Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Eidgenössische Zollverwaltung EZV
Direktionsbereich Planung & Steuerung
Value Stream «Sicherheit und Grenzübertritt»

Pflichtenheft
(21152) 606
Mobiles Grenzkontrollsystem (EZV)

Dieses Verfahren erfolgt nach dem Bundesgesetz über das öffentliche Beschaffungswesen (BöB). Dies bedeutet, dass während des Verfahrens keine Kommunikation zwischen dem Anbieter und den Bedarfsstellen geführt werden darf. Für Fragen wenden Sie sich ausschliesslich an das BBL, Dienst öffentliche Ausschreibungen.

Inhaltverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Begriffe und Abkürzungen

Aus Gründen der einfachen Lesbarkeit wurde im ganzen Dokument die männliche Form erwähnt. Selbstverständlich sind dabei auch die weiblichen Personen mit einbezogen.

Begrifflichkeiten	Definition/Erklärung
10FP	Zehn Fingerabdrücke
2FP	Zwei Fingerabdrücke
4FP	Vier Fingerabdrücke
AFIS	AFIS steht für Automatisiertes Fingerabdruck-Identifikations-System. Das System ermöglicht die eindeutige Personenidentifikation mittels Fingerabdrücken innert weniger Minuten. Business Owner: fedpol
AGB	Allgemeine Geschäftsbedingungen des Bundes
App	Applikation für Smartphone
ASF	ASF steht für "Automated Search Facility". Bei ASF handelt es sich um die Fahndungsdatenbank von Interpol. ASF beinhaltet die folgenden Teildatenbanken: • ASF-SLTD - Stolen and Lost Travel Documents (ehemals ASF-STD) • ASF-SMV - Stolen Motor Vehicle • ASF-Nominals - Personenfahndungen Business Owner Datenbanken: Interpol Business Owner Schnittstelle: fedpol
ASTRA	Bundesamt für Strassen Das Bundesamt ist dem eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) unterstellt.
BBL	Bundesamt für Bauten und Logistik Hierbei handelt es sich um die Beschaffungsstelle dieser Ausschreibung. Diese ist dem EFD unterstellt.
Bedarfsstelle	Organisationseinheit des Bundes, für welche die Leistung schlussendlich erbracht wird (hier EZV).
Beschaffungsstelle	Zentral zuständige Beschaffungsstelle nach Org-VöB (hier BBL)
BIT	Bundesamt für Informatik Das BIT ist dem EFD unterstellt.
BöB	Bundesgesetz über das öffentliche Beschaffungswesen (SR 172.056.1)
CEC	Anschlusspunkt zum C-EES Business Owner: SEM
C-EES	Zentrales Entry-Exit System der EU Business Owner: EU
CSCA-Data Collection	Schnittstelle der eDoc N-PKD, um die Zertifikate der an der Grenze gelesenen elektronischen Reisedokumente der N-PKD-Applikation zu übertragen. Business Owner: fedpol

C-SIS	C-SIS ist der zentrale, EU-seitige Datenserver des Schengener Informationssystems SIS. Der Zugriff erfolgt über N-SIS, das Nationale SIS, welches eine Kopie der Daten in C-SIS enthält. Im Schengener Informationssystems sind einerseits Personenfahndungen (unerwünschte, vermisste und zur Fahndung ausgeschriebene Personen) und andererseits Sachfahndungen (gestohlene und zu überwachende Motorfahrzeuge, Banknoten, gestohlene Dokumente und Schusswaffen) erfasst. Business Owner C-SIS: EU
CVC	Anschlusspunkt zum C-VIS Business Owner: SEM
C-VIS	C-VIS ist der zentrale, EU-seitige Datenserver des Visa-Informationssystems VIS. VIS enthält die Schengen-Visa für den kurzzeitigen Aufenthalt im Schengen-Raum inkl. deren Annullierungen und Aufhebungen. Der Zugriff auf C-VIS erfolgt über die Komponente CVC. Business Owner C-VIS: EU.
d.h.	das heisst
DaziT	Das Programm DaziT ist das Schlüsselelement zur Modernisierung und Digitalisierung der Eidgenössischen Zollverwaltung (EZV). «Dazi» steht für Zoll (rätoromanisches Wort für Zoll), das «i» steht für Informatik und das «T» steht für Transformation.
EAC IS-Service	Dies ist die Schnittstelle der eDoc PKI, für die Authentifizierung des GKV-Arbeitsplatzes bzw. des Inspection-System (Dokumentleser). Diese wird nach einer "Chip-Authentifizierung" durchgeführt. Sie stellt damit die "Erweiterte Zugangskontrolle (EAC)" dar. Das EAC kontrolliert den Zugriff auf den geschützten Teil des Passes, welcher die Fingerabdrücke enthält. Business Owner: fedpol
EES	Entry-Exit-System für den Schengenraum
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EJPD SSO Portal	Single Sign On Portal des EJPD: Stellt insbesondere die Zugänge zu den Fahndungs- und Informationssystemen sicher.
EK	Eignungskriterium
eMRTD	Electronic Machine Readable Travel Document Elektronisches maschinenlesbares Reisedokument (beinhaltet einen Chip)
ETIAS	European Travel Information and Authorization System Europäisches Reiseinformations- und -genehmigungssystem
EU	Europäische Union
EZV	Eidgenössische Zollverwaltung Bei der EZV handelt es sich um die Bedarfsstelle dieser Ausschreibung. Diese ist dem EFD unterstellt.
FABER	FABER (automatisiertes Fahrberechtigungsregister) dient dem Bund, den Kantonen und dem Fürstentum Liechtenstein und ist für die Erteilung von Lernfahr-, Führer- und Fahrlehrerausweisen sowie für die Kontrolle der zivilen und militärischen Fahrberechtigungen zuständig.

	Business Owner: ASTRA
fedpol	Bundesamt für Polizei Das fedpol ist dem EJPD unterstellt.
FP-Leser App	App, um Fingerabdrücke mittels dem Fingerabdruckleser zu erfassen
ggf.	gegebenenfalls
GKS	Grenzkontrollsystem
GKV	Grenzkontrollverantwortliche
gm.	gemäss
HOOGAN	In der HOOGAN-Datenbank werden Personen erfasst, gegen welche anlässlich einer Sportveranstaltung in der Schweiz oder im Ausland eine polizeiliche Massnahme verfügt wurde. Business Owner: fedpol
i.e.	id est: das heisst
ICD	Interface Control Document
Interpol	Internationale kriminalpolizeiliche Organisation Bei Interpol handelt es sich um einen Verein zur Stärkung der Zusammenarbeit nationaler Polizeibehörden.
IOP	Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa
iOS	iOS ist ein von Apple entwickeltes mobiles Betriebssystem für das iPhone und den iPod touch.
ISA	Informationssystem Ausweisschriften ISA dient der Ausstellung von Ausweisschriften für Schweizer Bürger und enthält die Daten der Ausweisarten Pass und Identitätskarte. Passarten: ordentlicher Pass, provisorischer Pass, ordentlicher Diplomatenpass, provisorischer Diplomatenpass, ordentlicher Dienstpass und provisorischer Dienstpass Business Owner: fedpol
ISBO	Informatiksicherheitsbeauftragter
ISC EJPD	Informatik Service Center des EJPD
ISR	Informationssysteme für Reisedokumente ISR dient der Ausstellung von Schweizer Reisedokumenten für ausländische Personen. Die Reiseausweise für Flüchtlinge und Pässe für ausländische Personen enthalten einen Datenchip mit biometrischen Daten. Business Owner: SEM
JMH	Java Message Handler Service, um Resultate von AFIS asynchron zu erhalten.
MAM	Mobile Application Management
MDM	Mobile Device Management Tool
mobGKS	Mobiles GKS
mobApp GKS	Mobile GKS App (auf dem Smartphone)
mobGKS Server	Mobile GKS Server (Backend)

MOFIS	Motorfahrzeuginformationssystem der Eidg. Fahrzeugkontrolle In MOFIS (automatisiertes Fahrzeug- und Fahrzeughalterregister) sind alle in der Schweiz und im Fürstentum Liechtenstein gegenwärtig und früher zugelassenen Fahrzeuge sowie die dazu gehörigen Daten über die Halter geführt. Business Owner: ASTRA
MRTD	Machine Readable Travel Document: Maschinenlesbares Reisedokument
MRZ	Machine Readable Zone: Optisch maschinenlesbare Zone eines MRTD
NFC	Near Field Communication
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology Das National Institute of Standards and Technology ist eine Bundesbehörde der Vereinigten Staaten.
N-SIS	Nationaler Anschlusspunkt zum C-SIS Business Owner: fedpol
OCR	Optical Character Recognition
ORBIS	Bei ORBIS handelt es sich um das Visa System der Schweiz. Schweizer Behörden bearbeiten damit Schengen-Visa für den kurzfristigen Aufenthalt, welche zusätzlich in C-VIS gespeichert werden, sowie die Nationalen Visa für den längerfristigen Aufenthalt, welche ausschliesslich in ORBIS gespeichert werden. Business Owner: SEM
PCN	Process Control Number: eindeutige Prüffallnummer des Systems AFIS
PKD Schnittstelle	Public Key Directory Webservice-Schnittstelle (ZertServer der EZV) Schnittstelle des ZertServers, um folgende Zertifikate und Daten für die Echtheitsprüfung von Reisedokumenten herunterzuladen und zu verwalten: Country Signer Certificate Authority (CSCA), Document-Signer (DS), Certificate Revocation List (CRL). Business Owner: EZV
PKI	Public Key Infrastructure
Q1	Erstes Quartal des Jahres (Januar bis März)
Q2	Zweites Quartal des Jahres (April bis Juni)
QR Code	Quick Response Code: Maschinenlesbarer zweidimensionaler Code
RIPOL	Recherches informatisées de la police Bei RIPOL handelt es sich um das automatisierte Polizeifahndungssystem der Schweiz und enthält Fahndungen und Fernhaltemassnahmen zu Personen, Ausweisen, Fahrzeugen und Sachen. Business Owner: fedpol
S/N	Seriennummer
SAML	Die Security Assertion Markup Language ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen.

SAVIDA	Mit SAVIDA können in den Rapportierungssystemen Argos, RUMACA und eLynx Gruppenanfragen durchgeführt werden, um nach Personen, Firmen oder Fahrzeugen zu fahnden.
SDK	Software Development Kit
SEM	Staatssekretariat für Migration Dieses ist dem EJPD unterstellt.
simap	Informationssystem über das öffentliche Beschaffungswesen in der Schweiz (simap.ch)
TS	Technische Spezifikation
UC	Use Case
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VIN	Vehicle Identification Number
VIZ	Visual Inspection Zone: Visuelle Zone eines Reisedokumentes
VöB	Verordnung über das öffentliche Beschaffungswesen (SR 172.056.11)
WSBV	Web-Service-Bewilligungs-Verfahren: Nutzungsbewilligung für Webservices des Bundes
WTO	World Trade Organisation
z.B.	zum Beispiel
ZEMIS	Zentrales-Migrations-Informations-System Das ZEMIS dient der Bearbeitung von Personendaten aus dem Ausländer- und Asylbereich. In ZEMIS werden die Arbeitsbewilligungen, die Einbürgerungen und die Asylverfahren bearbeitet. ZEMIS beinhaltet auch die Schweizer Ausländerausweise und von der Schweiz ausgestellte Einreiseverbote. Business Owner: SEM
ZertServer	siehe PKD Schnittstelle
ZK	Zuschlagskriterium

Tabelle 1: Abkürzungsverzeichnis

2 Einleitung, Zweck des Dokuments

Das vorliegende Pflichtenheft beschreibt die Zielsetzungen, welche mit dem vorliegenden Beschaffungsgegenstand verfolgt und erreicht werden sollen. Es regelt Vorgehen und Form der Angebotseinreichung und dient zusammen mit den Allgemeinen Geschäftsbedingungen des Bundes (AGB) und dem Bundesgesetz vom 21. Juni 2019 über das öffentliche Beschaffungswesen (BöB, SR 172.056.1) sowie der Verordnung vom 12. Februar 2020 über das öffentliche Beschaffungswesen (VöB, SR 172.056.11) als Grundlage für das vorliegende Verfahren.

Das Verfahren richtet sich nach den Bestimmungen des Gesetzes für Verfahren innerhalb des Staatsvertragsbereichs.

3 Ausgangslage und Beschreibung des Beschaffungsgegenstandes

3.1 Ausgangslage

Im Rahmen der Grenzkontrolle verwendet die EZV aktuell das mobile Grenzkontrollsystem «eneXs mobile» (nachfolgend auch «altes mobiles GKS» genannt). Das alte mobile GKS wird hauptsächlich an der Landesgrenze (z.B. Zollposten, Aussenstandorte) und im Inland (z.B. in Bahnkontrollen) verwendet.

Mit der Assoziierung an Schengen hat sich die Schweiz einer engeren Kooperation der Grenzverwaltungsorgane verpflichtet. In diesem Rahmen werden die Instrumente für die Grenzkontrolle schrittweise ausgebaut. Insbesondere wird im Q2-2022 das Entry-Exit System (EES) eingeführt.

Das alte mobile GKS (eneXs mobile) ist aktuell nicht EES tauglich. Die EZV will ein EES taugliches "mobiles Grenzkontrollsystem" über das vorliegende öffentliche Verfahren beschaffen. Das neue mobile GKS muss mindestens die Funktionalität des alten mobilen GKS aufweisen und bis Q2-2022 betriebsbereit sein. Zum Zeitpunkt der Einführung des EES (Entry-Exit System) muss das neue mobile GKS "EES Ready" sein.

3.2 Altes mobiles Grenzkontrollsystem (Ist-Zustand)

Das alte mobile GKS steht den Grenzkontrollverantwortlichen als App auf iOS Smartphones zur Verfügung. Beim alten mobilen GKS handelt es sich in erster Linie um ein Abfragesystem, welches keine eigene Datenbank beinhaltet, jedoch viele Datenbanken zu Abfragezwecken nutzt.

Die App des alten mobilen GKS ermöglicht der EZV eine hohe Flexibilität bei Kontrollen und ist im Sinne einer ersten Abfrage unverzichtbar. Vertiefte Untersuchungen, Datenerfassungen und Berichterstattungen erfolgen mittels stationären Arbeitsstationen an einem Hauptgrenzkontrollpunkt, oder in Zukunft auch mittels portablen Arbeitsstationen (beide nicht Gegenstand dieser Ausschreibung).

Das alte mobile GKS unterstützt folgende Anwendungsfälle:

- Personenkontrolle: Mittels der eingebauten Kamera des Smartphones werden per OCR Scan die Personen- und Ausweisdaten der MRZ von maschinenlesbaren Dokumenten ausgelesen. Diese Daten können auch manuell eingegeben bzw. korrigiert werden. Das alte mobile GKS fragt mit den ausgelesenen Personen- und Dokumentdaten automatisch die Fahndungs- und Informationssysteme des fedpol, SEM, EU, Astra und Interpol auf Einträge ab. Das System stellt die Abfrageresultate einheitlich dar.
- Fahrzeugkontrolle: Mittels der eingebauten Kamera des Smartphones werden per OCR Scan die Kontrollschilder von Fahrzeugen gelesen. Diese Daten können auch manuell eingegeben bzw. korrigiert werden. Mit den Daten des ausgelesenen Kontrollschildes werden Fahrzeug- und Kennzeichenfahndungen sowie in den Informationssystemen des ASTRA Einträge zu Fahrzeug, Kennzeichen und Halter gesucht.
- Sachkontrolle: Die entsprechenden Daten (z.B. Seriennummer) werden manuell erfasst. Das alte mobile GKS fragt mit den Daten die entsprechenden Datenbanken nach Fahndungen ab.
- Personenidentifikation mittels Fingerabdrücken: Die Fingerabdrücke werden mittels einem kabellos angebundenen Fingerabdruckleser (S.I.C Biometrics IdentiFI45) ausgelesen. Das alte mobile GKS fragt mit den Fingerabdrücken die Systeme AFIS, C-VIS und SIS-AFIS (ab Q2-2021) ab, um die Person zu identifizieren.

Das alte mobile GKS nutzt die Datenbanken der nachfolgenden Anwendungen, welche Fahndungen, Personendaten, Bewilligungen, Entscheide, Ausweise oder Visa enthalten:

- RIPOL;
- ISA;
- ISR;
- ASF-SLTD, ASF-SMV, ASF-Nominals;
- C-SIS (Anschlusspunkt N-SIS);
- FABER;
- MOFIS;
- HOOGAN;
- C-VIS (Anschlusspunkt CVC);
- ORBIS (N-VIS);
- ZEMIS;
- SAVIDA;
- AFIS;
- SIS-AFIS (ab Q2-2021).

3.3 Neues mobiles Grenzkontrollsystem: Ziele und Ausblick

Mit der Erneuerung des mobilen Grenzkontrollsystems werden folgende Ziele verfolgt.

- Die aktuellen und zukünftigen rechtlichen Vorgaben für die Grenzkontrolle müssen eingehalten werden bzw. eingehalten werden können.
- Die Kontrollen müssen einfach, zuverlässig und flexibel - sowohl im Inland als auch im grenznahen in- und ausländischen Gebiet - durchgeführt werden können.
- Die Personenidentifikation muss schnell, korrekt und am Ort der Kontrolle erfolgen können.
- Um die bereits getätigten Investitionen zu schützen, muss das System mit den bestehenden Fingerabdrucklesern (S.I.C Biometrics IdentiFI45 und IdentiFI60/Kojak) kompatibel sein.

Das neue mobile Grenzkontrollsystem muss EES-tauglich sein, i.e. es muss prüfen können, ob die entsprechenden EES-Einträge vorhanden sind und diese anzeigen. Somit muss das System die bereits heute angesprochenen Anwendungen sowie das EES abfragen. Die Schnittstelle zum zentralen EES System der EU (C-EES) wird durch das CEC als Webservices zur Verfügung gestellt. Das EES wird in Zukunft auch für die Personenidentifikation verwendet.

Das neue mobile Grenzkontrollsystem muss erweiterbar sein, um den zukünftigen Anforderungen genügen zu können. Im Rahmen des Ausbaus der Schengen-Grenze sind insbesondere Integrationen mit den folgenden zukünftigen Systemen hinsichtlich Personenkontrollen bzw. Personenidentifikationen und -verifikationen vorgesehen:

- ETIAS (Anschlusspunkt offen);
- IOP (Anschlusspunkt offen);
- usw.

Das Auslesen des Datenchips eines eMRTD wird aktuell von eneXs mobile nicht unterstützt. Um die Daten im Chip mit jenen in der MRZ vergleichen und somit Manipulationen des Dokuments besser erkennen zu können, ist diese Fähigkeit im Nachfolgesystem zwingend zu implementieren.

Weiter hat die EZV die Wichtigkeit der Digitalisierung erkannt. Im Rahmen des Programms DaziT ist die EZV daran, ihre Systeme und Daten besser zu vernetzen resp. zu verknüpfen. Zum Beispiel werden die der EZV vorliegenden Informationen in den Grenzkontrollen besser integriert werden. Diesbezüglich

sind weitere Systeme wie z.B. das neue Rapportierungs- und Fallbearbeitungssystem für die mobilen Applikationen miteinzubeziehen.

3.4 Beschaffungsgegenstand

3.4.1 Lieferumfang

Mit der vorliegenden Ausschreibung will die EZV (nachfolgend «Auftraggeber» genannt) Anbieter evaluieren, welche in der Lage sind, ein Standard-Produkt für das in diesem Pflichtenheft ausgeschriebene mobile Grenzkontrollsystem:

- zu liefern und für den Auftraggeber zu konfigurieren;
- in die IT Landschaft (insbesondere MDM) des Auftraggebers zu integrieren;
- mit den oben genannten Datenbanken und Schnittstellen zu verknüpfen;
- in der Organisation des Auftraggebers einzuführen;
- den technischen Support, die Wartung und die Weiterentwicklung zu leisten.

Für die Beschaffung der Lösung ist von einer Dimensionierung von bis zu 700 «concurrent users» auszugehen.

Nachfolgend zeigt die Systemübersicht grob, welche Software zu liefern ist.

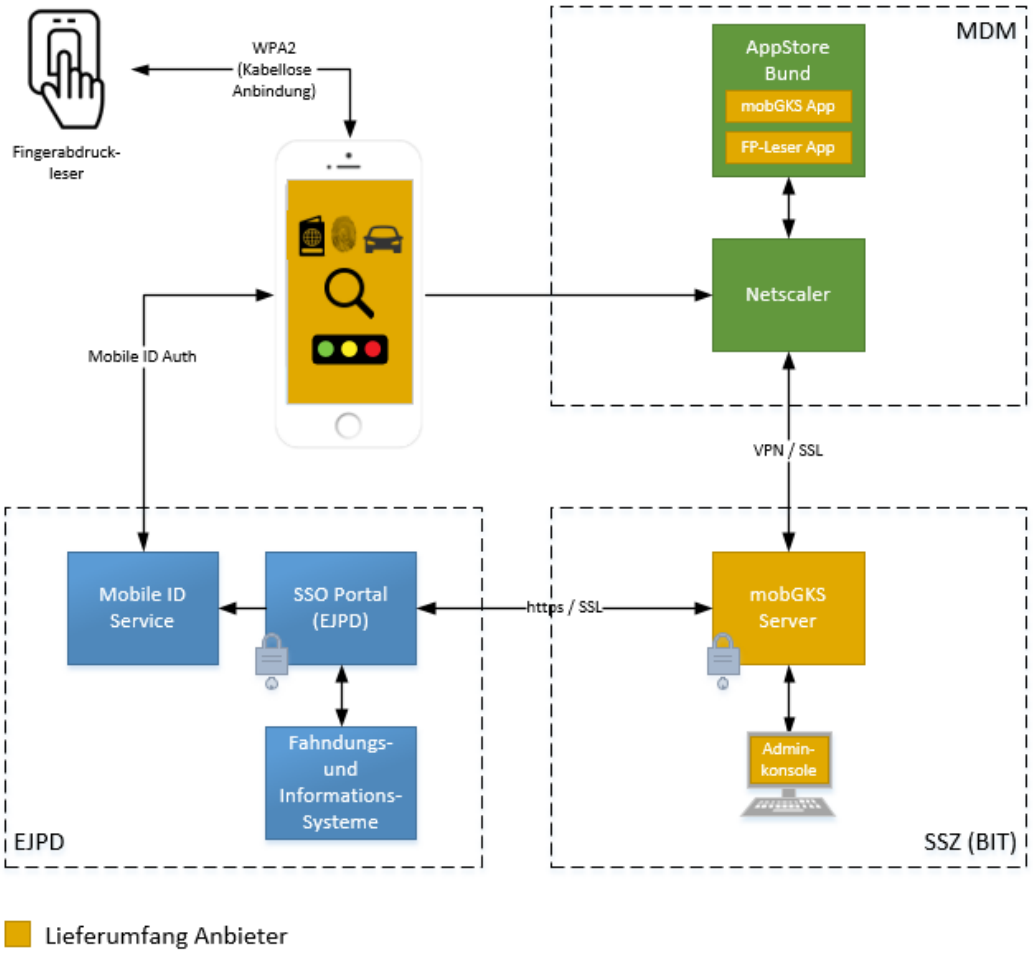

Abbildung 1: Systemübersicht mobGKS

Zu liefern sind folgende Objekte:

- **Mobile App GKS (nachfolgend «mobApp GKS»):** Der Grenzkontrollverantwortliche führt die Grenzkontrolle anhand dieser App durch. Die App muss die Grenzkontrolle bei Abfragen zu aktuellen Fahndungen, Personen-, Fahrzeug- und Sachdaten, Bewilligungen, Entscheide, Ausweise oder Visa unterstützen. [Preisblatt: siehe B-A und/oder B-C]
- **Fingerabdruckleser App (nachfolgend «FP-Leser App»):** Der Grenzkontrollverantwortliche erfasst die Fingerabdrücke der zu kontrollierenden Personen mittels dieser App und dem Fingerabdruckleser. Aus technischen Gründen kann die Erfassung der Fingerabdrücke nicht in der mobApp GKS erfolgen (siehe Ziffer 3.5.2.4). [Preisblatt: siehe B-A und/oder B-C]
- **Mobiler GKS Server (nachfolgend «mobGKS Server»):** Der mobGKS Server dient hauptsächlich der Kommunikation im Zusammenhang mit den Fahndungs- und Informationssystemen, sowie der Aufbereitung und Rücksendung der Resultate an die Apps. Die Erzeugung der Abfragen sowie die Aufbereitung der Resultate (Auswertung, Filterung) erfolgt im mobGKS Server mittels dem sogenannten «Logik Layer». [Preisblatt: siehe A-A und/oder A-C]
- **Administrationskonsole:** Dient der Konfiguration und Überwachung des Systems. [Preisblatt: siehe A-A und/oder A-C]

Die Ausschreibungsgegenstände (Software, Dienstleistungen) sind nachfolgend im Pflichtenheft in der Ziffer 3.5 und in dessen Beilagen vollständig beschrieben.

3.4.2 Abgrenzung

Folgende Leistungen gehören nicht zum Lieferumfang des Anbieters:

- Anwendersupport (1st Level Support) - dieser wird durch die Supportorganisation des Auftraggebers sichergestellt;
- Smartphones und Fingerabdruckleser, sowie Laptops, PCs, Bildschirme, Tastaturen und Mäuse (z.B. für Systemadministratoren) - diese Komponenten werden vom Auftraggeber zur Verfügung gestellt;
- Hosting und Betrieb von zentralen Komponenten - diese werden vom BIT gewährleistet (Modell Full Service des Bundesamts für Informatik BIT, Verfügbarkeit der zentralen Komponenten durch SLA BIT bestimmt – weiterführende Informationen: siehe Beilage P *«Infosheet Betrieb Fachanwendung BIT»*);
- MDM inklusive AppStore des Bundes (siehe Ziffer 3.5.2.1) - dies ist ein Service des ISC und wird vom BIT bereitgestellt und betrieben;
- EJPD SSO Portal (siehe Ziffer 3.5.2.1) - Die Webservices des EJPD werden mit dem EJPD SSO Portal vom ISC EJPD bereitgestellt und betrieben.

3.4.3 Arbeitspakete

Für die einfachere Gliederung der Leistungen sind diese in Arbeitspakete unterteilt:

- Die Arbeitspakete A bis C umfassen den Grundauftrag sowie die Optionen. Der Auftraggeber beabsichtigt die Leistungen des Grundauftrags zu beziehen, behält sich aber vor, optionale Leistungen vollumfänglich, teilweise oder gar nicht zu beziehen. Der Anbieter hat kein Anrecht auf Erbringung der als Optionen gekennzeichneten Leistungen.
- Das Preisblatt (Anhang 2) enthält alle, nach Arbeitspaketen gegliederten Leistungen. Der Grundauftrag und alle Optionen müssen offeriert werden. Alle erforderlichen Software Lizenzen, welche als Infrastrukturkosten zu verstehen sind, müssen vom Anbieter im Preis eingerechnet werden. Die im vorliegenden Pflichtenheft beschriebenen Hardwarekomponenten für den Betrieb der Lösung, werden von der EZV respektive vom Betreiber zur Verfügung gestellt und müssen nicht im Preis eingerechnet werden.

Arbeitspaket	*Bezeichnung*	*Auftragsart*	*Vertrag*
A	Einmalige Kosten für Mobile App GKS, Fingerabdruckleser App, Mobiler GKS Server und Administrationskonsole, Projektkosten	Grundauftrag (Festbestellmenge) und Optionsmenge	Rahmenvertag, Grundprojektvertrag
B	Weiterentwicklungsaufwände	Optionsmenge (Pooltage)	Rahmenvertrag, Projektvertrag oder Abrufbestellung
C	Wiederkehrende Kosten für Wartung und Pflege des mobilen Grenzkontrollsystem (EZV)	Grundauftrag (Festbestellmenge) und Optionsmenge	Rahmenvertrag, Wartungsvertrag

Tabelle 2: Übersicht der Leistungen

Der Auftraggeber wird gestützt auf den ausgeschriebenen Leistungsgegenstand, jeweils nach seinem Bedarf, Leistungen beim Zuschlagsempfänger beziehen bzw. abrufen.

3.5 Detaillierter Leistungsbeschrieb

Dieses Kapitel enthält die Beschreibung der gewünschten Systeme und Dienstleistungen.

3.5.1 Fachliche Anforderungen

Dieses Kapitel enthält die fachlichen Anforderungen für das System.

3.5.1.1 Prozessunterstützung (TS 1.1)

Das mobile Grenzkontrollsystem wird hauptsächlich als Abfragesystem verwendet. Die App muss die Grenzkontrolle bei Abfragen zu aktuellen Fahndungen, Personen-, Fahrzeug- und Sachdaten, Bewilligungen, Entscheide, Ausweise oder Visa unterstützen. Das System muss insbesondere folgende Anwendungsfälle unterstützen:

- Personen-, Dokument-, Fahrzeug- und Sachprüfungen an der Binnengrenze und im Inland;
- Personen- und Dokumentprüfungen an der Schengen-Aussengrenze (1. Kontrolllinie, ohne EES Erfassungen);
- Personenidentifikation mittels Fingerabdrücken.

Diesbezüglich muss das System die entsprechenden Vorgaben der Schweiz und der EU zu den Grenzkontrollprozessen erfüllen, insbesondere SR 142.20 (Ausländer- und Integrationsgesetz), SR 142.204 (Verordnung über die Einreise und die Visumerteilung), EU 2016/399 (Schengener Grenzkodex), EU 2017/2225 (EES), EU 2017/2226 (EES), EU 2018/1240 (ETIAS), EU 2019/329 (Verwendung biometrischer Daten EES) und SR 361.3 (Bearbeitung biometrischer erkennungsdienstlicher Daten).

3.5.1.2 Dokumente und Kontrollschilder scannen (TS 1.2)

Die mobApp GKS muss dem Grenzkontrollverantwortlichen die Auswahl zwischen dem Scannen eines maschinenlesbaren Dokuments (mindestens optische Erfassung der MRZ) und eines Fahrzeugkontrollschildes anbieten. Das Scannen hat mit der Kamera des Smartphones zu erfolgen.

Um die Erfassung für den Grenzkontrollverantwortlichen zu vereinfachen und der Spiegelung der Smartphone-Beleuchtung auf dem Reisedokument entgegenzuwirken, muss das System maschinenlesbare Dokumente bis zu einer Entfernung von 30 cm, mit einem Winkel bis 30 Grad in der Längsachse ("roll") sowie in der Querachse ("pitch") scannen und auslesen können. Fahrzeug-Kontrollschilder müssen bis zu einer Entfernung von 4 Metern gescannt und ausgelesen werden können.

Für das Scannen muss der Grenzkontrollverantwortliche das Licht des Smartphones bei Bedarf manuell aktivieren können.

3.5.1.3 Personenprüfung anhand von Reisedokumenten

3.5.1.3.1 Dokumente auslesen und Abfrage auslösen (TS 1.3, ZK 1.1, ZK 1.2)

Die mobApp GKS muss mittels der Kamera des Smartphones die MRZ von ICAO konformen Reisedokumenten (gemäss ICAO Doc 9303) folgender Dokumenttypen auslesen können (TS 1.3):

- Maschinenlesbare Reisedokumente (MRTD und eMRTD) in den Grössen TD1, TD2 und TD3;
- Visa, insbesondere auch Schengen-Visa und nationale Visa der Schweiz und weiterer Schengen-Mitgliedstaaten.

Das System soll mittels der Kamera des Smartphones die MRZ der folgenden gängigen nicht-ICAO-konformen Dokumente gemäss Beilage K *«Non-ICAO-Konformitaet_der_MRZ.pdf»* aus der mobApp GKS einlesen und erkennen können (ZK 1.1):

- Deutschland: Reisepass ID3, Modell 2007;
- Deutschland: Notpass ID3;
- Frankreich: Identitätskarte ID2;
- Schweiz: Führerausweis ID1;
- Liechtenstein: Führerausweis ID1;
- Belgien: Identitätskarte ID1, aktuelles Modell;
- Belgien: Identitätskarte ID1, Modell 2003;
- Belgien: Aufenthaltstitel für Freizügigkeitsberechtigte ID1.

Das mobile Grenzkontrollsystem soll den Chip von elektronischen maschinenlesbaren Dokumenten mit einem Smartphone auslesen können (z.B. mittels NFC). Um die Informationen auf dem Chip und aus der maschinenlesbaren Zone des Reisedokuments (MRZ) vergleichen zu können, sind mindestens die Informationen, welche auch in der MRZ vorhanden sind, anhand der App vom Chip auszulesen. (ZK 1.2)

Anhand der ausgelesenen Personen- und Dokumentdaten, muss das System automatisch die entsprechenden Fahndungs- und Informationssysteme auf Einträge abfragen. Der Grenzkontrollverantwortliche muss die Daten prüfen, bei Bedarf manuell korrigieren und Abfragen mit den korrigierten Daten auslösen können. Im Fehlerfall muss der Grenzkontrollverantwortliche den Auslesevorgang wiederholen können (TS 1.3).

3.5.1.3.2 Echtheit der elektronischen maschinenlesbaren Reisedokumente prüfen (ZK 1.3)

Das mobile Grenzkontrollsystem soll die Echtheit eines eMRTD anhand der Zertifikate prüfen können. Diesbezüglich soll das System die Zertifikate gemäss Ziffer 3.5.2.7.2 beziehen können.

Weiter soll das System unbekannte Zertifikate sammeln und mittels der Schnittstelle DS Data Collection (siehe Ziffer 3.5.2.7.2) zur Überprüfung weiterreichen können.

3.5.1.3.3 Manuelle Abfrage auf Personen und Dokumente (TS 1.4)

Das mobile Grenzkontrollsystem muss dem Grenzkontrollverantwortlichen ermöglichen, eine manuelle Abfrage in Bezug auf Personen und Dokumente auszulösen (z.B. für Dokumente ohne MRZ). Dafür muss der Grenzkontrollverantwortliche die Angaben der Personalien sowie der Reisedokumente in der mobApp GKS manuell eingeben bzw. bearbeiten können.

Mindestens folgende Angaben müssen eingegeben werden können:

- Name, Vorname;
- Geburtsdatum von (Jahr), Geburtsdatum bis (Jahr);
- Ausweis-Nr.;
- Ausstellendes Land;

- Adresse (Strasse, Postleitzahl, Ort) als Suchkriterium für juristische Personen;
- Juristisch (Suchoption, um nur nach Einträgen von juristischen Personen zu suchen).

Diese Liste von Angaben muss bei Bedarf angepasst oder erweitert werden können (z.B. Nationalität).

Die mobApp GKS muss die Eingabe durch Auswahlfelder unterstützen können (z.B. Land).

Der Grenzkontrollverantwortliche soll die Inhalte der Suchkriterien Name und Vorname mittels einer Funktion tauschen können.

3.5.1.3.4 Gesichtsbildvergleich (ZK 1.4)

Das mobile Grenzkontrollsystem soll eine Funktionalität anbieten, um einen Gesichtsbildvergleich aus der mobApp GKS durchführen zu können. Dafür soll der Grenzkontrollverantwortliche die Bilder aus verschiedenen Quellen auswählen können (z.B. Livebild, Bild auf Chip, Bild auf Personalseite des Dokuments (VIZ), Bild auf Smartphone, Bilder aus Fahndungs- und Informationssystemen). Die Funktionalität soll den Übereinstimmungsgrad der Bilder berechnen und darstellen.

Die Qualität der Bilder soll vor einem Gesichtsbildvergleich vom System geprüft werden. Dafür dürfen keine externen Services (von Dritten) aufgerufen werden. Für diese Prüfung und den Gesichtsbildvergleich ist ein, im Kontext der Grenzkontrolle, bewährter Algorithmus zu verwenden (keine Freeware oder Individualentwicklung).

3.5.1.3.5 Fingerabdruckvergleich Chip eMRTD (ZK 1.5)

Das mobile Grenzkontrollsystem soll eine Funktionalität anbieten, um einen Fingerabdruckvergleich aus der mobApp GKS durchführen zu können. Dafür sollen die Grenzkontrollverantwortlichen die Fingerabdrücke aus dem Chip des Reisedokumentes mit den Fingerabdrücken aus dem Fingerabdruckleser vergleichen können. Die Funktionalität soll den Übereinstimmungsgrad der Fingerabdrücke berechnen und darstellen.

Für den Vergleich der Fingerabdrücke ist ein, im Kontext der Grenzkontrolle, bewährter Algorithmus zu verwenden. Der Algorithmus soll im System vorhanden sein. Dafür dürfen keine externen Services (von Dritten) aufgerufen werden.

Um die Fingerabdrücke aus dem geschützten Bereich des Chips mittels der erweiterten Zugangskontrolle (EAC) auslesen zu können, soll das mobile GKS sich über die Schnittstelle EAC IS Service (siehe Ziffer 3.5.2.7.2) authentifizieren können.

3.5.1.3.6 EES-Prüfung (TS 1.5)

Bei Reisenden, welche dem EES unterstellt sind, muss das mobile Grenzkontrollsystem die EES-Einträge des Reisenden abfragen und prüfen ob der benötigte EES Eintrag vorhanden ist.

Bei jeder EES-Prüfung muss das mobile Grenzkontrollsystem die Aufenthaltsdauer und ggf. die verbleibende Anzahl Tage bis zum Stichtag der geforderten Ausreise resp. die Überschreitung der zulässigen Aufenthaltsdauer anzeigen.

3.5.1.3.7 ETIAS-Prüfung (TS 1.6)

Für Reisende, welche dem ETIAS unterstellt sind, wird das mobile Grenzkontrollsystem die ETIAS Daten der ersten Kontrolllinie gemäss EU 2018/1240 anzeigen müssen.

3.5.1.3.8 Einlesen Barcodes und 2D Codes (TS 1.7)

Das mobile Grenzkontrollsystem muss die folgenden Barcodes und 2D Codes aus Reisedokumenten mittels Smartphone-Kamera aus der mobApp GKS einlesen, prüfen und entschlüsseln/interpretieren können:

- Code 39 (ISO/IEC 16388);
- Aztec Code (ISO/IEC 24778);
- Data Matrix (ISO/IEC 16022);

- PDF417 (ISO/IEC 15438);
- QR-Code (ISO/IEC 18004).

3.5.1.4 Fahrzeug- und Sachprüfungen

3.5.1.4.1 Kontrollschild auslesen / Abfrage auslösen (TS 1.8, ZK 1.7)

Das mobile Grenzkontrollsystem muss dem Grenzkontrollverantwortlichen das Auslesen der Fahrzeug-Kontrollschilder mittels Videobilder aus der mobApp GKS ermöglichen. Die Erfassung muss sowohl im Hoch- als auch im Querformat möglich sein. Die Erkennung muss für Kontrollschilder mit einer Zeile sowie mit zwei Zeilen funktionieren (TS 1.8).

Sobald das mobile Grenzkontrollsystem das Kontrollschild erkannt hat, muss es ein Bild des Kontrollschilds sowie die erkannten Zeichen anzeigen. Das System muss mindestens die Kontrollschilder der folgenden Länder automatisch erkennen und auslesen können (TS 1.8):

- Schweiz;
- Liechtenstein;
- Deutschland;
- Österreich;
- Italien;
- Frankreich.

Weiter soll das System die Kontrollschilder von weiteren Ländern Europas automatisch erkennen und auslesen können. Der Anbieter soll aufzeigen, von welchen Ländern das System die Kontrollschilder automatisch erkennen und auslesen kann (ZK 1.7).

Der Grenzkontrollverantwortliche muss die Daten prüfen, bei Bedarf manuell korrigieren und Abfragen mit den korrigierten Daten auslösen können. Im Fehlerfall muss der Grenzkontrollverantwortliche den Scanvorgang wiederholen können (TS 1.8).

Für die Erkennung muss eine bewährte Standardsoftware verwendet werden (keine Freeware oder Individualentwicklung). Die Erkennung hat im System zu erfolgen (keine Aufrufe auf externen Servern) (TS 1.8).

3.5.1.4.2 Manuelle Abfrage auf Fahrzeuge oder Sachen (TS 1.9)

Die mobApp GKS muss dem Grenzkontrollverantwortlichen ermöglichen, eine manuelle Abfrage in Bezug auf Fahrzeuge oder Sachen auslösen zu können.

Mindestens folgende Angaben müssen für die Fahrzeugprüfungen eingegeben werden können:

- Kennzeichen;
- VIN;
- Stamm-Nr.;
- Fahrzeugart.

Mindestens folgende Angaben müssen für die Sachprüfungen eingegeben werden können:

- Identifikations-Nr.;
- Sachbezeichnung;
- Gravurtext oder Datum.

Diese Liste von Angaben muss bei Bedarf angepasst oder erweitert werden können (z.B. Motornummer, Sach-Nationalität).

Das System muss die Eingabe durch Auswahlfelder unterstützen können (z.B. Fahrzeugart, Sachbezeichnung).

3.5.1.5 Personenidentifikation

3.5.1.5.1 Identifikation über Fingerabdrücke (TS 1.10)

Das mobile Grenzkontrollsystem muss dem Grenzkontrollverantwortlichen ermöglichen, Personen mittels Fingerabdrücken zu identifizieren (i.e. 1:n Matching). Für diese Identifikation muss das mobile Grenzkontrollsystem die Fingerabdrücke mittels dem Fingerabdruckleser (siehe Ziffer 3.5.2.6) erfassen können.

Vorerst werden die Identifizierungen in den Datenbanken AFIS, SIS-AFIS, C-VIS und EES durchgeführt.

Der Grenzkontrollverantwortliche muss auswählen können, in welchen Systemen die Abfrage durchgeführt wird. Dabei muss er Abfragen in einzelnen oder in mehreren Systemen gleichzeitig durchführen können.

- Abfragen in AFIS, SIS-AFIS und C-VIS müssen mittels 2FP (Zeigefinger linke und rechte Hand) erfolgen können.
- Abfragen in EES müssen mittels 4FP (Zeigefinger bis kleiner Finger rechte Hand) erfolgen können.
- Zusätzlich müssen Abfragen in C-VIS und SIS-AFIS auch mittels 4FP oder 10FP erfolgen können.

Das System muss den Grenzkontrollverantwortlichen durch den Fingerabdruckerfassungsprozess führen. Die Fingerabdruckerfassung für die verschiedenen Datenbanken ist so zu gestalten, dass jeder Finger max. einmal zu erfassen ist.

3.5.1.5.2 PCN für AFIS Abfrage (TS 1.10)

Die Abfrage zur Identifikation mittels Fingerabdrücken in der Datenbank AFIS, muss eine eindeutige PCN (Process Control Number) beinhalten.

Das mobile Grenzkontrollsystem muss für die Abfrage diese eindeutige PCN berechnen können. Dafür muss das mobile Grenzkontrollsystem die entsprechenden PCN Nummernkreise verwalten können.

Die PCN ist aktuell 12-stellig, wovon die letzten zwei Ziffern als Prüfziffer fungieren. Die PCN-Kennung wird wie folgt aufgebaut:

PCN-Stelle	Wert	Bedeutung
1-2	50	Behörde EZV
3-10	00000001	fortlaufende Nummer der FP-Erfassung, beginnend bei 00000001
11-12	nn	berechnete Prüfziffer

Tabelle 3: PCN Nummer

Die eindeutige PCN ist zu generieren, in dem die letzte verwendete Nummer inkrementell erhöht wird und die Prüfziffer mit einem Divisionsalgorithmus («Modulo») berechnet wird.

3.5.1.5.3 Resultate asynchron abholen (TS 1.10)

Die Antwortzeiten von AFIS, C-VIS und EES auf die getätigten Abfragen können mehrere Sekunden (ca. 11 bis 14 Sek. für EES gemäss ICD 4.0.0) bis Minuten (für AFIS) betragen. Während dieser Zeit muss der Grenzkontrollverantwortliche mit dem Grenzkontrollsystem weiterarbeiten können. Deshalb muss das mobile Grenzkontrollsystem die Antworten aus den Datenbanken AFIS, C-VIS und gegebenenfalls EES asynchron abholen können.

Das mobile Grenzkontrollsystem muss dem Grenzkontrollverantwortlichen in der mobApp GKS eine Übersicht der Datenbankenabfragen mit dem Status der Antwort (z.B. ausstehend, abholbereit, abgeholt, Timeout/Fehler) anzeigen. In der Übersicht muss der Zeitpunkt der Abfrage ersichtlich sein.

Wenn eine Antwort eingetroffen ist, muss das System dies dem Grenzkontrollverantwortlichen melden.

Die Treffer müssen in einer Ansicht (Trefferliste oder ähnliches) dargestellt werden. Aus dieser Ansicht heraus muss der Grenzkontrollverantwortliche zu den Details eines Treffers navigieren können.

Da der Name der Person bei einer Identifikation nicht immer vorhanden ist und die Antwort der Abfrage einige Zeit in Anspruch nehmen kann, soll das Grenzkontrollsystem den Grenzkontrollverantwortlichen unterstützen, die Person in der Übersicht der Identifikationsabfragen zu finden (z.B. mittels eines Gesichtsbildes).

3.5.1.5.4 Qualitätsprüfungen bei der Erfassung der Fingerabdrücke (ZK 1.6)

Das mobile Grenzkontrollsystem soll dem Grenzkontrollverantwortlichen allfällige Probleme bei der Fingerabdruckerfassung anzeigen (z.B. Fingerabdruck verdreht, Fehler Papillaren, gleicher Finger mehrfach aufgelegt, Verbindung verloren, Bild in ungenügender Qualität).

Wenn kein Fingerabdruck erzeugt werden kann, soll der Grenzkontrollverantwortliche im mobilen Grenzkontrollsystem den entsprechenden Finger für die Abfrage markieren können (z.B. nicht erfasst, bandagiert, amputiert).

Das mobile Grenzkontrollsystem soll einen Algorithmus zur Qualitätsprüfung der Fingerabdrücke einsetzen. Für die Qualitätsbewertung der Fingerabdruckbilder ist der Algorithmus NIST NFIQ 2.0 oder höher zu verwenden.

Das System soll den Grenzkontrollverantwortlichen bei ungenügender Qualität (< NFIQ 3) warnen. Der Grenzkontrollverantwortliche soll in diesem Fall entscheiden können, ob er die Fingerabdrücke für die Identifikation einreichen will oder ob er die Erfassung (z.B. einzelner Finger) wiederholen möchte.

3.5.1.6 Logik Layer mobiles GKS

Das mobile Grenzkontrollsystem muss sich an komplexen Webservices im Kontext von Fahndungs- und Informationssystemen anbinden können (siehe Ziffer 3.5.2.7.1).

Die Komponente des mobilen Grenzkontrollsystems, welche die Abfragen an die Fahndungs- und Informationssysteme erstellt und die Resultate dieser Abfragen für die Darstellung in der mobApp GKS aufbereitet, wird als «Logik Layer mobGKS» bezeichnet.

Der Logik Layer hat also zwei Hauptfunktionen:

1. **Umsysteme abfragen**: Der Logik Layer mobGKS muss bei einer automatischen oder manuellen Abfrage die verschiedenen Datenbanken parallel ansprechen können. Die verfügbaren Suchkriterien sowie deren Kombinationen für die Abfragen können sich abhängig von den verschiedenen Fahndungs- und Informationssystemen unterscheiden. Der Logik Layer muss diese Kombinationen erstellen und die entsprechenden Abfragen durchführen.
2. **Resultate der Abfragen aufbereiten**: Die Abfragen der Umsysteme können eine grosse Anzahl Resultate zurückliefern. Jedoch ist die Grösse der Smartphone-Bildschirme begrenzt. Das Ziel der Aufbereitung ist, die Resultate so auszuwerten und zu filtrieren, dass der Grenzkontrollverantwortliche nur die relevanten Resultate als Entscheidungsgrundlage erhält.

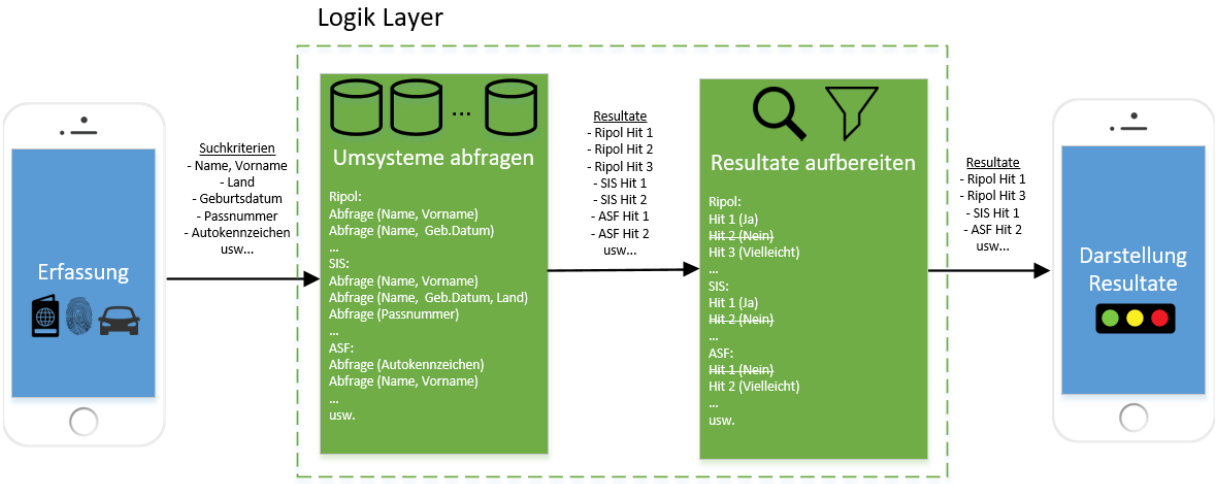

Abbildung 2: Logik Layer mobGKS

3.5.1.6.1 Umsysteme abfragen (Suchkriterien / Kombinationen) (ZK 1.8)

Um kurze Antwortzeiten zu garantieren, soll der Logik Layer mobGKS mit ausgewählten Kombinationen der Suchkriterien, entsprechende Abfragen auf den verschiedenen Fahndungs- und Informationssystemen auslösen können.

Pro Fahndungs- und Informationssystem sollen mehrere Kombinationen angewandt werden können. Welche Kombinationen abgefragt werden, hängt vom jeweiligen System ab.

Auf Grund der belegten Eingabefelder soll der Logik Layer mobGKS für jedes System bestimmen, welche Kombinationen der Suchkriterien, gültige Abfragekombinationen sind. Für jede gültige Abfragekombination soll der Logik Layer mobGKS anschliessend die Abfrage mit den Werten aus den Eingabefeldern auslösen. Die nachfolgende Abbildung zeigt exemplarisch die zulässigen Kombinationen von Suchkriterien (vertikal) pro System (horizontal).

	Namen + Vornamen (phonetisch)	Namen + Geburtsdatum (phonetisch)	Namen + Geburtsdatum (nicht phonetisch)	Namen + Geburtsjahr (nicht phonetisch)	Namen + Geburtsjahr von (phonetisch)	Namen + Geburtsjahr von (nicht phonetisch)	…en + Geburtsjahr von + Geburtsjahr bis (phonetisch)	…	Ausweisnummer	…	VIN	Motoren Nummer	Kennzeichen	Kennzeichen + Nation	…
System A (Personen)	x	x			x		x		x						
System A (Fahrzeuge)											x	x	x	x	
System A (Sachen)															
System B (Ausweise)									x						
System B (Fahrzeuge)											x	x	x		
System C (Personen)	x		x			x		x							
System C (Ausweise)	x		x	x					x						
System D (Fahrzeuge)											x		x	x	
System D (Kennzeichen)													x	x	
System E	x	x			x			x			x		x		
…															

Abbildung 3: Logik Layer - Abfragekombinationen (Beispiel)

Ein Systemadministrator soll die zulässigen Kombinationen der Suchkriterien einsehen, anpassen, addieren und löschen können. Es sollte idealerweise möglich sein, die Kombinationen für die Anfragen von einer Datei (z.B. xlsx, csv) ins System zu importieren, bzw. aus dem System heraus in eine Datei (z.B. xlsx, csv) zu exportieren.

Der Anbieter soll die Funktionalität zur Erstellung der Abfragen an Umsysteme, welche bereits im System vorhanden ist, aufzeigen (unabhängig davon, ob diese der oben beschriebenen Abfragekombinationen entspricht).

3.5.1.6.2 Resultate der Abfragen aufbereiten (Auswertung / Filtrierung) (ZK 1.9)

Der Logik Layer mobGKS soll die Resultate aus den verschiedenen Informations- und Fahndungssystemen aufbereiten können. Pro Informations- und Fahndungssystem soll dieser festlegen können, welche Treffer für den Grenzkontrollverantwortlichen relevant sind.

Die Relevanz ist anhand der Übereinstimmung (z.B. «exakt», «nicht exakt», «keine Übereinstimmung») der Suchkriterien, mit den entsprechenden Attributen der Treffer der Systeme (z.B. Name, Vorname, Geburtsdatum, Land, Geschlecht, Kontrollschildnummer, Seriennummer, usw.) zu bestimmen. Die Auswertung soll anhand von Regeln, basierend auf den möglichen Kombinationen, erfolgen können.

Nachfolgend ist ein Beispiel der Regeln für die Auswertung der Treffer einer Personensuche in einem Fahndungssystem abgebildet. Die Treffer sollen Kategorien zugeteilt werden können (z.B. «relevant», «vielleicht relevant», «nicht relevant»).

Nr.	Namen exakt	Namen nicht exakt	Vornamen exakt	Vornamen nicht exakt	Geburtsdatum exakt	Geburtsdatum nicht exakt	Geschlecht	Nationalität	**Resultat**
1		x		x		x	x	x	Relevant
2		x		x		x	x		Relevant
3		x	x				x		Nicht relevant
4		x			x		x		Vielleich relevant
…	…	…	…	…	…	…	…	…	…

Abbildung 4: Logik Layer - Auswertung Resultate (Beispiel)

Der Name, der Vorname oder das Geburtsdatum in einem Treffer sind «exakt», wenn diese mit dem Namen, Vornamen bzw. Geburtsdatum des Reisedokuments vollständig übereinstimmen. Wenn diese nur teilweise übereinstimmen, sind diese «nicht exakt». Stimmen die Angaben des Treffers mit jenen des Reisedokuments nicht überein, werden diese mit «keine Übereinstimmung» klassiert.

Beispiel:

	Angaben Pass	**exakt**	**nicht exakt**	**keine Übereinstimmung**
Name	de Bruijn	de Bruijn	Vedder de Bruijn	Vedder
Vorname	Lieselotte Anja	Lieselotte Anja	Lieselotte	Lisa
Geburtsdatum	14.12.1965	14.12.1965	1965	14.12.1973

Die Auswertung für Treffer zu Abfragen von Fahrzeugen und Sache hat gemäss dem gleichen Prinzip, jedoch mit anderen Attributen zu erfolgen.

Basierend auf der Auswertung soll der Logik Layer die Resultate filtern können. Nur die relevantesten Resultate sind der App zurückzugeben (z.B. Auswertung = «relevant» oder «vielleicht relevant»).

Ein Systemadministrator soll die Parameter und Regeln für die Aufbereitung (i.e. Auswertung und Filterung) der Resultate einsehen und konfigurieren können. Es sollte idealerweise möglich sein, die Regeln für die Auswertung aus einer Datei (z.B. xlsx, csv) ins System zu importieren, bzw. aus dem System heraus in eine Datei (z.B. xlsx, csv) zu exportieren.

Der Anbieter soll die Funktionalität zur Aufbereitung der Treffer (Auswertung und Filtrierung), welche bereits im System vorhanden ist, aufzeigen (unabhängig davon, ob diese der oben beschriebenen Funktionalität entspricht).

Bemerkung 1: Die gewünschte Darstellung der Resultate (z.B. Ampelsystem) ist unter Ziff. 3.5.1.7 beschrieben.

Bemerkung 2: Die Filterung der Resultate stellt keinen Ersatz für die Mechanismen, welche für den Umgang mit der limitierten Bandbreite unter Ziff. 3.5.1.9.4 angedeutet sind, dar.

3.5.1.7 Bedienung

3.5.1.7.1 Mehrsprachigkeit (TS 1.11)

Die Bedienoberflächen der mobApp GKS und der FP-Leser App müssen in deutscher, französischer und italienischer Sprache vorhanden sein.

3.5.1.7.2 Darstellung der Zusammenfassung der Resultate (ZK 1.10)

Die mobApp GKS soll eine Zusammenfassung der Treffer darstellen. Der Grenzkontrollverantwortliche soll auf einen Blick ohne scrollen sehen können, ob relevante Treffer gefunden wurden (z.B. mittels eines Ampelsystems - Grün="Alles OK", Gelb="Vielleicht relevant", Rot="Relevante Treffer"). Die Sichtung «auf einen Blick» soll mindestens mit der Schriftgrösse und Auflösung der Grundeinstellung der App bzw. des Smartphones möglich sein.

Die Zusammenfassung soll das Ergebnis der Suche je Gruppierung (z.B. nach System/Datenbank) ausweisen, d.h. ob Treffer erzielt wurden oder nicht. Dabei soll die Anzahl exakte/nicht exakte Treffer je Gruppierung ersichtlich sein. Falls ein System/eine Datenbank für die Suche deaktiviert wurde oder nicht zur Verfügung steht, soll die Zusammenfassung dies anzeigen.

Weiter sollen die eingegebenen Suchkriterien in der Zusammenfassung ersichtlich sein.

Auf dieser Stufe soll eine Navigation zur Ansicht der Treffer (Trefferliste oder ähnliches) vorhanden sein.

3.5.1.7.3 Darstellung Trefferliste (oder Gleichwertiges) (ZK 1.11)

Die mobApp GKS soll eine Trefferliste (oder Gleichwertiges) anbieten. Auf dieser Stufe sollen folgende Informationen ersichtlich sein:

- Treffertyp (Person, Fahrzeug, etc.);
- System/Datenbank, aus welcher der Treffer stammt;
- Kurzauskunft/Kurzansicht zum Treffer;
- Warnungen, Fahndungsauftrag und Hinweis zum Treffer.

Die Trefferdarstellung ist so zu gestalten, dass die relevantesten Treffer zuoberst in der Liste erscheinen und als solche klar erkennbar sind. Die Sortierung in der Trefferliste soll auf Gesamtsystemebene konfigurierbar sein.

Auf dieser Stufe soll eine Navigation zur Detailansicht je Treffer sowie zur Zusammenfassung vorhanden sein.

3.5.1.7.4 Darstellung Detailansicht Treffer (ZK 1.12)

Die mobApp GKS soll eine Detailansicht eines Treffers anbieten. Die Detailansicht soll alle Daten zum Treffer aus dem Fahndungs- bzw. Informationssystem enthalten.

Die App soll auch Bilder (z.B. Gesichtsbilder), Dokumente oder Alias-Angaben anzeigen und darstellen können, sofern solche Informationen in den Resultaten vorhanden sind. Hyperlinks sollen klar als solche zu erkennen sein (z.B. Farbe, unterstrichen).

Auf dieser Stufe soll eine Navigation zur Trefferliste (oder ähnliches) sowie zur Zusammenfassung vorhanden sein.

Der Grenzkontrollverantwortliche kann aus der Detailansicht in die manuelle Suche verzweigen und dabei die Daten als Suchkriterien übernehmen.

3.5.1.7.5 Manuelle Abfragen auf Basis Treffer (ZK 1.13)

Auf der Basis eines Treffers aus einem Fahndungs- und Informationssystem sowie aus einer Personenidentifikation soll der Grenzkontrollverantwortliche eine manuelle Suche zum gleichen Treffertyp (z.B. Personen, Fahrzeug, Sachen) auslösen können. Das System soll die entsprechenden Parameter aus dem Treffer, um die Abfrage durchführen zu können, in die manuelle Suche übernehmen.

Auf der Basis eines Treffers zu einem schweizerischen Kontrollschild soll der Grenzkontrollverantwortliche eine manuelle Suche zum Fahrzeughalter auslösen können. Das System soll die entsprechenden Parameter aus dem Treffer, um die Fahrzeughalterabfrage durchführen zu können, in die manuelle Suche übernehmen.

3.5.1.7.6 Transliterationen (ZK 1.14)

Die mobApp GKS soll Transliterationen bei der Erfassung von Zeichen unterstützen.

Die Transliterationen sind gemäss den Vorgaben des EJPD vorzunehmen (siehe Beilage G «Transliterationstabelle.pdf»).

3.5.1.7.7 Historie (ZK 1.15)

Die mobApp GKS soll dem Grenzkontrollverantwortlichen die Sichtung seiner letzten Abfragen in einer Historie ermöglichen.

Die Bedienung der Historie soll insbesondere Folgendes erlauben:

- die Trefferliste der Abfrage anzeigen;
- die Abfrage und deren Trefferliste löschen;
- die Abfrage wiederholen (mit den alphanumerischen Daten);
- die Suchkriterien der Abfrage für eine neue Abfrage übernehmen.

Das mobile Grenzkontrollsystem soll alle historisierten Abfragen automatisch löschen können.

Bemerkung: Die Historie darf ausschliesslich auf der mobApp GKS persistiert werden.

3.5.1.7.8 Nachtmodus (TS 1.12)

Die mobApp GKS muss einen Nachtmodus anbieten. In diesem Modus darf die Beleuchtung des Smartphones im Dunkeln durch Dritte nicht erkennbar sein.

3.5.1.8 Weitere Funktionen

3.5.1.8.1 Persönliche Einstellungen (ZK 1.16)

Der Grenzkontrollverantwortliche soll im mobilen Grenzkontrollsystem seine persönlichen Einstellungen persistent setzen können, insbesondere:

- Benutzersprache;
- Benutzeridentifikationen und Passwörter;
- Grösse der Darstellung (z.B. Schriftgrösse);
- Anzahl Abfragen in der Historie konfigurieren.

3.5.1.8.2 Kontrollprofil (TS 1.13)

Der Grenzkontrollverantwortliche muss das Profil der Kontrolle je nach Einsatz anwählen oder ändern können. Dieses Profil ist insbesondere für Abfragen (z.B. VIS Identifikation, ETIAS, sowie andere Fahndungs- und Informationssysteme) oder automatische Datenexporte relevant. Im Profil sind mindestens folgende Parameter festzuhalten:

- Kontrolltyp: Border Check (Aussengrenze), Territory Check (z.B. Binnengrenze, Inlandkontrolle, Bahnkontrolle);
- Reiserichtung: Einreise, Ausreise, beide Richtungen.

Es wird davon ausgegangen, dass die meisten Einsätze nach dem Profil Kontrolltyp = Territory Check / Reiserichtung = beide Richtungen erfolgen werden.

Es muss möglich sein, bei Bedarf weitere Kontrollprofile zu definieren (z.B. Zollkontrolle). Diese Profilverwaltung muss zentral möglich sein.

3.5.1.8.3 Abfragesystem deaktivieren (ZK 1.17)

Für die Abfragen sollen einzelne Fahndungs- und Informationssysteme deaktiviert und wieder aktiviert werden können (z.B. falls diese wegen technischer Probleme oder Wartungsarbeiten nicht verfügbar sind). Die deaktivierten Systeme sind von der Abfrage auszunehmen.

Der Anbieter muss aufzeigen, wie dies erfolgen kann (z.B. zentral / lokal, automatisch / manuell). Falls die Deaktivierung lokal und manuell auf Stufe App erfolgt, sollen beim erneuten Öffnen der App alle Fahndungs- und Informationssysteme wieder aktiviert werden.

3.5.1.8.4 Version Apps (TS 1.14)

Der Grenzkontrollverantwortliche muss in den Apps (mobApp GKS, FP-Leser App) die Version der Apps einsehen können.

3.5.1.8.5 Übersicht der neuen RIPOL Fahndungen (ZK 1.18)

Das mobile Grenzkontrollsystem soll dem Grenzkontrollverantwortlichen eine Übersicht der letzten publizierten Personen-, Fahrzeug- und Sach-Fahndungen (z.B. letzte 24 Stunden, letzte 3 Tage) aus RIPOL anzeigen können.

3.5.1.8.6 Fachliches Logging (ZK 1.19)

Um die Anwendung der Lösung zu Führungszwecken auswerten zu können, soll das System ein fachliches Logging von Daten ermöglichen. Zum Beispiel:

- Allgemeine Verwendung der Lösung durch die Grenzkontrollverantwortlichen (z.B. durchschnittliche Anzahl Abfragen pro Tag/Zeitintervall und pro Region/Standort, Anzahl User, welche die App in den letzten bspw. 28 Tagen nie benutzt haben, usw.);
- Häufigkeit der Verwendung der einzelnen Funktionalitäten der Lösung (z.B. Erfassung Personen/Fahrzeuge/Sachen via Kamera, manuelle Erfassung Personen/Fahrzeuge/Sachen, weitere Funktionen wie Wechsel Name <-> Vorname, Übernahme Resultat in die manuelle Suche, Nachtmodus, Grossschrift, usw.).

Dieses Logging darf keine sensitiven Daten aus den Kontrollen beinhalten (z.B. Fahndungen, biometrische Daten, usw.).

Der Anbieter soll aufzeigen, welche Möglichkeiten zum fachlichen Logging für die Lösung bereits vorhanden sind.

3.5.1.8.7 Revisionssicheres Logging (ZK 1.20)

Auf dem Server soll ein revisionssicheres Logging erfolgen können.

Die Systemnutzung der Serverumgebung GKS mobile Server ist lückenlos und nicht veränderbar zu historisieren und soll nachträglich jederzeit nachvollzogen werden können. In den Logfiles der geprüften Personen, Dokumente und Fahrzeuge sind keine datenschutzrelevanten Logeinträge vorzunehmen. Zur Kontrolle können durch den zuständigen ISBO Stichproben der Protokollierungen durchgeführt werden.

3.5.1.8.8 Automatischer Datenexport (ZK 1.21)

Das System soll automatisch Datenexporte der Grenzkontrollabfragen und der Geokoordinaten der Kontrollen erstellen können, wenn eine der im System definierten Regel (z.B. Nationalität=CHE und Alter<=18, usw.) zutrifft. Als Regelkriterien sind sämtliche, während des Grenzkontrollprozesses gewonnenen Informationen in allen möglichen Kombinationen anzubieten. Die Datenexporte sind vom System in Dateiordnern in einem gängigen Format (z.B. XML, PDF) für die Weiterverwendung durch Fremdsysteme bereitzustellen.

3.5.1.8.9 Anzeige Status der Apps und deren Anbindungen (ZK 1.22)

Die Apps sollen mittels einer einfachen Anzeige dem Grenzkontrollverantwortlichen mitteilen, ob die Apps einsatzfähig und mit den Umsystemen (Informations- und Fahndungssysteme, Fingerabdruckleser) verbunden sind.

3.5.1.9 Nicht-Funktionale Anforderungen

3.5.1.9.1 Fehlerhandling (TS 1.15)

Das mobile Grenzkontrollsystem muss mit Kommunikationsunterbrüchen, Netzwerkproblemen, Fehleingaben oder Ausfällen von zentralen Komponenten, Fingerabdrucklesern oder Umsystemen (u.a. Fahndungs- und Informationssysteme, SSO-Portal EJPD) umgehen können. Ein Ausfall oder Unterbruch einer Komponente oder eines Umsystems darf das Gesamtsystem nicht blockieren, sondern dieses muss mit reduzierter Funktionalität weiterarbeiten können.

Der Anbieter muss aufzeigen, wie das Fehlerhandling inklusive der Wiederaufnahme (erneute Verbindung oder Neustart der Systeme nach dem Kommunikationsunterbruch oder Ausfall) erfolgt.

3.5.1.9.2 Neustart Apps (TS 1.16)

Der Grenzkontrollverantwortliche muss die Apps (mobApp GKS und FP-Leser App) auf seinem Smartphone beenden und neu starten können, ohne hierfür das Smartphone neu starten zu müssen.

Die Maximalzeit für einen Neustart der Apps muss je App unter 20 Sekunden liegen.

3.5.1.9.3 Neustart Fingerabdruckleser (TS 1.17)

Wenn der Grenzkontrollverantwortliche den Fingerabdruckleser (siehe Ziffer 3.5.2.6) neu startet, muss die FP-Leser App sich mit diesem innerhalb von 10 Sekunden verbinden können, ohne die App neu starten zu müssen.

3.5.1.9.4 Bandbreite Kommunikation (TS 1.18)

Das mobile Grenzkontrollsystem muss möglichst unabhängig von einer Verfügbarkeit von breitbandigen Kommunikationskanälen funktionieren können. Der Grenzkontrollverantwortliche muss mit einer Anbindung an ein 3G Netz der Swisscom und höher in der ganzen Schweiz eine Kontrolle durchführen können.

Vorausgesetzt, dass die Verbindung performant genug ist, muss der Grenzkontrollverantwortliche eine Kontrolle auch mit einer Anbindung über Roaming im benachbarten Ausland durchführen können (z.B. für Grenzkontrollen im Zug in Deutschland, Frankreich, Italien und Österreich).

3.5.1.9.5 Performance (TS 1.19)

Für einen reibungslosen und effizienten Prozessablauf der Grenzkontrolle ist die technische Systemdurchlaufzeit der Dokumenten- und Personenkontrolle massgeblich, so dass diese Durchlaufzeit beim mobilen Grenzkontrollsystem < 6 Sekunden sein muss.

Definition der technischen Systemdurchlaufzeit: Dauer vom Einlesen der MRZ mittels Kamera in der mobApp GKS bis zur Anzeige sämtlicher relevanter Ergebnisse (inklusive Abfrage der Fahndungs- und Informationssysteme durch den Logik Layer, exklusive Antwortzeiten der externen Systeme) in der mobApp GKS.

Annahmen für die technische Systemdurchlaufzeit: Antwortzeit der Fahndungs- und Informationssysteme = 4 Sek., 4G Netzwerk und < 10 Resultate vorhanden.

Weiter soll die App folgende Leistungsmerkmale aufweisen:

- Maximal 4 Sekunden, um den Chip eines eMRTDs auszulesen (Zeit ohne Zertifikatsprüfung).
- Maximal 5 Sekunden, um ein Fahrzeug-Kontrollschild zu detektieren, einzulesen und darzustellen.

3.5.1.9.6 Last und Skalierbarkeit (TS 1.20)

Das mobile Grenzkontrollsystem muss mit mindestens 700 Smartphone-Anwendern gleichzeitig umgehen können ("concurrent users").

3.5.2 Technische Anforderungen

Dieses Kapitel enthält die technischen Anforderungen und Rahmenbedingungen für das System.

3.5.2.1 Systemarchitektur

Das mobile GK-System besteht aus zwei Mobilapplikationen die miteinander kommunizieren: die Mobile GKS App und die FP App. Diese Aufteilung in zwei unterschiedliche Apps hat aus Sicherheitsgründen zu erfolgen.

In der nachfolgenden Abbildung ist die Systemübersicht dargestellt:

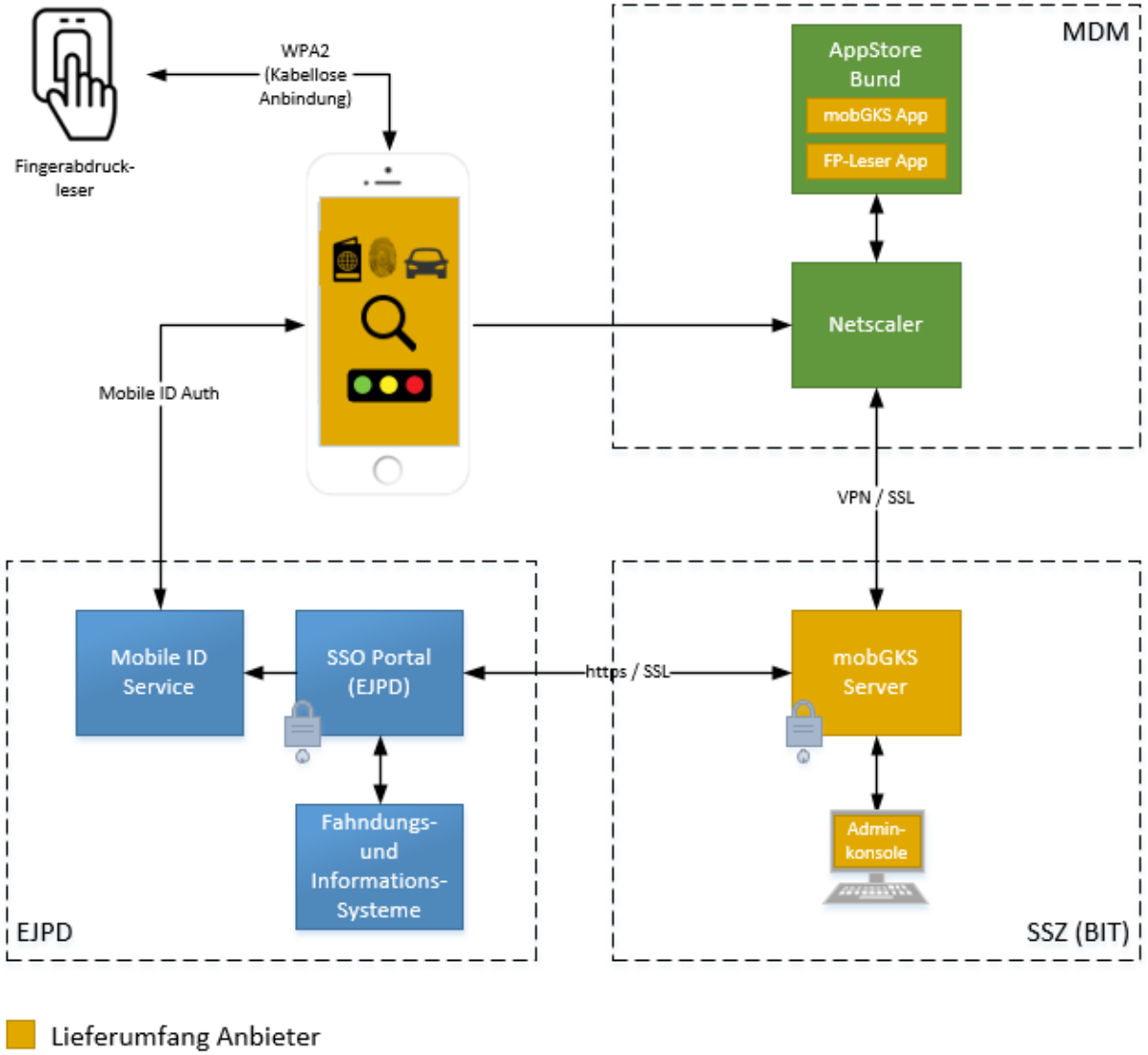

Abbildung 5: Systemübersicht mobGKS

Das mobile Grenzkontrollsystem besteht aus den folgenden Systemteilen:

Mobil GKS App: Das ist die Haupt Mobil-Applikation des mobilen GK-Systems. Sie enthält die gesamte Ablauflogik und das User Interface. Sie kommuniziert mit der zusätzlichen FP-Leser App.

FP-Leser-App: Diese Mobil-Applikation wird zur Anbindung des und zur Kommunikation mit dem FP-Lesegerät über WiFi benötigt.

FP-Leser: Fingerabdruck Lesegerät

MDM: Mobile Device Management Umgebung des Bundes. Die Apps müssen im Mobile Device-Management (MDM) des Bundes integriert werden sowie im privaten App-Store des Bundes bereitgestellt und verwaltet werden.

Alle iOS Smartphones des Bundes werden durch das MDM verwaltet und mit Updates versorgt. Über das MDM werden die Datensicherheit und der Virenschutz aller iOS Smartphones des Bundes sichergestellt.

Auf dem Smartphone ist die MDM App «Secure Hub» installiert. Diese bietet einen geschützten Bereich (Sandbox) in welchem die App läuft.

MDM-App Store: Application Store des Bundes (Bestandteil des MDM des Bundes).

MDM Netscaler: Application Delivery Controller arbeitet als Policy Enforcement Point. Der MDM Netscaler ist für das Routing des Traffics zuständig. Die App kommuniziert über den MDM Netscaler mit dem mobGKS Server. Die Apps sowie der mobGKS Server befinden sich im Bundesnetzwerk.

mobGKS Server: Backend Server des mobile GK-Systems mit zentralen Funktionen - beispielsweise um mit Fahndungs- und Informationssystemen zu kommunizieren (siehe Ziffer 3.5.2.7) sowie die Übertragung der Resultate zur App zu optimieren, usw.

SSO-Portal EJPD: Single-Sign-On Portal des EJPD. Für die Authentifizierung wird zusätzlich Mobil-ID verwendet.

Die Fahndungs- und Informationssysteme sind über das EJPD SSO Portal erreichbar. Der mobGKS Server macht die Abfragen via EJPD SSO Portal und stellt die Resultate der mobApp GKS zur Verfügung. Das EJPD SSO Portal befindet sich in einem separaten Netzwerk des EJPD.

Fahndungs- und Informationssysteme: Abfrage-Datenbanken hinter dem SSO-Portal

Admin Konsole: Client zum Administrieren des mobilen GK-Systems

3.5.2.2 Integration und Betrieb der Apps im MDM (TS 2.1)

Die Apps müssen ins aktuelle MDM des Bundes integriert werden. Dabei sind die aktuellen und zukünftigen technischen Rahmenbedingungen der MDM Plattform einzuhalten.

Aktuell wird die MDM Plattform von Citrix verwendet. In Zukunft könnte diese Plattform durch ein anderes Produkt abgelöst und ersetzt werden. Die Applikation muss in diesem Falle an die technischen Rahmenbedingungen des zukünftigen MDM angepasst werden. Dies würde jedoch im Rahmen des Change Managements bzw. optionaler Weiterentwicklungen erfolgen.

Für die Integration und den Betrieb der Apps in das aktuelle Citrix-MDM des Bundes sind folgende Vorgaben zu berücksichtigen:

- Für die Integration in das MDM ist es erforderlich das sogenannte MAM SDK von Citrix[1] in die App zu integrieren. Das MAM SDK ist für ObjectiveC / Swift verfügbar.
- Die App muss auf den jeweils zwei neusten iOS Versionen der Smartphones lauffähig sein (siehe Ziffer 3.5.2.5). Der Lieferant muss die Anpassungen vor dem Erscheinen einer neuen iOS Version bereitstellen. Nötige Patches müssen rechtzeitig für die Verteilung bereitgestellt werden. Dafür muss der Ablauf und Zeitplan mit dem MDM-Team des BITs koordiniert werden.
- Die GKS-Mobile-App wird als eine Verwaltungseinheit spezifische App (Schale 3) eingestuft. Die IKT-Vorgaben A735 für Apps im AppStore Bund sind einzuhalten (siehe Beilage O «A735_Apps_im_App_Store_Bund_v1-1.pdf»).

[1] MAM SDK von Citrix siehe: https://docs.citrix.com/en-us/mdx-toolkit/mam-sdk-overview.html

3.5.2.3 Vorgaben für die Apps (TS 2.2)

Die Apps müssen in das Mobile Device-Management des Bundes integriert werden (siehe Ziffer 3.5.2.2).

Des Weiteren sind folgende Vorgaben durch die Apps einzuhalten:

- Die Verwendung von öffentlichen Libraries muss deklariert werden;
- Die Verwendung von Opensource Lizenzen muss deklariert werden;
- Die Apps dürfen keine Telemetrie- oder andere Daten ungefragt an die Entwickler oder an Dritte senden. Sie müssen die Datenschutz- und Sicherheitsvorgaben einhalten (siehe Ziffer 3.5.2.15);
- Es werden ausschliesslich verschlüsselte Protokolle verwendet und angeboten (z.B. HTTPS)
- Die verwendeten Cypher-Suit, Kryptoalgorithmen und Hashfunktionen entsprechen dem heute verwendeten Standard (siehe Beilage N. «*Kryptographie Grundschutz*»)
- Caches müssen regelmässig geleert werden, sensitive Daten dürfen nicht in Cachefiles gespeichert werden;
- Sensitive Daten dürfen ausschliesslich im "internal storage" der APP gespeichert werden;
- Geheimnisse (Zugangscodes, API-Keys) dürfen nicht in der APP gespeichert werden. Für geschützte Zugänge muss ein Authentisierungsmechanismus auf dem Backend verwendet werden.

3.5.2.4 2 App Lösung: mobApp GKS und FP-Leser App (TS 2.3)

Aufgrund der Sicherheitsvorgaben darf das MDM des Bundes nur eine Netzwerkverbindung pro App zulassen. Das heisst, dass eine gleichzeitige Anbindung der App am mobGKS Server und am Fingerabdruckleser vorerst nicht möglich ist (Stichwort: Split tunneling). Weiter können die Fingerabdruckleser nicht über Bluetooth angebunden werden. Daher ist eine Lösung mit zwei Apps zu implementieren die miteinander kommunizieren.

Der Grenzkontrollverantwortliche führt die Grenzkontrolle mit der mobApp GKS durch. Die App muss die Grenzkontrolle bei Abfragen auf Fahndungen, Personendaten, Bewilligungen, Entscheide, Ausweise oder Visa unterstützen.

Die Erfassung der Fingerabrücke hat in der FP-Leser App zu erfolgen. Die Resultate der Abfragen sind in der mobApp GKS anzuzeigen. Für die Erfassung der Fingerabrücke muss ein Absprung oder Ähnliches von der mobApp GKS zur FP-Leser App möglich sein.

3.5.2.5 Smartphone (TS 2.4, ZK 2.1)

Das System muss mit den Smartphones des Auftraggebers funktionieren. Dies sind Apple iPhones ab Version 8 (und neuer). Die Mobile App des mobilen GKS muss auf den jeweils neusten zwei iOS Versionen der Smartphones lauffähig sein.

Für den Fall, dass der Auftraggeber in Zukunft andere Smartphones einsetzt, soll das System auch mit weiteren Smartphone-Typen (z.B. Android) funktionieren können.

3.5.2.6 Fingerabdruckleser (TS 2.5)

Das System muss mit den Fingerabdrucklesern des Auftraggebers funktionieren. Diese sind vom Typ S.I.C Biometrics IdentiFI45 und IdentiFI60/Kojak.

Der Grenzkontrollverantwortliche muss einen beliebigen Fingerabdruckleser dieses Typs mit der App auf seinem persönlichen Smartphone verwenden können. Der Fingerabdruckleser muss kabellos angebunden werden können. Um die Anbindung herzustellen muss das mobile Grenzkontrollsystem vorerst die Anbindungsdaten von einem QR-Code, welcher auf dem Fingerabdruckleser vorhanden ist, auslesen können.

Weiter muss das System in Bezug auf die Abnahme der Fingerabdrücke zukünftig neue Geräte und Lösungen integrieren können. Eine Integration neuer Geräte würde jedoch im Rahmen des Change Managements bzw. optionaler Weiterentwicklungen erfolgen.

3.5.2.7 Anbindung Umsysteme

3.5.2.7.1 Schnittstellen (TS 2.6)

Das mobile Grenzkontrollsystem muss sich an komplexen Webservices im Kontext von Fahndungs- und Informationssystemen anbinden können.

Für den Anschluss resp. die Nutzung der Webservices muss eine Nutzungsbewilligung des Bundes eingeholt werden. Das System muss den Bewilligungsprozess (WSBV) in einer Integrationsumgebung durchlaufen, um die Betriebsbewilligung für den Anschluss der produktiven Systeme zu erhalten. Für den Bewilligungsprozess sind ca. 12 Wochen einzuplanen.

Zum Zeitpunkt der Offertabgabe muss der Anbieter nachweisen können, dass die Anbindung des Systems an den Datenbanken der nachfolgend aufgeführten Fahndungs- und Informationssysteme umgesetzt ist:

- RIPOL;
- ISA;
- ISR;
- ASF-STD, ASF-SMV, ASF Nominals;
- C-SIS (Anschlusspunkt N-SIS);
- FABER;
- MOFIS;
- HOOGAN;
- C-VIS (Anschlusspunkt CVC);
- ORBIS (N-VIS);
- ZEMIS;
- AFIS (inklusive JMH).

Der Anbieter muss sicherstellen, dass weitere Anbindungen im Rahmen der Umsetzungsarbeiten zeitgerecht realisiert werden können, insbesondere:

- C-EES (Anschlusspunkt CEC);
- SIS-AFIS;
- SAVIDA (siehe Beilage L);
- ETIAS (Anschlusspunkt offen);
- RaFA (Neue Fachanwendung Rapportierung der EZV).

Das mobile Grenzkontrollsystem muss beliebige weitere Fahndungs- und Informationssysteme integrieren können. Eine Integration neuer Systeme würde jedoch im Rahmen des Change Managements bzw. optionaler Weiterentwicklungen erfolgen.

3.5.2.7.2 Chip Reisedokumente (eMRTD): Zertifikatshandling (ZK 1.3, ZK 1.5)

Die Zertifikate für die vertiefte Chipprüfung sind über folgende Schnittstellen zu beziehen:

- PKD-Webservice-Schnittstelle ZertServer (lesend: EZV)
  Schnittstelle des ZertServers, um folgende Zertifikate und Daten für die Echtheitsprüfung von Reisedokumenten herunterzuladen und zu verwalten: Country Signer Certificate Authority (CSCA), Document-Signer (DS), Certificate Revocation List (CRL);

- EAC IS-Service (lesend: SSO-Portal)
  Schnittstelle der eDoc PKI, für die Authentifizierung des GKV-Arbeitsplatzes bzw. des Inspection-System (Dokumentlesers). Diese wird nach einer "Chip-Authentifizierung" durchgeführt. Sie stellt damit die "Erweiterte Zugangskontrolle (EAC)" dar. Das EAC kontrolliert den Zugriff auf den geschützten Teil des Passes, welcher die Fingerabdrücke enthält.

Zertifikatserfassung und Einlieferung:

- CSCA-Data Collection (schreibend: SSO-Portal)
  Schnittstelle der eDoc N-PKD, um die Zertifikate der an der Grenze gelesenen elektronischen Reisedokumente der N-PKD-Applikation zu übertragen.

3.5.2.8 Rollen und Rechteverteilung (TS 2.7)

Das System muss eine Rollen- und Rechteverteilung beinhalten. Aus fachlicher Sicht sind folgende Rollen vorerst vorgesehen:

- **Systemadministrator**: Systemadministrator auf Seite Anbieter oder EZV (z.B. Applikationsverantwortlicher). Dieser kann das System fachlich konfigurieren (z.B. Abfragen, Aufbereitung der Abfrageresultate, Sortierung der Resultate in der Trefferliste, Stammdaten, Codewerte, usw.), User Berechtigungen verwalten und gegebenenfalls Abfragen zu Fahndungs- und Informationssystemen deaktivieren oder aktivieren.
- **Systemauditor**: Mitarbeiter der EZV, welcher das Logging (inklusive die fachlichen Logs – siehe Ziffern 3.5.1.8.6 und 3.5.1.8.7) lesen und auswerten kann.
- **Grenzkontrollverantwortlicher**: Mitarbeiter der EZV, welcher die Grenzkontrolltätigkeiten mit der mobilen App ausführt und dafür verantwortlich ist.

Bei Bedarf müssen weitere Rollen definiert werden können.

3.5.2.9 Authentifizierung und Autorisierung (TS 2.8)

Aufgrund der Sicherheitsvorgaben müssen sich die Benutzer stark authentisieren (siehe Ziffer 3.5.2.15.2).

Daraus ergeben sich folgende technische Anforderungen:

- **Administrationskonsole:** Für das Identity- und Access-Management sind die IKT-Standard-Dienste der Bundesverwaltung zu integrieren Die Benutzer authentisieren sich dazu mit der persönlichen Smartcard (Swiss Government PKI Klasse B Zertifikat vom BIT).

  Je nachdem ob ein Web-Client oder ein Windows-Client angeboten wird bedeutet dies eine Integration ins eIAM oder ins IAM / ADB des Bundes (siehe IT-Leitfaden für Lieferanten).

  In beiden Fällen hat die feingranulare Rechteverwaltung durch die Fachapplikation zu erfolgen**.**
- **Mobile GKS-App:** Bei jedem Starten der mobile GKS App in der MDM Sandbox muss der Benutzer sich mit seinem PIN authentifizieren.

  Für die Abfrage der Informations- und Fahndungsdatenbanken des EJPD muss sich der Benutzer zusätzlich am SSO-Portal authentifizieren. Es wird der Identitätsprovider des SSO-Portal versendet. Die 2FA Authentifizierung der Benutzer im EJPD SSO Portal muss über die mobApp GKS mittels Mobile ID von Swisscom erfolgen. Nach erfolgreichem Login am EJPD SSO Portal wird von diesem ein SAML Token für den Benutzer erstellt. Mit dem Token kann der Benutzer 10 Stunden lang Abfragen am EJPD SSO Portal durchführen, ohne erneute Anmeldung.

3.5.2.10 Systemkonfiguration

3.5.2.10.1 Systemkonfigurierbarkeit (ZK 2.2)

Ein Systemadministrator soll die Konfigurationen des Systems einfach verwalten können, zum Beispiel:

- Timeoutparameter des Systems;

- Timeoutparameter und Abfragewiederholungen (Schnittstellen Umsysteme, Fingerabdruckleser);
- Konfiguration Logik Layer mobGKS (siehe Ziffer 3.5.1.6);
- Templates für die Erkennung von Kontrollschildern und Reisedokumenten;
- Referenzdaten (z.B. Codewerte, PLZ).

Änderungen dieser Konfigurationen dürfen keine neuen Software-Releases notwendig machen. Die Konfigurationen müssen jederzeit und unabhängig von den Releases eingespielt werden können.

Der Anbieter soll aufzeigen, welche Parameter durch einen Systemadministrator angepasst und verwaltet werden können.

3.5.2.10.2 Aktualität der Konfigurationen (ZK 2.3)

In Bezug auf die Erkennung von Kontrollschildern und Reisedokumenten soll das System mindestens alle 3 Monate durch den Anbieter auf den aktuellsten Stand gebracht werden, um allfällige Anpassungen oder Neuigkeiten zu berücksichtigen. Falls dies aus betrieblichen Gründen notwendig ist, sollen einzelne Templates ad-hoc angepasst oder angelegt werden können.

Der Anbieter hat in seinem Angebot einen Vorschlag zu unterbreiten, wie die Aktualität sichergestellt wird. Falls die Aktualisierungen nicht konfigurativ erfolgen können, sind diese mit der Bereitstellung der Patches und Updates zu synchronisieren.

3.5.2.11 Administrationskonsole (ZK 2.4, TS 2.13)

Das System soll eine Administrationskonsole zur Verfügung stellen, damit:

- die Systemadministratoren die Konfigurationen des Systems verwalten können (siehe Ziffer 3.5.2.10);
- die Systemauditoren die geloggten Daten lesen und exportieren können (siehe Ziffer 3.5.1.8.6 und 3.5.1.8.7).

Es wird eine Implementierung der Administrationskonsole als Webanwendung bevorzugt. Falls die Administrationskonsole lediglich als Windows-Client vorhanden ist, muss diese (TS 2.13):

- auf einem Arbeitsplatz des Bundes (BAB-Arbeitsplatz) mit Betriebssystem Microsoft Windows 10 (oder höher) funktionieren (technische Spezifikationen: siehe Beilage M *«APS_Geräte_2020»*);
- entsprechend vom Anbieter hinsichtlich der Installation «paketiert» und Updates/Patches mit dem Release Zyklus des Service Operators abgestimmt werden.

3.5.2.12 Strategische Produktvorgaben (TS 2.9)

Das BIT, als Betreiber des Auftraggebers, stellt für Fachanwendungen seiner Kunden strategische Produktkombinationen bereit. Es handelt sich hierbei um Technologien und Herstellerprodukte, welche konform zu den Vorgaben bzw. Standards der Bundesverwaltung und abgeleitet davon den Vorgaben des Betreibers sind. Überdies stellen diese Produktkombinationen den wirtschaftlichen Betrieb sicher.

Diese Produktkombinationen sind in der Beilage C *«Kombinationsmatrix»* ersichtlich und gelten ebenfalls als Vorgabe.

3.5.2.13 Vorgaben Systemarchitektur (TS 2.10)

Der Anbieter muss die Vorgaben des BIT bzw. des Bundes in Bezug auf die Systemarchitektur einhalten. Diese Vorgaben sind der Beilage F «IT-Leitfaden für Lieferanten» Kapitel 3.1 zu entnehmen. Die Architekturhinweise des Kapitels 3.7 sind, soweit zutreffend, ebenfalls zu berücksichtigen.

3.5.2.14 Server / Plattform

Der mobGKS Server (siehe Ziffer 3.5.2.1) wird beim BIT (Bundesamt für Informatik und Telekommunikation) im Modell «Full Service» gehostet (siehe Beilage P *«Infosheet Betrieb Fachanwendung BIT»*).

Folgende Umgebungen (inklusive Peripheriegeräte) sind vorgesehen:

- Entwicklungsumgebung (Zuständigkeit: Anbieter / beim Anbieter);
- Integrationsumgebung (Zuständigkeit: BIT): Die Integrationsumgebung (vom BIT auch Referenzumgebung genannt) wird an der Integrationsinstanzen des EJPD SSO Portals und der Abfragesysteme angebunden. Sie wird von berechtigten Entwicklern, Technikern und Fachpersonen des Auftraggebers genutzt.
- Abnahmeumgebung (Zuständigkeit: BIT: Die Abnahmeumgebung wird an das produktive EJPD SSO Portal und an die produktiven Abfragesysteme angebunden. Diese wird von berechtigen Technikern und Fachpersonen des Auftraggebers für die Abnahmetests genutzt. Die Apps stehen für Endanwender nicht zur Verfügung.
- Produktionsumgebung (Zuständigkeit: BIT): Die Produktionsumgebung wird an das produktive EJPD SSO Portal und an die produktiven Abfragesysteme angebunden. Die Apps stehen für Endanwender zur Verfügung.

In den Lizenzkosten ist die Anwendung von Referenz-, Abnahme- und Produktionsumgebungen seitens Auftraggeber zu berücksichtigen (siehe Preisblatt A-A und A-C).

3.5.2.14.1 Wiederherstellung der Lauffähigkeit (TS 2.11)

Ein Totalausfall allfälliger zentraler Komponenten (mobGKS Server, siehe Ziffer 3.5.2.1) hat als Folge, dass mobile Grenzkontrollen landesweit nicht mehr möglich sind. Deshalb sind Mechanismen vorzusehen, um die Lauffähigkeit der zentralen Komponenten nach einem Ausfall einfach wiederherstellen zu können.

Der mobGKS Server muss redundant ausgelegt werden können.

Der Anbieter muss diesbezüglich die Möglichkeiten seiner Lösung aufzeigen.

3.5.2.14.2 Systemmonitoring / technisches Logging (TS 2.12)

Die Daten des technischen Loggings werden für das Operation Control Center (OCC) des Betreibers (BIT), sowie für das Applikations-Dashboard der EZV verwendet. Zudem soll damit eine schnelle Fehlerdetektion und Diagnose ermöglicht werden.

Für den Betrieb muss das System ein Monitoring der zentralen Systemkomponenten (z.B. mobGKS Server) in Echtzeit ermöglichen. Dazu muss dieses in das zentrale Enterprise Monitoring System (Dynatrace, Splunk) des Betreibers eingebunden werden.

Das Grenzkontrollsystem muss ein technisches Logging für eine mögliche Überwachung des Systems aufweisen. Dazu soll dieses die Logdaten in einem gängigen Standard Format dem zentralen Enterprise Monitoring System des Betreibers zur Verfügung stellen.

Das Logging muss verschiedene Dringlichkeitsstufen aufweisen und bei Bedarf ein- und ausgeschaltet werden können. Die folgenden gängigen Log-Levels sollten unterstützt werden:

- **Fatal:** Fehler, welcher zur Terminierung der Anwendung führt.
- **Error:** Laufzeitfehler, welcher die Funktion der Anwendung behindert oder unerwartete Programmfehler.
- **Warning:** Aufruf einer veralteten Schnittstelle, fehlerhafter Aufruf einer Schnittstelle, Benutzerfehler oder ungünstiger Programmzustand.
- **Info:** Laufzeitinformationen wie der Start und Stopp der Anwendung, Benutzeranmeldungen und -abmeldungen, sowie durchgeführte Geschäftstransaktionen, Anbindung Scanner.
- **Debug:** Informationen zum Programmablauf. Wird im Normalfall nur in der Entwicklung oder zur Nachvollziehung eines Fehlers verwendet.
- **Trace:** Detaillierte Verfolgung des Programmablaufs, insbesondere zur Nachvollziehung eines Programmierfehlers.

Wichtig ist hierbei, dass in den Logdateien nur Informationen zum Programmablauf und -zustand erhoben werden sollen, jedoch keine Informationen zu den Benutzern des Programms.

Der Anbieter muss aufzeigen, welche Daten auf welcher Stufe (z.B. App, Server) jeweils geloggt werden können.

3.5.2.15 Datenschutz- und Sicherheitsvorgaben

Dieses Kapitel enthält die wichtigsten technischen und organisatorischen Vorgaben an den Anbieter in Bezug auf Datenschutz und Sicherheit.

3.5.2.15.1 Grundschutz (EK 11)

Die Vorgaben des BIT bzw. des Bundes in Bezug auf die Sicherheit und den Datenschutz (Grundschutz) sind einzuhalten. Diese Vorgaben sind der Beilage F «*IT-Leitfaden für Lieferanten*» Kapitel 3.1 zu entnehmen.

3.5.2.15.2 Erhöhter Schutzbedarf (EK 11)

Das mobile Grenzkontrollsystem behandelt Informationen die nach der Informationsschutzverordnung (ISchV) INTERN klassifiziert sind und gemäss dem Datenschutzgesetz als besonders schützenwerte Personendaten eingestuft sind. Dadurch besteht, zusätzlich zum Grundschutzbedarf, ein erhöhter Schutzbedarf. Grundsätzlich muss die Vertraulichkeit jederzeit gewährleistet werden sowie jede Behandlung nachvollziehbar erfolgen.

Die wichtigsten Massnahmen für den erhöhten Schutzbedarf sind nachfolgend aufgelistet. Während der Realisierung wird ein ISDS-Konzept, welches alle nötigen Massnahmen präzisiert, erstellt.

- **Datenschutz:** Im Normalbetrieb des Systems GKS Mobile dürfen keine datenschutzrelevanten Daten mehr auf sämtlichen Komponenten (Datenbank, sämtlichen Logdateien, usw.), nach Abschluss des Grenzkontrollprozesses, vorhanden sein. Nach einer konfigurierbaren Zeit oder gem. anderer Trigger, müssen alle abgelegten oder zwischengespeicherten Daten gelöscht werden.

  Der Schutz sensibler personenbezogener Daten (z.B. biometrische Daten) muss bei jeder Verarbeitung gewährleistet sein.

- **eIAM / Starke Authentisierung:** Für das Identity- und Access-Management sind die IKT-Standard-Dienste der Bundesverwaltung zu integrieren (siehe Beilage F *«IT-Leitfaden für Lieferanten»*). Sämtliche Zugriffe auf Systeme sind stark (Multi-Faktor) zu authentisieren.

  Die Grob-Autorisierung erfolgt dabei durch eIAM / IAM und die feingranulare Rechteverwaltung durch die Fachapplikation.

- **Zugriff SSO Portal:** Für den Zugriff auf Informations- und Fahndungsdatenbanken muss sich der Benutzer am SSO-Portal authentifizieren. Bei der Mobil GKS App wird für die Identifikation als zweiter Faktor die Mobile-ID verwendet.

- **Verschlüsselung der Datenkommunikation:** Sämtliche Kommunikation zwischen Smartphone und Server sowie Server zu Server (auch innerhalb der Rechenzentren) hat verschlüsselt zu erfolgen. Es dürfen nur sichere Cipher und gültige Zertifikate verwendet werden (siehe Beilage N. «Kryptographie Grundschutz»).

  Bemerkung: Auf der Strecke des mobilen GKS-Servers zu den Informations- und Abfragesystemen (SSO-Portal EJPD), ist die Kommunikation lediglich mit einer Transportlayer-Verschlüsselung versehen

- **Schwachstelle Analyse:** Das System wird vor der Inbetriebnahme auf Schwachstellen durch den Auftraggeber geprüft. Die Ergebnisse werden dokumentiert sein. Entdeckte Schwachstellen müssen analysiert und entsprechend vom Anbieter behoben werden.

- **Sicherheitsvorfall:** Der Anbieter muss bei Sicherheitsvorfällen oder Sicherheitslücken, die ihn selber betreffen, die EZV umgehend darüber informieren.

- **Server Zertifikate:** Auf den Servern werden Zertifikate der Swiss Government PKI verwendet (https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki.html). Diese werden durch den Auftraggeber (EZV in Zusammenarbeit mit dem BIT) beschafft und auf

den entsprechenden Servern eingespielt. Falls weitere Zertifikate innerhalb vom System zum Einsatz kommen, müssen diese durch den Anbieter begründet und bereitgestellt werden.

- **Security-Patch:** Der Anbieter muss Security-Patches für das System möglichst zeitnah liefern.

3.5.3 Projekt und Weiterentwicklung

Dieses Kapitel enthält die Anforderungen an den Anbieter bez. der Realisierung und Einführung des Systems.

3.5.3.1 Vorgehen (TS 3.1, ZK 3.1)

Der Anbieter soll ein Konzept zum Vorgehen beilegen (ZK 3.1), welches die Umsetzung und Einführung des mobilen Grenzkontrollsystems bis Q2-2022 umfasst, insbesondere:

- Projektorganisation (inkl. Ansprechpartner);
- Konzeptarbeiten / Realisierung / Konfiguration (inkl. Integration Umsysteme);
- Reporting der Fortschritte und Qualitätssicherung;
- Abnahme;
- Inbetriebsetzung / Einführung in der Organisation / Schulungen;
- Mitwirkungspflichten des Auftraggebers.

Das **Testing** erfolgt gemäss dem Testkonzept (siehe Ziffer 3.5.4.6).

Für die **Abnahme** sind Vorgaben gemäss Rahmenvertragsentwurf, Ziff. 4.4 (siehe Anhang 4) zu berücksichtigen.

Im Vorgehenskonzept sollen folgende **Meilensteine** ersichtlich sein:

- Genehmigung Lösungskonzept (Architektur, Umsetzung, Einführung) durch den Auftraggeber;
- Durchstich des Systems auf Integrationsumgebung umgesetzt (Integration SSO Portal, Authentifizierung Benutzer, Integration mobApp GKS und FP-Leser App in MDM, Zusammenspiel beider Apps, Anbindung Fingerabdruckleser, Installation mobGKS Server);
- System bereit für Abnahme auf Abnahmeumgebung;
- System abgenommen und eingeführt.

Die nachfolgende Abbildung zeigt die Meilensteine im Gesamtkontext des Vorhabens, inklusive einer groben Zeitplanung als Richtwerte.

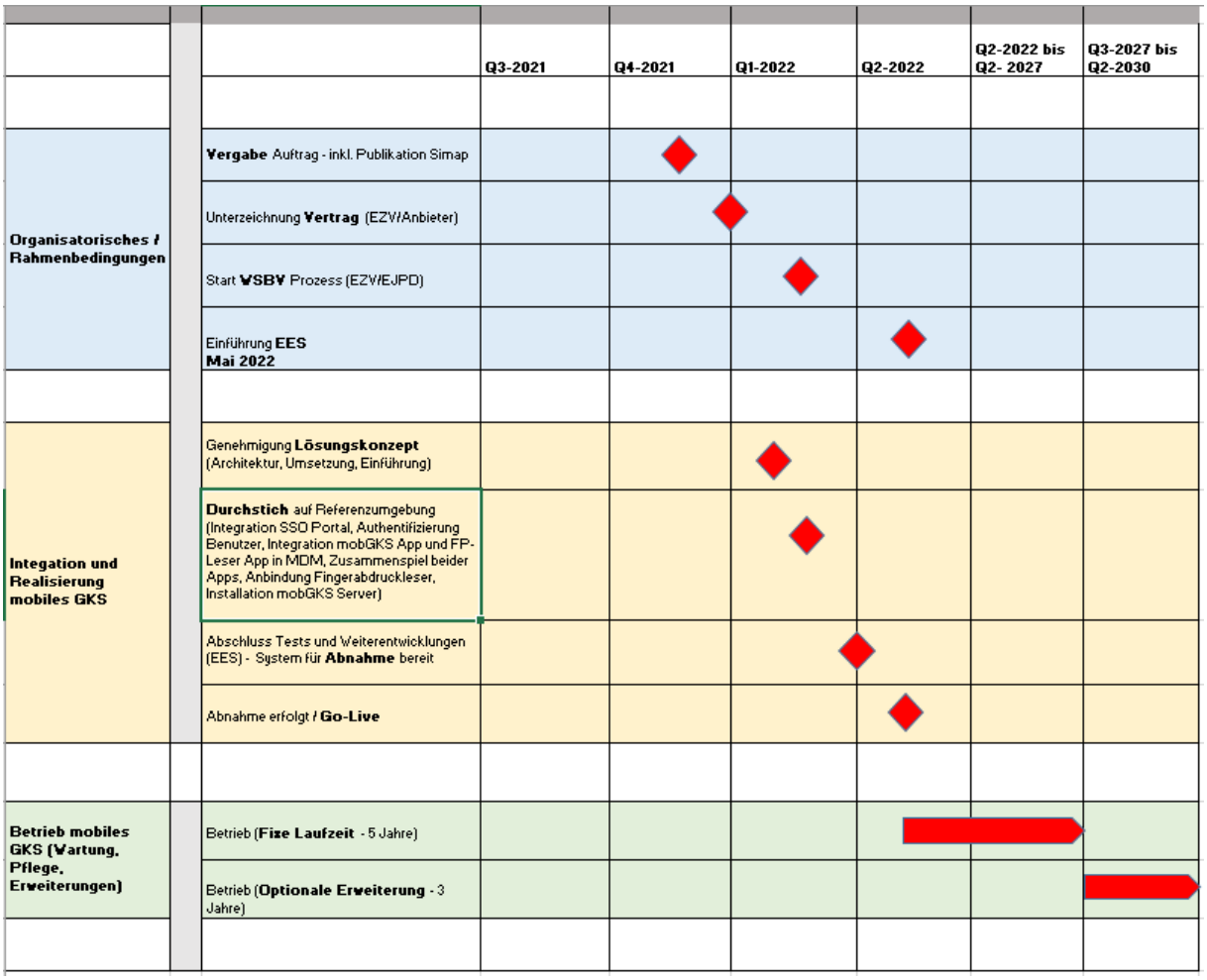

Abbildung 6: Meilensteine

Die Projektkosten für die Konzeption, Umsetzung, Inbetriebsetzung und Einführung sind im Preisblatt, Position C-A einzugeben.

3.5.3.2 Pooltage

3.5.3.2.1 Einleitung / Bedarf an Pooltage (TS 3.3)

Im Rahmen der Realisierung des neuen mobilen Grenzkontrollsystems der EZV und dessen Wartung und Pflege werden folgende Pooltage angefragt:

- **Weiterentwicklungen**, 1000 Tage
  In den nächsten Jahren wird es im Kontext der europäischen Grenzsicherheit diverse Weiterentwicklungen geben, welche die Schweiz als Schengenstaat ebenfalls umzusetzen hat. Grundsätzlich werden diese Weiterentwicklungen als Projekte umgesetzt. Die Anforderungen und die Termine werden von der EU vorgegeben.
  Nebst diesen europäischen Themen, wird es in den kommenden Jahren auch EZV-Vorhaben geben, welche im Zusammenhang mit dem Programm DaziT entstehen (z.B. Anfragen an neues Rapportierungssystem).
  Bei dieser Kalkulation wird davon ausgegangen, dass es jährlich Weiterentwicklungen im Umfang von 100-120 Tagen geben wird.
- **Minor Release**, 150 Tage
  Bei dieser Kalkulation wird davon ausgegangen, dass es jährlich einen Minor Release im Umfang von 10-20 Tagen geben wird.
- **Major Release**, 350 Tage
  Bei dieser Kalkulation wird davon ausgegangen, dass es jährlich einen Major Release im Umfang von 20-40 Tagen geben wird.
- **Phase out**, 150 Tage
  Dieser Punkt beinhalten den Parallelbetrieb und Migration, welche im Zusammenhang mit der Einführung eines neuen mobilen GKS entsteht. Aufgrund einer Schätzung wird davon ausgegangen, dass einmalig 150 Tage für diese Aufgaben ausreichend sind.

Die Pooltage liegen einer Schätzung zu Grunde, von der Realisierung des Projekts über die Lebenszeit des GKS-Systems (bis 8 Betriebsjahre). Es besteht keine Abnahmeverpflichtung. Die Pooltage können innerhalb der Jahre und Kategorien verschoben werden. Die Anzahl der Pooltage ist mit einem maximalen Pooltagedach von 1'650 Tage begrenzt.

Die Preise der Pooltage sind im Preisblatt unter Lasche B einzugeben.

3.5.3.2.2 Definition Pooltage (TS 3.3)

Der Tagessatz für Pooltage beinhaltet den Ansatz für den Einsatz von Mitarbeitenden des Anbieters oder von allfälligen Unterlieferanten für die in diesem Kapitel beschriebenen Tätigkeiten. Je nach Bedarf der EZV können unterschiedliche Rollen/Profile für die Pooltage angefordert werden. Dies sind die Rollen welche benötigt werden, um das mobile GKS weiter zu entwickeln. Konkret werden mindestens die Rollen Projektleiter, Architekt, Entwickler und Testmanager inkl. Qualitätssicherung benötigt.

Alle Spesen und Abgaben (exkl. MwSt.) sind im Tagessatz zu inkludieren.

3.5.3.2.3 Prozess Abruf der Pooltage (TS 3.2)

Leistungen, welche über Pooltage bezogen werden, werden mit dem im Rahmenvertragsentwurf beschriebenen Prozess abgerufen (siehe Anhang 04, Rahmenvertrag, Ziff. 3.6.4).

3.5.4 Wartung und Pflege

Dieses Kapitel enthält die Anforderungen an den Anbieter für den Betrieb des Systems.

3.5.4.1 Betriebsdauer (TS 4.1)

Das mobile Grenzkontrollsystem muss 8 Jahre ab Inbetriebsetzung betrieben werden können. Mit der Vergabe wird eine Mindestbetriebsdauer von 5 Jahre vereinbart. Weitere 3 Betriebsjahre sind optional ausgeschrieben und können vom Auftraggeber zu einem späteren Zeitpunkt zu den offerierten Konditionen bezogen werden. Als Annahme gilt die Inbetriebsetzung des mobilen Grenzkontrollsystems bis Q2-2022.

3.5.4.2 Verantwortung für Wartung und Support

Die Verantwortungen für den technischen Betrieb des mobilen Systems und die Dienstleistungen des Anbieters nach der Inbetriebsetzung des Systems sind nachfolgend dargestellt.

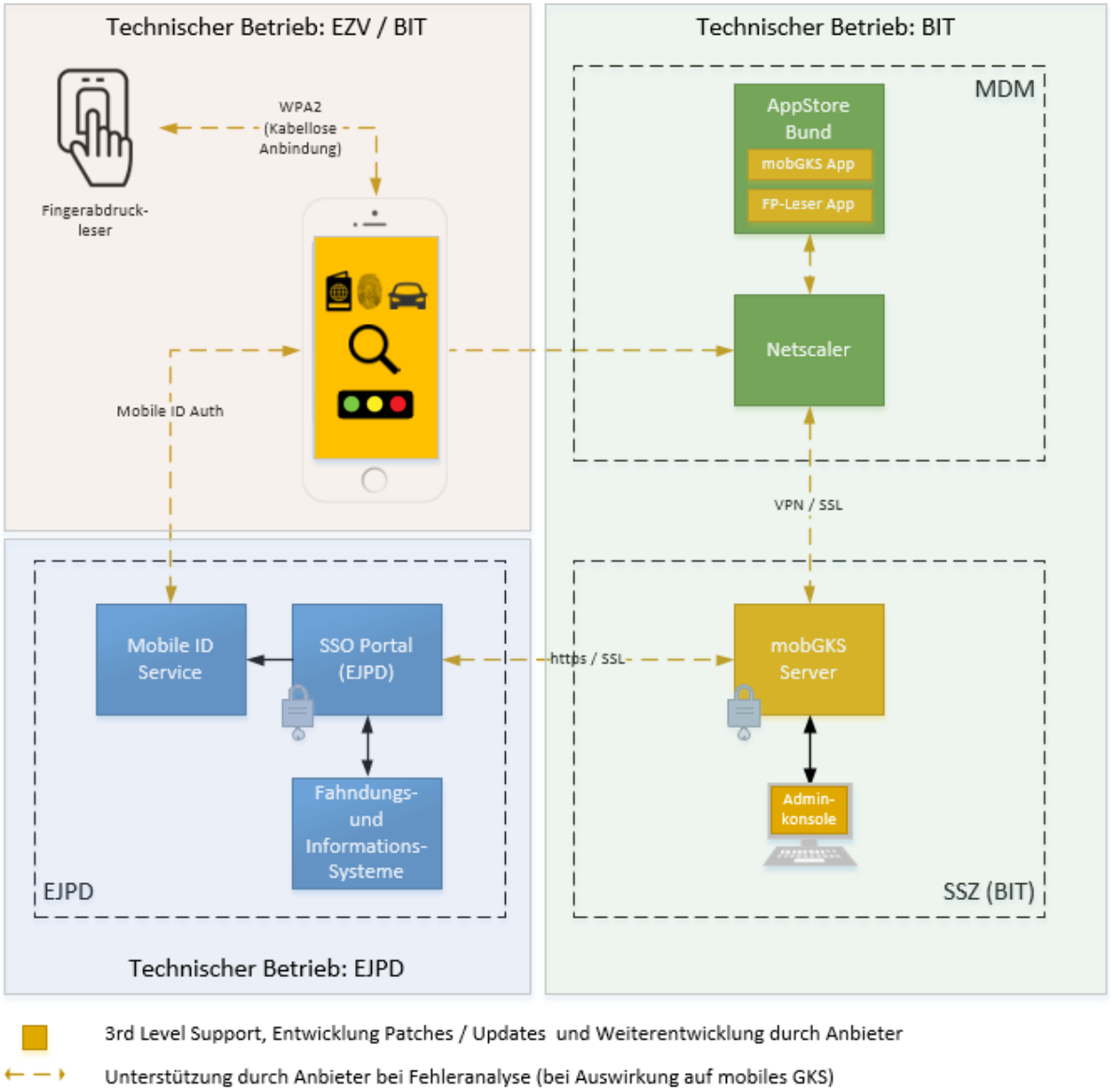

Abbildung 7: Systemübersicht – Verantwortungen Wartung und Support

In der folgenden Tabelle sind die Teilsysteme sowie die Verantwortungen und Aufgaben für Wartung und Betrieb detailliert dargestellt.

Teilsysteme	mobApp GKS FP-Leser App	mobGKS Server (inkl. Adminkonsole)	Smart-phone Fingerab-druckleser	Netzwerke MDM-SSZ SSZ-EJPD	MDM Ser-ver	EJPD SSO Portal	MobileID MobileID Service
Verantwor-tung	Auftragge-ber/BIT	Auftragge-ber/BIT	Auftragge-ber/BIT	BIT	BIT	EJPD	EJPD
Lieferant od. Hersteller	Anbieter	Anbieter	Apple / S.I.C Biometrics	Swisscom	Citrix	Diverse	Swisscom
Techn. Be-trieb	BIT	BIT	EZV / BIT	BIT	BIT	EJPD	Swisscom
Supportzeit*	11/5	11/5	11/5	24/7	24/7	24/7	24/7 (online)
Servicezeit**	24/7	24/7	-	24/7	24/7	24/7	24/7
Mitwirkung Auftragge-ber	1st Level Support	1st Level Support	1st Level Support inkl. Austausch	-	-	Zugriffe be-antragen, WSBV an-stossen	-
Mitwirkung techn. Be-trieb	2nd Level Support, Wartung, Monitoring	2nd Level Support, Wartung, Monitoring	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)
Leistungen Anbieter	3rd Level Support, Entwicklung Patches/Up-dates, Wei-terentwick-lung	3rd Level Support, Entwicklung Patches/Up-dates, Wei-terentwick-lung	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)	Fehlerana-lyse (bei Auswirkung auf mobGKS)

Tabelle 4: Verantwortungen und Aufgaben für Wartung und Betrieb

* **Supportzeit**: Zeitraum, in welchem der technische Betrieb gegenüber seinen Kunden für Anliegen zur spezifischen Marktleistung die Unterstützungsleistungen bzw. Hilfestellungen erbringt und bei Bedarf den Stand kommuniziert. Die Bearbeitung der Anliegen erfolgt auf unterschiedlichen Kanälen wie E-Mail, Ticketing-System, Telefon, remote oder vor Ort beim Kunden.

** **Servicezeit**: Zeitraum, in welchem der technische Betrieb die Einhaltung der Service-Level-Elemente Wartung, Verfügbarkeit und Sicherheit gewährleistet.

Die jährlichen wiederkehrenden Kosten für die Lieferung der Patches/Updates des mobGKS Servers (inkl. Administrationskonsole) und der Apps sind im Preisblatt unter Position A-C bzw. B-C (jährliche Lizenzkosten) / Optionen D-C bis E-C, G-C bis K-C einzuberechnen.

Die jährlichen wiederkehrenden Kosten für den 3rd Level Support (inkl. Fehleranalyse) sind im Preisblatt unter C-C einzugeben / Option F-C.

3.5.4.3 Technischer Support (TS 4.2)

Störungsmeldungen werden normalerweise in der Supportorganisation der EZV triagiert und im Bedarfsfall an das BIT weitergeleitet. Falls der Anbieter für die Behebung des Fehlers benötigt wird, wird dieser durch das BIT kontaktiert.

Im Rahmen des Projektes ist ein gemeinsam abgestimmter Supportprozess zwischen dem Anbieter und den Supportorganisationen des Auftraggebers (i.e. EZV und BIT) zu definieren.

Im Rahmen des technischen Supports hat die Kommunikation zwischen dem Auftraggeber und dem Anbieter in deutscher Sprache (mindestens Stufe C1) zu erfolgen.

Supportzeit

Für die Unterstützung des BIT muss der Anbieter folgende Supportzeiten abdecken:

- 11/5: Werktags von 07:00 Uhr bis 18:00 Uhr, ausgenommen sind Samstag und Sonntag sowie allgemeine Feiertage am Standort Bern.

Der Anbieter garantiert, einen Bereitschaftsdienst für die Behebung von Fehlern zu verfügen und anzubieten, welcher während der oben genannten Supportzeiten erreichbar und einsatzbereit ist.

Reaktionszeit: Die maximale Reaktionszeit während der Supportzeiten beträgt 1 Stunde. Die Reaktionszeit ist die Zeit zwischen dem Eingang des Tickets und der ersten Rückmeldung durch einen Mitarbeitenden des Anbieters.

Mitwirkung Fehleranalyse: Der Anbieter muss eine Mitwirkung bei der Analyse von Fehlern in einem der angeschlossenen Systeme sicherstellen, sofern der Fehler im Drittsystem einen Einfluss auf das vom Anbieter gelieferte System hat.

Fehlerbehebungszeiten: Die Fehlerbehebungszeiten hängen von der Fehlerklasse ab. Diese sind unten definiert (ansonsten gilt "Best Effort"). Die Fehlerbehebungszeiten verstehen sich innerhalb der Supportzeiten und gelten für Fehler, welche dem Anbieter geschuldet sind.

- Fehlerklasse 1: Fehler der Fehlerklasse 1 muss der Anbieter innerhalb von 11 Arbeitsstunden (Supportzeit) beheben. Die Zeit läuft ab Erhalt des Tickets innerhalb der Supportzeiten. Falls der Fehler innerhalb dieser Zeit nicht behoben ist, muss der Anbieter den Auftraggeber über den Fortschritt der Fehlerbehebung innerhalb der Supportzeiten stündlich informieren.

Es werden im Störungsfall die folgenden Fehlerklassen unterschieden:

Fehlerklasse 1 (kritische Störung / fatale, betriebsverhindernde Mängel)

Beschreibung	Die Hauptaufgaben können von mehr als 100 Anwendern nicht mehr erfüllt werden. Keine Workarounds sind möglich.
Konsequenz	Die Nutzung des Systems wird dadurch entweder unmöglich oder nur mit wirtschaftlich nicht vertretbarem Aufwand möglich.
Beispiel	▪ Freeze der gesamten Applikation durch Fehleingabe; ▪ SW Update schlägt fehl und ist nicht rückwärts kompatibel; ▪ SW und Hardware interoperieren nicht durch Mismatch Firmware; ▪ Schnittstelle zu wichtigem Umsystem wurde beschädigt (z.B. eIAM, SIS). Die Beispiele verstehen sich nicht abschliessend.

Tabelle 5: Fehlerklasse 1

Fehlerklasse 2 (erhebliche Störung / wesentliche, betriebsbehindernde Mängel)

Beschreibung	Der Betrieb ist gewährleistet. Die Hauptaufgabe kann nur noch eingeschränkt erfüllt werden, beispielsweise, wenn geschäftskritische Funktionen nicht mehr funktionieren.
Konsequenz	Der Betrieb wird (potentiell) beeinträchtigt.
Beispiel	▪ Geschäftskritische Funktionen sind nicht mehr vorhanden; ▪ Performance sinkt signifikant; ▪ App geht regelmässig in einen Freeze und lässt sich nur sporadisch bedienen; ▪ Benutzereingaben führen gehäuft zu Abbruch der Erfassung. Die Beispiele verstehen sich nicht abschliessend.

Tabelle 6: Fehlerklasse 2

Fehlerklasse 3 (mittlere Mängel)

Beschreibung	Beeinträchtigung mittlerer oder niederwertiger Funktionen des Systems. Das System bleibt aber operationell bzw. kann operationell verwendet werden.
Konsequenz	Die Nutzung von einzelnen Funktionen des Systems ist leicht eingeschränkt.
Beispiel	▪ Einschränkung einer Komponente; ▪ Ausfall z.B. eines einzelnen Moduls, dessen Funktion kurzfristig durch ein anderes Modul (Redundanz) oder Ersatzgerät (z.B. Fingerabdruckleser) sichergestellt werden kann; ▪ Nutzer kann nur unter erschwerten Bedienungen Eingaben tätigen; ▪ Fehlerhafte Warnmeldungen welche keinen Fehler als Hintergrund haben. Die Beispiele verstehen sich nicht abschliessend.

Tabelle 7: Fehlerklasse 3

Fehlerklasse 4 (unwesentliche Mängel)

Beschreibung	Fehler ohne Auswirkungen auf die Funktionalität, den Betrieb, die Wartbarkeit und/oder die Weiterentwicklung des Systems.
Konsequenz	Die Nutzung der Systems ist nicht eingeschränkt.
Beispiel	▪ Typo, Farbe, Darstellungsfehler; ▪ Ein Label in der Eingabemaske ist nicht vollständig angezeigt; ▪ Das Ausgabeformat für eine Datumsangabe ist nicht korrekt. Die Beispiele verstehen sich nicht abschliessend.

Tabelle 8: Fehlerklasse 4

Der Auftraggeber entscheidet über die Zuordnung der einzelnen Störungen/Fehler zu einer Fehlerklasse. Ist der Anbieter mit einer Zuordnung nicht einverstanden, so muss er dies dem Auftraggeber umgehend mitteilen.

3.5.4.4 Wartung (TS 4.3)

In Bezug auf die Wartung muss der Anbieter während des Betriebs des Systems, regelmässig Software-Updates und Patches bereitstellen. Insbesondere muss der Anbieter die Software regelmässig auf Schwachstellen und Sicherheitslücken überprüfen und Sicherheitspatches zeitnah bereitstellen.

3.5.4.5 Change- und Release-Management (TS 4.4)

Der Anbieter muss Change- und Release-Management Prozesse implementiert haben. Siehe in Bezug auf das Change Management Verfahren auch Ziffer 3.5 des Rahmenvertragsentwurfs (Anhang 04).

Der Auftraggeber muss Einsicht in den Stand der Changes sowie in die Release-Planung des Produktes erhalten, sowie Change Requests einreichen können.

Notwendige Anpassungen des mobilen Grenzkontrollsystems, bedingt durch Anpassungen und wesentliche Veränderungen von Schnittstellen, Umsystemen oder Hardware- und Software-Infrastruktur (z.B. Server, Smartphones, Fingerabdruckleser) sind ebenfalls im Umfang des Change-Managements enthalten.

Das Deployment von Releases und Updates der mobilen Apps («Schale 3 Applikation») hat über den AppStore des Bundes (siehe Ziffer 3.5.2.1) zu erfolgen. Das Deployment wird vom Auftraggeber beim BIT in Auftrag gegeben. Das BIT prüft den Code der gelieferten App und publiziert sie auf dem Bundes App-Store. Die Vorgaben des Kap. 3.5.2.2 müssen eingehalten werden.

3.5.4.6 Testing (ZK 4.1)

Bevor Releases, Updates und Patches auf der produktiven Umgebung eingespielt werden, müssen diese einen Test- und Abnahmeprozess durchlaufen. Das Testing hat auf produktionsnahen Testumgebungen zu erfolgen (siehe Ziffer 3.5.2.14).

Der Anbieter muss Releases, Updates und Patches auf ihre Funktionsfähigkeit prüfen, bevor er diese dem Auftraggeber bzw. dem technischen Betrieb zum Testing und Deployment liefert. Während der Testphase muss der Anbieter den entsprechenden Support auf den Releases, Updates und Patches sicherstellen.

Der Anbieter soll ein Testkonzept beilegen, welches das Testing des ganzen Systems aus seiner Sicht umfasst und beschreibt (inkl. Ansprechpartner).

Für das Testkonzept sind insbesondere die folgenden Punkte zu berücksichtigen:

- Der Anbieter soll eine Code Abdeckung durch Unit Tests von mindestens 80% erreichen. Falls diese Abdeckung nicht möglich oder aus Sicht des Anbieters nicht sinnvoll ist, soll er dies begründen.
- Das Testing soll negative Testfälle beinhalten.
- Der Anbieter soll die Integrationstests auf der Integrationsumgebung end-to-end durchführen und mit Service Providern (z.B. der Lieferant der Fingerabdruckleser Sitasys) interagieren.
- Der Anbieter soll umfangreiche Exception Tests und Recovery nach Strom- und Verbindungsunterbrüchen vor einem Major Release durchgeführt haben. Die Resultate soll er dem Auftraggeber als Lieferobjekt zur Verfügung stellen.
- Der Anbieter soll Regressionstests vor jedem Release durchgeführt haben. Die Resultate soll er dem Auftraggeber als Lieferobjekt zur Verfügung stellen.
- Der Anbieter soll den Support des Testsystems während der Testphasen sicherstellen. Der Anbieter soll aufzeigen, in welchen Zeiträumen dieser die Fehler im Rahmen von Tests analysiert und Fixes bereitstellen kann. Weiter soll er aufzeigen, wie er mit Support-Tickets während der Testphasen umgeht.
- Für die Testphase soll sichergestellt werden, dass der Anbieter geeignete Tracing und Logging Funktionalitäten bereitstellt, so dass er ohne Hilfe des Auftraggebers Fehler nachvollziehen kann.
- Der Anbieter soll im Rahmen der Tests - auf Anfrage des Auftraggebers - Unterstützung vor Ort leisten können.

3.5.4.7 Dokumentation (ZK 4.2)

Der Anbieter soll eine geeignete Dokumentation hinsichtlich des Systems in elektronischer Form zur Verfügung stellen, damit die Anwender das System effizient und schnell erlernen können.

Die Dokumentation für die Grenzkontrollverantwortlichen (z.B. Benutzerhandbuch, Quickguide, html-Online-Hilfe, e-Learning) soll in deutscher, französischer und italienischer Sprache zur Verfügung gestellt werden.

Die Dokumentation für Systemadministratoren sowie den technischen Betrieb (z.B. technische Dokumentation, Systemarchitektur, Release-Dokumentation, Spezifikationen, Betriebshandbuch) soll in deutscher Sprache zur Verfügung gestellt werden.

Bei Änderungen im System soll der Anbieter die Dokumentation entsprechend aktualisieren.

Der Anbieter soll aufzeigen, welche Dokumentationen er zur Verfügung stellen und wie er deren Aktualität sicherstellen wird.

3.5.5 Präsentation der Lösung

3.5.5.1 Zielsetzung

Im Rahmen dieser Beschaffung, werden Präsentationen der Lösungen, durch die in Frage kommenden Anbieter durchgeführt. Die Präsentationen dienen der Beurteilung der nachfolgend aufgeführten Zuschlagskriterien. Hierfür wurden die verschiedenen Use Cases beschrieben, welche im Rahmen der Grenz- und Inlandkontrollen vorkommen können. Anhand der definierten Abläufe soll u.a. die «intuitive» Unterstützung der anfallenden Kontrollen durchs System bewertet werden.

Nachfolgend sind die aus der Präsentation der Lösung zu erfüllenden Hauptziele aufgeführt:

Hauptziel 1	**Vollständige Abbildung des Prozesses**
Hauptziel 2	**Effiziente Umsetzung**
Hauptziel 3	**Benutzerfreundliche Umsetzung**
Hauptziel 4	**Qualität des Systems, der Projekt- und Supportarbeit des Anbieters**

Tabelle 9: Präsentation der Lösung - Hauptziele

3.5.5.2 Vorgehen

Die Präsentation der Lösung findet in den Räumlichkeiten des Auftraggebers statt.

Die Präsentation der Lösung wird nur mit denjenigen Anbietern durchgeführt, welche die Eignungskriterien sowie die technischen Spezifikationen erfüllen und nach der Bewertung der Zuschlagskriterien ZK 1 bis 5 (gem. Pflichtenheft) aufgrund der Punkte, die aus der Präsentation der Lösung selbst maximal erreicht werden können, noch für den Zuschlag in Frage kommen.

Die Präsentation der Lösung findet voraussichtlich im Q3 2021 statt. Die Anbieter werden aufgefordert, diesen Termin freizuhalten. Die Einladung zur Präsentation der Lösung erfolgt ca. 3 Wochen vor der Präsentation. Die Präsentation der Lösung erfolgt in deutscher oder französischer Sprache. Der Auftraggeber behält sich vor, nach Evaluation der EK, TS sowie ZK 1 bis 5 (gem. Pflichtenheft Ziffer 6.1) die Präsentation der Lösung nicht durchzuführen, wenn der Vergabeentscheid eindeutig ist.

Seitens Auftraggeber wird ein Gremium bestehend aus 5 Personen, welches sich aus Vertretern des Evaluationsteams zusammensetzt, an der Präsentation der Lösung teilnehmen.

Von Seite Anbieter dürfen anlässlich der Präsentation maximal drei Personen anwesend sein.

Der Ablauf der Präsentation der Lösung gliedert sich gem. nachfolgenden Traktanden:

Thema	**Dauer in Std.**
Begrüssungsrunde, Vorstellung der anwesenden Personen Der Anbieter stellt sein Unternehmen, allfällige Subunternehmer und die an der Präsentation mitwirkenden Personen vor. Der vorgesehene Projektleiter sowie seine Stellvertretung stellen sich anhand ihres Lebenslaufs inkl. der relevanten Projekterfahrung vor.	0.5
Präsentation, Erläuterung der Lösung Der Anbieter erklärt seine Lösung (Systemarchitektur, Realisierung, Einführung, Betrieb) aufgrund der aktuellen Situation, inkl. aller Besonderheiten, welche er zu berücksichtigen hat.	1.0

Thema	Dauer in Std.
Demo - Use Cases Der vorgesehene Projektleiter sowie seine Stellvertretung zeigen die sechs Use Cases gemäss Ziff. 3.5.5.3 auf, anhand einer Lösung mit vollständigem Funktionsumfang. Für die Umsetzung der Use Cases sind die Anforderungen gem. Ziffer 3.5.1 relevant. *Wichtig*: Alle gezeigten Funktionen im Rahmen der Präsentation der Use Cases sollen auch im Angebot des Anbieters enthalten sein.	2.0
Fragen Der Auftraggeber behält sich vor, bei Bedarf auch laufend zu den präsentieren Use Cases Fragen zu stellen.	1.0
Reserve	0.5
Total	**5.0**

Tabelle 10: Präsentation der Lösung - Agenda

3.5.5.3 Use Cases

Die nachfolgenden Use Cases beschreiben den groben Ablauf der vorgenommenen Kontrollen.

Die Use Cases sollen – wenn immer möglich – in einem produktionsnahen Umfeld präsentiert werden. Falls Teile der Use Cases (z.B. EES) noch nicht im produktiven Betrieb sind, dürfen die betroffenen Use Cases auch auf einem nicht-produktiven System (z.B. Prototyp) präsentiert werden.

3.5.5.3.1 Use Case – Negative Kontrolle (ZK 5.1)

Der nachstehende Ablauf stellt den groben Kernprozess des Use Case dar:

UC Schritt	Beschreibung
1.1	Der Reisende tritt zur Kontrolle an.
1.2	Der Reisende übergibt seinen Reisepass dem GKV.
1.3	Der GKV liest die MRZ und den Chip mit der mobilen App aus: a. MRZ Reisepass wird mit der Smartphone-Kamera eingelesen; b. Chip wird mit der App ausgelesen; c. Manuelle Eingabe der im Dokument erfassten Daten.
1.4	Abfrage wird automatisch via Schnittstelle in den Datenbanken gestartet (resp. die Anfrage der Informations- und Fahndungssysteme kann durch den GKV übersteuert werden – manuelle Deaktivierung von Datenbankabfragen).
1.5	Rückmeldungen aus den Datenbanken werden dem GKV via mobiler GKS App angezeigt.
1.6	Anhand der Rückmeldungen (und ggf. Antworten aus der Befragung) soll der GKV entscheiden ob: a. weitere Abklärungen notwendig sind (→ vertiefte Kontrolle). b. resp. die Weiterreise gestattet wird (bei Resultat «Person ist nicht verzeichnet» resp. keine kritische Verzeichnung in der Datenbank).
1.7	Der GKV händigt dem Reisenden den Pass wieder aus und dieser reist im Anschluss daran weiter.
1.8	Ende

Tabelle 11: Ablauf Use Case negative Kontrolle

Präzisierungen zu den einzelnen Use Case Schritten:

UC Schritt	Präzisierungen
1.2	In einer Binnen- bzw. Inlandkontrolle ist die Basis für die Kontrolle nicht zwingend der Reisepass. Diese kann auch eine Identitätskarte, ein Führerschein, weitere nicht ICAO-konforme Dokumente oder eine mündliche bzw. vor Ort notierte Information zu Name, Vorname, Geburtsdatum und Nationalität sein.
1.3	**Start eines neuen Abfragevorgangs** Das Dokument ist mit der Kamera des Smartphones durch den Grenzkontrollverantwortlichen mit einfacher, intuitiver, Dokumentenpositionierung einlesbar. Im MRZ-Scan-Modus soll das Licht des Mobiltelefons wahlweise ein- oder ausgeschaltet werden können. Dies, um flexibel auf die aktuell herrschende Beleuchtungssituation reagieren zu können. Der MRZ-Scan-Modus soll sich bezüglich Blickwinkel (bspw. Abweiche-Toleranz von 30 Grad auf jeder Achse) von Kamera auf Dokument tolerant zeigen und in Bezug auf die Auslesegeschwindigkeit keine Einbussen erleiden. Dies, weil Dokumente bspw. auch in fahrenden Zügen ausgelesen werden sollen.
1.3	**MRZ Erfassen** Die MRZ soll vom System automatisch erfasst werden. Bei Bedarf (z.B. Ausfall Kamera, beschädigte MRZ) kann der GKV die notwendigen Dokumentdaten manuell erfassen.
1.3	**Qualität MRZ Erfassung** Die Erfassung der MRZ soll für verschiedene Dokumente (insb. nicht ICAO-konforme Dokumente wie FR-ID), Winkel und Lichtverhältnisse gut funktionieren.
1.3	**MRZ Korrekturen** Von der App fehlerhaft gelesene MRZ sollen vor dem nächsten Prozessschritt korrigiert werden können. Das System hat die fehlerhaft gelesenen Zeichen oder den fehlerhaft ausgelesenen Bereich dem GKV anzuzeigen und die Korrektur aktiv zu unterstützen.
1.3	**Statusinformationen Chip eDokument** Dem GKV ist auf einfache Art anzuzeigen, ob mit dem Chip eines eDokuments kommuniziert werden kann oder nicht.
1.3	**Performance Chip auslesen** Das System soll maximal 4 Sekunden benötigen, um den Chip eines eMRTDs auszulesen.
1.3	**Transliterationstabellen** Bei der Erfassung von Zeichen soll eine Transliteration möglich sein, das heisst die buchstabengetreue Übertragung von Wörtern aus einer Buchstabenschrift in eine andere Buchstabenschrift.
1.3	**Manuelle Abfrage** Alle angeschlossenen Informations- und Fahndungssysteme können manuell abgefragt werden. Dies kann entweder durch die Verwendung / Ergänzung der Daten der gescannten MRZ oder durch die manuelle Erfassung der Daten erfolgen. Hierbei sollen die Datenfelder «Name» und «Vorname» mit einem Klick getauscht werden können. Die Datenfelder der Personalien und Angaben zu den Reisedokumenten sollen so gestaltet sein, dass sie auf einfache und übersichtliche Weise manuell bearbeitet werden können.

1.4	Der eigentliche Prozessverlauf beginnt wenn die MRZ des Dokuments durch die Kamera eingelesen wurde, und endet nach dem Vorliegen des Resultats der am längsten dauernden Abfrage in einem Informations-/Fahndungssystem, dessen „Timeout“ oder durch Abschluss der Kontrolle durch den GKV.
1.5	**Bildschirmgliederung** Übersichtliche Anzeige, welche für einen mobilen Bildschirm konzipiert ist. • «Übersicht» enthält eine Grobübersicht über die Abfrageresultate der verschiedenen DBs. • Die Resultate pro Überprüfungskategorie (z.B. Informations-DBs, Personenfahndungen, Fahrzeuge, Sachen) sind mit einem Ampelsystem (grün, gelb, rot) anzuzeigen. • Suchkriterien ersichtlich. In wenigen Schritten, intuitiv von der Übersicht zur Detailansicht Treffer. • «Detail»: bei der Auswahl des entsprechenden Resultats werden allfällig enthaltene Details angezeigt (bspw.: PopUp-Fenster, fixer Bereich in der GKS-Oberfläche oder andere Lösung). • Wenn ergänzende Informationen von den Informations- und Fahndungssystemen bereitgestellt werden (Fotos, Dokumente) sind diese Informationen dem GKV anzuzeigen.
1.5	**Positionierung der angezeigten Informationen** Die Position der angezeigten Informationen sowie die Reihenfolge der Fahndungssysteme bei der Trefferanzeige, hat per Default immer dieselbe zu sein.
1.5	**Designkonzept** Die Ergebnisse sind übersichtlich zu präsentieren und Befunde werden hervorgehoben. Die Farb- und Schriftgestaltung soll dem raschen und einfachen Ablauf einer Grenzkontrolle Rechnung tragen. • Farbgestaltung: o Kontraste (hell / dunkel); o Kritische Ergebnisse entsprechend markiert (z.B. in rot); o Nachtmodus ein/ausschalten. • Schriftgestaltung: o Schriftgrössen (z.B. klein, normal, gross); o Überschrift von Normaltext soll hervorgehoben werden (z.B. **Fett**, <u>unterstrichen</u>); o Schriftart: gut lesbare Schrift (z.B. Arial), *nicht kursiv.*
1.8	**History (mehrstufige Beurteilung)** Möglichkeit zur Sichtung der letzten Vorgänge (Personen- und Dokumentenprüfungen -> Scans), welche gut wiederzufinden sind (z.B. Miniaturansicht mit Foto)."

Tabelle 12: Präzisierungen Use Case negative Kontrolle

3.5.5.3.2 Use Case – Positive Kontrolle (kritische Verzeichnung in der DB) (ZK 5.2)

Der beschriebene Use Case unter Ziffer 3.5.5.3.1 geht bei einer kritischen Rückmeldung der DB in Punkt 1.6 a) über, was bedeutet, dass die Person vertieft kontrolliert wird. Je nach Ausgang der Abklärungen kann die Person entweder weiterreisen oder die Weiterreise wird ihr verweigert.

UC Schritt	Präzisierungen
1.6 a)	**Resultate hervorheben** Kritische Resultate sind auffällig und gut lesbar anzuzeigen. Das System soll die Resultate in Trefferlisten gruppiert anzeigen können (z.B. nach Personen / Fahrzeugen / Sachen oder Datenbanken). Innerhalb dieser Trefferlisten soll das System die Resultate nach einer vorgegebenen Bewertung ordnen können. Für die Darstellungen sind die SIS Vorgaben der EU einzuhalten, insbesondere: • Warnungen sollen immer zusätzlich mit einem farbigen Warndreieck versehen werden. Dies gilt bereits bei der Trefferliste, auch wenn noch nicht klar ist, ob die Anfrage effektiv zu einem Hit führt. • Missbrauchte Identitäten "misused identity" sollen zwingend rot markiert werden. Die Detailinformationen der Treffer sind effizient einsehbar.
1.6 a)	**Performance** Für einen reibungslosen und effizienten Prozessablauf der Grenzkontrolle ist die technische Systemdurchlaufzeit der Dokumenten- und Personenkontrolle massgeblich. Diese Zeit hat beim mobilen Grenzkontrollsystem < 6 Sekunden zu liegen. Definition der technischen Systemdurchlaufzeit: Dauer vom Einlesen der MRZ mittels Kamera in der mobApp GKS bis zur Anzeige sämtlicher relevanter Ergebnisse (exkl. Antwortzeiten Abfrage der Fahndungs- und Informationssysteme) in der mobApp GKS.
1.6 a)	**Detailansicht** Der GKV soll aus der Trefferliste innert kurzer Zeit (Zielwert max. 2 Sekunden) eine Detailansicht zum Treffer aufrufen können. Die Detailergebnisse sind übersichtlich darzustellen und Befunde/Abweichungen werden hervorgehoben. Das System soll auch Bilder (z.B. Gesichtsbilder), Dokumente oder Alias-Angaben anzeigen und darstellen können, sofern solche Informationen in den Resultaten vorhanden sind. Hyperlinks sollen klar als solche zu erkennen sein (z.B. Farbe, unterstrichen).

Tabelle 13: Präzisierungen Use Case positive Kontrolle

3.5.5.3.3 Use Case – Visa Verifikation (ZK 5.3)

Der Use Case Visa startet nach Prozessschritt 1.5 des unter Ziff. 3.5.5.3.1 beschriebenen Use Case und geht nach Abschluss in Prozessschritt 1.6 des gleichen Use Case über.

Der nachstehende Ablauf stellt den groben Teilprozess des Use Case dar:

UC Schritt	Beschreibung
1.5.1	Beginn Teilprozess Visa
1.5.2	Visum einscannen
1.5.3	Resultat überprüfen
1.5.4	Ende Teilprozess Visa

Tabelle 14: Ablauf Use Case Visa Verifikation

3.5.5.3.4 Use Case – Kontrollschild auslesen (ZK 5.4)

Der nachstehende Ablauf stellt den groben Kernprozess des Use Case dar:

UC Schritt	Beschreibung
4.1	Kontrollschild mit Kamera auslesen.
4.2	Eingabedaten prüfen und ggf. korrigieren.

4.3	Abfrage wird via Schnittstelle in den Datenbanken gestartet.
4.4	Rückmeldungen aus den Datenbanken werden dem GKV via mobile GKS App angezeigt.
4.5	Anhand der Rückmeldungen (und ggf. Antworten aus der Befragung) soll der GKV entscheiden ob: a. weitere Abklärungen notwendig sind (→ vertiefte Kontrolle); b. resp. die Weiterreise gestattet wird.
4.6	Ende

Tabelle 15: Ablauf Use Case Kontrollschild auslesen

Präzisierungen zu den einzelnen Use Case Schritten:

UC Schritt	Präzisierung
4.1	Die Auslesung des Kontrollschildes soll rasch und effizient erfolgen (bspw. mittels auslesen aus einem VideoStream). Das Auslesen soll unabhängig der Ausrichtung des Mobiletelefons erfolgen können (Hoch- und Querformat). Die Erkennung soll sowohl für Kontrollschilder mit einer Zeile als auch mit zwei Zeilen funktionieren. Die Auslesung soll eine gewisse Stabilitäts-Toleranz gegenüber den Lichtverhältnissen aufweisen und bis zu einer Entfernung von 4 Meter erfolgen können. Eine Zoom-Funktion soll eine Erfassung auf Distanz unterstützen.
4.1	**Performance** Das System soll maximal 5 Sekunden benötigen, um ein Fahrzeug-Kontrollschild zu detektieren, einzulesen und darzustellen.
4.2	Die Software kann mindestens die Kennzeichen der Nachbarländer erkennen und auslesen. Die erfassten Informationen werden direkt in die dafür vorgesehenen Suchparameterfelder eingefüllt. Hier können sie kontrolliert und korrigiert werden. Hat die Software erkannt, dass ein Lesefehler vorliegt, wird sofort in den Korrekturmodus gewechselt. Der GKV wird bei der Fehlerkorrektur softwareseitig durch Markierung des Fehlers unterstützt.
4.3	Der eigentliche Prozessverlauf beginnt wenn das Kontrollschild des Fahrzeugs durch die Kamera eingelesen wurde, und endet nach dem Vorliegen des Resultats der am längsten dauernden Abfrage in einem Informations-/Fahndungssystem, dessen „Timeout“ oder durch Abschluss der Kontrolle durch den GKV.

Tabelle 16: Präzisierungen Use Case Kontrollschild auslesen

3.5.5.3.5 Use Case – Sachfahndung (ZK 5.5)

Die App kommt nicht nur für zu kontrollierende Personen zum Einsatz, sondern auch für mitgeführte Sachen, Fahrzeuge oder Waren. Daher sollen die relevanten Abfrageparameter (analog einer Personenabfrage) in einer Suchmaske eingegeben werden können.

3.5.5.3.6 Use Case – Personenidentifikation mittels Fingerabdrücken (ZK 5.6)

Mit der mobilen GKS App sollen Abfragen von Fingerabdrücken in den relevanten Umsystemen möglich sind. Aktuell sind dies AFIS und VIS, künftig kommt EES (und allenfalls weitere) hinzu.

Der nachstehende Ablauf stellt den groben Kernprozess des Use Case dar:

UC Schritt	Beschreibung
6.1	Eine biometrische Kontrolle (Fingerabdrücke) soll gemacht werden.
6.2	Der Fingerabdruckleser wird mit dem Mobiltelefon verbunden.

6.3	Es wird eine PCN-Nummer bezogen.
6.4	Optional kann ein Gesichtsbild der Person erfasst werden.
6.5	Die Fingerabdruckerfassung wird gestartet.
6.6	Die Abfrage wird versendet.
6.7	Das Abfrageresultat kommt auf das Absendergerät zurück und wird gelesen.
6.8	Der GVK startet auf Basis eines Abfrageresultats eine Abfrage an die Fahndungs- und Informationssysteme.
6.9	Ende

Tabelle 17: Ablauf Use Case Personenidentifikation mittels Fingerabdrücken

Präzisierungen zu den einzelnen Use Case Schritten:

UC Schritt	Präzisierung
6.2	Es handelt sich um einen WiFi FP-Reader, welcher mit dem Mobiltelefon gekoppelt werden soll. Die Kopplung für eine sichere Verbindung erfolgt via Geräte-Benutzername und Passwort. Die Kopplung soll einfach, rasch und sicher sein, bspw. mittels Scan eines QR-Codes.
6.3	Die einmalige Process Control Number (PCN) soll bezogen werden, bevor die Anfrage ans AFIS / VIS (oder andere) versendet wird. Im Anschluss der Abfrage soll es möglich sein, die Person der PCN zu zuordnen. Aus diesem Grund wird die Nummer heute vor der Fingerabdruckerfassung bezogen und angezeigt.
6.4	Um Personen im Nachgang der, zu ihren Fingern gehörenden, PCN-Nummer zuweisen zu können, soll die Möglichkeit bestehen, vor der Fingerabdruckerfassung ein Gesichtsbild der Person mit der Kamera aufzunehmen und mit der PCN zu verknüpfen (oder Gleichwertiges).
6.5	Das System führt den GKV durch den Fingerabdruckerfassungsprozess. Das vorgängige Bestimmen, welche Datenbanken abgefragt werden, soll einen Einfluss auf die Fingerabdruckerfassung haben. Ziel wäre, die Fingerabdruckerfassung für die verschiedenen Datenbanken so zu gestalten, dass jeder Finger max. 1x zu erfassen ist. Die korrekten NIST-Files sowie der Versand der korrekten Daten an die verschiedenen Datenbanken erfolgt hinterher. Das System zeigt dem GKV, welcher Finger gerade erfasst werden soll. Ist die erforderliche Qualität erreicht (NFIQ 3), springt das System automatisch zum nächsten Finger. Gibt es Qualitätsprobleme, so wird der GKV App-seitig in der Fehlersuche unterstützt (bspw. Live View, Druck/Feuchtigkeit des Fingers prüfen, Lebenderkennung aktivieren, Finger mehr links/rechts/oben/unten auf Sensor legen, etc.). Bei einer schlechten Abnahmequalität soll der Prozess übersteuerbar sein (bspw. nach 3 Versuchen).
6.6	Die Abfrage wird automatisch nach der Erfassung des letzten Fingerabdrucks (sofern Qualität ausreichend) versendet.
6.7	Das Abfrageresultat kommt (samt Details) auf das absendende/anfragende Mobiltelefon zurück.
6.8	Die Daten eines Abfrageresultats können für eine manuelle Abfrage übernommen werden, ohne dass die Daten manuell eingegeben werden sollen, aber mit der Möglichkeit, sie vor der Ausführung der Abfrage manuell zu korrigieren.

Tabelle 18: Präzisierungen Use Case Personenidentifikation mittels Fingerabdrücken

3.5.5.4 Beurteilung

3.5.5.4.1 Kriterien für die Beurteilung von Effizienz und Benutzerfreundlichkeit

Effizienz:

- der User soll mit dem kleinstmöglichen (Zeit-)Aufwand an sein Resultat kommen (Aufstarten, Clickrate);
- im Fehlerfall Korrektur möglich;
- technisch performante Einbindung des Fingerabdrucklesers;
- die technische Systemdurchlaufzeit soll möglichst kurz sein;
- das System hebt für den Benutzer wichtige Informationen hervor (bspw. abgelaufener Pass, Overstay, Fehler Dokumentenprüfung, Problem bei Erfassung Biometrie);
- adaptive Darstellung.

Benutzerfreundlichkeit:

- Schriftgrösse, Anzeige gut und schnell lesbar sein;
- der Anwender kann bei Bedarf die Schriftgrösse verändern;
- ähnliche Objekte auf verschiedenen Screens an gleicher Stelle;
- Farbgebung (basierend auf einem Farbkonzept) soll dezent, gut lesbar und Prozessbezogene Hilfe ermöglichen;
- übersichtliche Darstellung, wenig scrollen um an die relevanten Informationen zu gelangen;
- einfache, klare, selbsterklärende, verständliche Navigation, Bedienung und Darstellung (bspw. mittels selbstsprechenden Icons, logischer Aufbau);
- Informationsanzeige aufs Wesentliche beschränken;
- einfacher und übersichtlicher Aufbau;
- automatische Fehlererkennung, Plausibilitätscheck;
- Warnungen, wenn Informationen im Prozess fehlen;
- Verzicht auf nicht benötigte Inhalte oder Designelemente, die keine Benutzeraufgaben unterstützen, die Pain Points und die User Journey der Zielgruppe berücksichtigen;
- expliziter Abschluss von Prozessen.

3.5.5.4.2 Tabelle zur Beurteilung der Use Cases

***Achtung**: Die folgenden Kriterien werden durch den Auftraggeber während der Präsentation der Lösung ausgefüllt. Der Anbieter muss in untenstehender Tabelle keine Angaben vornehmen:*

Innerhalb eines Use Cases wird jede ID gleich gewichtet sowie einzeln beurteilt. Pro UC wird aus den Noten eine Summe gebildet. Bsp. ID 1 = vollständig / ID 2 = teilweise / ID 3 = vollständig, was in vorliegendem Beispiel 7.5 von maximal 9 Punkten ergibt.

Ergibt die Bewertung nicht die maximale Punktzahl, erfolgt ein linearer Abzug der Maximalpunkte (gemäss Anhang 03).

ID	Kriterium	Note	Note	Note	Begründung (*Es muss immer eine Begründung erfasst werden, wenn nicht mit „Note 3“ bewertet wird.*)
		3	**1.5**	**0**	
Use Case – Negative Kontrolle					
1.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	
2.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
3.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
Use Case – Positive Kontrolle (kritische Verzeichnung in der DB)					
4.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	
5.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
6.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
Use Case – Visa Verifikation					
7.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	
8.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
9.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
Use Case – Kontrollschild auslesen					
10.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	

ID	Kriterium	Note	Note	Note	Begründung (*Es muss immer eine Begründung erfasst werden, wenn nicht mit „Note 3“ bewertet wird.*)
		3	**1.5**	**0**	
11.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
12.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
Use Case – Sachfahndung					
13.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	
14.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
15.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
Use Case – Personenidentifikation mittels Fingerabdrücke					
16.	Der Use Case wurde vollständig durchlaufen (Standard Use Case inkl. Exceptions). Der Use Case wurde in einem Testsystem gezeigt. Werden an einem Punkt Mockups o.ä. benutzt, so ist das transparent auszuweisen und zu begründen.	☐ vollständig	☐ teilweise	☐ eher nicht	
17.	Der Use Case ist effizient umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	
18.	Der Use Case ist benutzerfreundlich umgesetzt.	☐ vollständig	☐ teilweise	☐ eher nicht	

Tabelle 19: Beurteilung der Use Cases

4 Preise und Kosten

Der Anbieter hat funktionstüchtige Systeme inkl. Lizenzen und Dienstleistungen zu offerieren. Sollten einzelne für ein einwandfreies und nachhaltiges Funktionieren des ausgeschriebenen Gesamtsystems erforderliche Leistungen oder Anlageteile in der Leistungszusammenstellung nicht aufgeführt sein, so werden die Anbieter ausdrücklich aufgefordert, dies in der Fragerunde zu thematisieren. Der Auftraggeber prüft die aus Sicht des Anbieters fehlenden Leistungen oder Anlageteile und informiert in der Antwort, ob sie in den Offerten in den dafür vorgesehenen freien Feldern ergänzend anzubieten sind. Sie werden bei der Bewertung der Angebote und der Festlegung der Zuschlagssumme mitberücksichtigt. Das vorliegende Leistungsverzeichnis schränkt die fachtechnische Verantwortung des Anbieters für die Funktion der Systeme nicht ein.

5 Zwingende Anforderungen: Teilnahmebedingungen, Eignungskriterien und technische Spezifikationen

5.1 Zwingende Anforderungen

Alle wirtschaftlich und technisch leistungsfähigen Unternehmen, welche die nachfolgenden Teilnahmebedingungen, Eignungskriterien und die technischen Spezifikationen erfüllen, sind aufgerufen, ein Angebot in CHF zu unterbreiten.

5.2 Erfüllung der zwingenden Anforderungen

Die im Anhang 03 pro Arbeitspaket aufgeführten zwingenden Anforderungen (Teilnahmebedingungen, Eignungskriterien und technischen Spezifikationen) müssen vollständig und ohne Einschränkung oder Modifikation mit der Unterbreitung des Angebotes erfüllt und nachgewiesen werden, ansonsten wird nicht auf das Angebot eingegangen. Wo verlangt, ist eine entsprechende Dokumentation beizulegen.

Teilweise wird in den Anforderungen Anhang 03 auf das vorliegende Pflichtenheft referenziert. Bei Referenzierungen im Anhang 03 auf das vorliegende Pflichtenheft müssen die referenzierten Anforderungen ebenfalls erfüllt werden.

6 Zuschlagskriterien (ZK)

6.1 Übersicht

Anhand der Zuschlagskriterien findet eine detaillierte Punktebewertung der Angebote statt.

Nr.	Bezeichnung	Punkte	Gewichtung in %
ZK 1	Fachliche Anforderungen, gemäss Anforderungen Ziff. 3.5.1	3000	30%
ZK 2	Technische Anforderungen, gemäss Anforderungen Ziff. 3.5.2	1000	10%
ZK 3	Projekt und Weiterentwicklung, gemäss Anforderungen Ziff. 3.5.3	500	5%
ZK 4	Wartung und Pflege, gemäss Anforderungen Ziff. 3.5.4	500	5%
ZK 5	Präsentation der Lösung, gemäss Anforderungen Ziff. 3.5.5	2000	20%
ZK 6	Total Preis gemäss Preisblatt, Anhang 02, A_mobGKS und C_mobGKS_Wartung_Pflege / Massgeblicher Gesamtpreis für Bewertung des ZK 6	2000	20%
ZK 7	Total Preis gemäss Preisblatt, Anhang 02, Zusammenfassung B_mobGKS_Pooltage / Massgeblicher Gesamtpreis für Bewertung des ZK 7	1000	10%

Tabelle 20: Übersicht Zuschlagskriterien

6.2 Erfüllung des Anforderungskatalogs

Die im Anhang 03 aufgeführten Anforderungen müssen vollständig, detailliert und klar verständlich formuliert und beantwortet sein. Wo verlangt, sind die entsprechenden Dokumente und Nachweise beizulegen. Allfällige Referenzierungen auf weiterführende Unterlagen sind erlaubt, müssen jedoch exakt auf die relevanten Textabschnitte/-stellen der Unterlagen verweisen. Ist eine Anforderung in Einzelpunkte untergliedert, muss auf all diese Einzelpunkte detailliert eingegangen werden. Die im Anhang 03 geforderten Angaben sind vollständig und nachvollziehbar auszufüllen.

Wichtig: Die Beschaffungsstelle behält sich vor, die von Seiten der Anbieter im Angebot aufgeführten Dokumentationen und/oder referenzierten Informationen inhaltlich zu verifizieren und bei Bedarf vom Anbieter dazu zusätzliche Informationen einzufordern. Sind die Antworten nicht nachvollziehbar oder unverständlich, die geforderten Angaben oder Unterlagen nicht vorhanden oder mangelhaft, so kann dies zu einer tieferen Bewertung der Antwort des Anbieters oder zu dessen Ausschluss führen.

6.3 Bewertung der Preise und Kosten

Zuschlagskriterium Preis

Bewertet wird pro Angebot der massgebliche Gesamtpreis für die Punktevergabe. Dieser wird wie folgt berechnet:

Massgeblicher Gesamtpreis für Bewertung =

Kosten des ausgeschriebenen Beschaffungsvolumens (Grundauftrag + Option)

Alle Werte, die in der **Brandbreite von 100%** liegen, erhalten Punkte (lineare Interpolation zwischen 100% und 200%).
Alle Werte, die den tiefsten Wert um mehr als 100% überschreiten, erhalten 0 Punkte. Alle Angebote welche gemäss Formel ein Resultat unter 0 ergeben, werden mit 0 Punkten bewertet (keine Minuspunkte).

Formel zur Berechnung des Preises:

$$\text{Punkte} = M \times \frac{(P_{max} - P)}{(P_{max} - P_{min})}$$

M = Maximale Punktezahl
P = Preis des zu bewertenden Angebots
Pmin = Preis des tiefsten zulässigen Angebots
Pmax = Preis, bei welchem die Preiskurve den Nullpunkt schneidet (Pmin * 200%)

Rechnungsbeispiel: Maximal 3000 (2000 + 1000) Punkte für den Preis
Pmin = CHF 500‘000.00
Pmax = CHF 1'000'000.00 (2 x 500‘000.00)

Anbieter A	CHF 500‘000.00	3000 Punkte
Anbieter B	CHF 520‘000.00	2880 Punkte
Anbieter C	CHF 800‘000.00	1200 Punkte

7 Evaluation

7.1 Evaluationsphasen

Folgende Schritte erfolgen bis zum Zuschlagsentscheid:

Pos.	Beschreibung der Aktivität	Grobterminplan
1	Publikation der Ausschreibung auf der simap-Plattform	Q2 2021
2	Abgabe der Unterlagen nach Unterschrift der Geheimhaltungsverpflichtung	Q2 2021
3	Fragerunde	Q3 2021
4	Eingang der Angebote	Q3 2021
5	Prüfen der eingegangen Angebote (vgl. Kap. 9.4.3)	Q3 2021
6	Allfällige Bereinigung der Angebote (vgl. Kap. 9.4.3)	Q3 2021
7	Präsentation der Lösung	Q3 2021
8	Bewertung und Evaluationsentscheid	Q4 2021
9	Zuschlagspublikation auf der simap-Plattform	Q4 2021

Tabelle 21: Übersicht Evaluationsphasen

8 Strukturvorgaben und Inhalt des Angebots

8.1 Allgemeines

Im Interesse einer fairen und schnellen Evaluation hat sich der Anbieter zwingend an folgenden Aufbau seines Angebots zu halten.

8.2 Gliederung des Angebots

Kapitel Offerte	**Inhalt**	**Referenz in Ausschreibungsunterlagen**
	Offertzusammenfassung (max. 2 A4 Seiten)	
Nr. 01	Ausgefüllter **Anhang 01a Angaben zum Anbieter** Ausgefüllter und rechtsgültig unterzeichneter **Anhang 01b Referenzen der Unternehmung**	Anhang 01a bis 01b
Nr. 02	Ausgefüllter und rechtsgültig unterzeichneter **Anhang 02 Preisblatt**	Anhang 02
Nr. 03	Ausgefüllter und rechtsgültig unterzeichneter **Anhang 03 Anforderung**	Anhang 03
Nr. 04	**Offerte des Anbieters** (Lösungsbeschreibung)	Pflichtenheft
Nr. 05	**Beilagen und Nachweise zum Anforderungskatalog** (Nachweise zu den einzelnen Kriterien, wie bspw. Selbstdeklaration BKB, Beilagen zu den Referenzen der Unternehmung)	Allfällige Nachweise und Beilagen des Anhang 03

Tabelle 22: Übersicht Gliederung des Angebots

9 Administratives

9.1 Auftraggeber

9.1.1 Offizieller Name und Adresse des Auftraggebers

Bedarfsstelle
Eidgenössische Zollverwaltung EZV
Direktionsbereich Planung & Steuerung
Taubenstrasse 16
3003 Bern

Beschaffungsstelle/Organisator
Bundesamt für Bauten und Logistik BBL
Fellerstrasse 21
CH-3003 Bern

9.1.2 Angebote sind an folgende Adresse zu schicken

Bundesamt für Bauten und Logistik BBL
Dienst öffentliche Ausschreibungen DöA
Projekt (21152) 606 Mobiles Grenzkontrollsystem (EZV)
Fellerstrasse 21
CH-3003 Bern
E-Mail: beschaffung.wto@bbl.admin.ch

9.1.3 Gewünschter Termin für schriftliche Fragen

Fragerunde: 06.07.2021, 23:59

Bemerkungen:

Falls sich beim Erstellen des Angebotes Fragen ergeben, können Sie diese anonymisiert ins Frageforum auf www.simap.ch stellen.

Zu spät eingereichte Fragen können nicht mehr beantwortet werden.

Die Anbieter werden per E-Mail informiert, sobald die Antworten auf www.simap.ch publiziert sind.

Fragen zur vorliegenden Ausschreibung sind in der **Fragerunde** bis spätestens **06.07.2021, 23:59** anonymisiert im Frageforum auf www.simap.ch einzugeben. Sollten in der vorliegenden Ausschreibung Komponenten oder Leistungen fehlen, welche aus Sicht des Anbieters für ein reibungsloses Funktionieren erforderlich sind, so müssen die entsprechenden Punkte vom Anbieter im Rahmen dieser Fragerunde eingebracht werden.

Die Antworten zu den in der **Fragerunde** gestellten Fragen werden bis spätestens **13.07.2021** im Frageforum www.simap.ch beantwortet.

9.1.4 Frist für die Einreichung des Angebots

02.08.2021

Formvorschriften:

Das vollständige Angebot (vgl. Vorgaben unter Ziffer 8.2) ist bis spätestens 02.08.2021 in vierfacher Ausführung (zweifach in Papierform und zweifach in elektronischer Form auf USB-Stick* **unverschlüsselt**) dem BBL an die unter Ziffer 9.1.2 aufgeführte Adresse zuzustellen.

* USB-Stick: Bitte beachten Sie, dass einerseits die gesamte Offerte auf dem USB-Stick enthalten sein muss und andererseits die Dokumente auf dem USB-Stick mit der Papierversion identisch sein müssen.

a) Bei Abgabe an der Warenannahme des BBL (durch Anbieter oder Kurier):

   Die Abgabe hat bis spätestens am oben erwähnten Abgabetermin, noch während der Öffnungszeiten der Warenannahme 08:00 – 12:00 und 13:00 – 16:00 Uhr gegen Ausstellung einer Empfangsbestätigung des BBL zu erfolgen.

b) Bei Einreichung auf dem Postweg:
Massgeblich für die Fristwahrung ist der Poststempel oder Strichcodebeleg mit Möglichkeit der Sendungsverfolgung einer schweizerischen oder staatlich anerkannten ausländischen Poststelle (Firmenfrankaturen gelten nicht als Poststempel). Bei Versand mit WebStamp Frankatur liegt die Beweislast für die fristgerechte Eingabe beim Anbieter.

c) Bei Übergabe des Angebots an eine diplomatische oder konsularische Vertretung der Schweiz im Ausland:
Ausländische Anbieter können ihr Angebot bis spätestens am oben erwähnten Abgabetermin, noch während der Öffnungszeiten gegen Ausstellung einer Empfangsbestätigung einer diplomatischen oder konsularischen Vertretung der Schweiz in ihrem Land übergeben. Sie sind dabei verpflichtet, die Empfangsbestätigung der entsprechenden Vertretung bis spätestens am Abgabetermin per E-Mail an die unter Ziffer 9.1.2 aufgeführte Adresse zu senden.

Der Anbieter hat in jedem Fall den Beweis für die Rechtzeitigkeit der Angebotseinreichung sicherzustellen.

Zu spät eingereichte Angebote können nicht mehr berücksichtigt werden. Sie werden an den Anbieter zurückgesandt.

9.1.5 Art des Auftraggebers

Bund

9.1.6 Verfahrensart

Offenes Verfahren

9.1.7 Auftragsart

Dienstleistungsauftrag

9.1.8 Gemäss GATT/WTO-Abkommen, resp. Staatsvertrag

Ja

9.2 Beschaffungsobjekt

9.2.1 Art des Dienstleistungsauftrages

Datenverarbeitung und verbundene Tätigkeiten

9.2.2 Ort der Dienstleistungserbringung

3003 Bern

9.2.3 Laufzeit des Vertrags

5 Jahre für den Grundauftrag
3 Jahre für die optionale Verlängerung

Siehe dazu auch die Bestimmungen des Rahmenvertrages selbst (insbesondere Ziffer 8.1.1 RV).

9.2.4 Aufteilung in Lose

Nein

9.2.5 Werden Varianten zugelassen?

Nein

9.2.6 Werden Teilangebote zugelassen?

Nein

9.2.7 Ausführungstermin

Folgender Grobterminplan ist pro Arbeitspaket vorgesehen. Das Go Live vom Mai 2022 wurde von der EU vorgegeben (Stand heute: Ab Mai 2022 muss EES live sein).

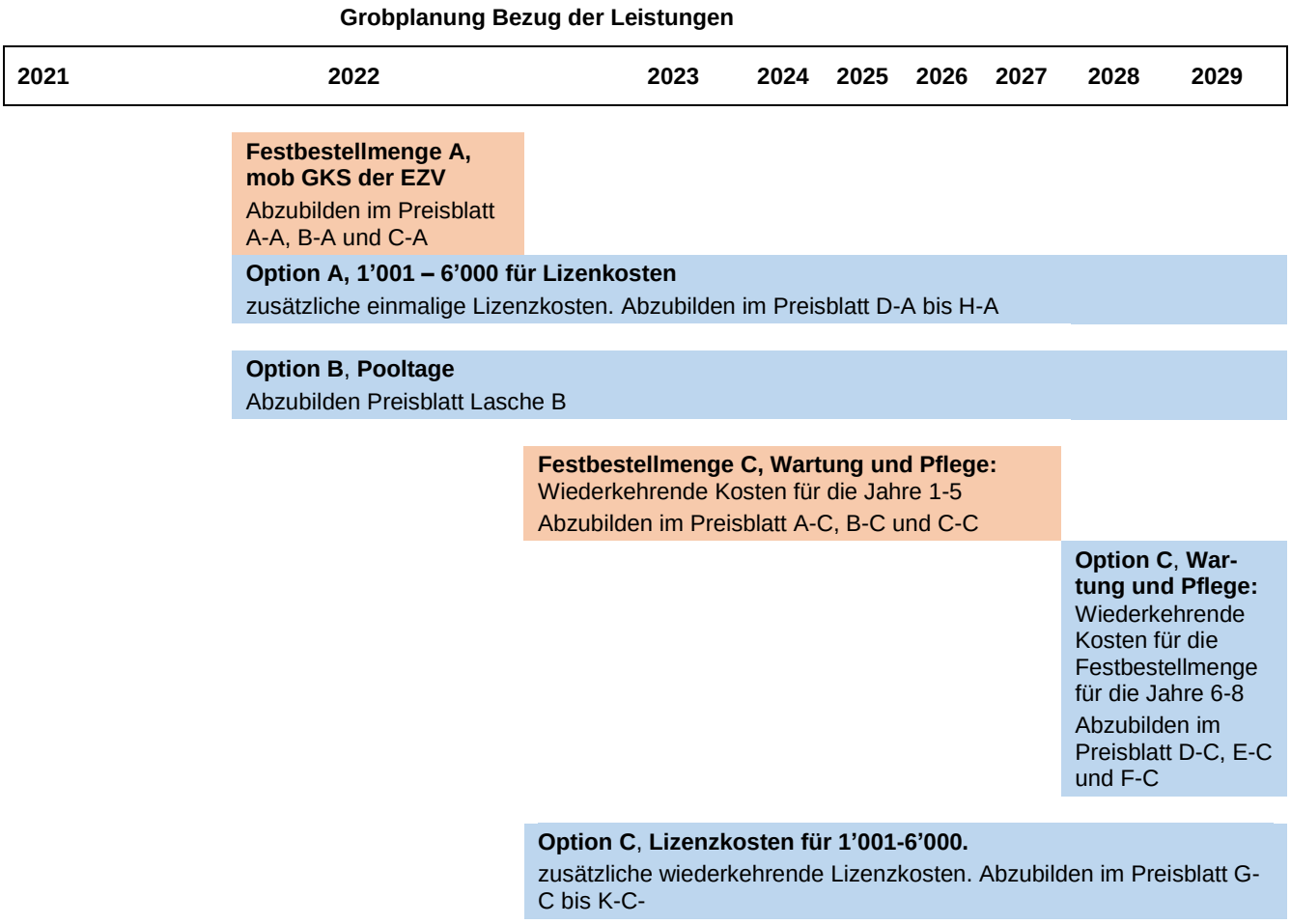

Abbildung 8: Grobplanung Bezug der Leistungen

9.3 Bedingungen

9.3.1 Kautionen/Sicherheiten

Keine

9.3.2 Zahlungsbedingungen

30 Tage nach Erhalt der Rechnung, netto in CHF, zuzüglich MwSt. Korrekte Rechnungsstellung mittels E-Rechnung vorausgesetzt.

Informationen der Bundesverwaltung zur E-Rechnung finden Sie auf folgender Webseite: http://www.e-rechnung.admin.ch/index.php

9.3.3 Einzubeziehende Kosten

Alle Preisangaben sind in Schweizer Franken (CHF) und exkl. MwSt. auszuweisen. Der Preis exkl. MwSt. beinhaltet insbesondere Versicherung, Spesen, Sozialabgaben, Transport und Zoll etc.

9.3.4 Bietergemeinschaften

Nicht zugelassen

9.3.5 Subunternehmer

Zugelassen. Zieht der Anbieter zur Leistungserfüllung Subunternehmer bei, übernimmt er die Gesamtverantwortung. Er führt alle beteiligten Subunternehmer mit den ihnen zugewiesenen Rollen auf.

Die charakteristische Leistung ist grundsätzlich vom Anbieter zu erbringen.

9.3.6 Mehrfachbewerbungen von Subunternehmer oder von Bietergemeinschaften

Nur Mehrfachbewerbungen von Subunternehmern sind zugelassen.

9.3.7 Vergütung für die Offerte / Präsentation

Es wird keine Vergütung geleistet.

9.3.8 Sprachen für Angebote

Deutsch

9.3.9 Gültigkeit des Angebots

180 Tage ab Schlusstermin für den Eingang der Angebote.

9.3.10 Sprache der Ausschreibungsunterlagen

Ausschreibungsunterlagen sind in deutscher Sprache erhältlich.

9.3.11 Verfahrenssprache

Das vorliegende Beschaffungsverfahren wird in deutscher Sprache geführt. Dies bedeutet, dass alle Äusserungen seitens der Vergabestelle mindestens in dieser Sprache erfolgen.

9.4 Andere Informationen

9.4.1 Voraussetzung für nicht dem WTO-Abkommen angehörige Länder

Keine

9.4.2 Geschäftsbedingungen

Geschäftsabwicklung gemäss den Allgemeinen Geschäftsbedingungen des Bundes (AGB) für
- Informatikdienstleistungen (Ausgabe Oktober 2010, Stand Januar 2021)
- Werkverträge im Informatikbereich und die Pflege von Individualsoftware (Ausgabe Oktober 2010, Stand Januar 2021)
- Kauf und Wartung von Hardware (Ausgabe Oktober 2010, Stand Januar 2021)
- die Beschaffung und Pflege von Standardsoftware (Ausgabe Oktober 2010, Stand Januar 2021)

Abrufbar unter AGB (admin.ch)

9.4.3 Prüfung und Bereinigung der Angebote

Die Prüfung der Angebote erfolgt gemäss Art. 38 BöB. Eine Bereinigung der Angebote erfolgt ausschliesslich unter den Voraussetzungen und nach Massgabe von Art. 39 BöB sowie auf explizite Aufforderung der Vergabestelle hin.

9.4.4 Geheimhaltung

Die Parteien behandeln alle Tatsachen und Informationen vertraulich, die weder offenkundig noch allgemein zugänglich sind. Im Zweifelsfall sind Tatsachen und Informationen vertraulich zu behandeln. Die Parteien verpflichten sich, alle wirtschaftlich zumutbaren sowie technisch und organisatorisch möglichen Vorkehrungen zu treffen, damit vertrauliche Tatsachen und Informationen gegen den Zugang und die Kenntnisnahme durch Unbefugte wirksam geschützt sind.

Keine Verletzung der Geheimhaltungspflicht liegt vor bei der Weitergabe vertraulicher Informationen durch den Auftraggeber innerhalb des eigenen Konzerns (resp. innerhalb der Bundesverwaltung) oder an beigezogene Dritte. Für den Anbieter gilt dies, soweit die Weitergabe für die Vertragserfüllung erforderlich ist oder Bestimmungen des Vertrages konzernintern weitergegeben werden.

Ohne schriftliche Einwilligung des Auftraggebers darf der Anbieter mit der Tatsache, dass eine Zusammenarbeit mit dem Auftraggeber besteht oder bestand, nicht werben und den Auftraggeber auch nicht als Referenz angeben.

Die Parteien überbinden die Geheimhaltungspflicht auf ihre Mitarbeitenden, Subunternehmer, Unterlieferanten sowie weitere beigezogene Dritte.

9.4.5 Integritätsklausel

Der Anbieter und der Auftraggeber verpflichten sich, alle erforderlichen Massnahmen zur Vermeidung von Korruption zu ergreifen, so dass insbesondere keine Zuwendungen oder andere Vorteile angeboten oder angenommen werden.

Bei Missachtung der Integritätsklausel hat der Anbieter dem Auftraggeber eine Konventionalstrafe zu bezahlen. Diese beträgt 10 % der Vertragssumme, mindestens CHF 3 000 pro Verstoss.

Der Anbieter nimmt zur Kenntnis, dass ein Verstoss gegen die Integritätsklausel in der Regel zur Aufhebung des Zuschlags sowie zu einer vorzeitigen Vertragsauflösung aus wichtigen Gründen durch den Auftraggeber führt.

9.4.6 Sonstige Angaben

Vorbehalten bleiben die Beschaffungsreife des Projektes sowie die Verfügbarkeit der Kredite.
Der Auftraggeber behält sich vor, zugeschlagene Leistungen auch zugunsten weiterer Bedarfsstellen innerhalb der Bundesverwaltung erbringen zu lassen sowie, die als Optionen definierten Leistungen ganz, teilweise oder gar nicht zu beziehen.

10 Anhänge

10.1 Referenzierte Anhänge und Beilagen

Beschreibung	Vom Anbieter auszufüllen	Zur Information
Anhang 01a Angaben zum Anbieter	x	
Anhang 01b Referenz der Unternehmung	x	
Anhang 02 Preisblatt	x	
Anhang 03 Anforderungsliste Selbstevaluation	x	
Anhang 04 Vertragsentwurf		x
Beilage A Selbstdeklaration allgemein	x	
Beilage B Geheimhaltungsverpflichtung für die Herausgabe vertraulicher Unterlagen zur Offerterstellung	x	
Beilage C Kombinationsmatrix		x
Beilage D Übersicht IKT Vorhaben		x
Beilage E Empfehlungen für den Einsatz von Betriebsumgebungen im BIT		x
Beilage F IT-Leitfaden für Lieferanten		x
Beilage G Transliterationstabelle		x
Beilage H IT-Richtlinien für SOAP Webservices +R0065		x
Beilage I IT-Richtlinie R0045		x
Beilage J Richtlinie IT-Sicherheit AD Accounts		x
Beilage K Non-ICAO-Konformität der MRZ		x
Beilage L Schnittstellenbeschreibung SAVIDA		x
Beilage M APS Geräte 2020		x
Beilage N Kryptografie Grundschutz		x
Beilage O A735 Apps im App Store Bund		x
Beilage P Infosheet Betrieb Fachanwendungen BIT		x

Tabelle 23: Übersicht referenzierte Anhänge

10.2 Referenzierte Weisungen und Vorgaben

Nr.	Dokument	Quelle
[1]	AIG	SR 142.20 Bundesgesetz vom 16. Dezember 2005 (Stand am 1 April 2020) über Ausländerinnen und Ausländer und über die Integration https://www.admin.ch/opc/de/classified-compilation/20020232/index.html
[2]	VEV	SR 142.204 Verordnung vom 15. August 2018 (Stand am 1. Januar 2021) über die Einreise und die Visumerteilung https://www.admin.ch/opc/de/classified-compilation/20173253/index.html - a6

[3]	Bearbeitung biometrischer Daten	SR 361.3 Verordnung vom 6. Dezember 2013 (Stand am 1. April 2021) über die Bearbeitung biometrischer erkennungsdienstlicher Daten https://www.admin.ch/opc/de/classified-compilation/20130645/index.html
[4]	Schengener Grenzkodex	Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32016R0399
[5]	Entry/Exit System (EES)	Verordnung (EU) 2017/2225 des Europäischen Parlaments und des Rates vom 30. November 2017 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32017R2225
[6]	Daten EES	Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R2226
[7]	European Travel Information and Authorisation System (ETIAS)	Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018R1240
[8]	Verwendung biometrische Daten EES	Durchführungsbeschluss (EU) 2019/329 der Kommission vom 25. Februar 2019 zur Festlegung der Spezifikationen für die Qualität, Auflösung und Verwendung von Fingerabdrücken und Gesichtsbildern für die biometrische Verifizierung und Identifizierung im Einreise-/Ausreisesystem (EES) https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019D0329
[9]	Vorgabe Transliterationstabelle	Transliterationstabelle Ripol Siehe Beilage G «Transliterationstabelle.pdf»
[10]	ICD euLISA	Schnittstellendokumentation der ICD_euLISA_V1.0

		(Dokumentation kann aufgrund der Klassifizierung erst nach der Unterzeichnung vom Rahmen- und Werkvertrag abgegeben werden)
[11]	ICAO Dokumente Doc 9303	Machine Readable Travel Documents (Part 1- Part 12) http://www.icao.int/publications/pages/publication.aspx?docnum=9303
[12]	DTI Sicherheitsvorgaben	Informationssicherheitsvorgaben des Bundes: • W002 - Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) • Si001 - IKT-Grundschutz in der Bundesverwaltung • Si003 - Netzwerksicherheit in der Bundesverwaltung • P041 - Schutzbedarfsanalyse (Schuban) • P042 - Informationssicherheits- und Datenschutzkonzept (ISDS)
[13]	IT Sicherheit AD Account	Richtlinie IT-Sicherheit AD Account Typen Siehe Beilage J «Richtlinie_IT-Sicherheit_AD_Accounts_V100.pdf»
[14]	Kryptographie	Sicherheitsvorgaben Kryptographie Siehe Beilage N «Kryptographie_Grundschutz_v1-2.pdf»
[15]	IT-Leitfaden für Lieferanten	IT-Leitfaden des BITs für Lieferanten Siehe Beilage F «IT-Leitfaden_für_Lieferanten.pdf»
[16]	R0045 (BIT)	IT Richtlinie Architekturprinzipen zur Technologiearchitektur BIT Siehe Beilage I «IT-Richtlinie R0045.pdf»
[17]	R0065 (BIT)	IT-Richtlinie für SOAP Web Services BIT Seihe Beilage H «IT-Richtlinie für SOAP Webservices +R0065_V1.02.pdf»
[18]	Unterstütze Technologien im BIT	Unterstützte Technologien im BIT Siehe Beilage C «Kombinationsmatrix.xls»
[19]	Betrieb BIT	Betrieb von Fachanwendungen durch BIT: Siehe Beilage P «Infosheet_Betrieb_Fachanwendung_BIT.pdf»
[20]	Betriebsumgebungen im BIT	Empfehlung für den Einsatz von Betriebsumgebungen im BIT Siehe Beilage E «Empfehlung_für_den_Einsatz_von_Betriebsumgebungen_im_BIT.pdf»
[21]	AppStore Bund	Vorgaben für Apps im AppStore Bund Siehe Beilage O «A735_Apps_im_App_Store_Bund_v1-1.pdf»
[22]	APS Geräte 2020	Standard Arbeitsplatzgeräte Bund Siehe Beilage M «APS_Geräte_2020.pdf»
[23]	Nicht ICAO Konformität	Gängige Nicht-ICAO konforme Dokumente: Siehe Beilage K «Non-ICAO-Konformitaet_der_MRZ.pdf»

[24]	SAVIDA	Schnittstellenbeschreibung SAVIDA Siehe Beilage L «Schnittstellenbeschreibung-SAVIDA.pdf»
[25]	Code 39	Code 39 (Barcode) ISO/IEC 16388: https://www.iso.org/standard/43897.html
[26]	Aztec Code	Aztec Code (2D Code) ISO/IEC 24778: https://www.iso.org/standard/41548.html
[27]	Data Matrix	Data Matrix (2D Code) ISO/IEC 16022: https://www.iso.org/standard/44230.html
[28]	QR-Code	QR-Code (2D Code) ISO/IEC 18004: https://www.iso.org/standard/62021.html
[29]	PDF417	PDF417 (2D Code) ISO/IEC 15438: https://www.iso.org/standard/65502.html

Tabelle 24: Referenzierte Weisungen und Vorgaben

10.3 Weiterführende Informationen

Nr.	Dokument	Quelle
[30]	Interpol-Verordnung	SR 366.1 Verordnung vom 21. Juni 2013 (Stand am 1. Januar 2019) über das Nationale Zentralbüro Interpol Bern (Interpol Verordnung) https://www.admin.ch/opc/de/classified-compilation/20130208/index.html
[31]	Ausweisgesetz	SR 143.1 Bundesgesetz vom 22. Juni 2001 (Stand am 1. Januar 2018) über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG) https://www.admin.ch/opc/de/classified-compilation/19994375/index.html
[32]	ISA-Verordnung	SR 143.111 Verordnung des EJPD vom 16. Februar 2010 (Stand am 1. Januar 2019) über die Ausweise für Schweizer Staatsangehörige https://www.admin.ch/opc/de/classified-compilation/20092157/index.html
[33]	BPI	SR 361 Bundesgesetz vom 13. Juni 2008 (Stand am 1. März 2019) über die polizeilichen Informationssysteme des Bundes https://www.admin.ch/opc/de/classified-compilation/20032054/index.html
[34]	RIPOL-Verordnung	SR 361.0 Verordnung vom 26. Oktober 2016 (Stand am 1. April 2021) über das automatisierte Polizeifahndungssystem https://www.admin.ch/opc/de/classified-compilation/20161966/index.html
[35]	N-SIS-Verordnung	SR 362.0 Verordnung vom 8. März 2013 (Stand am 1. April 2021) über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro https://www.admin.ch/opc/de/classified-compilation/20111704/index.html
[36]	BGIAA	SR 142.51 Bundesgesetz vom 20. Juni 2003 (Stand am 1. April 2020) über das Informationssystem für den Ausländer- und den Asylbereich https://www.admin.ch/opc/de/classified-compilation/20020693/index.html
[37]	ZEMIS-Verordnung	SR 142.513 Verordnung vom 12. April 2006 (Stand am 1. April 2021) über das Zentrale Migrationsinformationssystem https://www.admin.ch/opc/de/classified-compilation/20050566/index.html
[38]	HOOGAN-Verordnung	SR 120.52 Verordnung vom 4. Dezember 2009 (Stand am 1. April 2021) über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN (VVMH) https://www.fedlex.admin.ch/eli/cc/2009/847/de
[39]	Visa-Informationssystem-Verordnung, VISV	SR 142.512 Verordnung vom 18. Dezember 2013 (Stand am 1. April 2021) über das zentrale Visa-Informationssystem und das nationale Visumsystem https://www.fedlex.admin.ch/eli/cc/2014/2/de

[40]	IKT Vorgaben Bund	IKT Vorgaben Bund: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/alle-ikt-vorgaben.html
[41]	Übersicht IKT Vorgaben BIT	Übersicht IKT-Vorgaben: Informationen für die Leistungsbezüger des BIT Siehe Beilage D «Uebersicht _KT_Vorgaben.pdf»
[42]	Strategie der integrierten Grenzverwaltung 2027	Strategie der integrierten Grenzverwaltung 2027 https://www.sem.admin.ch/dam/data/sem/einreise/ibm/strategie-ibm-2027-d.pdf
[43]	Integrierte Grenzverwaltung IBM	Integrierte Grenzverwaltung IBM https://www.sem.admin.ch/sem/de/home/themen/einreise/ibm.html
[44]	Bundesgesetz über den Datenschutz (DSG)	Bundesgesetz über den Datenschutz (DSG, SR 235.1) https://www.admin.ch/opc/de/classified-compilation/19920153/index.html
[45]	Verordnung zum Bundesgesetz über den Datenschutz	Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR. 235.11) https://www.admin.ch/opc/de/classified-compilation/19930159/index.html
[46]	Bundesinformatikverordnung, BinfV	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung; BinfV, SR. 172.010.58) https://www.admin.ch/opc/de/classified-compilation/20081009/index.html
[47]	Informationsschutzverordnung (ISchV)	Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV, SR 510.411) https://www.admin.ch/opc/de/classified-compilation/20070574/index.html
[48]	Verordnung über die Bearbeitung von Personendaten	Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442) https://www.admin.ch/opc/de/classified-compilation/20111415/index.html
[49]	Informationsschutzverordnung (ISchV)	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV, SR 120.73) https://www.fedlex.admin.ch/eli/cc/2020/416/de/
[50]	Archivierungsgesetz (BGA)	Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA, SR 152.1) https://www.admin.ch/opc/de/classified-compilation/19994756/index.html
[51]	Online-Weisung EJPD	Weisung vom 12. August 2013 über den Zugriff auf die Fachanwendungen des EJPD (Online-Weisung EJPD) (Dokument kann aufgrund der Klassifizierung erst nach der Unterzeichnung vom Rahmen- und Werkvertrag abgegeben werden)

[52]	EJPD Webservice Richtlinie	Richtlinie für Zugriffe auf EJPD Informatikanwendungen via Webservice Schnittstellen (EJPD Webservice Richtlinie) (Dokument kann aufgrund der Klassifizierung erst nach der Unterzeichnung vom Rahmen- und Werkvertrag abgegeben werden)
[53]	ICAO Best Practise für optische MRTD	MRTD Best Practice Guidelines for Optical Machine Authentication: https://www.icao.int/Security/FAL/TRIP/Documents/Best%20Practice%20Guidelines%20for%20Optical%20Machine%20Authentication%20V1.2.pdf
[54]	ISO / IEC DIS 7816 1-4	Identification cards - Integrated circuit cards: Part 1: Cards with contacts - Physical characteristics Part 2: Cards with contacts - Dimensions and location of the contacts Part 3: Cards with contacts - Electrical interface and transmission protocols Part 4: Organization, security and commands for interchange --- https://www.iec.org/ https://www.vde-verlag.de/iec-normen.html
[55]	Technischen Standards für biometrische Merkmale für die Einrichtung des Visa-Informationssystems	2006/648/EG: Entscheidung der Kommission vom 22. September 2006 über die technischen Standards für biometrische Merkmale im Hinblick auf die Einrichtung des Visa-Informationssystems (Bekannt gegeben unter Aktenzeichen K(2006) 3699) EUR-Lex - 32006D0648 - EN - EUR-Lex (europa.eu)

Tabelle 25: Weiterführende Informationen