicherstellen, dass nur qualitätsgesicherte, für den Nutzungszweck geeignete und vertragskonforme Liefergegenstände an den AG geliefert werden.

Der AN hat durch geeignete und dokumentierte Maßnahmen sicherzustellen, dass seine Produkte und Dienstleistungen zum Zeitpunkt der Lieferung fehlerfrei sind und die als Anforderungen festgelegten Merkmale aufweisen. Der AN muss sicherstellen, dass die von ihm hierzu eingesetzten Prüfmittel geeignet sind, alle vereinbarten Merkmale auf Einhaltung der Vorgaben zu prüfen. Wenn Serviceänderungen auch Änderungen der Prüfmittel erfordern, sind diese gleichzeitig vorzunehmen.

Die Prüfergebnisse müssen dokumentiert werden. Die Dokumentation muss der AN dem AG auf erstes Anfordern vollständig übergeben.

Änderungen am Vertragsgegenstand müssen gekennzeichnet und aufgezeichnet werden. Die Änderungen müssen, soweit angemessen, bewertet, verifiziert und validiert werden und sind nur mit Zustimmung durch den AG zulässig.

5.5 Datenschutz und Datensicherheit

Der AN muss während der gesamten Vertragslaufzeit und in jedem Stadium seiner Leistungserbringung zwingend die gesetzlichen Vorgaben zu Datenschutz und Datensicherheit befolgen. Der AN wird die Rechenzentren, in denen seine Produkte betrieben werden, in der EU einrichten und betreiben. Eine Verlagerung der Rechenzentren darf nur nach vorheriger Zustimmung des AGs erfolgen. Die Daten dürfen die EU zu keinem Zeitpunkt verlassen.

5.6 Change-Verfahren

Relevante Änderungen der vertraglichen Leistungen und des Projektplans, durch den AN müssen durch den AG genehmigt werden.

Der AG kann nach Zuschlagserteilung seinerseits jederzeit Änderungen der vertraglichen Leistung und des Projektplans verlangen; dies betrifft insbesondere die Weiterentwicklung der Software, bspw. die Entwicklung und Programmierung zusätzlicher und/oder erweiternder Funktionen und Programme etc. Entsprechende Änderungsverlangen erfolgen im Rahmen des vertraglich fixierten Change-Request-Managements und sind durch den AN im Projektplan abzubilden.

Die Anforderungen an das vertragliche Change-Verfahren ergeben sich aus dem Vertrag und den dazugehörigen Bestimmungen der EVB-IT System-AGB.

Der AN nutzt einen dokumentierten Change-Verfahren-Prozess, welcher mit Hilfe standardisierter Methoden und Prozeduren die kontrollierte, wirtschaftliche, transparente und termingerechte Umsetzung von Changes im Projektverlauf sicherstellt.

Dabei hat der AN insbesondere folgende Aufgaben sicherzustellen:

(1) Entgegennehmen und Aufzeichnen der Änderungsanträge des AG durch den AN

(2) Erstellung eigener Änderungsanträge

(3) Einschätzen der Auswirkungen, Kosten, Nutzen und Risiken der geplanten Änderungen

(4) (Nach-)Führen des Change-/Release-Plans während der Projektlaufzeit

(5) Steuern der Implementierung in Abstimmung mit dem AG und

(6) Überwachen des Change-Prozesses und Berichten über den Umsetzungserfolg an den AG.

5.7 Sprache

Die Leistungserbringung des AN erfolgt grundsätzlich in deutscher Sprache auf dem Niveau C1 oder höher (vgl. https://www.europaeischer-referenzrahmen.de/).

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AG	Auftraggeber
AN	Auftragnehmer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
LG	Liefergegenstand
MS	Meilenstein
PKI	Public Key Infrastructure
PVS	Praxisverwaltungssysteme
SMC-B	Security Modul Card Typ B
TI	Telematikinfrastruktur (nach § 306 SGB V)

A2 – Abbildungsverzeichnis

Abbildung 1: Übersicht elektronischer Impfnachweis....4
Abbildung 2: Erstellung in Impfzentren....5
Abbildung 3: Erstellung in Arztpraxen....6
Abbildung 4: Validierung von Prüfzertifikaten....7
Abbildung 5: Projektphasen und Meilensteine....17

A3 – Tabellenverzeichnis

Tabelle 1: Dokumente des Projektmanagements....20

A4 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI_TR-02102-1]	BSI: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 24.03.2020
[EU_proof_of_vaccination]	EU: eHealth Network - Guidelines on proof of vaccination for medical purposes, V1.1, 27.01.2021 https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf
[Vertrag]	EVB-IT Systemvertrag, Anlage 5 evb_it_systemvertrag_Impfnachweis.docx

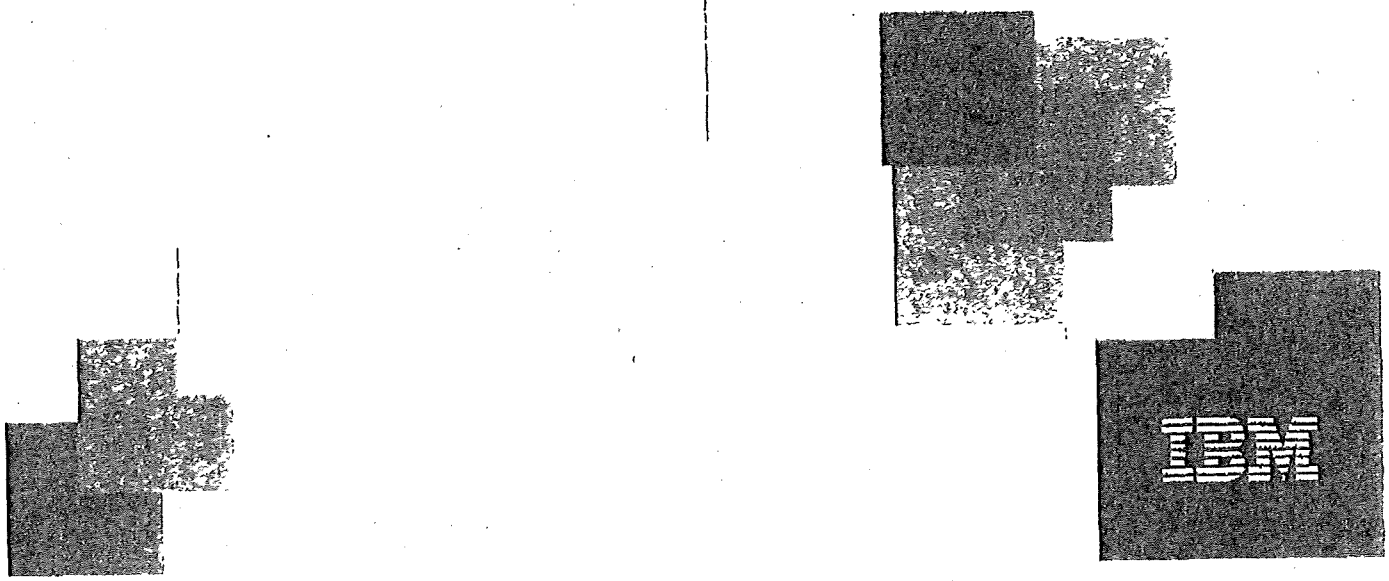
Anlage 2
Angebot des Bieters

Angebotsdatum: 01. März 2021

IBM Angebot für das Bundesministerium für Gesundheit

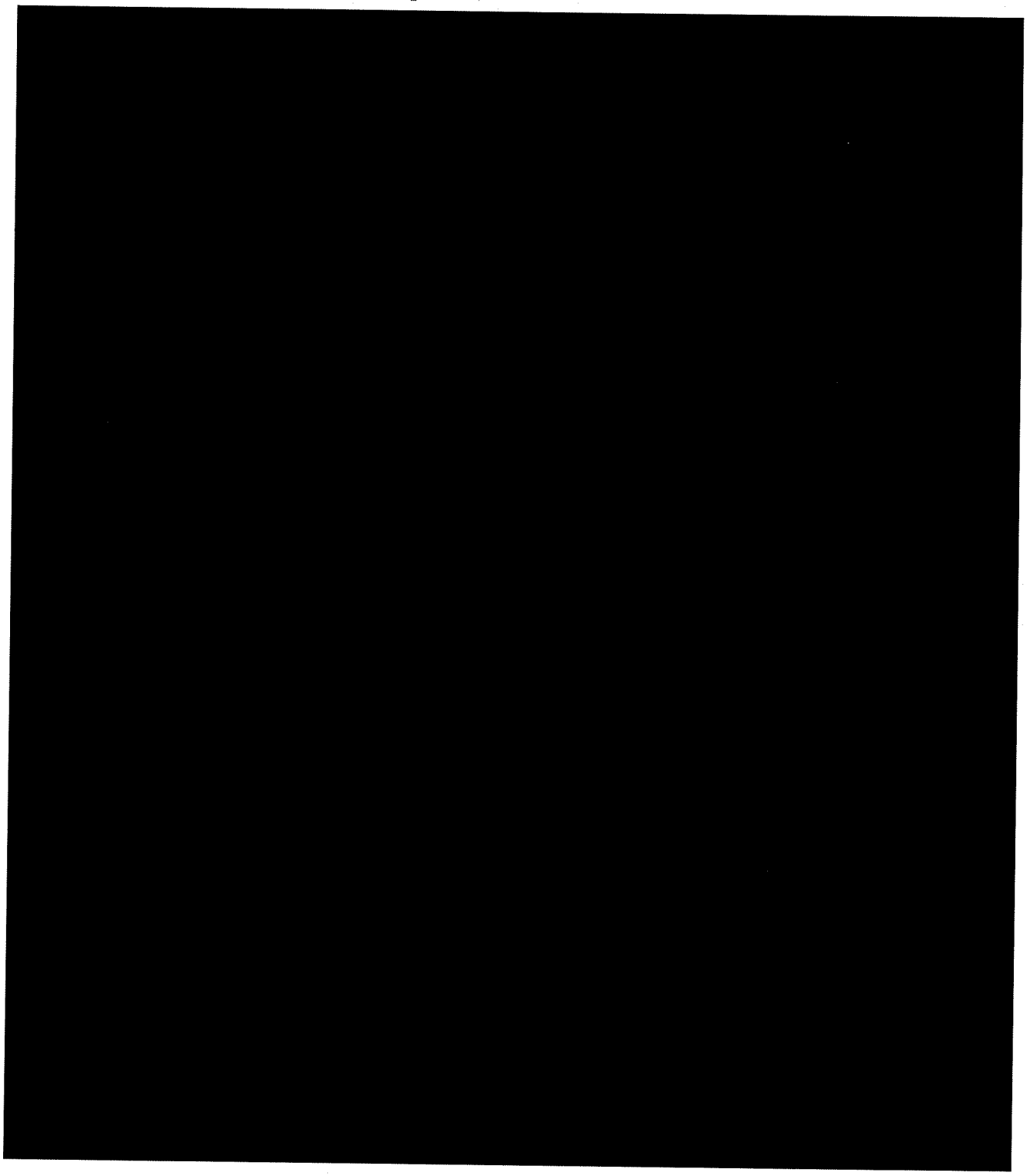
Vergabeverfahren elektronischer Impfnachweis

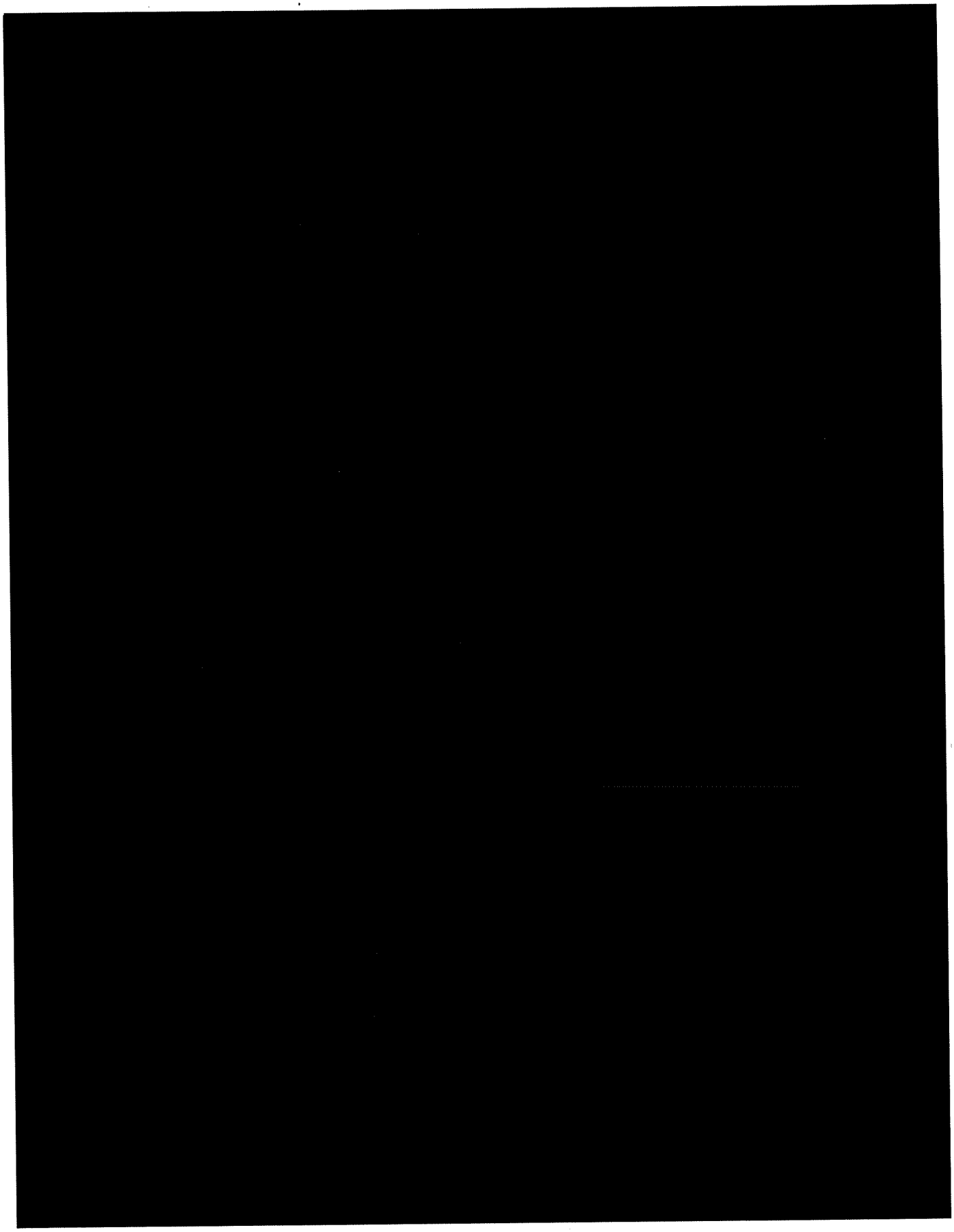
AZ: Z15-04800-05/006
Konzept 1 (K-01): Lösungsskizze

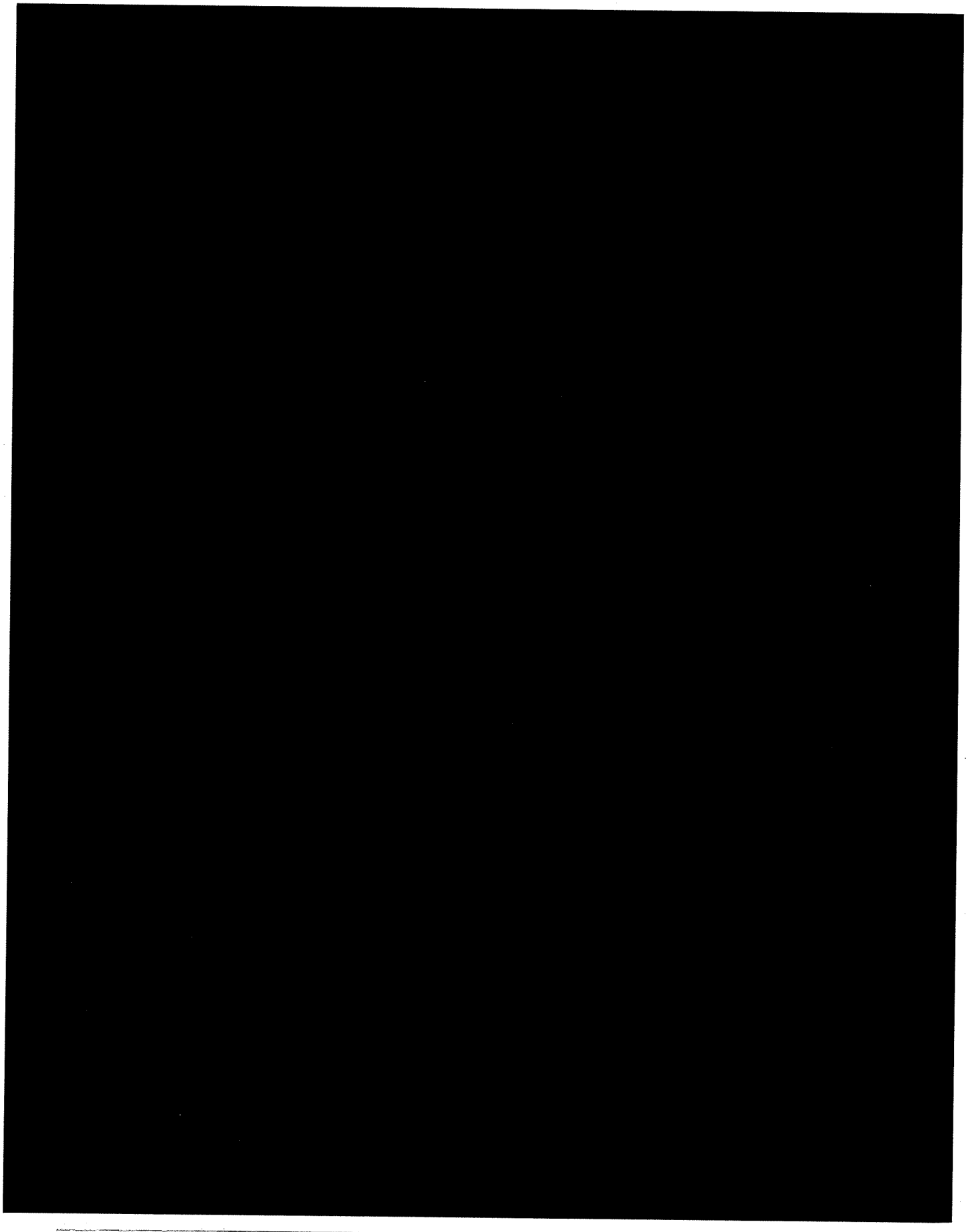


1) Vorbemerkung

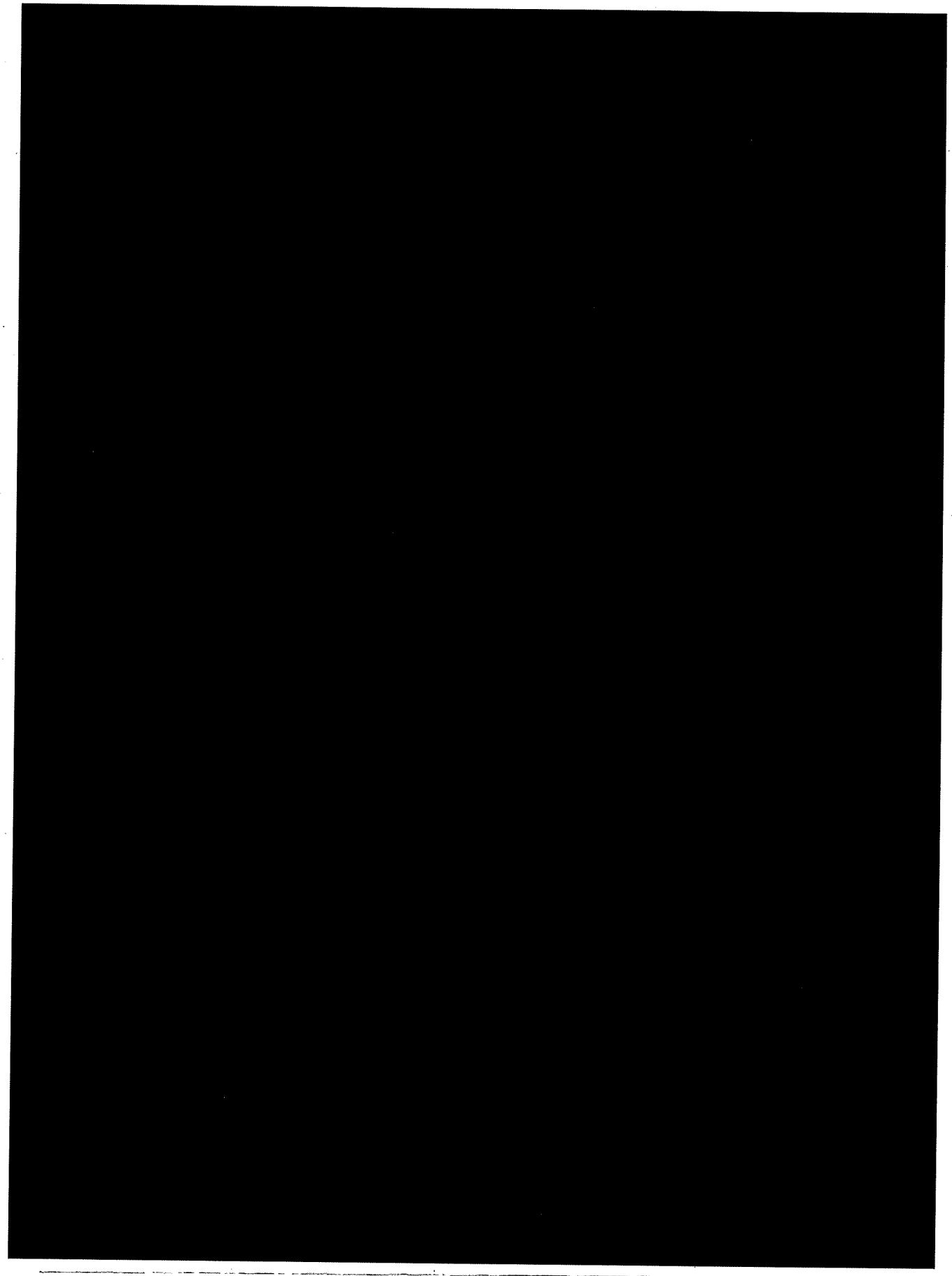
Die vorgeschlagene System-Architektur implementiert das Impfzertifikat datenschutzkonform nach Grundprinzipien von Self-Sovereign-Identity (SSI) und nutzt bereits für den Zweck produktiv erprobte Komponenten, um eine sehr zügige Bereitstellung des Gesamtsystems zuverlässig und risikoarm zu ermöglichen. Das erzeugte Impfzertifikat ist nach den Richtlinien der EU eHealth-Plattform gestaltet, fälschungssicher und barrierefrei verifizierbar. Dies ist eine zentrale Anforderung, um das Ziel einer breiten Akzeptanz in der Bevölkerung auch praktisch zu erreichen.







[redacted]



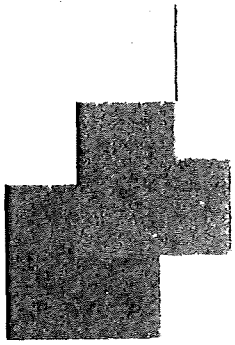
IBM Angebot für das Bundesministerium für Gesundheit

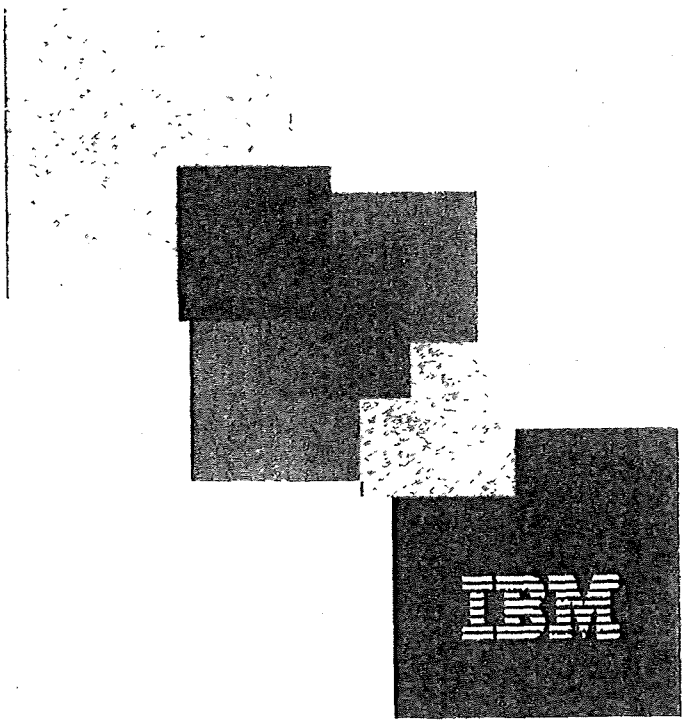
Vergabeverfahren elektronischer Impfnachweis

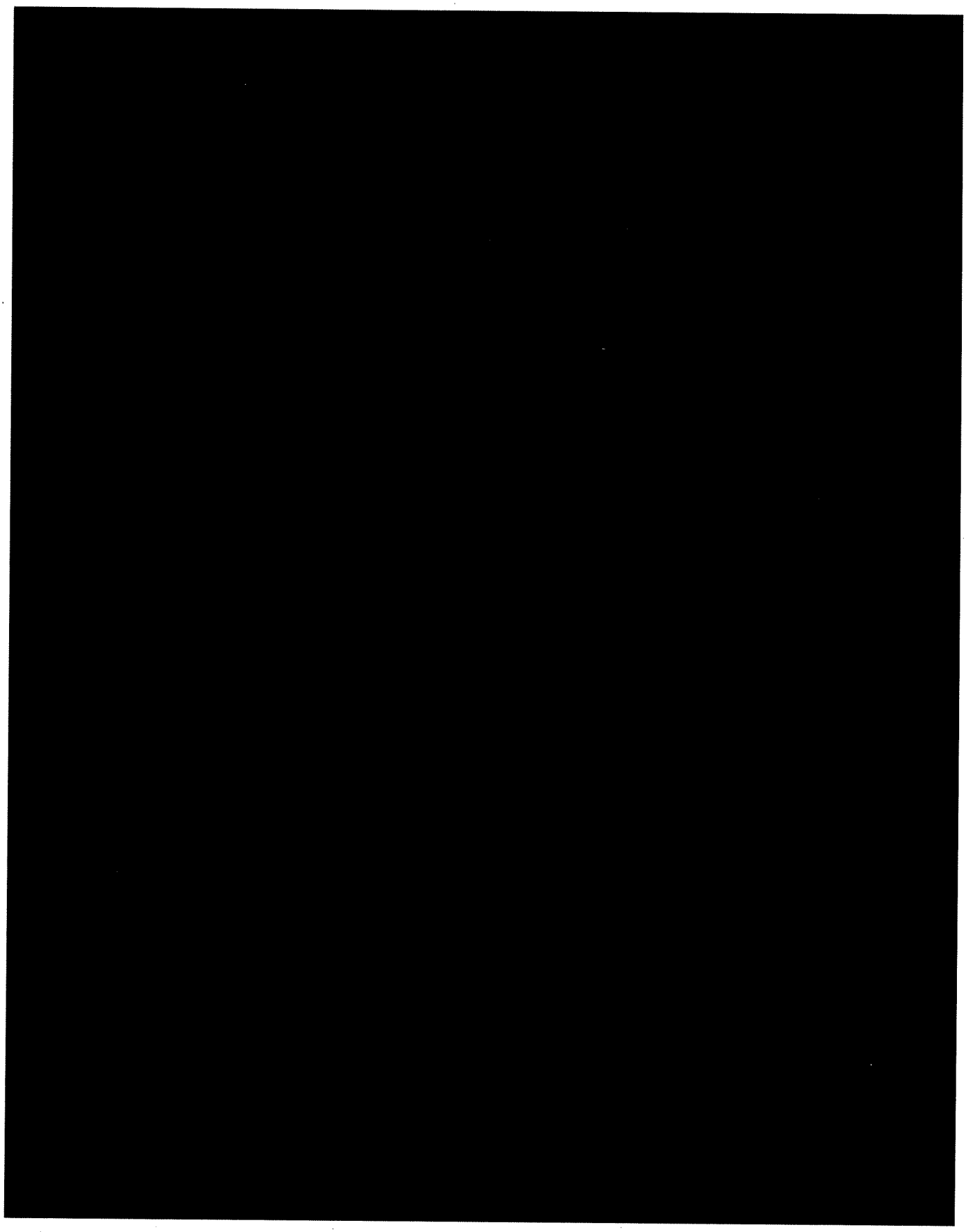
AZ: Z15-04800-05/006

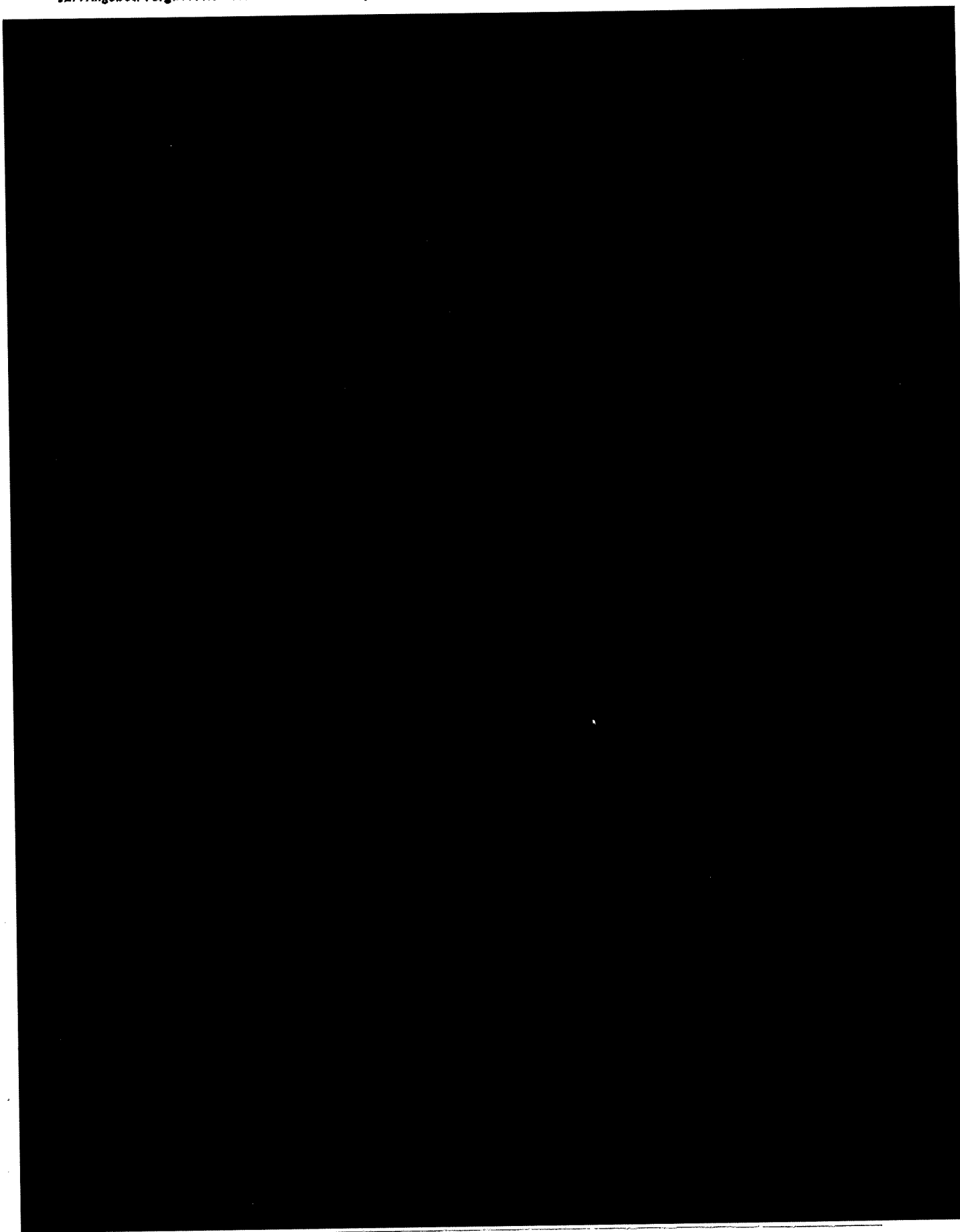
Konzept 2 (K-02): Projektplan

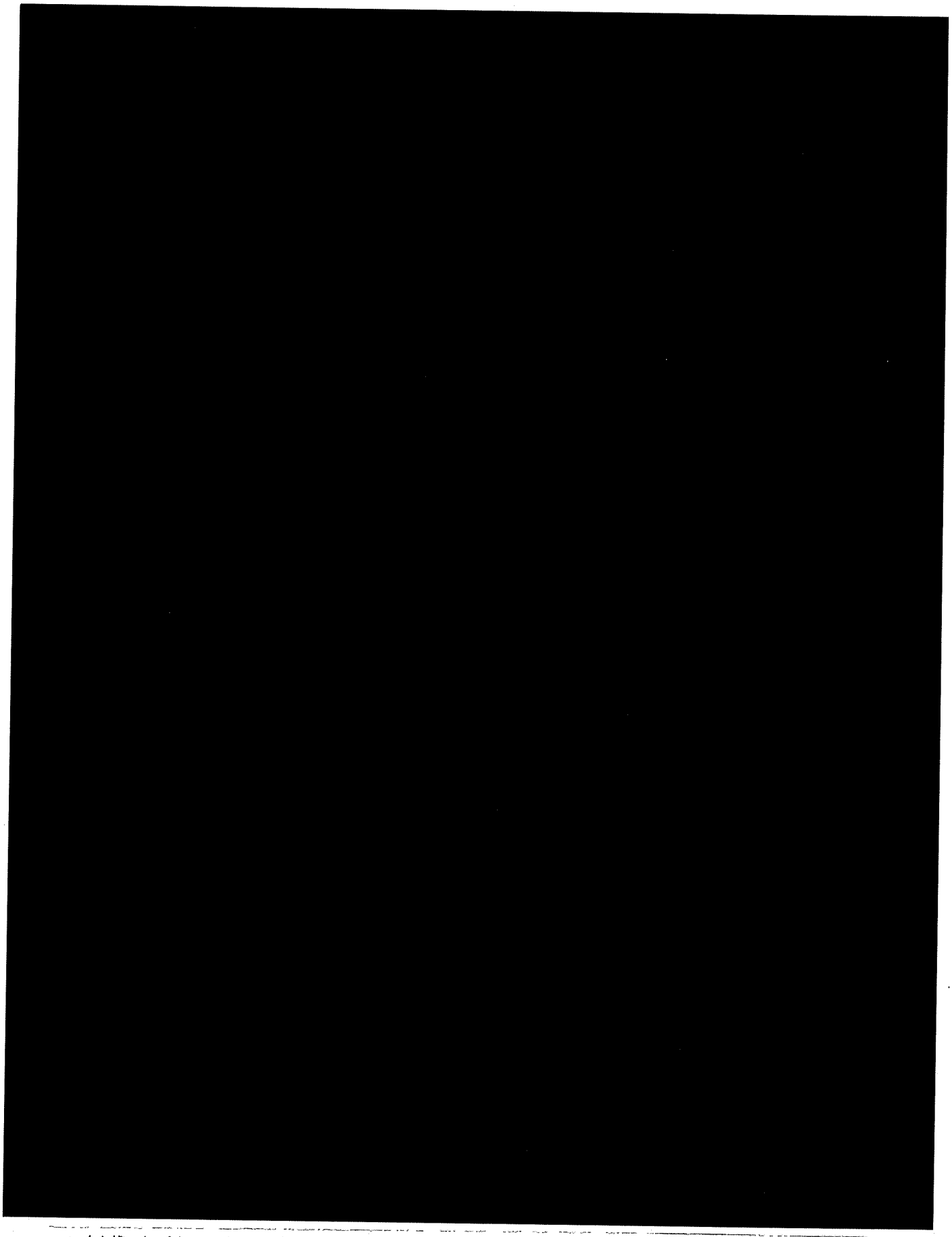
Angebotsdatum: 1. März 2021











Formblatt Erklärung zur Eignung:

Bezeichnung des Bieters:

IBM Deutschland GmbH

Bezeichnung und Funktion des Erklärenden:

☒ Einzelbieter
☐ Mitglied einer Bietergemeinschaft
☐ Eignungsverschaffendes Unternehmen (Eignungsleihe)

* Dieses Formblatt ist von dem Bieter, im Fall einer Bietergemeinschaft von jedem Mitglied der Bietergemeinschaft und im Fall der Eignungsleihe von dem eignungsverleihenden Unternehmen auszufüllen.

Firmenname und Adresse:	IBM Deutschland GmbH IBM-Allee 1 71139 Ehningen
Ansprechperson für das Vergabeverfahren:	[redacted]
Telefon/Fax:	
E-Mail	

I. Erklärung zu den Ausschlusstatbeständen gemäß §§ 123, 124 GWB

☒ Ich erkläre/Wir erklären, dass keine Ausschlussgründe gemäß den §§ 123 und 124 GWB vorliegen, die meine/unsere Zuverlässigkeit in Frage stellen.

☐ Ich erkläre/Wir erklären, dass wir die vorgenannten Erklärungen nicht abgegeben können, weil der in der Anlage beschriebene Sachverhalt vorliegt (Erklärung vom Erklärenden zu erstellen und beizufügen).

☐ Ich erkläre/Wir erklären, dass wir folgende Selbstreinigungsmaßnahmen gemäß § 125 GWB vorgenommen haben (Erklärung vom Erklärenden zu erstellen und beizufügen).

Hamburg 26.02.2021
Ort, Datum

Unterzeichnung* durch den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffende Unternehmen:

IBM Deutschland GmbH
Name des Bieters, des bevollmächtigten Mitglieds der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmens

[redacted]

Vollständiger Name der natürlichen Person, die die Erklärung für den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmen abgibt

[redacted]

****

Formblatt Erklärung zur Eignung:

Bezeichnung des Bieters:

IBM Deutschland GmbH

Bezeichnung und Funktion des Erklärenden:

☐ Einzelbieter
☐ Mitglied einer Bietergemeinschaft
☒ Eignungsverschaffendes Unternehmen (Eignungsleihe)

* Dieses Formblatt ist von dem Bieter, im Fall einer Bietergemeinschaft von jedem Mitglied der Bietergemeinschaft und im Fall der Eignungsleihe von dem eignungsverleihenden Unternehmen auszufüllen.

Firmenname und Adresse:	UBIRCH GmbH Im Mediapark 5 50670 Köln
Ansprechperson für das Vergabeverfahren:	[redacted]
Telefon/Fax:	
E-Mail	

I. Erklärung zu den Ausschlusstatbeständen gemäß §§ 123, 124 GWB

☒ Ich erkläre/Wir erklären, dass keine Ausschlussgründe gemäß den §§ 123 und 124 GWB vorliegen, die meine/unsere Zuverlässigkeit in Frage stellen.

☐ Ich erkläre/Wir erklären, dass wir die vorgenannten Erklärungen nicht abgegeben können, weil der in der Anlage beschriebene Sachverhalt vorliegt (Erklärung vom Erklarenden zu erstellen und beizufügen).

☐ Ich erkläre/Wir erklären, dass wir folgende Selbstreinigungsmaßnahmen gemäß § 125 GWB vorgenommen haben (Erklärung vom Erklärenden zu erstellen und beizufügen).

Köln, 26.02.2021
Ort, Datum

Unterzeichnung* durch den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffende Unternehmen:

UBIRCH GMBH
Name des Bieters, des bevollmächtigten Mitglieds der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmens

[redacted]
Vollständiger Name der natürlichen Person, die die Erklärung für den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmen abgibt

****

Formblatt Erklärung zur Eignung:

Bezeichnung des Bieters:

IBM Deutschland GmbH

Bezeichnung und Funktion des Erklärenden:

☐ Einzelbieter
☐ Mitglied einer Bietergemeinschaft
☒ Eignungsverschaffendes Unternehmen (Eignungsleihe)

* Dieses Formblatt ist von dem Bieter, im Fall einer Bietergemeinschaft von jedem Mitglied der Bietergemeinschaft und im Fall der Eignungsleihe von dem eignungsverleihenden Unternehmen auszufüllen.

Firmenname und Adresse:	govdigital eG Charlottenstr. 65 10117 Berlin
Ansprechperson für das Vergabeverfahren:	[redacted]
Telefon/Fax:	
E-Mail	

I. Erklärung zu den Ausschlusstatbeständen gemäß §§ 123, 124 GWB

☒ Ich erkläre/Wir erklären, dass keine Ausschlussgründe gemäß den §§ 123 und 124 GWB vorliegen, die meine/unsere Zuverlässigkeit in Frage stellen.

☐ Ich erkläre/Wir erklären, dass wir die vorgenannten Erklärungen nicht abgegeben können, weil der in der Anlage beschriebene Sachverhalt vorliegt (Erklärung vom Erklärenden zu erstellen und beizufügen).

☐ Ich erkläre/Wir erklären, dass wir folgende Selbstreinigungsmaßnahmen gemäß § 125 GWB vorgenommen haben (Erklärung vom Erklärenden zu erstellen und beizufügen).

__Berlin am 26.02.2021_____
Ort, Datum

Unterzeichnung* durch den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffende Unternehmen:

govdigital eG

Name des Bieters, des bevollmächtigten Mitglieds der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmens

[redacted]

Vollständiger Name der natürlichen Person, die die Erklärung für den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffenden Unternehmen abgibt

****

Formblatt Erklärung zur Eignung:

Bezeichnung des Bieters:

IBM Deutschland GmbH

Bezeichnung und Funktion des Erklärenden:

☐ Einzelbieter
☐ Mitglied einer Bietergemeinschaft
☒ Eignungsverschaffendes Unternehmen (Eignungsleihe)

* Dieses Formblatt ist von dem Bieter, im Fall einer Bietergemeinschaft von jedem Mitglied der Bietergemeinschaft und im Fall der Eignungsleihe von dem eignungsverleihenden Unternehmen auszufüllen.

Firmenname und Adresse:	Bechtle AG Bechtle Platz 1 74172 Neckarsulm
Ansprechperson für das Vergabeverfahren:	[redacted]
Telefon/Fax:	
E-Mail	

I. Erklärung zu den Ausschlusstatbeständen gemäß §§ 123, 124 GWB

☒ Ich erkläre/Wir erklären, dass keine Ausschlussgründe gemäß den §§ 123 und 124 GWB vorliegen, die meine/unsere Zuverlässigkeit in Frage stellen.

☐ Ich erkläre/Wir erklären, dass wir die vorgenannten Erklärungen nicht abgegeben können, weil der in der Anlage beschriebene Sachverhalt vorliegt (Erklärung vom Erklärenden zu erstellen und beizufügen).

☐ Ich erkläre/Wir erklären, dass wir folgende Selbstreinigungsmaßnahmen gemäß § 125 GWB vorgenommen haben (Erklärung vom Erklärenden zu erstellen und beizufügen).

Neckarsulm, 26.02.2021
Ort, Datum

Unterzeichnung* durch den Bieter, das bevollmächtigte Mitglied der Bietergemeinschaft bzw. das eignungsverschaffende Unternehmen:

Bechtle AG

[redacted]gemeinschaft bzw. das

BECHTLE
Bechtle AG
Bechtle Platz 1 · 74172 Neckarsulm
Telefon 0 71 32 / 981-4143
Telefax 0 71 32 / 981-4100

[redacted]ng für den Bieter, das [redacted]ignungsverschaffenden

****

Vergabeverfahren „Digitaler Impfnachweis“
AZ: Z15-04800-05/006

Eigenerklärung Versicherungsschutz gemäß Nr. 7, 3. Aufzählungszeichen der Aufforderung zur Angebotsabgabe vom 24.02.2021

Firmenname und Adresse:	IBM Deutschland GmbH
Ansprechperson für das Vergabeverfahren:	[redacted]
Telefon/Fax:	
E-Mail:	

Wir erklären, dass ein Versicherungsschutz über eine Deckungssumme für Schäden bis zu [redacted] durch Abschluss eines entsprechenden Vertrags nach Zuschlagserteilung sichergestellt werden wird.

Hamburg 26. Februar 2021

[redacted]

Senior Partner
IBM Deutschland GmbH

Senior Managing Consultant
IBM Deutschland GmbH

UBIRCH

UBIRCH GmbH Im Mediapark 5 50670 Köln

IBM Deutschland GmbH

UBIRCH GmbH
Im Mediapark 5
50670 Köln
www.ubirch.com

Ihr Ansprechpartner
[redacted]

26.02.2021

Verpflichtungserklärung
„Leistungen anderer Unternehmen"
Vergabeverfahren: Elektronischer Impfnachweis
AZ: Z15-04800-05/006

Ich/wir verpflichte/n mich/uns, der Bewerberin/Bieterin

IBM Deutschland GmbH

im Rahmen ihres Angebotes zur o. a. Vergabe und im Fall der Auftragsvergabe, für die folgenden Teilleistungen mit den Fähigkeiten und Kapazitäten (personell, sachlich) meines/unseres Unternehmens zur Verfügung zu stehen:

„Beratungs-, Entwicklungs- und Unterstützungsleistungen in allen Teilbereichen des Vorhabens"

UBIRCH
ubirch GmbH
Im Mediapark 5
50670 Köln
ubirch.de

Köln, 26.02.2021 [redacted]
Ort, Datum

VDIGITAL

govdigital eG - Charlottenstraße 65 - 10117 Berlin

IBM Deutschland GmbH

Charlottenstraße 65
10117 Berlin
[redacted]

Datum
28. Februar 2021

Verpflichtungserklärung

„Leistungen anderer Unternehmen"

Vergabeverfahren: Elektronischer Impfnachweis
AZ: Z15-04800-05/006

Ich/wir verpflichte/n mich/uns, der Bewerberin/Bieterin

IBM Deutschland GmbH

im Rahmen ihres Angebotes zur o. a. Vergabe und im Fall der Auftragsvergabe, für die folgenden Teilleistungen mit den Fähigkeiten und Kapazitäten (personell, sachlich) meines/unseres Unternehmens zur Verfügung zu stehen:

„Beratungs-, Entwicklungs- und Unterstützungsleistungen in allen Teilbereichen des Vorhabens"

Berlin, 28.02.2021

[redacted]

Ort, Datum

Bechtle AG, Bechtle Platz 1, 74172 Neckarsulm

Verpflichtungserklärung
„Leistungen anderer Unternehmen"

Vergabeverfahren: Elektronischer Impfnachweis
AZ: Z15-04800-05/006

Wir verpflichten uns, der Bewerberin/Bieterin

IBM Deutschland GmbH

im Rahmen ihres Angebotes zur o. g. Vergabe und im Fall der Auftragsvergabe, für die folgenden Teilleistungen mit den Fähigkeiten und Kapazitäten (personell, sachlich) unseres Unternehmens zur Verfügung zu stehen:

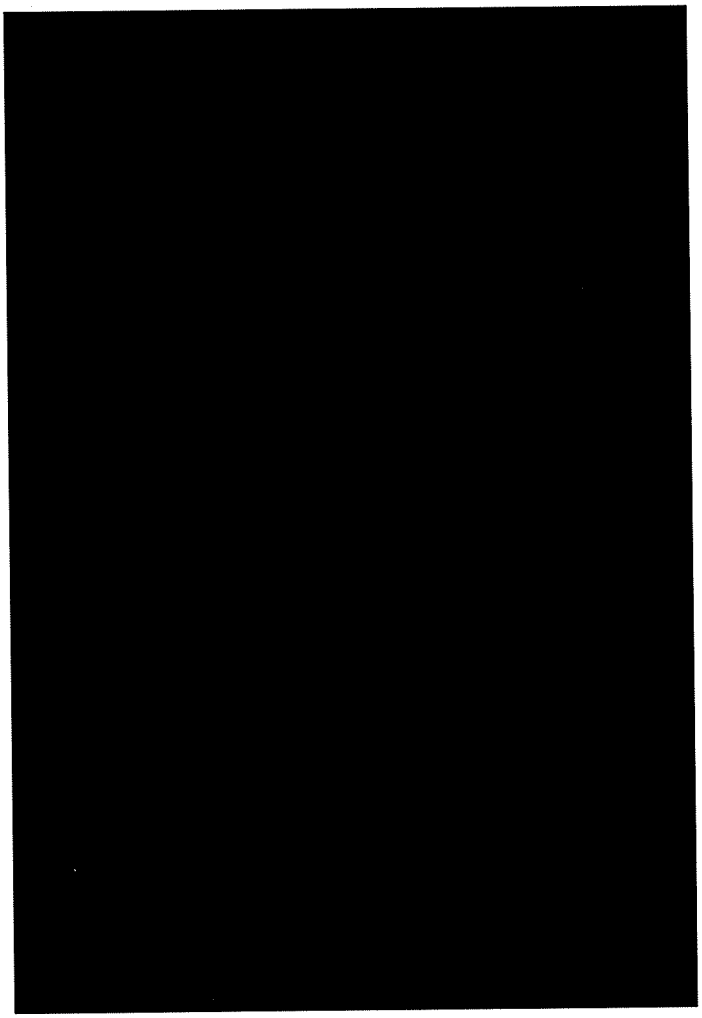
„Beratungs-, Entwicklungs- und Unterstützungsleistungen in allen Teilbereichen des Vorhabens"

Neckarsulm, 26.02.2021

Ort, Datum

[redacted]

Bechtle AG
Bechtle Platz 1 · 74172 Neckarsulm
Telefon 0 71 32 / 981-4143
Telefax 0 71 32 / 981-4100



Anlage 3

Preisblatt

Anlage 4

Vertragsstrafen für die Nichteinhaltung der geregelten Reaktions- und Wiederherstellungszeiten

Anlage 4

Vertragsstrafen bei Verstoß gegen Wiederherstellungszeiten:

1. Der Auftragnehmer hat bei Überschreitung der vertraglich vorgegebenen Wiederherstellungszeiten nachfolgende Vertragsstrafe zu zahlen. Diese beträgt für jeden vollendeten Arbeitstag: 1 Prozent desjenigen Teils der Leistung, der nicht genutzt werden kann. Im Zweifel gilt als Berechnungsgrundlage der „Pauschalpreis für den Betrieb pro Monat („netto").

2. Die Vertragsstrafe nach Ziff. 1 wird in ihrer Höhe kumuliert auf insgesamt 10 Prozent der Gesamt-Auftragssumme (netto) begrenzt. Gesamt-Auftragssumme im vorgenannten Sinne ist der „Pauschalfestpreis für Entwicklung, Einrichtung, Inbetriebnahme sowie Betrieb über 8 Monate (netto)".

3. Die Geltendmachung weitergehender Schadensersatzansprüche bleibt dem Auftraggeber vorbehalten.

5. Referenz	Nr. 4 [redacted]
a) Name und Adresse des Auftraggebers; Benennung eines Ansprechpartners mit Telefonnummer oder E-Mail-Adresse	[redacted]
b) Bezeichnung des Referenzprojektes/-vertrages und Angabe des/der Auftragnehmer/s	IT System zur Ausstellung von digitalen Corona-Test Zertifikaten (im Januar 2021eine 6-stellige Anzahl), [redacted]
c) Leistungszeitraum (von – bis)	ab Mai 2020 - Mai 2022
d) Auftragsvolumen (Honorar des Auftragnehmers) - <u>mindestens 500.000 Euro (Mindestanforderung)</u>	[redacted]
e) Angabe des Auftragnehmers	UBIRCH GmbH Im Mediapark 5 50670 Köln

f) Inhalt des Projektes und Umfang der erbrachten Leistungen (**<u>Mindestanforderung, jedes Gebiet gemäß Ziffer (1) – (6) muss durch die vorgelegten Referenzen insgesamt abgedeckt sein, wobei eine Referenz auch mehrere Gebiete abdecken kann</u>**)
Ergänzende Angaben zum Inhalt des Projektes und Umfang der erbrachten Leistungen
(<u>bitte Zutreffendes ankreuzen und kurz beschreiben</u>)

☐ (1) - Projekt mit App-Entwicklung (iOS, Android) einschl. einem zentralen im RZ gehosteten Backend-Anteil und Nutzung durch mehr als 100.000 Nutzer.

☒ (2) - Projekt für die Entwicklung und den Betrieb von Anwendungen, in denen personenbezogene medizinische Daten, also besonders schützenswerte Daten im Sinne des Artikel 9 DSGVO, zentral in einem sicheren Rechenzentrum verarbeitet wurden.

In dem Projekt wurde eine Anwendung entwickelt und betrieben, in der personenbezogene medizinische Daten, also besonders schutzwürdige Daten im Sinne von Artikel 9 DSGVO, verarbeitet werden; Datenschutzkonforme Anonymisierung von medizinischen Daten und Übertragung im UBIRCH Client und UBIRCH Trust Service in Deutschland für PCR Laborergebnisse des Auftraggebers.

- Persönliche Daten der Patienten (u.a Vorname, Nachname, geb. Datum und optional Pass- oder Personalausweisnummer)

• Gesundheitsdaten – konkret: Ergebnisse eines PCR-Tests mit Testtyp, Testergebnis und Testzeitpunkt – die über ein IT-System des Auftraggebers erfasst und an die hier genannten Anwendung über eine entsprechende API übergeben werden. Die Verarbeitung der persönlichen Daten und der zugehörigen personenbezogenen Laborergebnisse erfolgt ausschließlich nach erfolgter Einwilligung der Testpersonen und auf Anweisung des Auftraggebers unter Berücksichtigung der Betroffenenrechte nach DSGVO.
☐ 3) - Projekt, bei dem umfassende technische Sicherheitsmechanismen für einen mindestens hohen Schutzbedarf im Rahmen eines sicheren Entwicklungsprozesses umgesetzt wurden.
☐ (4) - Projekt im Bereich von hochverfügbaren und sicherheitskritischen Internet-Anwendungen im Gesundheits- oder Versicherungswesen oder im Verteidigungsbereich mit mehr als 100.000 aktiven Nutzern.
☐ (5) - Projekt unter Nutzung von kartengebundenen Identitäten
☐ (6) - Projekt mit Steuerung des Aufbaus und Support-Leistungen von mindestens 100 unterschiedlichen Client-Standorten im Business Bereich von mindestens 10 verschiedenen Organisationen

5. Referenz	Nr. [redacted]
a) Name und Adresse des Auftraggebers; Benennung eines Ansprechpartners mit Telefonnummer oder E-Mail-Adresse	[redacted]
b) Bezeichnung des Referenzprojektes/-vertrages und Angabe des/der Auftragnehmer/s	Bezeichnung: RV Hardware, Help-Desk, Drucker, Rechenzentrumsausstattung, Dienstleistungen Auftragnehmer: Bechtle AG, Bechtle Platz 1, 74172 Neckarsulm
c) Leistungszeitraum (von – bis)	01.01.2019 - 31.12.2021
d) Auftragsvolumen (Honorar des Auftragnehmers) - <u>mindestens 500.000 Euro (Mindestanforderung)</u>	[redacted]
e) Angabe des Auftragnehmers	Bechtle AG, Bechtle Platz 1, 74172 Neckarsulm

f) Inhalt des Projektes und Umfang der erbrachten Leistungen (**<u>Mindestanforderung, jedes Gebiet gemäß Ziffer (1) – (6) muss durch die vorgelegten Referenzen insgesamt abgedeckt sein, wobei eine Referenz auch mehrere Gebiete abdecken kann</u>**)
Ergänzende Angaben zum Inhalt des Projektes und Umfang der erbrachten Leistungen
(<u>bitte Zutreffendes ankreuzen und kurz beschreiben</u>)

☐ (1) - Projekt mit App-Entwicklung (iOS, Android) einschl. einem zentralen im RZ gehosteten Backend-Anteil und Nutzung durch mehr als 100.000 Nutzer.

☐ (2) - Projekt für die Entwicklung und den Betrieb von Anwendungen, in denen personenbezogene medizinische Daten, also besonders schützenswerte Daten im Sinne des Artikel 9 DSGVO, zentral in einem sicheren Rechenzentrum verarbeitet wurden.

☐ 3) - Projekt, bei dem umfassende technische Sicherheitsmechanismen für einen mindestens hohen Schutzbedarf im Rahmen eines sicheren Entwicklungsprozesses umgesetzt wurden.

☐ (4) - Projekt im Bereich von hochverfügbaren und sicherheitskritischen Internet-Anwendungen im Gesundheits- oder Versicherungswesen oder im Verteidigungsbereich mit mehr als 100.000 aktiven Nutzern.

☐ (5) - Projekt unter Nutzung von kartengebundenen Identitäten

☒ (6) - Projekt mit Steuerung des Aufbaus und Support-Leistungen von mindestens 100 unterschiedlichen Client-Standorten im Business Bereich von mindestens 10 verschiedenen Organisationen

Ausschreibungsgegenstand ist der Abschluss eines Rahmenvertrags über die Lieferung von:
-Hardware zur IT-Arbeitsplatzausstattung sowie dazugehöriger User-Help-Desk-Dienstleistungen (Los 1);
- Hardware zur Rechenzentrumsausstattung und dezentraler Recheninfrastruktur, sowie dazugehöriger Dienstleistungen (Los 2);
- Drucker-, Scanner- und Tisch-Multifunktionshardware sowie Zubehör (Los 3);
- Hardware für die IPTelefonausstattung sowie Zubehör (Los 4).

Inhalt Los 1:
Das Vergabeverfahren umfasst im LOS 1 die Lieferung der nachfolgend aufgeführten Hardware zur IT-Arbeitsplatzausstattung und hardwarenahe Dienstleistungen (IMAC/RD) für die durch den Auftraggeber unterstützte IT-Endgeräteinfrastruktur. Der Lieferumfang umfasst jährlich geschätzt:
• ca. 15.000 stationäre Arbeitsplatzrechner (Desktop-PCs incl. Monitor, Tastatur, Maus)
• ca. 1.500 Windows-Based-Terminals bzw. Thin-Clients (z.T. inkl. Monitor, Tastatur, Maus)
• ca. 7.500 Notebooks und Tablets (z.T. incl. Monitor, Tastatur, Maus)
• sowie die erforderlichen, typgebundenen Nachrüstkomponenten.
Im Leistungsumfang der hardwarenahen Dienstleistungen und Managed-Services sind enthalten:
• IMAC/RD Prozesse incl. Softwareinstallation für die o.g. Geräte, Bestandshardware und IP-Telefone sowie die Integration von Zubehör, Druckern, Multifunktionsgeräten, Scannern und weiteren fachbezogenen Peripheriekomponenten am Arbeitsplatz. Die zu integrierenden Geräte stammen auch aus anderen Lieferbeziehungen (Beistellungen).
• Überlauf des UHD für die Annahme und Bearbeitung von Calls
• Entstörung und Wartung vor Ort der o.g. Geräte, Hardware aus LOS 3 und LOS 4 und Bestandshardware.
• Abwicklung von Garantie und Gewährleistung aus LOS 3 und LOS 4

Inhalt Los 2:
Basis des Beschaffungsgegenstandes ist die Begründung einer technologischen Partnerschaft. Ziel der Partnerschaft ist die Begleitung und Unterstützung von Dataport aus

verschiedenen Perspektiven über die gesamte Vertragslaufzeit in der Erbringung der Rechenzentrums- sowie der dezentralen Infrastruktur-Dienstleistungen den eigenen Kunden gegenüber. Der aus dem Vergabeverfahren resultierende Beschaffungsvertrag soll nicht nur der Beschaffung von Hardware sowie damit zusammenhängender Software und Dienstleistungen dienen. Auch die sich verändernden Anforderungen in Marktgängigkeit und Anforderungen die Leistungserfüllung von Dataport müssen in Form notwendiger Nachjustierungen Eingang finden.

Die Beschaffungsgegenstände im Überblick:

- Server für die zentrale RZ-Infrastruktur:
  - o Nach Leistungsmerkmalen definierte Standardservertypen, die häufiger abgerufen werden;
  - o Spezielle Hardware, die aufgrund von Abhängigkeiten oder Zertifizierungen im Einzelfall zu definieren ist;
- Storage und Datensicherungshardware;
- Dezentrale Server- und Storage-/Datensicherungshardware für den Einsatz bei Dataport-Kunden;
- Software, die mit dem Betrieb der Hardware zusammenhängt;
- Steuerungshardware, die den Betrieb der Hardware ermöglicht (z.B. Switches, Avocent-Konsolen etc.) sowie deren Software;
- Erweiterungen und Ersatzteile für Bestands- und Neuhardware sowie abhängiges Zubehör (z.B. Racks, Kabel etc.);
- Hardwareabhängige Dienstleistungen:
  - o Gewährleistungs- und Entstörungsdienstleistungen für die neu zu liefernde Hardware sowie die Übernahme aller Services für die bestehende Hardware unter Beibehaltung der gültigen Servicemerkmale (z. B. SLA);
  - o Allgemeine Dienstleistungen rund um die Installation und den Betrieb der Hardware (z. B. IMAC/RD);
  - o Transitions-, PoC-, Integrations-, Transfer- und Beratungsdienstleistungen. Mit der Vergabe der Gegenstände, insbesondere der zu beschaffenden Hardware, beabsichtigt Dataport im Rahmen der Rechenzentrumsarchitektur einen weitest möglichen Wettbewerb der Hersteller und Lieferanten zu ermöglichen. Hierzu werden die Anforderungen, soweit möglich, funktional ausgeschrieben, um aus den Angeboten unter Berücksichtigung aller Kosten (inkl. Transitionskosten) das wirtschaftlichste auszuwählen

Inhalt Los 3:

Das Vergabeverfahren umfasst im LOS 3 die Lieferung der nachfolgend aufgeführten Hardware zur ITArbeitsplatzausstattung

- ca. 2.200 lokale Schwarz-Weiß- und Farbdrucker
- ca. 6.000 Schwarz-Weiß- und Farb-Netzwerkdrucker
- ca. 100 Scanner
- ca. 400 lokale Multifunktionsdrucker sowie die erforderlichen, typgebundenen Nachrüstkomponenten.

Die zuvor beschriebenen Gerätetypen des LOSES 3 sind für die Versorgung der Arbeitsplätze im Bereich Managed Service an den Leistungserbringer für die hardwarenahen Dienstleistungen (IMAC/RD) des LOSES 1 zu liefern, welcher die Geräte aus LOS 3 im Auftrag des Auftraggebers bestellt und in ausreichendem Maße zur Erfüllung der Anforderungen an die hardwarenahen Dienstleistungen bevorratet. Weiterhin ist eine

Abwicklung der Garantie und Gewährleistung über den Bieter aus LOS1 gewünscht. Hier wird ein enger Bedarf an Abstimmung gefordert.

Inhalt Los 4:
Das Vergabeverfahren umfasst im LOS 4 die Lieferung der nachfolgend aufgeführten IPTelefone

- ca. 2.750 IP Sprachendgerät (SIP) Standard mit Basisfunktion
- ca. 4.000 IP Sprachendgerät (SIP) Standard mit Komfortfunktionen
- ca. 750 IP Sprachendgerät (SIP) für Chef/Sek
- ca. 2.250 Erweiterungsmodul für IP Sprachendgerät Standard mit Komfortfunktionen
- ca. 500 Erweiterungsmodul für IP Sprachendgerät für Chef/Sek
- ca. 4.000 Netzteil für IP Sprachendgerät Standard mit Basisfunktion, IP Sprachendgerät Standard mit Komfortfunktionen und IP Sprachendgerät für Chef/Sek
- ca. 2.500 Anschlusskabel für IP Sprachendgerät, Länge 4 m, Cat 5
- ca. 2.500 Anschlusskabel für IP Sprachendgerät, Länge 6 m, Cat 5

Die zuvor beschriebenen Gerätetypen des LOSES 4 sind für die Versorgung der Arbeitsplätze im Bereich Managed Service (Freie und Hansestadt Hamburg) an den Leistungserbringer für die hardwarenahen Dienstleistungen (IMAC/RD) des LOSES 1 zu liefern, welcher die Geräte aus LOS 4 im Auftrag des Auftraggebers bestellt und in ausreichendem Maße zur Erfüllung der Anforderungen an die hardwarenahen Dienstleistungen bevorratet. Weiterhin ist eine Abwicklung der Garantie und Gewährleistung über den Bieter aus LOS1 gewünscht. Hier wird ein enger Bedarf an Abstimmung gefordert.

Die oben beschriebenen Projektleistungen beinhalten die Steuerung des Aufbaus und Support-Leistungen von mehr als 100 unterschiedlichen Client-Standorten in den Bundesländern Hamburg, Schleswig-Holstein, Sachsen-Anhalt, Bremen und Niedersachsen im Business-Bereich von mehr als 10 verschiedenen Organisationen.

5. Referenz	Nr. 1 TK-Safe ePA/ePA+
a) Name und Adresse des Auftraggebers; Benennung eines Ansprechpartners mit Telefonnummer oder E-Mail-Adresse	Techniker Krankenkasse, Bramfelder Chaussee 140, 22305 Hamburg [redacted]
b) Bezeichnung des Referenzprojektes/-vertrages und Angabe des/der Auftragnehmer/s	Programm zur Entwicklung und Betrieb der elektronischen Patientenakte (ePA) und kassenspezifischer Zusatzservices (ePA+) Auftragnehmer: IBM Deutschland GmbH
c) Leistungszeitraum (von – bis)	01.10.2019 - 31.03.2023
d) Auftragsvolumen (Honorar des Auftragnehmers) - mindestens 500.000 Euro (Mindestanforderung)	[redacted]
e) Angabe des Auftragnehmers	IBM Deutschland GmbH, IBM-Allee 1, 71139 Ehningen

f) Inhalt des Projektes und Umfang der erbrachten Leistungen (**Mindestanforderung, jedes Gebiet gemäß Ziffer (1) – (6) muss durch die vorgelegten Referenzen insgesamt abgedeckt sein, wobei eine Referenz auch mehrere Gebiete abdecken kann**)
Ergänzende Angaben zum Inhalt des Projektes und Umfang der erbrachten Leistungen (bitte Zutreffendes ankreuzen und kurz beschreiben)

☒ (1) - Projekt mit App-Entwicklung (iOS, Android) einschl. einem zentralen im RZ gehosteten Backend-Anteil und Nutzung durch mehr als 100.000 Nutzer.

IBM stellt bereit und betreibt für die Versicherten der TK (ca. 10,5 Mio Versicherte) die elektronische Patientenakte (ePA) der IBM mit kassenspezifischen Zusatzservices (ePA+). Innerhalb der mobilen Anwendung TK-App (> 1 Mio Anwender) benutzen derzeit mehr als 250.000 Anwender ihre ePA/ePA+ Anwendung TK-Safe der IBM (siehe zu Nutzung durch mehr als 100.000 aktive Anwender auch Antwort (4))

Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung standardisierter, mobiler ePA Frontend-Module (native iOS / native Android) nebst zugehöriger Whitelabel- und kassenspezifischer Frontend-UX/UI

Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung kassenspezifischer, mobiler ePA+ Frontend-Module (native iOS / native Android) nebst zugehöriger Whitelabel- und kassenspezifischer Frontend-UX/UI

Integration der ePA/ePA+ Frontend-Module in TK-Safe und die TK-App, Test, Betatest, Pentest und Release in Apple AppStore und Google PlayStore

Entwicklung und Betrieb der zentralen, verschlüsselten Datenhaltung und des zentralen ePA/ePA+ Applikationsbackend im Rechenzentrum der IBM in Deutschland. Weitere Ausführungen zum zentralen Anwendungs- und Infrastrukturbetrieb des ePA/ePA+ Backends: siehe Antwort (4).

☒ (2) - Projekt für die Entwicklung und den Betrieb von Anwendungen, in denen personenbezogene medizinische Daten, also besonders schützenswerte Daten im Sinne des Artikel 9 DSGVO, zentral in einem sicheren Rechenzentrum verarbeitet wurden.

In dem Projekt werden Anwendungen entwickelt und betrieben, in denen personenbezogene medizinische Daten nach Artikel 9 DSGVO verarbeitet werden: Übertragung und inhaltsverschlüsselte Speicherung von versichertenbezogenen medizinischen und Sozialdaten im zentralen ePA/ePA+ Backend der IBM in Deutschland, u.a. für

- Patientenquittungsdaten nach §305 SGB V aus der Umgebung der Techniker Krankenkasse
- Gesundheitsdaten, die über die mobile Applikation TK Safe manuell eingegeben wurden
- Gesundheitsdaten aus Leistungserbringer-Umgebungen, die inhaltsverschlüsselt und versichertenbezogen übertragen werden

Die Verarbeitung von medizinischen und Sozialdaten in der ePA/ePA+ findet ausschließlich nach erfolgter Einwilligung des Versicherten unter Berücksichtigung der Betroffenenrechte nach DSGVO statt.

Weitere Ausführungen zum zentralen Anwendungs- und Infrastrukturbetrieb des ePA/ePA+ Backends: siehe Antwort (4)

☒ 3) - Projekt, bei dem umfassende technische Sicherheitsmechanismen für einen mindestens hohen Schutzbedarf im Rahmen eines sicheren Entwicklungsprozesses umgesetzt wurden.

Im Kontext dieses Projektes Vorhabens wurde ein sicherer Entwicklungsprozess für Systeme mit einem hohen Schutzbedarf auf Basis des „Microsoft SDL" definiert. Ergänzend wurden ausgewählte Anforderungen, Praktiken und Bausteine aus der „Microsoft SDL for Agile Development", „BSI IT-Grundschutz", „BSI Leitfaden zur Entwicklung sicherer Webanwendungen", „OWASP Open SAMM", „BSIMM", „OWASP Application Security Verification Standard (ASVS)" übernommen. Darüber hinaus wurden die expliziten Anforderungen der Gematik hinsichtlich des sicheren Entwicklungsprozesses berücksichtigt. Der Gesamtprozess wurde in einem übergreifenden Konzept dokumentiert und von externen, Gematik-zugelassenen Gutachtern (SRC, PWC) bestätigt.

Die einzelnen Aktivitäten und Maßnahmen werden entlang der Phasen: Training, Requirements, Design, Implementation, Verfikation, Release und Response definiert und kontinuierlich kontrolliert. Der SDL wird durch ein umfassendes, über weite Strecken automatisiertes Tooling unterstützt.

☒ (4) - Projekt im Bereich von hochverfügbaren und sicherheitskritischen Internet-Anwendungen im Gesundheits- oder Versicherungswesen oder im Verteidigungsbereich mit mehr als 100.000 aktiven Nutzern.

Nutzung durch mehr als 100.000 aktive Anwender: Die dem TK-Safe zugrundeliegende, zertifizierte IBM ePA/ePA+ ist als Mehrmandantensystem mit mehr als 100.000 Anwendern im Einsatz und auf Basis der regulatorischen Vorgaben der gematik derart bereitgestellt und in Nutzung, dass Backend-seitig sogar 120.000 gleichzeitig aktive Nutzersessions

unterstützt sind. (SLA-Vorgabe: 100 neue Session pro Sekunde und ein Session Timeout von 20min. Dabei ist für jede aktive Aktensession eine individuelle separate vertrauenswürdige Ausführungsumgebung (VAU) bereitzustellen. Somit werden von IBM im Minimum 120.000 Nutzersessions sowie 120.000 parallele VAUs (100 Sessions * 60 Sekunden * 20 = 120.000) unterstützt.)

Das Projekt setzt höchste Sicherheitsanforderungen um, um die Gesundheits-und Sozialdaten zu sichern. Die Hochverfügbarkeit des Rechenzentrumsbetriebs erfolgt über Georedundanz und entsprechendem Cluster-Betrieb:

Das System verarbeitet und speichert personenbezogene Daten und Sozialdaten.

Der Betrieb der projektierten Lösung wird in betriebs-redundanten Rechenzentren über drei Standorte hinweg realisiert. Die Anwendungskomponenten wurden für einen Active-Active-Cluster Betrieb ausgelegt und stützen sich auf ein Active-Active-Active Object Storage Management System and Master/Replika/Replika Datenbank Systeme.

Die Rechenzentren und deren Infrastrukturbetrieb verfügen über Sicherheitszertifizierungen gemäß ISO 27001 und dem BSI C5 Standard. Sie werden ergänzt durch diverse technische und organisatorische Sicherheitsmaßnahmen zur Absicherung des projektspezifischen Infrastruktur- und Anwendungsbetriebes. Die Anforderungen werden mittels einer strukturierten Modellierung auf Basis BSI Grundschutz und der spezifischen gematik Anforderungen ermittelt und umgesetzt. Die Dokumentation erfolgt in spezifischen Sicherheitskonzepten, die Gegenstand der Sicherheitsgutachten und Zulassungen durch die gematik sind.

Bei den ergänzenden Maßnahmen handelt es sich unter anderem um folgende Punkte:

- Sicherer Betrieb von Systemen und Sub-Systemen in Form eines sicheren Konfigurationsmanagements (Hardening) gegen Standards wie die CIS Benchmarks und eines kontinuierlichen Patch-Managements
- Umsetzung eines mehrschichtigen Netzwerk-Zonenmodells und kontinuierliche Daten-flusskontrolle durch Firewalls und andere Netzwerksicherheitsbausteine
- Betrieb eines Identity & Access Managements zur Verwaltung und Überwachung der ad-ministrativen und privilegierten Nutzer und deren Zugriffe auf die Systeme und Sub-Systeme der ePA Platform
- Kontinuierliche Überwachung der Infrastruktur auf sicherheitsrelevante Ereignisse mittels eines SIEMs, L1 und L2 Event Monitoring und Analyse durch Security Analysten, sowie der Integration in die übergreifenden ITIL Incident Management Prozesse zur L3 Bearbei-tung
- Betrieb eines integrierten Infrastruktur Schwachstellenmanagements (Vulnerability Ma-nagement) mit regelmäßigen Scans und einer Analyse durch Security Analysten, sowie der Integration in die übergreifenden ITIL Incident Management Prozesse zur Behebung der Schwachstellen
- Durchführung regelmäßiger erweiterter Sicherheitstests auf Ebene der Anwendungen und Infrastrukturen durch unabhängige interne und externe Pen-Testing-Teams

☒ (5) - Projekt unter Nutzung von kartengebundenen Identitäten

Das Projekt umfasst die Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung eines kartengebundenen Registrierungs- und Authentifizierungsverfahren. Neben der alternativen Versichertenidentität (al.vi) ist die Nutzung der ePA durch einen an die eGK bzw. eGK-Identität gebundenen Registrierungs- und Authentifizierungsmechanismus auf dem mobilen Endgerät möglich. Im Registrierungs- und Authentifizierungsprozess hält der Versicherte hierzu seine eGK an das mobile Endgerät, wodurch mittels NFC-Kommunikation die Identitätsdaten (u.a. KV-Nummer) an die ePA-Anwendung übertragen werden sowie in einem Challenge Response Verfahren zur Authentifizierung des Nutzers Signaturen auf der Karte erzeugt werden. Ebenso werden einzelne

	Nutzeraktivitäten, zum Beispiel die Vergabe von ePA Zugriffsberechtigungen für den Arzt, in diesem Fall nur dann erfolgreich abgeschlossen, wenn der Nutzer sich erneut mit seiner eGK-Kartenidentität am mobilden Endgerät authentifiziert.
☐ (6) -	Projekt mit Steuerung des Aufbaus und Support-Leistungen von mindestens 100 unterschiedlichen Client-Standorten im Business Bereich von mindestens 10 verschiedenen Organisationen

5. Referenz	Nr. 2 BARMER eCare
a) Name und Adresse des Auftraggebers; Benennung eines Ansprechpartners mit Telefonnummer oder E-Mail-Adresse	BARMER, Lichtscheider Straße 89, 42285 Wuppertal Ansprechpartner: [redacted]
b) Bezeichnung des Referenzprojektes/-vertrages und Angabe des/der Auftragnehmer/s	Entwicklung und Betrieb der elektronischen Patientenakte (ePA) und der dazugehörigen Frontends (App und Portal) Auftragnehmer: IBM Deutschland GmbH
c) Leistungszeitraum (von – bis)	01.11.2019 - 31.12.2025
d) Auftragsvolumen (Honorar des Auftragnehmers) - <u>mindestens 500.000 Euro (Mindestanforderung)</u>	[redacted]
e) Angabe des Auftragnehmers	IBM Deutschland GmbH, IBM-Allee 1, 71139 Ehningen

f) Inhalt des Projektes und Umfang der erbrachten Leistungen (**<u>Mindestanforderung, jedes Gebiet gemäß Ziffer (1) – (6) muss durch die vorgelegten Referenzen insgesamt abgedeckt sein, wobei eine Referenz auch mehrere Gebiete abdecken kann</u>**)
Ergänzende Angaben zum Inhalt des Projektes und Umfang der erbrachten Leistungen
(<u>bitte Zutreffendes ankreuzen und kurz beschreiben</u>)

☒ (1) - Projekt mit App-Entwicklung (iOS, Android) einschl. einem zentralen im RZ gehosteten Backend-Anteil und Nutzung durch mehr als 100.000 Nutzer.

IBM stellt bereit und betreibt für die Versicherten der BARMER (ca. 9,5 Mio Versicherte) eine neue mobile Anwendung eCare mit integrierter elektronischer Patientenakte (ePA) und kassenspezifischen Zusatzservices ePA+ der IBM.

Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung standardisierter, mobiler ePA Frontend-Module (native iOS / native Android) nebst zugehöriger Whitelabel- und kassenspezifischer Frontend-UX/UI

Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung kassenspezifischer, mobiler ePA+ Frontend-Module (native iOS / native Android) nebst zugehöriger Whitelabel- und kassenspezifischer Frontend-UX/UI

Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung der ummantelnden eCare App (native iOS / native Android) nebst zugehöriger Whitelabel- und kassenspezifischer Frontend UX/UI; Release in Apple Appstore und Google Playstore

Die eCare-Lösung der BARMER wird dahingehend ummantelt, dass a) zusätzlich eine eGK Adelung erfolgt, d.h. die kartengebundene Identität mit der realen Identität eines Versicherten automatisch im Rahmen eines Roboldent-Verfahrens überprüft wird und b) dass bei Registrierung für die ePA ebenfalls ein Abgleich der Versichertenidentität mit der kartengebundenen Identität auf Basis des Roboldent-verfahrens erfolgt.	
☐ (6) -	Projekt mit Steuerung des Aufbaus und Support-Leistungen von mindestens 100 unterschiedlichen Client-Standorten im Business Bereich von mindestens 10 verschiedenen Organisationen

Entwicklung und Betrieb der zentralen, verschlüsselten Datenhaltung und des zentralen ePA/ePA+ Applikationsbackend im Rechenzentrum der IBM in Deutschland. Weitere Ausführungen zum zentralen Anwendungs- und Infrastrukturbetrieb des ePA/ePA+ Backends: siehe Antwort (4)
Bzgl. der Nutzung durch mehr als 100.000 aktive Anwender: siehe Antwort (4)

☒ (2) - Projekt für die Entwicklung und den Betrieb von Anwendungen, in denen personenbezogene medizinische Daten, also besonders schützenswerte Daten im Sinne des Artikel 9 DSGVO, zentral in einem sicheren Rechenzentrum verarbeitet wurden.

In dem Projekt werden Anwendungen entwickelt und betrieben, in denen personenbezogene medizinische Daten nach Artikel 9 DSGVO verarbeitet werden: Übertragung und inhaltsverschlüsselte Speicherung von versichertenbezogenen medizinischen und Sozialdaten im zentralen ePA/ePA+ Backend der IBM in Deutschland, u.a. für

- Gesundheitsdaten, die über die mobile Applikation eCare manuell eingegeben wurden
- Gesundheitsdaten aus Leistungserbringer-Umgebungen, die inhaltsverschlüsselt und versichertenbezogen übertragen werden

Die Verarbeitung von medizinischen und Sozialdaten in der ePA/ePA+ findet ausschließlich nach erfolgter Einwilligung des Versicherten unter Berücksichtigung der Betroffenenrechte nach DSGVO statt.
Weitere Ausführungen zum zentralen Anwendungs- und Infrastrukturbetrieb des ePA/ePA+ Backends: siehe Antwort (4)

☒ 3) - Projekt, bei dem umfassende technische Sicherheitsmechanismen für einen mindestens hohen Schutzbedarf im Rahmen eines sicheren Entwicklungsprozesses umgesetzt wurden.

Im Kontext dieses Projektes Vorhabens wurde ein sicherer Entwicklungsprozess für Systeme mit einem hohen Schutzbedarf auf Basis des „Microsoft SDL" definiert. Ergänzend wurden ausgewählte Anforderungen, Praktiken und Bausteine aus der „Microsoft SDL for Agile Development", „BSI IT-Grundschutz", „BSI Leitfaden zur Entwicklung sicherer Webanwendungen", „OWASP Open SAMM", „BSIMM", „OWASP Application Security Verification Standard (ASVS)" übernommen. Darüber hinaus wurden die expliziten Anforderungen der Gematik hinsichtlich des sicheren Entwicklungsprozesses berücksichtigt. Der Gesamtprozess wurde in einem übergreifenden Konzept dokumentiert und von externen, Gematik-zugelassenen Gutachtern (SRC, PWC) bestätigt.
Die einzelnen Aktivitäten und Maßnahmen werden entlang der Phasen: Training, Requirements, Design, Implementation, Verfikation, Release und Response definiert und kontinuierlich kontrolliert. Der SDL wird durch ein umfassendes, über weite Strecken automatisiertes Tooling unterstützt.

☒ (4) - Projekt im Bereich von hochverfügbaren und sicherheitskritischen Internet-Anwendungen im Gesundheits- oder Versicherungswesen oder im Verteidigungsbereich mit mehr als 100.000 aktiven Nutzern.

Nutzung durch mehr als 100.000 aktive Anwender: Die der eCare Anwendung zugrundeliegende, zertifizierte IBM ePA/ePA+ wird bereits heute als Mehrmandatensystem von mehr als 100.000 Anwendern aktiv genutzt und ist auf Basis der regulatorischen Vorgaben der gematik derart bereitgestellt und in Nutzung, dass Backend-seitig sogar 120.000 gleichzeitig aktive Nutzersessions unterstützt sind. (SLA-Vorgabe: 100 neue Session pro Sekunde und ein Session Timeout von 20min. Dabei ist für jede aktive Aktensession eine individuelle separate vertrauenswürdige Ausführungsumgebung (VAU) bereitzustellen.

Somit werden von IBM im Minimum 120.000 Nutzersessions sowie 120.000 parallele VAUs (100 Sessions * 60 Sekunden * 20 = 120.000) unterstützt.)

Das Projekt setzt höchste Sicherheitsanforderungen um, um die Gesundheits-und Sozialdaten zu sichern. Die Hochverfügbarkeit des Rechenzentrumsbetriebs erfolgt über Georedundanz und entsprechendem Cluster-Betrieb:

Das System verarbeitet und speichert personenbezogene Daten und Sozialdaten.

Der Betrieb der projektierten Lösung wird in betriebs-redundanten Rechenzentren über drei Standorte hinweg realisiert. Die Anwendungskomponenten wurden für einen Active-Active-Cluster Betrieb ausgelegt und stützen sich auf ein Active-Active-Active Object Storage Management System and Master/Replika/Replika Datenbank Systeme.

Die Rechenzentren und deren Infrastrukturbetrieb verfügen über Sicherheitszertifizierungen gemäß ISO 27001 und dem BSI C5 Standard. Sie werden ergänzt durch diverse technische und organisatorische Sicherheitsmaßnahmen zur Absicherung des projektspezifischen Infrastruktur- und Anwendungsbetriebes. Die Anforderungen werden mittels einer strukturierten Modellierung auf Basis BSI Grundschutz und der spezifischen gematik Anforderungen ermittelt und umgesetzt. Die Dokumentation erfolgt in spezifischen Sicherheitskonzepten, die Gegenstand der Sicherheitsgutachten und Zulassungen durch die gematik sind.

Bei den ergänzenden Maßnahmen handelt es sich unter anderem um folgende Punkte:

- Sicherer Betrieb von Systemen und Sub-Systemen in Form eines sicheren Konfigurationsmanagements (Hardening) gegen Standards wie die CIS Benchmarks und eines kontinuierlichen Patch-Managements
- Umsetzung eines mehrschichtigen Netzwerk-Zonenmodells und kontinuierliche Daten-flusskontrolle durch Firewalls und andere Netzwerksicherheitsbausteine
- Betrieb eines Identity & Access Managements zur Verwaltung und Überwachung der ad-ministrativen und privilegierten Nutzer und deren Zugriffe auf die Systeme und Sub-Systeme der ePA Platform
- Kontinuierliche Überwachung der Infrastruktur auf sicherheitsrelevante Ereignisse mittels eines SIEMs, L1 und L2 Event Monitoring und Analyse durch Security Analysten, sowie der Integration in die übergreifenden ITIL Incident Management Prozesse zur L3 Bearbei-tung
- Betrieb eines integrierten Infrastruktur Schwachstellenmanagements (Vulnerability Ma-nagement) mit regelmäßigen Scans und einer Analyse durch Security Analysten, sowie der Integration in die übergreifenden ITIL Incident Management Prozesse zur Behebung der Schwachstellen
- Durchführung regelmäßiger erweiterter Sicherheitstests auf Ebene der Anwendungen und Infrastrukturen durch unabhängige interne und externe Pen-Testing-Teams

☒ (5) - Projekt unter Nutzung von kartengebundenen Identitäten

Das Projekt umfasst die Entwicklung, Test, Freigabe und kontinuierliche Weiterentwicklung eines kartengebundenen Registrierungs- und Authentifizierungsverfahren. Neben der alternativen Versichertenidentität (al.vi) ist die Nutzung der ePA durch einen an die eGK bzw. eGK-Identität gebundenen Registrierungs- und Authentifizierungsmechanismus auf dem mobilen Endgerät möglich. Im Registrierungs- und Authentifizierungsprozess hält der Versicherte hierzu seine eGK an das mobile Endgerät, wodurch mittels NFC-Kommunikation die Identitätsdaten (u.a. KV-Nummer) an die ePA-Anwendung übertragen werden sowie in einem Challenge Response Verfahren zur Authentifizierung des Nutzers Signaturen auf der Karte erzeugt werden. Ebenso werden einzelne Nutzeraktivitäten, zum Beispiel die Vergabe von ePA Zugriffsberechtigungen für den Arzt, in diesem Fall nur dann erfolgreich abgeschlossen, wenn der Nutzer sich erneut mit seiner eGK-Kartenidentität am mobilden Endgerät authentifiziert.