BRZ

**Bundesrechenzentrum GmbH**

**in Zusammenarbeit mit**

SCHIEFER
VERGABE · RECHT · ANWÄLTE

**und**

42 virtual

# Verhandlungsverfahren mit vorheriger EU-weiter Bekanntmachung

## „Ausweisplattform“

# AUSSCHREIBUNGSUNTERLAGE

**Geschäftszahl BRZ 2020-0.186.733**

| | | |
|---|---|---|
| **Abgabe und Einreichungsform des Angebotes**<br><br>Alle Bestandteile des Angebots sind **ausschließlich in elektronischer Form am Beschaffungsportal der vergebenden Stelle unter https://schiefer.vemap.com einzureichen.** Alle Bestandteile des Angebotes sind entsprechend elektronisch auszufüllen bzw. zu erstellen, einzuscannen und elektronisch auf das Beschaffungsportal hochzuladen (insbesondere Beilagen).<br><br>Die Angebote müssen mit einer **qualifizierten elektronischen Signatur** abgegeben werden.<br><br>Unterlagen in Papierform werden ebenso wenig berücksichtigt wie eine Einreichung per Fax oder per E-Mail. | | **Anfragen** bis längstens<br>22.09.2020, 12:00 Uhr (Einlangen)<br>Anfragen bzw Anfragenbeantwortungen sind ausschließlich über das Beschaffungsportal zu stellen bzw herunterzuladen.<br><br>**Ende der Angebotsfrist**<br>09.10.2020, 12:00 Uhr (Einlangen)<br><br>**Verhandlungsrunde**<br>voraussichtlich 21. bis 23.10.2020<br>Gesonderte Einladung folgt |

# Erstangebot

| Allgemeine Informationen | |
|---|---|
| **Auftraggeber** | **Bundesrechenzentrum GmbH**<br>Hintere Zollamtsstraße 4<br>A-1030 Wien |
| **vergebende Stelle** | **Schiefer Rechtsanwälte GmbH**<br>Rooseveltplatz 4-5/5<br>1090 Wien |
| **Leistungsgegenstand** | Lieferung, Implementierung, Wartung und Support sowie Weiterentwicklung einer IT-Lösung zur Umsetzung einer Ausweisplattform |
| **Verfahrensart** | Verhandlungsverfahren mit Bekanntmachung im Oberschwellenbereich gemäß § 31 Abs 5 BVergG 2018 zum Abschluss einer Rahmenvereinbarung |
| **Erfüllungsort** | Österreich |
| **Leistungsbeginn** | voraussichtlich Jänner 2021 |
| **Kontakt** | Dr. Ralf Blaha<br>brz-ausweisplattform@schiefer.at |

# INHALTSVERZEICHNIS

# 1. ALLGEMEINE AUSSCHREIBUNGSBESTIMMUNGEN

## 1.1 Auftraggeber

Auftraggeber ist die

**Bundesrechenzentrum GmbH**
Hintere Zollamtsstraße 4
A-1030 Wien
(in der Folge „**Auftraggeber**“ oder „**BRZ**“ genannt).

Soweit in den Ausschreibungsunterlagen personenbezogene Bezeichnungen nur in männlicher oder weiblicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

## 1.2 Vergebende Stelle

Vergebende Stelle ist die

**Schiefer Rechtsanwälte GmbH**
Rooseveltplatz 4-5/5
1090 Wien

Die Schiefer Rechtsanwälte GmbH erklärt im Hinblick auf § 11 der Richtlinien für die Ausübung des Rechtsanwaltsberufes, für die Überwachung der Pflichten des Rechtsanwaltes und für die Ausbildung der Rechtsanwaltsanwärter (RL-BA 2015 idgF), dass sie in einem allfälligen Rechtsstreit zwischen dem Auftraggeber einerseits und einem Bieter oder Bewerber andererseits ausschließlich den Auftraggeber vertreten wird.

## 1.3 Technische Verfahrensbegleitung

Die technische Verfahrensbegleitung erfolgt durch die

**42 virtual Business Services GmbH**
Palais Savoy
Johannesgasse 15/3
1010 Wien

## 1.4 Beitrittsrechte

Siehe Punkt 2 der Rahmenvereinbarung.

## 1.5 Verfahrensart, Vergabekontrollbehörde

Das Vergabeverfahren wird als Verhandlungsverfahren nach vorheriger EU-weiter Bekanntmachung zum Abschluss einer Rahmenvereinbarung mit einem Unternehmen gemäß § 31 Abs 5 Bundesvergabegesetz 2018, BGBl I Nr 65/2018 idgF (in der Folge „**BVergG**“) durchgeführt. Es handelt sich um die Vergabe eines Auftrages im Oberschwellenbereich.

Die zuständige Stelle für Nachprüfungsverfahren ist das

**Bundesverwaltungsgericht**
Erdbergstraße 192-196, 1030 Wien
E-Mail: einlaufstelle@bvwg.gv.at
Telefon: +43/1/601 49 – 0
Telefax: +43/1/531 09 – 153357/153364

Als Verfahrenssprache für das gegenständliche Vergabeverfahren und die nachfolgende Leistungserbringung wird Deutsch festgelegt.

## 1.6 Ausschreibungsunterlagen

Mit Zulassung zur zweiten Stufe werden den Bewerbern die detaillierten Ausschreibungsunterlagen (insbesondere Leistungsbeschreibung sowie die Beilagen zur Ausschreibungsunterlage) zur Verfügung gestellt. Der Auftraggeber behält sich gemäß § 101 BVergG vor, Berichtigungen und Ergänzungen zu den Ausschreibungsunterlagen innerhalb der Angebotsfrist vorzunehmen und diese allen Bietern schriftlich mitzuteilen. Sofern der Umfang oder der Zeitpunkt der Ergänzungen es erforderlich macht, wird der Auftraggeber die Angebotsfrist erstrecken. Der Bieter ist verpflichtet, diese Berichtigungen und Ergänzungen bei seiner Angebotslegung zu berücksichtigen.

Die Ausschreibungsunterlagen werden kostenlos an den Bewerber übergeben. Alle Ausschreibungsunterlagen sind urheberrechtlich geschützt. Die Weitergabe der Ausschreibungsunterlagen im Original, als Kopie oder elektronisch ist nur in dem Umfang gestattet, als die Weitergabe zur Erstellung des Angebotes erforderlich ist (zB Weitergabe an Subunternehmer). Eine darüberhinausgehende Weitergabe ist nicht gestattet.

## 1.7 Vertraulichkeit

Die Bieter nehmen zur Kenntnis, dass der Text des gegenständlichen Formulars des Auftraggebers urheberrechtlich geschützt ist.

Der Bieter verpflichtet sich während und auch nach der Durchführung oder Beendigung des Vergabeverfahrens zur Geheimhaltung der Teilnahme- und Ausschreibungsunterlagen sowie von Geschäfts- und Betriebsgeheimnissen des Auftraggebers. Diese Verpflichtung des Bieters gilt örtlich und zeitlich unbeschränkt und auch gegenüber mit dem Bieter verbundenen Unternehmen.

Die vom Auftraggeber zur Verfügung gestellten Unterlagen dürfen vom Bieter nicht an andere Personen oder Institutionen weitergegeben und nur zum Zwecke der Erstellung des Angebotes verwendet werden. Davon ausgenommen sind Berater des Bieters, insoweit diese Berater beruflich zur Verschwiegenheit verpflichtet sind oder insoweit der Bieter diese Berater nachweislich zur Wahrung der Vertraulichkeit verpflichtet hat und letztere diese Verpflichtung nachweislich gegenüber dem Bieter abgegeben haben. Ausgenommen sind weiters mögliche Partner des Bieters, insoweit auch diese nachweislich zur Wahrung der Vertraulichkeit verpflichtet wurden und sich nachweislich gegenüber dem Bieter solcher Art verpflichtet haben, sowie Referenzauftraggeber, denen der Bieter Formulare aus dem Beilagenteil übermittelt.

Darüber hinaus verpflichtet sich der Bieter, auch gegenüber den Medien bis zur Zuschlagserteilung keine Informationen über den Umstand seiner Beteiligung, den Stand des Vergabeverfahrens oder sonstige Umstände der gegenständlichen Ausschreibung zu erteilen. Ein Verstoß gegen diese Verschwiegenheitspflicht kann zum Ausscheiden des betreffenden Bieters führen.

Der Bieter hat diese Verpflichtungen jedenfalls an Dritte zu überbinden (zB an Subunternehmer).

Der Auftraggeber wird den vertraulichen Charakter aller die Bieter und deren Unterlagen betreffenden Angaben gegenüber Dritten wahren.

Mit der Abgabe des Teilnahmeantrags hat der Bieter die Bedingungen des Auftragsverarbeitervertrages des Auftraggebers, soweit dieser im Vergabeverfahren anwendbar ist, akzeptiert und wird diese weiterhin einhalten.

## 1.8 Verfahrensablauf

Der Auftraggeber führt das Verhandlungsverfahren als zweistufiges Verfahren durch.

Mit Übermittlung der Zulassungen ist die 2. Stufe des Verhandlungsverfahrens eingeleitet. Der Auftraggeber lädt die drei bestgereihten ausgewählten Bewerber zur Angebotslegung ein.

Der Ablauf des Verhandlungsverfahrens in der zweiten Stufe ist wie folgt vorgesehen:

a. Schriftliche Anfragen zu den Ausschreibungsunterlagen sind bis zu dem auf Seite 2 vorgesehenen Zeitpunkt in deutscher Sprache auf die Vergabeplattform hochzuladen.

b. Der Auftraggeber wird den Bietern eine konsolidierte Fragenbeantwortung zur Verfügung stellen, die bei der Legung des Erstangebotes zwingend zu berücksichtigen ist.

c. Das Erstangebot ist bis spätestens zu dem auf Seite 2 vorgesehenen Zeitpunkt zu legen. Das Erstangebot muss ausschreibungskonform sein.

   Die Öffnung der Erstangebote erfolgt nach Ablauf der Angebotsfrist und wird kommissionell durchgeführt. Die Teilnahme der Bieter an der Öffnung ist nicht gestattet.

   Dem Bieter steht es frei, gleichzeitig mit seinem Angebot Verhandlungsvorschläge für die auf die Abgabe des Erstangebotes folgende Verhandlungsrunde einzureichen, in denen zu einzelnen Vertragsbestimmungen (**Anlage ./1**) abweichende Vorschläge konkreter Art enthalten sind, welche der Bieter zum Gegenstand der Vertragsverhandlungen zu machen beabsichtigt.

   Diese Verhandlungsvorschläge müssen hinreichend substantiiert sein, um als solche zum Gegenstand der Vertragsverhandlungen gemacht werden zu können. Nicht ausreichend wäre daher bspw ein bloßer Verweis darauf, dass eine Vertragsbestimmung „noch zu diskutieren“, „noch zu verhandeln“ oder „nicht akzeptabel“ ist. Der Vorschlag einer ersatzlosen Streichung einer genau bezeichneten Vertragsbestimmung wäre hingegen zulässig. Die Verhandlungsvorschläge sind in einem eigenem Dokument (**Beilage ./3**) einzureichen.

   Der Auftraggeber behält sich die Entscheidung vor, solche Verhandlungsvorschläge abzulehnen, oder zu akzeptieren und die vorgeschlagenen Vertragsbestimmungen entsprechend anzupassen.

   Der Auftraggeber beabsichtigt, die Verhandlungen zu einem zügigen Abschluss zu bringen. Er erwartet daher, dass sich allfällige Verhandlungsvorschläge der Bieter auf Punkte von erheblicher wirtschaftlicher Bedeutung beschränken. Es obliegt dem Bieter, die Bedeutung seiner Verhandlungsvorschläge und insbesondere den daraus resultierenden Vorteil für den Auftraggeber mit seinen Verhandlungsvorschlägen zu erläutern bzw. in den Verhandlungsgesprächen konkret darzulegen.

d. Der Auftraggeber wird mit allen Bietern, die ein ausschreibungskonformes Angebot gelegt haben, über ihre Angebote verhandeln. Es ist eine Verhandlungsrunde mit jedem Bieter, der ein ausschreibungskonformes Angebot gelegt hat, vorgesehen (voraussichtliche Termine siehe Seite 2).

   Die Verhandlungen werden in fachlicher sowie in rechtlich/kommerzieller Hinsicht geführt. Diese Verhandlungsrunde findet in Wien statt. Die genaue Uhrzeit und der genaue Ort werden mit gesonderter Einladung bekannt gegeben.

   Auf Bieterseite dürfen gleichzeitig maximal 5 Personen an der Verhandlung teilnehmen, darunter zwingend eine der in der ersten Stufe namhaft gemachten Schlüsselpersonen.

Ein Austausch von Teilnehmern während der Verhandlung ist zulässig. Der Auftraggeber behält sich ausdrücklich vor, weitere Verhandlungsrunden durchzuführen Verhandlungen über die Zuschlagskriterien sowie die bereits in der Teilnahmeunterlage festgelegten Mindestanforderungen sind ausgeschlossen.

Der Auftraggeber behält es sich vor, die Verhandlungen mittels Videokonferenz durchzuführen.

Weiter behält es sich der Auftraggeber vor, vor Aufforderung zur Abgabe der Letztangebote eine zweite Angebots- und Verhandlungsrunde durchzuführen. Das Vorgehen erfolgt dabei analog zur ersten Angebots- und Verhandlungsrunde.

e. Nach den Verhandlungen werden die Bieter aufgefordert, ihre Letztangebote abzugeben. Der Auftraggeber wird den Bietern dazu vorab den Abschluss der Verhandlungen bekannt geben und diese unter gleichzeitigen Hochladens allenfalls geänderter Ausschreibungsunterlagen auf die Vergabeplattform zur Abgabe der Letztangebote einladen.

f. In der Folge wird der Auftraggeber die Letztangebote bewerten und mit dem Bieter, welcher das wirtschaftlich und technisch günstigste Angebot gelegt hat, die Rahmenvereinbarung abschließen.

Der Auftraggeber behält sich jedoch in diesem Zusammenhang vor, mit dem bestgereihten Bieter vor der Auswahlentscheidung noch Exklusivverhandlungen zu führen. Sollten diese Verhandlungen nicht erfolgreich abgeschlossen werden, behält es sich der Auftraggeber vor, entweder Exklusivverhandlungen mit den anderen Bietern (Bieter mit dem zweitbestgereihten Angebot, Bieter mit dem drittbestgereihten Angebot) zu führen oder nochmals mit allen oder einzelnen verbliebenen Bietern gleichzeitig zu verhandeln.

g. Die Angebote gemäß lit c und e sind auf Basis folgender Ausschreibungsunterlagen (jeweils in der Fassung für das Erstangebot bzw für das Letztangebot) zu erstellen:

- Allfällige Fragenbeantwortung(en) zu den Ausschreibungsunterlagen;
- Bietererklärung gemäß Beilage ./0.1 der Ausschreibungsunterlage;
- gegenständliche Ausschreibungsunterlage;
- Rahmenvereinbarung (**Anlage ./1**);
- weitere Beilagen der Ausschreibungsunterlage.

### 1.9 Vollständigkeit der Angebote

Die Angebote müssen, um vollständig zu sein, alle in den Ausschreibungsunterlagen (insbesondere in der Rahmenvereinbarung) enthaltenen Vorgaben abdecken. Wird ein MUSS-Kriterium im Angebot nicht erfüllt, stellt dies einen Ausscheidensgrund nach § 141 Abs 1 Z 7 BVergG dar.

### 1.10 Preise und Rechenfehler

Die Angebotspreise sind im Preisangebotsverfahren (ohne Richtpreise der Auftraggeber) zu erstellen. Gefordert werden Preise in EUR inklusive aller Gebühren und Abgaben, exklusive der gesetzlichen Umsatzsteuer. Nachlässe oder Preisminderungen sind in die Preise zu inkludieren. Sämtliche anfallenden Nebenkosten sind in die angebotenen Preise zu inkludieren. Erklärungen an anderer Stelle, die Auswirkungen auf den Preis haben, werden bei der Bewertung des Angebotes nicht berücksichtigt.

Die Preisangaben im Preisblatt (Beilage ./1) haben bis 31.12.2021 als Festpreise zu erfolgen. Ein Festpreis ist ein Preis, der auch bei Eintreten von Änderungen der Preisgrundlagen (wie insbesondere Kollektivvertragslöhne, Materialpreis, soziale Aufwendungen) unveränderlich bleibt. Näheres dazu ist in der Rahmenvereinbarung festgelegt.

Zur Bewertung wird ein bewertungsrelevanter Gesamtpreis gebildet. Bei Abweichungen zwischen den auf der Vergabeplattform im Leistungsverzeichnis angegebenen Preisen und den entsprechenden Angaben im Preisblatt, sind die Angaben des Bieters im Preisblatt verbindlich.

Rechnerisch fehlerhafte Angebote werden nicht ausgeschieden, eine Vorreihung infolge Berichtigung eines Rechenfehlers ist zulässig. Allfällige im Zuge einer vertieften Angebotsprüfung vorgelegte Kalkulationsblätter werden nicht Vertragsbestandteil.

### 1.11 Einhaltung des österreichischen Arbeits- und Sozialrechts

Bei der Erstellung des Angebotes ist zu berücksichtigen, dass für in Österreich zu erbringende Leistungen die in Österreich geltenden arbeits- und sozialrechtlichen Vorschriften einzuhalten sind. Auch im Auftragsfall hat der Bieter bzw zukünftige Auftragnehmer diese Vorschriften, soweit die Leistungen in Österreich erbracht werden, einzuhalten.

Der Bieter hat darüber hinaus die sich aus den Übereinkommen Nr 29, 87, 94, 95, 98, 100, 105, 111, 138, 182 und 183 der Internationalen Arbeitsorganisation, BGBl Nr 228/1950, Nr 20/1952, Nr 39/1954, Nr 81/1958, Nr 86/1961, Nr 111/1973, BGBl III Nr 200/2001, BGBl III Nr 41/2002 und BGBl III Nr 105/2004, ergebenden Verpflichtungen einzuhalten.

Auskünfte über die bei der Durchführung des Auftrages geltenden arbeits- und sozialrechtlichen Vorschriften erteilen die örtlich zuständigen Gliederungen der gesetzlichen Interessensvertretungen der Arbeitgeber und der Arbeitnehmer.

### 1.12 Bietergemeinschaften

Bieter bzw Bietergemeinschaften haben ihre Angebote in der Zusammensetzung abzugeben, in der sie zur Angebotslegung eingeladen wurden. Die nachträgliche Bildung von Bietergemeinschaften oder ein Wechsel von Mitgliedern einer solchen ist unzulässig. Wird dem Angebot einer Bietergemeinschaft zugeschlagen, so haben die erfolgreichen Bieter eine Arbeitsgemeinschaft (ARGE) zu bilden.

Alle Mitglieder der Arbeitsgemeinschaft sind zur vertragsgemäßen Erbringung der Leistungen und sonstigen Verpflichtungen aus dem Vertrag solidarisch verpflichtet. Die Arbeitsgemeinschaft hat dem Auftraggeber einen in allen Belangen der Vertragsabwicklung bevollmächtigten Vertreter (Federführer) schriftlich zu benennen. Allfällige Änderungen in der Person des für die Arbeitsgemeinschaft Bevollmächtigten sind ebenso schriftlich bekannt zu geben. Einschränkungen des Umfanges der Vollmacht(en) des Vertreters der Arbeitsgemeinschaft sind unwirksam.

Wenn von der Arbeitsgemeinschaft kein zur Abwicklung des Vertrages bevollmächtigter Vertreter namhaft gemacht wird oder dieser nicht mehr vorhanden ist, kann der Vertrag mit jedem beliebigen Mitglied der Arbeitsgemeinschaft mit Wirksamkeit für sämtliche Mitglieder derselben abgewickelt werden. Erklärungen eines ARGE-Partners oder Erklärungen an diesen, gelten in diesem Fall als von allen und gegenüber allen bindend abgegeben.

### 1.13 Subunternehmer

Es gelten die entsprechenden Vorgaben des Auftraggebers in der Teilnahmeunterlage, insbesondere die Festlegungen zu den kritischen Leistungsteilen (Punkt 2.8.2 der Teilnahmeunterlage). Die Weitergabe von Teilen der Leistung an Subunternehmer durch den Bieter ist darüber hinaus nur bis zu jenem Ausmaß zulässig, auf das sich der Bieter im Eignungs- und Auswahlverfahren festgelegt hat.

Während des Vergabeverfahrens hat der Bieter bzw Auftragnehmer jeden beabsichtigten Wechsel eines Subunternehmers oder jede beabsichtigte Hinzuziehung eines nicht im Teil-

nahmeantrag bzw Angebot bekannt gegebenen Subunternehmers dem Auftraggeber schriftlich und unter Anschluss aller zur Prüfung der Eignung des betreffenden Subunternehmers erforderlichen Nachweise mitzuteilen.

Jede allfällige Abweichung von den im Teilnahmeantrag gemachten Angaben ist dem Auftraggeber im Begleitschreiben zum Angebot anzuzeigen und in der Liste der Subunternehmer **Formblatt [SUL-AU]** besonders auszuweisen.

Sofern weitere bzw zusätzliche Subunternehmer hinzugezogen werden sollen, hat der Bieter – unter sinngemäßer Anwendung der Eignungsvoraussetzungen im Teilnahmeantrag – eine Subunternehmererklärung gemäß **Beilage [SUE-AU] zu Formblatt [SUL-AU]** vorzulegen.

Durch den Wechsel bzw die Hinzuziehung weiterer Subunternehmer darf sich keine Schlechterstellung des Auftraggebers ergeben. Die Beweislast diesbezüglich trifft den zukünftigen Auftragnehmer.

Auf Verlangen des Auftraggebers hat der zukünftige Auftragnehmer die mit seinen Subunternehmern in kommerzieller Hinsicht geschlossenen Vereinbarungen dem Auftraggeber zur Einsicht vorzulegen.

### 1.14 Mehrfachbeteiligung

Im Falle einer Mehrfachbeteiligung durch ein Unternehmen – sei es als Bieter oder Mitglied einer Bietergemeinschaft – haben diese Bieter nach Aufforderung des Aufraggebers unverzüglich einen ausreichenden Nachweis zu erbringen, dass

- sich das Verhältnis der betroffenen Unternehmer zueinander nicht auf das Verhalten im Rahmen des Vergabeverfahrens auswirkt,
- keine Beeinträchtigung des Wettbewerbs besteht, und
- die Angebote völlig unabhängig voneinander kalkuliert und erstellt werden.

Sofern der Nachweis nicht innerhalb der vom Auftraggeber vorgegebenen Frist erbracht wird, wird das Angebot im weiteren Verfahren nicht mehr berücksichtigt

### 1.15 Unzulässigkeit von Teilangeboten

Teilangebote bloß für einen Teil der Leistung sind gemäß § 125 Abs 3 BVergG unzulässig und führen zum Ausscheiden des Angebotes.

### 1.16 Alternativ- und Abänderungsangebote

Alternativangebote und Abänderungsangebote sind unzulässig.

### 1.17 Zuschlagsfrist

Die Zuschlagsfrist beträgt 5 Monate, gerechnet ab dem Ende der Angebotsfrist für das Letztangebot (Last and Best Offer). Der Bieter ist ab Abgabe seines Erstangebotes bis zum Ablauf der Zuschlagsfrist an seine jeweiligen Angebote gebunden, ein Zuschlag auf das gelegte Erstangebot ist nicht vorgesehen.

Für den Fall, dass der Bieter auf ausdrückliches Ersuchen des Auftraggebers einer Verlängerung der Angebotsbindung zustimmt, ist er bis zum vereinbarten Termin an sein Angebot gebunden.

### 1.18 Unklarheiten in den Ausschreibungsunterlagen

Der Bieter hat die Ausschreibungsunterlagen auf Vollständigkeit zu prüfen. Der Bieter bestätigt mit der Abgabe des Angebotes, dass die Leistungen in den Ausschreibungsunterlagen vollständig beschrieben sind und auch keine Teilleistungen fehlen, die zur einwandfreien Erfüllung der Rahmenvereinbarung notwendig sind. Bestehen nach Ansicht des Bieters bei der Auslegung des Ausschreibungstextes mehrere Möglichkeiten bzw erscheint etwas unklar, so hat der Bieter vor Abgabe des Angebotes eine Klärung mit dem Auftraggeber herbeizuführen. Nach Vertragsabschluss gilt die für den Auftraggeber günstigste Auslegung als vereinbart.

### 1.19 Berichtigungen und Ergänzungen

Der Auftraggeber behält sich vor, Berichtigungen und Ergänzungen zu den Ausschreibungsunterlagen innerhalb der Angebotsfrist vorzunehmen und diese allen Bietern schriftlich mitzuteilen. Sofern der Umfang oder der Zeitpunkt der Ergänzungen es erforderlich macht, wird der Auftraggeber die Angebotsfrist erstrecken. Der Bieter ist verpflichtet, diese Berichtigungen und Ergänzungen bei seiner Angebotslegung zu berücksichtigen.

### 1.20 Rügepflicht

Sollten sich für den Bieter bei Prüfung der Ausschreibungsunterlagen Widersprüche, sonstige Unklarheiten oder (vermutete) Verstöße gegen Vergabebestimmungen ergeben, so hat er dies dem Auftraggeber umgehend mitzuteilen. Mit Angebotsabgabe bestätigt der Bieter, dass die Ausschreibungsunterlagen einer vollständigen Prüfung unterzogen worden sind, dass die Ausschreibungsbestimmungen den gesetzlichen Vorgaben (insbesondere dem BVergG) entsprechen, dass die Ausschreibungsunterlagen zur Kalkulation des Angebotes ausreichend sind, und dass der Bieter die zu erbringenden Leistungen sowie alle damit verbundenen Kosten mit der erforderlichen Genauigkeit beurteilen kann. Mit Abgabe des Angebotes bestätigt der Bieter darüber hinaus, dass (Kalkulations-) Irrtümer sowie Fehleinschätzungen in Zusammenhang mit der Erstellung seines Angebotes einen Teil des Unternehmensrisikos darstellen und zu seinen Lasten gehen. Eine Irrtumsanfechtung aus diesen Gründen ist daher ausgeschlossen.

### 1.21 Wesentliche Änderungen der wirtschaftlichen Rahmenbedingungen

Der Auftraggeber behält es sich vor, bei einer wesentlichen Änderung der wirtschaftlichen Rahmenbedingungen (insbesondere bei einer Verweigerung der Genehmigung durch die zuständigen Gremien) von einer Vergabe der Leistungen Abstand zu nehmen, den vorgesehenen Zeitrahmen zu erstrecken oder das Verfahren zu widerrufen.

Diese Bestimmung berührt nicht das Recht des Auftraggebers, das gegenständliche Vergabeverfahren allenfalls aus anderen Gründen zu widerrufen.

## 2. LEISTUNGSBESCHREIBUNG

### 2.1 Einführung

Gegenstand der Ausschreibung ist eine erweiterbare **Ausweisplattform**.

Ein **Ausweis** ist ein Set von Attributen, das für einen bestimmten Anwendungsfall zusammengestellt wird und in einer App auf einem mobilen Endgerät (verschlüsselt oder nicht verschlüsselt) präsentiert werden kann; der hier verwendete Begriff „Ausweis“ entspricht sohin nicht dem „herkömmlichen“ Sichtausweis aus Papier oder Kunststoff.

Über dokumentierte Schnittstellen müssen weitere Ausweisquellen und mobile Apps auch durch Dritte angebunden werden können. Diese Plattform wird insbesondere in Kapitel 2.2 beschrieben.

Die Ausweisplattform muss vier Szenarien implementieren.

Die benötigten Szenarien werden in Kapitel 2.3 beschrieben. Ein **Szenario** ist die technische Umsetzung einer Ausweispräsentation gegenüber Personen oder Online-Services.

Auf dieser Ausweisplattform aufbauend werden dann konkrete Anwendungsfälle umgesetzt. Ein **Anwendungsfall** ist die fachliche Anwendung einer Kombination aus Ausweisdaten und einem Szenario.
In Kapitel 2.4 werden alle derzeit benötigten Anwendungsfälle beschrieben.

Um rasch erste Ergebnisse präsentieren zu können, soll ein Pilot aufgebaut werden. In Kapitel 2.5 wird der Umfang des Pilotbetriebs beschrieben.

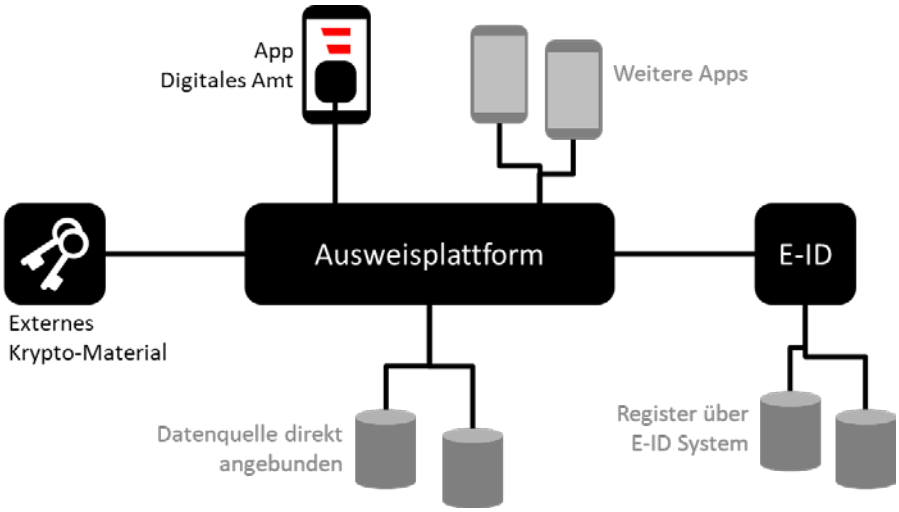
Die gesamte Lösung besteht aus:

- Erweiterbarer Plattform
- Auf dieser Plattform abgebildeten Szenarien
- Mit diesen Szenarien umgesetzte Anwendungsfälle
- Pilotaufbau

In Kapitel 2.6 sind alle Konzepte aufgelistet, die der Bieter erstellen muss, um die Lösung zu beschreiben. Der Leistungsumfang jedes Konzepts muss auch bepreist werden.

Für diese Ausschreibungsunterlage gelten auch die in der Teilnahmeunterlage angeführten Mindestanforderungen und Anforderungen – siehe dort Kapitel 3.3 und 3.4. In diesem Dokument werden diese, soweit erforderlich, konkretisiert. Siehe dazu insbesondere Kapitel 7.1 bis 7.8.

## 2.2 Plattform Überblick




Der Leistungsgegenstand umfasst im Kern eine erweiterbare, generische Ausweisplattform. Diese zeichnet sich durch folgende Eigenschaften aus:

- Die Plattform muss im BRZ oder bei Abrufberechtigten on-premises ohne Anbindung an eine Cloud betrieben werden können.
- Weder die Plattform noch Teile davon dürfen Verbindung zu anderen als den in den Schnittstellen definierten und für die jeweilige Instanz konfigurierten Services/Servern aufnehmen. Insbesondere sind Verbindungen mit Cloudservices des Anbieters oder Dritter zu unterbinden.
- Die Lösung darf kein kombiniertes System aus Hard- und Software sein, der Betriebssystem- und Netzwerklayer muss in der Hoheit des Auftraggebers liegen (keine Appliance).

- Der Bieter muss für die Lösung alle erforderlichen 3rd Party Lizenzen (oberhalb des Betriebssystems) aus dem Sizing mitanbieten bzw. im Preisblatt bepreisen.
- Die Plattform verwendet externes kryptographisches Material.
- Die Plattform verwendet ein elektronisches Identitätsverzeichnis, im Kontext der Bundesverwaltung das bestehende E-ID-System (elektronischer Identitätsnachweis https://eid.egiz.gv.at/?page_id=2900), für die Identitäten der Benutzer wie auch für die Anbindung von Registern/Ausweisquellen.
- Alle Schnittstellen sind derart zu gestalten, dass neben den o.g. Systemen auch alternative Identitätsverzeichnisse und Krypto-Stores integriert werden können.
- Über das E-ID-System können verschiedenste Attribute aus dahinterliegenden Registern geladen werden. Die Verwendung von diesen Attributen muss nur über Konfiguration der Plattform möglich sein.
- Weitere Ausweise/Attribute sowie weitere mobile Apps der Verwaltung oder von privaten Organisationen müssen durch den Auftraggeber selbst oder durch ihn beauftragte Dritte über definierte Schnittstellen an die Plattform angebunden werden können, ohne dass das Kernsystem re-startet, neu deployed bzw. programmatisch angepasst werden muss.

- Die Ausweisplattform muss in die bestehende App „Digitales Amt“ integriert werden. Das Management von Ausweisen wie auch die Überprüfung von Ausweisen muss ebenfalls mit dieser App möglich sein.
- Die App muss über dokumentierte Schnittstellen an die Plattform angebunden werden. Alle hierfür notwendigen APIs oder Bibliotheken müssen bereitgestellt werden.
- Für die Überprüfung von Ausweisen mit anderen Apps muss eine Bibliothek zur Verfügung gestellt werden.
- Bei der Zusammenstellung eines Ausweises aus verschiedenen Attributen muss ein bedingtes Umschreiben möglich sein, so muss z.B. aus einem Geburtsdatum das Attribut „älter als 18 Jahre“ erzeugt werden können oder aus einer Adresse das Attribut „ist/ist nicht Wiener“.

- Für die UI/UX Anforderungen gelten die Regeln der bestehenden App „Digitales Amt“.
- Für Apps bzw. deren Erweiterungen sind Public App Stores zu unterstützen.
- Mehrsprachigkeit sowie der Umgang mit diakritischen Zeichen muss unterstützt werden.
- Die Produktentwicklung muss der ISO/IEC 18013-5 entsprechen bzw. muss eine Roadmap diesbezüglich vorliegen.

Zusätzlich zu diesen Anforderungen gelten die detaillierten technischen und fachlichen Anforderungen in den Kapiteln 7.1 bis 7.8.

## 2.3 Plattform Szenarien

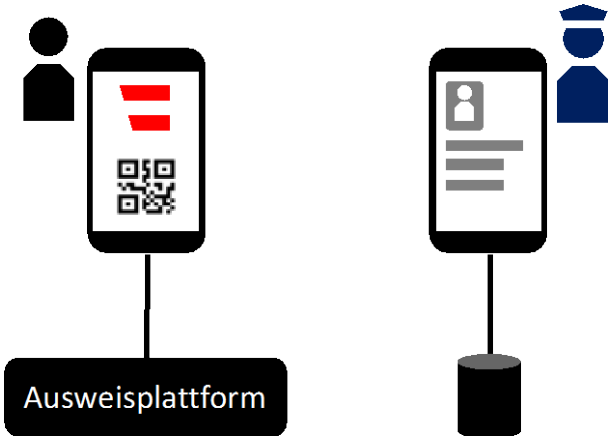
Die Plattform bildet vier generische Szenarien ab. Auf dieser Basis können dann Anwendungsfälle mit unterschiedlichen Datenquellen und Abläufen umgesetzt werden - in den Ausprägungen „Ausweispräsentation gegenüber einer Person“ und „Ausweispräsentation gegenüber einem Online-Service“.

**Offline-Daten** bedeutet, dass die gesamten Ausweisdaten in der App am Mobilgerät gespeichert sind und nicht erst von der Plattform geladen werden müssen. Dieser Begriff steht in keinem Zusammenhang mit der tatsächlichen Internet-Anbindung des Geräts.

### 2.3.1 Szenario 1 – Offline Daten mit Offline Verifikation

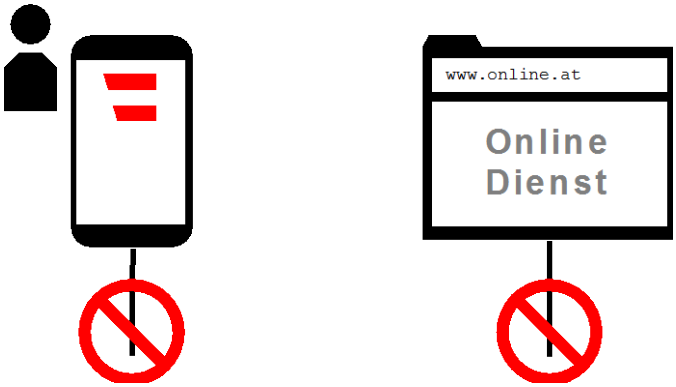

- Sobald ein Nutzer initial einen Anwendungsfall auswählt, werden alle Ausweisdaten geladen und zur Gänze in der App gespeichert. Die Daten müssen regelmäßig aktualisiert werden.
- In der serverseitigen Plattform werden keine Daten dauerhaft gespeichert.
- Die Überprüfung kann durch einen anderen Nutzer ebenfalls mit der App „Digitales Amt“ erfolgen.
- Für die Überprüfung wird von keinem der beiden Geräte eine Verbindung mit der zentralen Ausweisplattform hergestellt.
- Für die Überprüfung von Ausweisen mit anderen Apps muss eine Bibliothek zur Verfügung gestellt werden.

### 2.3.2 Szenario 2 – Offline Daten mit Online Verifikation



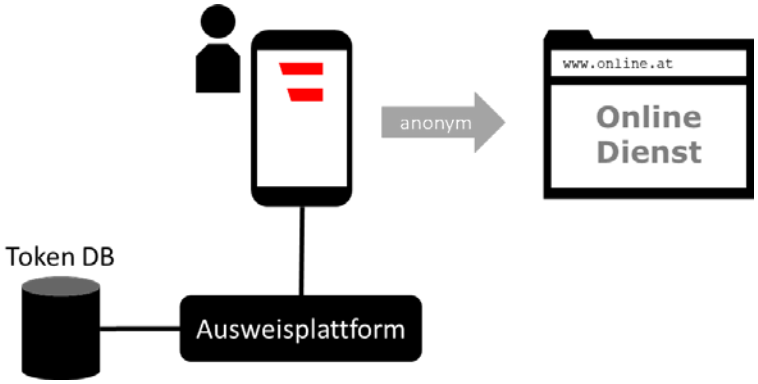

- Es befinden sich nur die für den jeweiligen Anwendungsfall notwendigen Daten in der App des Nutzers.
- Beim Start der Funktion Ausweisplattform in der App „Digitales Amt“ werden die Ausweisdaten aktualisiert.
- Bei einer Überprüfung wird je nach Anwendungsfall nur ein Primärschlüssel des Nutzers übermittelt (z.B. ein bereichsspezifisches Personenkennzeichen - bPK) oder ein Set an Attributen um die Online-Gegenprüfung zu ermöglichen.
- Die eigentlichen Daten werden vom Überprüfer mit Hilfe der übergebenen Attribute direkt aus dem jeweiligen Register bzw. der jeweiligen Ausweisquelle geladen.
- Die App des Prüfers ist nicht Gegenstand der Umsetzung.

### 2.3.3 Szenario 3 – Offline Daten für Online Identifikation




- Ein Offline-Ausweis muss auch für die Anmeldung und Datenübermittlung an einem beliebigen Online-Dienst dienen können.
- Ein Online-Dienst ist immer ein privates Unternehmen, nie eine Behörde.
- Die Ausweisplattform darf über diese Verwendung keine Kenntnis erlangen.

### 2.3.4 Szenario 4 – Offline Daten für pseudonymisierte Online Anmeldung




- Ein Offline-Ausweis muss auch für die pseudonymisierte Anmeldung an einem Online-Dienst verwendet werden können.
- Ein Online-Dienst ist immer ein privates Unternehmen, nie eine Behörde.
- Dazu muss seitens der Ausweisplattform in einer verschlüsselten Datenbank ein Token für die Anmeldung generiert werden.
- Der Benutzer muss seine Tokens selbst einsehen können.
- Im Überprüfungsfall muss eine protokollierte Einsicht in die Token-Datenbank möglich sein, um von einem Token eindeutig auf einen Benutzer schließen zu können.

## 2.4 Umsetzung von Anwendungsfällen

Folgende Anwendungsfälle müssen auf Basis der erweiterbaren Plattform sowie der vier generischen Szenarien umgesetzt werden:

### 2.4.1 Führerschein

- Der „Führerschein“ muss gemäß Szenario 1 als Offline-Ausweis umgesetzt werden.
- Die Führerscheindaten sollen über das E-ID-System geladen werden.
- Eine regelmäßige Überprüfung auf Entzug oder eine vorläufige Abnahme des Führerscheins muss durchgeführt werden.
- Im Falle einer vorläufigen Abnahme des Führerscheins, wird aus dem Führerscheinregister ein Webservice der Ausweisplattform aufgerufen, um ein Update des Ausweises (nämlich die vorläufige Abnahme des Führerscheins) anzustoßen.

### 2.4.2 Zulassungsschein

- Der „Zulassungsschein“ muss gemäß Szenario 1 als Offline-Ausweis umgesetzt werden.
- Die Daten sollen über das E-ID-System geladen werden.
- Der Zulassungsschein muss beliebig vielen Personen weitergegeben werden können.
- Die Auswahl dieser Personen muss ohne Suche in einem Register oder einer Eingabe von Schlüssel (z.B. SV-Nummer) erfolgen.
- Diese Weitergabe muss jederzeit widerrufen werden können und muss auch zeitlich begrenzt erfolgen können.

### 2.4.3 Verkehrskontrolle

- Für die Kontrolle von Führerschein und Zulassungsschein durch Organe der öffentlichen Sicherheit wird ein rasches Verfahren mit Online-Abfrage der entsprechenden Register benötigt.
- Sobald ein Nutzer den Führerschein in die Plattform lädt, muss auch die Option „Verkehrskontrolle“ automatisch angelegt werden.
- Sobald ein Nutzer einen Zulassungsschein in die Plattform lädt, muss dieser optional der Option „Verkehrskontrolle“ hinzugefügt werden.
- Ablauf gemäß Szenario 2:
  - Nutzer wird von einem Organ der öffentlichen Sicherheit um Führerschein und Zulassungsschein gebeten
  - Mit Auswahl der Option „Verkehrskontrolle“ überprüft die App, über eine Online-Rückfrage bei der Ausweisplattform, ob der Benutzer noch eine gültige Lenkberechtigung besitzt.
    - Falls ja werden die Daten aktualisiert.
    - Falls nicht wird der Vorgang mit einer Hinweismeldung abgebrochen.
  - Unabhängig davon, ob die App eine Verbindung mit der Ausweisplattform aufbauen konnte, wird die Überprüfung ermöglicht.
  - Es werden voraussichtlich folgende Daten direkt am Gerät des Nutzers angezeigt:
    - Vorname
    - Nachname
    - Führerscheinklasse(n)
    - Foto
    - Kennzeichen des gewählten Zulassungsscheins
    - Datum der letzten Aktualisierung der Daten
  - Für die Überprüfung werden dem Organ der öffentlichen Sicherheit nur folgende Daten technisch übermittelt:
    - bereichsspezifisches Personenkennzeichen - bPK des Nutzers
    - Kennzeichen des ausgewählten Zulassungsscheins (falls vorhanden)
  - Das Gerät des Organs der öffentlichen Sicherheit lädt mit diesen Primärschlüsseln die Führerschein- und Zulassungsscheindaten direkt aus den entsprechenden Registern.
  - Im Falle einer vorläufigen Abnahme ruft das Führerscheinregister ein Webservice der Ausweisplattform auf, um eine Aktualisierung der Ausweisdaten auszulösen.

### 2.4.4 Altersnachweis

- Ein Altersnachweis muss gemäß Szenario 1 als Offline-Ausweis umgesetzt werden.
  - Folgende Lebenssituation muss mit dieser Umsetzung abgebildet werden:
    - Nachweis des Alters u.a. in Trafik, Disco etc.
    - Die Überprüfung muss durch jeden anderen Bürger mit Hilfe der App „Digitales Amt“ erfolgen können
    - Der Überprüfer darf in jedem Fall nur die Information „bspw. älter als 18 Jahre“ sowie ein Foto des Nutzers für visuellen Vergleich angezeigt bekommen.
- Der Altersnachweis muss ebenfalls gemäß Szenario 3 konzipiert werden
  - Folgende Lebenssituation muss abgebildet werden:
    - Altersnachweis und Name bei Online Anmeldung, sofern bei einem Service erforderlich

- Der Altersnachweis muss ebenfalls gemäß Szenario 4 konzipiert werden
  - Folgende Lebenssituation muss abgebildet werden:
    - Altersnachweis bei pseudonymisierter Online Anmeldung, sofern bei einem Service erforderlich

- Das nachzuweisende Alter muss mittels Logik aus bestehenden Attributen abgeleitet werden können.
- In allen Fällen darf keine Online-Gegenprüfung mit den zentralen Backend-Systemen stattfinden.

### 2.4.5 Umsetzung eines generischen Anwendungsfalles

- Die Umsetzung eines weiteren Ausweises bestehend aus Attributen einer neuen Attributquelle
- Zur Attributquelle steht folgende Schnittstelle zur Verfügung:
  - Ein SOAP-Webservice mit WSDL
  - Die Ausweisplattform authentisiert sich am Service über Basic Auth.
  - In diesem Service wird eine Methode angeboten, mit der bei Übergabe eines bereichsspezifischen Personenkennzeichens - bPK alle Ausweisdaten des Nutzers mit einer Abfrage geladen werden können (die passende bPK wird vom E-ID System zur Verfügung gestellt).
  - Die Ausweisdaten sind im Webservice-Body ohne Verschachtelung in einer simplen Name-Value-Struktur abgebildet.
- Der Ausweis muss als Offline Ausweis gemäß Szenario 1 zur Verfügung stehen

## 2.5 Pilotierung

Als unmittelbar erster Schritt ist eine Pilotierung der Anwendungsfälle „Verkehrskontrolle“ und „Führerschein“ vorgesehen. Diese Pilotierung ist bis zum 31. März 2021 umzusetzen. Nachfolgend sind die dafür erforderlichen Inhalte definiert.

### 2.5.1 Pilot Verkehrskontrolle

- Auf Basis der Plattform des Bieters ist bis zum 31.März 2021 eine Pilotinstallation für den Anwendungsfall „Verkehrskontrolle“ umzusetzen.
- Folgende Ziele müssen erreicht werden:
  - Anbindung an die Register Führerscheinregister und Zentrale Zulassungsevidenz - Kraftfahrzeugzentralregister (KZR)
  - Setting: Nutzer - Online, Organ der öffentlichen Sicherheit - Online
  - Nutzeridentifikation mittels des bereichsspezifischen Personenkennzeichens (bPK)
  - Prüfung: Bieter App zu Bieter App
  - Prüfung: Bieter App zu bestehender App des zuständigen Bundesministeriums
  - Zu integrieren sind Führerschein und Zulassungsschein, ohne Weitergabe des Zulassungsscheines
  - Die Überprüfung beider Ausweise erfolgt in einem Schritt durch die App eines Organes der öffentlichen Sicherheit oder durch die Bieter App.

### 2.5.2 Pilot Führerschein

- Auf Basis der Plattform des Bieters muss bis zum 31.März 2021 eine Pilotinstallation für den Anwendungsfall „Führerschein“ umsetzen.
- Folgende Ziele müssen erreicht werden:
  - Anbindung an das Führerscheinregister
  - Prüfung: Bieter App zu Bieter App

## 2.6 Konzepte

Die folgenden Konzepte müssen aufeinander aufbauen, sich gegenseitig referenzieren und werden zur Bewertung auch in folgender Reihenfolge gelesen:

1. Konzept Erweiterbare Plattform Allgemein

2. Konzept Erweiterbare Plattform Szenarien
3. Konzept Anwendungsfall Führerschein
4. Konzept Anwendungsfall Zulassungsschein
5. Konzept Anwendungsfall Verkehrskontrolle
6. Konzept Anwendungsfall Altersnachweis
7. Konzept Anwendungsfall Generischer Ausweis
8. Konzept Pilot Verkehrskontrolle
9. Konzept Pilot Führerschein

Für die Konzepterstellung gilt:

- Neben den Anforderungen aus dem jeweils korrespondierenden Abschnitt im Kapitel 2, gelten immer auch die detaillierten Anforderungen der Kapitel 7.1-7.8.
- Zur maximal angegebenen Seitenanzahl können noch Deckblatt sowie Inhaltsverzeichnis hinzugefügt werden.
- Bei jeder Konzeptbeschreibung sind Fragestellungen hinterlegt die durch das Konzept eindeutig beantwortet werden müssen.
- Der jeweilige Umsetzungsumfang jedes Konzepts muss im Preisblatt bepreist werden.
- Es ist in den Konzepten anzuführen, welche der für diese Plattform zum Einsatz kommenden Komponenten bereits lauffähig (Teststellung oder Liveprojekt) sind.

### 2.6.1 Erweiterbare Plattform Allgemein

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 7.7 vorzunehmen.

Das Konzept darf maximal 15 Seiten umfassen.
Insbesondere müssen folgende Fragestellungen im Rahmen des Konzepts klar beantwortet werden:

- Lösungsdesign
  - Grundlegende Beschreibung des Technologiestacks
  - Begründete Auswahl des Infrastrukturmodells
  - Darstellung des Software-Schnitts inkl. Schnittstellen zu Drittsystemen
  - Deployment und Stagingkonzept
  - Beschreibung der Skalierung der Lösung gemäß den angeführten Mengensteigerungen in den Jahren der Vertragslaufzeit.
- Welche und wieviel an technischen Ressourcen (Server, DB etc.) sind zum Betrieb der Plattform für die Stages Test/Qualitätssicherung/Produktion erforderlich (siehe dazu insbesondere Kapitel 14 Operations Level Agreement in der Rahmenvereinbarung)?
- Darstellung des Wartungs- und Supportkonzeptes
- Darstellung des Lifecycle der Softwarelösung (Releaseplanung), insbesondere Darstellung der Umsetzung der Major und Minor Release Zyklen.
- Im Falle einer Standard-Softwarelösung ist für die Standardsoftware darzustellen, wie die Auswahl von funktionalen Erweiterungen priorisiert wird.
- Wie geht die Plattform mit Ungültigkeiten (z.B. Entzug, vorläufige Abnahme, Ablauf der Gültigkeit) eines Ausweises um?

### 2.6.2 Erweiterbare Plattform Szenarien

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.3 vorzunehmen.

Das Konzept darf maximal 15 Seiten umfassen.
Insbesondere müssen folgende Fragestellungen im Rahmen des Konzepts klar beantwortet werden:

- Es muss dargelegt werden, wie die in Kapitel 2.3 beschriebenen Szenarien auf Basis der angebotenen Plattform umgesetzt werden

- Zudem muss auf folgende Fragestellungen im Rahmen des Konzepts eingegangen werden:
  - Szenario 1: wie erfolgt die Überprüfung/Datenübermittlung bei zahlreichen Attributen innerhalb eines Anwendungsfalles?
  - Szenario 1: Wie kann ein Foto zur Sicherstellung der Identität des zu Überprüfenden dem Überprüfer zur Verfügung gestellt werden?
  - Szenario 1: wie wird gegen Abfotografieren (bspw. Screenshot des Bildschirms, des QR Codes; Abfotografieren durch Dritte) gesichert?
  - Szenario 2: wie wird gegen Abfotografieren (bspw. Screenshot des Bildschirms, des QR Codes; Abfotografieren durch Dritte) gesichert?
  - Szenario 3: was muss ein Online-Dienst implementieren, damit sich der Nutzer anmelden kann?
  - Szenario 4: was muss ein Online-Dienst implementieren, damit sich der Nutzer pseudonymisiert anmelden kann?

### 2.6.3 Anwendungsfall Führerschein

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.4.1 vorzunehmen.

Das Konzept darf maximal 5 Seiten umfassen.

Insbesondere müssen folgende Fragestellungen im Rahmen des Konzepts klar beantwortet werden:

- Wie wird eine Verwendung als „Sichtausweis“ verhindert?
- Wie kann die missbräuchliche Verwendung von Attributen und Fotos verhindert werden?

### 2.6.4 Anwendungsfall Zulassungsschein

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.4.2 vorzunehmen.

Das Konzept darf maximal 10 Seiten umfassen.
Insbesondere müssen folgende Fragestellungen im Rahmen des Konzepts klar beantwortet werden:

- Wie erfolgt der Widerruf einer Weitergabe?
- Wie erfolgt die Wahl der Zielperson für die Weitergabe?

### 2.6.5 Funktionalität Verkehrskontrolle

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.4.3 vorzunehmen.

Das Konzept darf maximal 15 Seiten umfassen.
Insbesondere müssen folgende Fragestellungen im Rahmen des Konzepts klar beantwortet werden:

- Wie kann eine Verkehrskontrolle in maximal 30 Sekunden pro Kontrolle erfolgen?
- Wie erfolgt die kombinierte (nur eine gemeinsame Prüfung zulässig) Präsentation/Verifikation der relevanten Daten von Führerschein und Zulassungsschein beim Nutzer bzw. Organ der öffentlichen Sicherheit?
- Wie erfolgt die Auswahl des zum Zeitpunkt der Verkehrskontrolle relevanten Zulassungsscheins?
- Wie wird mit einer vorläufigen Abnahme des Führerscheins umgegangen?

### 2.6.6 Altersnachweis

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.4.4 vorzunehmen.

Das Konzept darf maximal 5 Seiten umfassen.
Insbesondere folgende Fragestellungen müssen im Rahmen des Konzepts klar beantwortet werden:

- Wie kann ein Altersnachweis in maximal 5 Sekunden pro Kontrolle erfolgen?
- Wie kann die missbräuchliche Verwendung von Attributen und Fotos verhindert werden?
- Wie können die Szenarien 3 und 4 auf Basis der angebotenen Plattform realisiert werden?

### 2.6.7 Erweiterung um einen generischen Ausweis

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.4.5 vorzunehmen.

Das Konzept darf maximal 5 Seiten umfassen.
Insbesondere folgende Fragestellungen müssen im Rahmen des Konzepts klar beantwortet werden:

- Wie viel Aufwand in PT ist anzunehmen?
- Muss die Plattform neu deployed werden?
- Kann die Anbindung durch beliebige Dritte durchgeführt werden?
- Ändern sich durch die Anbindung Lizenz-/Wartungskosten?

### 2.6.8 Pilot Verkehrskontrolle

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.5.1 vorzunehmen.

Das Konzept darf maximal 7 Seiten umfassen.
Insbesondere folgende Fragestellung muss im Rahmen des Konzepts klar beantwortet werden:

- Beschreiben sie Ihre Lösung bei einem Umsetzungszeitraum von 3 Monaten.

### 2.6.9 Pilot Führerschein

Nachfolgend werden der Rahmen sowie die zu beantwortenden Fragestellungen des zu liefernden Konzepts erläutert. Die Erstellung des Konzepts ist insbesondere unter Berücksichtigung der Anforderungen in den Kapiteln 2.2 und 2.5.2 vorzunehmen.

Das Konzept darf maximal 7 Seiten umfassen.
Insbesondere folgende Fragestellung muss im Rahmen des Konzepts klar beantwortet werden:

- Beschreiben Sie Ihre Lösung bei einem Umsetzungszeitraum von 3 Monaten.

# 3. ZUSCHLAGSKRITERIEN

## 3.1 Allgemeines zu Kriterien und Gewichtung

Die Vergabe der Leistung erfolgt nach dem **Bestbieterprinzip**. Die Rahmenvereinbarung soll mit jenem Bieter abgeschlossen werden, der das wirtschaftlich und technisch günstigste Angebot gelegt hat.

## 3.2 Kriterien und Gewichtung

Folgende Zuschlagskriterien werden zur Bewertung herangezogen und wie folgt gewichtet:

| Zuschlagskriterium | Gewichtung (in %) | maximal erreichbare Punkte (gewichtet) |
|---|---|---|
| Gesamtpreis | **60** | **600** |
| Qualität | **40** | **400** |
| **Summe** | **100** | **1.000** |

Die jeweils für die Kriterien vergebenen Punkte werden summiert. Die Rahmenvereinbarung wird mit dem Bieter abgeschlossen, der das technisch und wirtschaftlich günstigste Angebot gelegt, also in Summe die höchste Punktezahl erhalten hat. Im Fall des Punktegleichstandes wird mit dem Bieter die Rahmenvereinbarung abgeschlossen, dessen Angebot im Zuschlagskriterium „Qualität“ die höchste Punkteanzahl erreicht hat.

## 3.3 Bewertung nach dem Zuschlagskriterium „Gesamtpreis“

Der bewertungsrelevante Gesamtpreis ergibt sich auf Basis der Angaben des Bieters im Preisblatt (**Beilage ./1**).

Die Punkte für die ausgewiesenen Preise werden anhand folgender Formel berechnet:

Punkte= (N*P)/WA

N = Gesamtpreis des Angebots mit dem niedrigsten angebotenen Gesamtpreis aller eingereichten Angebote

P = höchste in diesem Zuschlagskriterium zu vergebende Punkteanzahl (600)

WA = angebotener Gesamtpreis des zu bewertenden Angebots gemäß Angebotspreisblatt

Die so ermittelten Punkte fließen zu 60 % in die Angebotsbewertung mit ein. Im Zuschlagskriterium „Preis“ können daher insgesamt maximal 600 Punkte erreicht werden.

## 3.4 Bewertung nach dem Zuschlagskriterium „Qualität“

Der Bieter hat mit seinem Erstangebot als **Beilage ./2** die unter Kapitel 2.6 beschriebenen Konzepte schriftlich vorzulegen und folgende Konzepte im Rahmen der Verhandlungsrunde zu präsentieren:

- Konzept „Erweiterbare Plattform Allgemein“ - Kapitel 2.6.1
- Konzept „Erweiterbare Plattform Szenarien“ - Kapitel 2.6.2

Die Konzepte haben aus Textelementen und wo sinnvoll aus grafischen Darstellungen zu bestehen. Die Ausarbeitung der Konzepte darf die im jeweiligen Kapitel angegebene DIN A4 Seitenanzahl (bei Schriftgröße 12 und einfachem Zeilenabstand) nicht überschreiten. Von

dieser Seitenbeschränkung sind allfällige Abkürzungs- und Literaturverzeichnisse sowie Beilagen in Form von Abbildungen oder Schemata nicht umfasst.

Grundlage der Qualitätsbewertung ist neben den schriftlichen Konzepten deren Präsentation sowie gegebenenfalls eine Bewertung der vom Bieter bereits umgesetzten und verfügbaren, lauffähigen Komponenten des angebotenen Systems bzw eine Bewertung der existierenden Komponenten in Bezug auf definierte Anwendungsfälle (Bewertung auf Grundlage einer Teststellung oder eines Liveprojektes).

Die im Rahmen der Verhandlungsrunde zu demonstrierenden Anwendungsfälle sind wie folgt:

- Anwendungsfall „Führerschein“ – siehe Kapitel 2.4.1
- Ein selbst zu wählender Anwendungsfall, der zumindest einem der weiteren Szenarien wie in Kapitel 2.3 beschrieben entspricht

Die Vorlage der geforderten Konzepte ist zwingende Voraussetzung für den Vertragsabschluss (MUSS-Kriterium). Angebote von Bietern bzw Bietergemeinschaften, die keine Konzepte vorlegen, werden vom Vergabeverfahren ausgeschieden (Ausscheidensgrund gemäß § 141 Abs 1 Z 7 BVergG). Sollten einzelne definierten Inhalte im Konzept nicht oder nur mangelhaft dargestellt werden, so führt dies zu einer Reduktion der Punkte im Zuge der Bewertung. Sollte der Bieter keine Anwendungsfälle demonstrieren, führt dies nicht zum Ausscheiden, sondern können in den betroffenen Sub-Kriterien keine Punkte erreicht werden.

Die Präsentation und Demonstration hat zwingend durch zumindest eine der in der ersten Stufe des Vergabeverfahrens namhaft gemachten Schlüsselpersonen zu erfolgen. Der Einsatz anderer als der genannten Schlüsselpersonen ist nicht zulässig.

Für die Präsentation und Demonstration ist ein Zeitrahmen von maximal **120 Minuten** vorgesehen, davon entfallen maximal 60 Minuten auf die Präsentation der Konzepte (Plattform, Szenarien) und maximal 30 Minuten auf die Demonstration der beiden Anwendungsfälle sowie mindestens 30 Minuten für Fragen.

Konzepte, Präsentation und Demonstration der lauffähigen Komponenten werden anhand der unter Punkt 3.4.2 angeführten Sub-Zuschlagskriterien bewertet.

### 3.4.1 Ablauf der Bewertung

Die Punktezahl in diesem Zuschlagskriterium ergibt sich durch eine fachkundige Bewertungskommission des Auftraggebers wie folgt:

- Der Erfüllungsgrad in jedem definierten Subzuschlagskriterium wird mit einem Punktespektrum von 0 bis 5 bewertet, wobei 0 der schlechtestmöglichen und 5 der bestmöglichen Bewertung entspricht.

- Die kommissionelle Bewertung erfolgt durch die Bewertungskommission des Auftraggebers in gemeinsamer Diskussion. Ziel ist es, eine einheitliche Beurteilung zu erreichen.

- Die Beurteilung durch die Bewertungskommission wird in einem Protokoll dokumentiert. In diesem werden die Punkte, die das Konzept je Subzuschlagskriterium erhält, niedergeschrieben. Die Punktevergabe wird jeweils von der Bewertungskommission einheitlich verbal begründet. Die Gründe werden im Protokoll festgehalten. Eine gesonderte verbale Begründung durch jedes Kommissionsmitglied ist nicht vorgesehen.

### 3.4.2 Sub-Zuschlagskriterien Qualität

Die Bewertung im Kriterium „Qualität“ erfolgt im Bereich der schriftlichen Konzepte anhand folgender Sub-Zuschlagskriterien:

| Sub-Zuschlagskriterien schriftliche Konzepte | Max erreichbare Einzelpunkte | Multiplikationsfaktor | Max erreichbare Punkte (gewichtet) |
|---|---|---|---|
| **Konzept „Plattform Allgemein“** | 5 | 5,33 | 26,66 |
| **Konzept „Plattform Szenarien“** | 5 | 5,33 | 26,66 |
| **Konzept „Anwendungsfall Führerschein“** | 5 | 5,33 | 26,66 |
| **Konzept „Anwendungsfall Zulassungsschein“** | 5 | 5,33 | 26,66 |
| **Konzept „Funktionalität Verkehrskontrolle“** | 5 | 5,33 | 26,66 |
| **Konzept „Altersnachweis“** | 5 | 5,33 | 26,66 |
| **Konzept „Erweiterung um einen generischen Ausweis“** | 5 | 5,33 | 26,66 |
| **Konzept „Pilot Verkehrskontrolle“** | 5 | 5,33 | 26,66 |
| **Konzept „Pilot Führerschein“** | 5 | 5,33 | 26,66 |
| **Summe** | | | 240 |

| **Die schriftlichen Konzepte werden unter Berücksichtigung der folgenden Aspekte (keine Sub-Sub-Kriterien) bewertet** |
|---|
| **Qualität der Lösung**<br>In diesem Kriterium wird bewertet, wie umfassend und detailliert das beschriebene Konzept dargestellt wird, inwieweit das Konzept eine ausgereifte Lösung für Systemsicherheit, Fälschungssicherheit, Datenschutz und Zugriffssteuerung aufweist, wie nahe das Konzept am aktuellen technologischen Entwicklungszustand ist, und inwieweit die Lösungsansätze nachvollziehbar sind. Je umfassender und detaillierter, je konkreter und aussagekräftiger und je zweckmäßiger die Lösungsansätze, desto besser erfolgt die Bewertung. |
| **Lauffähigkeit der Komponenten**<br>In diesem Kriterium wird bewertet, wie viele der im beschriebenen Konzept dargestellten Komponenten bereits in einer Teststellung bzw. einem Liveprojekt lauffähig sind. Je mehr der dargestellten Komponenten bereits in einer Teststellung bzw. einem Liveprojekt lauffähig sind, desto besser erfolgt die Bewertung. |

| |
|---|
| **Anwendbarkeit für den Auftraggeber**<br>In diesem Kriterium wird bewertet, wie umfassend und detailliert das beschriebene Konzept im Hinblick auf die Anwendbarkeit des Auftraggebers dargestellt wird und in welchem Ausmaß der IST-Stand des Auftraggebers berücksichtigt wird. Je umfassender und detaillierter, je konkreter und aussagekräftiger und je mehr auf die individuellen Anforderungen des Auftraggebers eingegangen wird, desto besser erfolgt die Bewertung. |
| **Fragenbeantwortung**<br>In diesem Kriterium wird bewertet, wie umfassend und detailliert das beschriebene Konzept im Hinblick auf die geforderten Ergebnisse bzw. gestellten Fragen dargestellt wird und inwieweit die Lösungsansätze nachvollziehbar sind. Je umfassender und detaillierter, je konkreter und aussagekräftiger und je mehr auf die individuellen Anforderungen des Auftraggebers eingegangen wird, desto besser erfolgt die Bewertung. |

Im Bereich der schriftlichen Konzepte können daher maximal 240 Punkte (26,66 x 9) erreicht werden. Das Ergebnis wird kaufmännisch auf eine Ganzzahl gerundet.

Die Bewertung im Kriterium „Qualität“ erfolgt im Bereich der Präsentation und Demonstration anhand folgender Sub-Zuschlagskriterien:

| Sub-Zuschlagskriterien Präsentation und Demonstration | Max erreichbare Einzelpunkte | Multiplikationsfaktor | Max erreichbare Punkte (gewichtet) |
|---|---|---|---|
| **Präsentation Konzept „Erweiterbare Plattform Allgemein“**<br>In diesem Kriterium wird bewertet, wie aussagekräftig und gut verständlich das Konzept präsentiert wurde. Weiters wird bewertet wie gut die Schlüsselpersonen auf Rückfragen der Bewertungskommission eingehen und fachlich fundierte und thematisch passende Antworten geben. Je aussagekräftiger und verständlicher die Präsentation und je besser die Schlüsselpersonen auf die Rückfragen eingehen, desto besser erfolgt die Bewertung | 5 | 6,4 | 32 |
| **Präsentation Konzept „Erweiterbare Plattform Szenarien“**<br>In diesem Kriterium wird bewertet, wie aussagekräftig und gut verständlich das Konzept präsentiert wurde. Weiters wird bewertet wie gut die Schlüsselpersonen auf Rückfragen der Bewertungskommission eingehen und fachlich fundierte und thematisch passende Antworten geben. Je aussagekräftiger und verständlicher die Präsentation und je besser die Schlüsselpersonen auf die Rückfragen eingehen, desto besser erfolgt die Bewertung | 5 | 6,4 | 32 |
| **Umsetzung Anwendungsfall „Führerschein“**<br>In diesem Kriterium wird bewertet, wie umfassend und detailliert das angebotene System im Hinblick auf den Anwendungsfall „Führerschein“ dargestellt wird. Weiters wird bewertet, inwieweit die angebotene Lösung, die insbesondere in Punkt 2.4.1 der Ausschreibungsunterlage angeführten Anforderungen erfüllt. Je umfassender und detaillierter, je konkreter und aussagekräftiger, desto besser erfolgt die Bewertung. Je mehr Anforderungen insbesondere gemäß Punkt 2.4.1 der Ausschreibungsunterlage erfüllt sind, desto besser erfolgt die Bewertung. | 5 | 6,4 | 32 |
| **Umsetzung selbst gewählter Anwendungsfall**<br>In diesem Kriterium wird bewertet, wie umfassend und detailliert das angebotene System im Hinblick auf den selbst gewählten Anwendungsfall dargestellt wird. Je komplexer, umfassender und detaillierter, je konkreter und aussagekräftiger der gewählte Anwendungsfall, desto besser erfolgt die Bewertung. | 5 | 6,4 | 32 |

| | | | |
|---|---|---|---|
| **Fragenbeantwortung**<br>In diesem Kriterium wird bewertet wie gut die Schlüsselpersonen auf Rückfragen der Bewertungskommission eingehen und fachlich fundierte und thematisch passende Antworten geben. Je aussagekräftiger und verständlicher die Schlüsselpersonen auf die Rückfragen eingehen, desto besser erfolgt die Bewertung. | 5 | 6,4 | 32 |
| **Summe** | | | 160 |

Im Bereich der Präsentation und Demonstration können daher maximal 160 Punkte (32 x 5) erreicht werden. Das Ergebnis wird kaufmännisch auf eine Ganzzahl gerundet.

Im Zuschlagskriterium „Qualität“ können daher insgesamt maximal 400 gewichtete Punkte erreicht werden.

Die Bieter haben die Möglichkeit, im Last and Best Offer die im Erstangebot vorgelegten Konzepte zu überarbeiten und neu vorzulegen. In diesem Fall werden die neu vorgelegten Konzepte bewertet. Im Rahmen der Angebotsbewertung der Last and Best Offer werden die im Last and Best Offer vorgelegten, überarbeiteten Konzepte durch die Bewertungskommission bewertet und als endgültiges Punkteergebnis für das Zuschlagskriterium „Qualität der Konzepte“ herangezogen.

# 4. FORMELLE REGELN ZUM ANGEBOT

## 4.1 Verwendungs- und Verwertungsrechte

Die Auftraggeber erwerben das (sachenrechtliche) Eigentumsrecht an den Angeboten samt allen Beilagen und allen sonstigen im Rahmen des Vergabeverfahrens von den Bietern übergebenen Unterlagen. Diese Unterlagen werden daher den Bietern nicht zurückgestellt. Darüber hinaus erwerben die Auftraggeber keine Verwendungs- und Verwertungsrechte.

## 4.2 Vergütung von Angeboten

Die Auftraggeber machen darauf aufmerksam, dass für die Teilnahme an diesem Vergabeverfahren keine Vergütung bezahlt wird.

## 4.3 Angebotsabgabe und Einreichungsform

### 4.3.1 Einreichungsform des Angebots

Alle Bestandteile des Angebotes sind innerhalb der Angebotsfrist ausschließlich in **elektronischer Form am Beschaffungsportal** unter

**https://schiefer.vemap.com**

einzureichen.

Angebote per E-Mail, per Fax oder in postalischer Form sind unzulässig und werden nicht berücksichtigt.

### 4.3.2 Elektronische Signatur des Angebots

Die (elektronischen) Angebote müssen mit einer qualifizierten elektronischen Signatur und verschlüsselt abgegeben werden. Für die **qualifizierte elektronische Signatur** ist ausschließlich das Verfahren am Beschaffungsportal (Software „trustDesk vemap“) zu verwenden.

Wird das Angebot nicht von der laut Firmenbuch organschaftlich vertretungsbefugten Person signiert, so ist eine von den laut Firmenbuch organschaftlich vertretungsbefugten Personen

unterfertigte Vollmacht zur Unterfertigung des Angebotes als Beilage zu den Bietererklärungen vorzulegen. Bei Bietergemeinschaften muss das Angebot von einer bevollmächtigten Person signiert werden. In einem solchen Fall ist eine Vollmacht zur Signierung des Angebots als Beilage zu den Bietererklärungen vorzulegen, die von den laut Firmenbuch organschaftlich vertretungsbefugten Personen aller Mitglieder der Bietergemeinschaft unterfertigt ist.

**Hinweise zur elektronischen Signatur:**
Die Bieter haben rechtzeitig dafür zu sorgen, dass sie über eine Möglichkeit zur Durchführung der qualifizierten elektronischen Signatur (Bürgerkarte und Kartenlesegerät oder Handysignatur) verfügen. Dabei ist zu beachten, dass die Beantragung dieser Signaturmöglichkeiten entsprechend Zeit benötigt. Zur Durchführung dieser Signatur kann ausschließlich die am Beschaffungsportal kostenlos zur Verfügung gestellte Software „trustDesk vemap“ verwendet werden.

### 4.3.3 Bestandteile des Angebots

Alle in den Bietererklärungen (**Beilage ./0.1**) angeführten Bestandteile des Angebots (insbesondere Beilagen) sind entsprechend auszufüllen bzw zu erstellen, einzuscannen und elektronisch auf dem Beschaffungsportal hochzuladen. Soweit die Auftraggeber auf dem Beschaffungsportal elektronisch befüllbare Formulare (insbesondere Beilagen) zur Verfügung stellen, ist der Bieter verpflichtet, diese Formulare elektronisch zu befüllen.

Der Bieter hat ausschließlich die geforderten Felder der vorliegenden Ausschreibungsunterlagen auszufüllen und die in den Bietererklärungen (**Beilage ./0.1**) angeführten Unterlagen beizulegen. Das Angebot ist in deutscher Sprache zu verfassen. Beilagen sowie allfällige Nachweise und Bescheinigungen amtlicher Stellen sind ebenso in deutscher Sprache bzw in Kopie und beglaubigter Übersetzung beizulegen.

Die Auftraggeber machen ausdrücklich darauf aufmerksam, dass nur vollständig ausgefüllte und mit allen Nachweisen versehene Angebote bewertet werden. Der Bieter haftet für die Vollständigkeit und Richtigkeit aller im Angebot gemachten Angaben.

Die Angebote müssen, um vollständig zu sein, alle in den Ausschreibungsunterlagen enthaltenen Vorgaben abdecken. Mit der rechtsgültigen elektronischen Signatur anerkennt der Bieter ohne Einschränkungen alle Bestimmungen der vorliegenden Ausschreibungsunterlagen.

### 4.3.4 Dateiformate und Hochladen der Dateien

Es können alle Dateiformate am Beschaffungsportal hochgeladen werden, davon ausgenommen sind ausführbare Dateien wie zB .exe, .php, .js.

Für das **Hochladen der Dateien** auf die **Vergabeplattform** ist **nicht eine allfällige Drag-and-Drop-Funktion des Browsers,** sondern **ausschließlich der dafür vorgesehene Button auf der Webseite** zu verwenden. Die **Namen** der **hochgeladenen Dateien** dürfen **keine Umlaute oder sonstigen Sonderzeichen** enthalten.

### 4.3.5 Rechtzeitigkeit und Einhaltung von Fristen

Ein Angebot ist erst dann rechtzeitig eingelangt, wenn der gesamte Abgabeprozess (uploaden, signieren und verschlüsseln) auf dem Beschaffungsportal fristgerecht abgeschlossen ist. Das Risiko des rechtzeitigen Eingangs des Angebots trägt der Bieter. Nach Ablauf der Angebotsfrist können keine Angebote mehr am Beschaffungsportal hochgeladen werden.

Für alle Fristen gilt die Serverzeit am Beschaffungsportal.

## 4.4 Fragen zum Beschaffungsportal

Für systembedingte Fragen zum Beschaffungsportal steht den Bewerbern eine Supporthotline unter der Telefonnummer 0043/1/3157940 oder E-Mail: welcome@vemap.com kostenlos zur Verfügung.

### 4.5 Sonstige Korrespondenz

Die Korrespondenz zwischen der vergebenden Stelle und den Verfahrensteilnehmern während des Vergabeverfahrens wird ausschließlich über das elektronische Beschaffungsportal der Auftraggeber abgewickelt.

Minder bedeutsame Mitteilungen, Aufforderungen, Benachrichtigungen und Informationen können auch auf anderen geeigneten Wegen übermittelt werden.

Festgehalten wird, dass die gesamte Korrespondenz im Vergabeverfahren ausschließlich über die vergebende Stelle zu erfolgen hat.

### 4.6 Form von Anfragen

Anfragen sind in deutscher Sprache innerhalb der Anfragenfrist einlangend, über das elektronische Beschaffungsportal der Auftraggeber (Punkt „Fragen“) zu stellen.

Allfällige Anfragen werden gesammelt, anonymisiert beantwortet und stehen den Bietern am elektronischen Beschaffungsportal der Auftraggeber zum Download bereit. Der Bieter ist verpflichtet, Fragenbeantwortungen und allfällige Berichtigungen zu berücksichtigen und seinem Angebot zugrunde zu legen.

### 4.7 Schadenersatz

Die Auftraggeber bzw. die vergebende Stelle haften für einen Schaden, der dem Bieter im Vergabeverfahren allenfalls entsteht, ausschließlich bei nachgewiesenem hinreichend qualifizierten Verstoß gegen vergaberechtliche Bestimmungen.

## 5. BEILAGENVERZEICHNIS

| Formblätter | Bezeichnung (unmittelbar auf der Vergabeplattform auszufüllen) |
|---|---|
| Formblatt [BGE] | Erklärung einer Bietergemeinschaft |
| Formblatt [SUL-AU] | Liste allfälliger Subunternehmer |
| Beilage [SUE-AU] zu Formblatt [SUL-AU] | Subunternehmererklärung |
| **Beilagen** | **Bezeichnung (pdf-Dateien sind auszufüllen und auf die Vergabeplattform hochzuladen)** |
| Beilage ./0.1 | Bietererklärung |
| Beilage ./1 | Preisblatt |
| Beilage ./2 | Schriftliche Konzepte |
| Beilage ./3 | Verhandlungsvorschläge des Bieters |

## 6. ANLAGENVERZEICHNIS

| Nummer | Bezeichnung |
|---|---|
| Anlage ./1 | Rahmenvereinbarung |

## 7. ANHÄNGE

### 7.1 Detailanforderungen zu Sicherheit, Source Code und Lizenzen

In diesem Kapitel werden die Anforderungen zu den Themenstellungen Sicherheit sowie Source Code konkretisiert.

#### 7.1.1 Sicherheit

Dieser Abschnitt behandelt die MUSS-Anforderungen im Bereich „Sicherheit“.

- **Anforderungen an Kryptographie**: siehe insbesondere Kapitel 7.3
- **Anforderungen für mobile Apps:** siehe insbesondere Kapitel 7.6
- Kommunikation **mit Dritten (MUSS)**: Kommunikation mit externen Services (außerhalb der Ausweisplattform und dem E-ID System) müssen explizit vom Auftraggeber freigegeben und in der Prozessdokumentation dokumentiert werden.
- **Widerruf (MUSS)**: Widerrufsprozesse, die z.B. beim Verlust des Geräts relevant sind, müssen durchgängig umgesetzt werden und bestehende Prozesse integrieren. So muss z.B. der Widerruf des qualifizierten Signaturzertifikats des Benutzers beim Vertrauensdiensteanbieter - VDA zum Widerruf aller angemeldeten Geräte, bzw. Ausweisfunktionen führen. Für Offline-Daten, die nicht unmittelbar von einer Widerrufsoperation beeinflusst werden können, müssen Risikoeinschätzungen getroffen werden und bestmögliche Maßnahmen umgesetzt werden (z.B. Überprüfung beim jeweiligen Service Provider, Timeouts für die Gültigkeit der Offline Ausweise), um den Missbrauch von bereits widerrufenden Daten zu verhindern bzw. das Risiko dafür zu minimieren.

- **Drittbibliotheken (MUSS)**: Die Verwendung von Drittbibliotheken muss einer Sicherheitsprüfung unterliegen, so dass sichergestellt ist, dass in diesen Bibliotheken keine Sicherheitslücken vorhanden sind. Dazu ist einerseits in der Dokumentation eine Liste aller Bibliotheken durch den Bieter zu führen und andererseits wird Individual Software in der Continuous Integration/Continuous Deployment Pipeline der Source Code gecheckt. Für Standard Software Produkte siehe dazu auch Kapitel 7.1.2.
- **Dokumentation (allgemein und mit Bezug zur Sicherheit) (MUSS)**: Die Komponenten, aus denen die Ausweisplattform mit ihrer grundlegenden Funktion besteht, sowie auch die verwendeten Protokolle und kryptographischen Verfahren müssen offengelegt und dokumentiert werden
  Die vollständige detaillierte Dokumentation der einzelnen Prozesse (Ausstellung- bzw. Verwendung von Ausweisen) muss in Analogie zur bestehenden Dokumentation (Prozesse, Architektur, Kryptographie, Betrieb) durchgeführt werden. Jeder technische und organisatorische Prozess muss anhand des bestehenden Schemas nummeriert und dokumentiert werden. Die Abbildung der Prozessdokumentation erfolgt gekapselt in einem Word-Dokument und zusätzlich im Confluence-System des Auftraggebers. Diese Dokumentation stellt auch die Basis für externe Sicherheits-Reviews (Architektur-Review, Pen-Tests, etc.) dar.
- **Externe Überprüfung des Systems (MUSS)**: Das gesamte System wird wie folgt auf dessen Sicherheit, vor allem auch im Zusammenspiel mit existierenden Systemen (z.B. dem bestehenden E-ID System), überprüft bzw. muss die Sicherheit der Prozesse von Anfang an sichergestellt werden:
  - Security-by-Design Prozesse in Analogie zu jenen die beim E-ID System zum Einsatz kommen bzw. durch den Bieter ggf. ergänzt werden.
    - Erstellen eines detaillierten Kryptographiekonzepts zur Darstellung aller verwendeten Schlüssel und Erklärung aller notwendigen kryptographischen Prozesse zur Absicherung des Systems
    - Detaillierte Dokumentation der (sicherheitsrelevanten) Prozesse. Die Anforderungen, die sich aus bereits vorliegender Dokumentation des E-ID Systems ergeben, sind zu berücksichtigen.
  - Die Anforderung an Sicherheitskonzepte und die Durchführung der internen Risikoanalyse und Einschätzung der Risiken müssen in der Prozess-/Sicherheitsdokumentation berücksichtigt werden.
  - Interne Reviews (Bieter, Auftraggeber) der technischen und organisatorischen Sicherheit und Ableitung und Umsetzung von ggf. notwendigen weiteren Maßnahmen.
  - Externe Reviews des Source Codes, der Architektur, des Kryptographiekonzepts, der Risiken, des Datenschutzes, sowie Durchführung von umfangreichen Pen-Tests (White-Box, Blackbox)
- Um die zentrale Testautomatisierungsumgebung des Auftraggebers für die Prüfungen durch den Auftraggeber nutzen zu können, ist es erforderlich, dass der Bieter sowohl Unit Tests als auch fachliche Testfälle in Abstimmung und Zusammenarbeit mit dem Auftraggeber für das gegenständliche Projekt in dieser Umgebung dokumentiert, damit die Testfälle auch für eine künftige Nutzung bei Folgereleases zur Verfügung stehen. Die zu dokumentierende Testabdeckung muss mindestens 80% der Gesamtlösung betragen und muss alle fachlichen Anforderungen umfassen.

### 7.1.2 Source Code und lizenztechnische Rahmenbedingungen

- Der Auftragnehmer hat ausgewählten Experten des Auftraggebers einen geführten Einblick in den Source Code der Lösung zu gewährleisten
- Der Auftraggeber behält sich das Recht vor den Source Code der Lösung vollständig oder in Teilen gegen die Secure Coding Standards der BRZ in regelmäßigen Intervallen (Major Release Zyklus) zu prüfen. Dazu stellt der Auftraggeber die Secure Coding Standards der BRZ dem Bestbieter zu Beginn des Projektes zur Verfügung.
- Alle Schnittstellen zu externen Systemen sind in den Sprachen Java, C# oder C++ auszuführen.

- Sollten Erweiterungen (API) für den mobilen Client (APP) oder eine eigene App ausgeliefert werden, sind diese für IOS mit Objective-C und Swift und für Android mit Kotlin oder Java als „native“ App bzw. unter der Verwendung von Capacitor zu erstellen.
- Für Apps muss ein Skinning möglich sein.

Beim Einsatz von OpenSource Software, die miteinander kombiniert und/oder modifiziert wird, sind nur die folgenden Lizenzen zulässig – siehe dazu auch Rahmenvereinbarung Kapitel 15.2:

- BSD - Berkeley Software Distribution
- MIT - Massachusetts Institute of Technology, 1988
- Apache License 1.0, 1.1, 2.0

Andernfalls darf im Rahmen des Projektes Open Source Software mit den folgenden Lizenzen genutzt werden, die Projektergebnisse dürfen aber nicht unter eine dieser Lizenzen fallen:der beiden Varianten – reine Nutzung

- GNU - GPL, V1.0
- GNU - GPL, V2.0
- GNU - GPL, V3.0
- GNU - LGPL, V2.0
- GNU - LGPL, V2.1
- GNU - LGPL, V3.0
- GNU - AGPL, V3.0
- AGPL - AFFERO, V1.0
- CPL - Common Public License (IBM), V1.0
- EPL - Eclipse Public License, V1.0
- Ms-RL - Microsoft Reciprocal License
- MPL - Mozilla Public License, V1.0
- MPL - Mozilla Public License, V1.1
- EUPL - European Union Public License, V1.1
- Artistic License, V1.0
- Artistic License, V2.0
- BSD - Berkeley Software Distribution
- MIT - Massachusetts Institute of Technology, 1988
- Apache License 1.0, 1.1, 2.0

Der Einsatz von nicht gelisteten oder anders als kategorisiert verwendeten Lizenzen ist jeweils vorab mit dem Auftraggeber abzustimmen und von diesem freizugeben.

## 7.2 Detailanforderungen zu DSGVO bzw. Datenhaltung und Datenverarbeitung

In diesem Kapitel werden die Anforderungen zu DSGVO sowie zu Datenhaltung sowie Datenverarbeitung konkretisiert.

- Die Datenhaltung muss DSGVO konform sein. Der Auftragnehmer hat als Grundlage zur Erstellung eines Datenschutzkonzeptes nach gültiger DSGVO sämtliche dafür erforderliche Informationen zu liefern.
- Die personenbezogenen Daten des Nutzers dürfen nicht dauerhaft auf der Plattform gespeichert werden
- Es ist jede Transaktion mit einer Transaktions-ID zu versehen und eine Übersetzungstabelle von Transaktions-ID zu sprechendem Langtext für ein Monitoringsystem zu liefern, um die Fehlersuche zu erleichtern.
- **Umsetzung Datenschutzkonzept**: (MUSS) Es müssen die bestehenden Datenschutzkonzepte für das E-ID System umgesetzt bzw. nötigenfalls in Abstimmung mit dem Auftraggeber erweitert werden. Dies betrifft:
  - Es muss mittels pseudonymisierter Transaktions-IDs, also ohne personenbezogene Daten möglich sein Transaktionen für die Eingrenzung von Fehlern zusammen zu finden.
  - Umsetzung der Anforderungen aus den bestehenden Logging-Konzepten (Unterscheidung zwischen technischen Logs und Logs mit personenbezogenen Daten)
  - Integration von etwaigen pers. bezogenen Daten in die Auskunftsverfahren des BMDWs in Abstimmung mit dem Auftraggeber. Es muss minimal die Umsetzung der

nötigen Schnittstellen vorhanden sein, die datenschutzrechtliche Anfragen an den Datenschutzbeauftragten des BMDWs ermöglichen. Optional und in Abstimmung zwischen Bieter und Auftraggeber können dementsprechende Funktionen direkt dem Bürger zur Verfügung gestellt werden.

- **Sicherheit der Daten / Datenschutzfolgeabschätzung**: Die Anforderung an Sicherheitskonzepte und die Ergebnisse der Datenschutzfolgeabschätzung und Einschätzung der Risiken müssen in der Prozess/Sicherheitsdokumentation berücksichtigt werden.
- **IDs für Werbung / Tracking (MUSS)**: Die vom Bieter entwickelten Komponenten, sowie die verwendeten Drittbibliotheken dürfen keine Maßnahmen für Tracking, Werbung enthalten (dies gilt vor allem für Drittbibliotheken/Frameworks, die bei den mobilen Komponenten zum Einsatz kommen). Ebenso muss sichergestellt sein, dass etwaige Mechanismen für diese Zwecke, die direkt vom Betriebssystem oder von erweiterten Komponenten des Betriebssystems (z.B. Google Play Komponenten) bereitgestellt werden, deaktiviert werden.
- **Daten der Plattform (MUSS)**: Es muss eine vollständige Liste der Daten erstellt werden, die in der App verarbeitet werden. Dazu gehören prinzipiell Daten die der DSGVO unterliegen, darüberhinausgehend aber auch Daten ohne DSGVO-Bezug: Log-Daten, Daten, die zwischengespeichert werden, Daten die temporär verarbeitet werden. Die explizite Freigabe des Auftraggebers für die Verwendung und Verarbeitung von Daten ist erforderlich.

### 7.3 Detailanforderungen zur Offenlegung der kryptographischen Verfahren bzw. Kryptographie im Allgemeinen

Die Komponenten, aus denen die Ausweisplattform besteht mit ihrer grundlegenden Funktion wie auch die verwendeten Protokolle und kryptographischen Verfahren müssen offengelegt und dokumentiert werden.

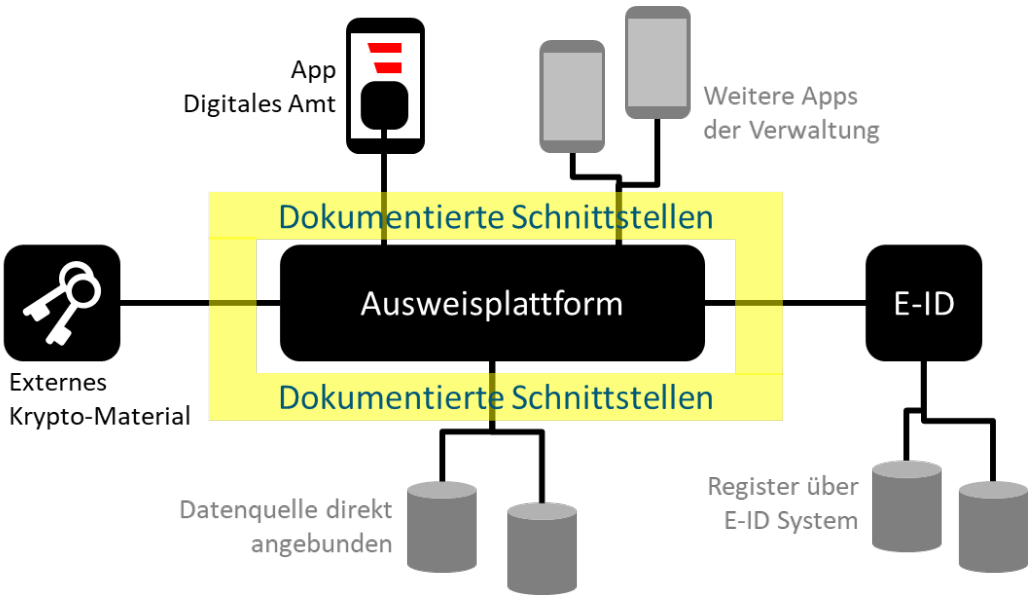
- **Kryptographie / Schlüssel / Prüfkonzept (MUSS)**: Es muss – in Analogie zum E-ID System – ein detailliertes Kryptographie-, Schlüssel- und Prüfkonzept in Zusammenarbeit mit dem Auftraggeber erstellt werden. Dieses Konzept muss alle schützenswerten Schlüssel (private Schlüssel im asymmetrischen Fall, symmetrische Schlüssel) und öffentlichen Schlüssel darlegen und deren Einsatz in den jeweiligen Prozessschritten in Analogie zur Dokumentation im E-ID System dokumentieren. Dies betrifft auch externes Schlüsselmaterial, wenn es bei internen Prozessschritten für Überprüfungen benötigt wird (z.B. externe Zertifikate, die in internen Prozessschritten überprüft werden müssen, z.B. die qualifizierte Signatur eines Benutzers). Das Konzept muss auch die Schnittstellen zu bestehenden Systemen (z.B. E-ID) berücksichtigen und Interaktionen dokumentieren.
- **Aufbewahrung und Handhabung der kryptographischen Schlüssel (öffentlich / privat) für mobile Komponenten (MUSS):** Kryptographische Schlüssel der Plattform muss über die bereits etablierten Systeme (E-ID PKI) ausgestellt werden und generell in Hardware-Komponenten (HSMs, iOS Secure Enclave, Android Keystore) aufbewahrt werden. Abweichungen davon müssen mit dem Auftraggeber explizit abgestimmt und vom Auftraggeber freigegeben werden.
- **Aufbewahrung und Handhabung der kryptographischen Schlüssel (öffentlich / privat) für Services (MUSS)**: Generell müssen private asymmetrische und symmetrische kryptographische Schlüssel in zentralen sicheren Elementen aufbewahrt werden (Hardware-Sicherheits-Module, die vom Auftraggeber bereitgestellt werden – z.B. HSMService, vgl. Grafik in Kapitel 2.2 „Externes Krypto-Material“). Ebenso müssen öffentliche Schlüssel und Zertifikate, die für Vertrauensstellungen benötigt werden, zentral gespeichert werden. Damit wird eine sichere, zentrale und einheitliche Verwaltung der kryptographischen Schlüssel und der notwendigen Verwaltungsprozesse (z.B. Schlüsselerneuerung, Austausch von Vertrauensstellungen) sowie die getrennte Behandlung in T/Q/P Stages ermöglicht. Die Anbindung der unterschiedlichen Stages muss vom Bieter in der Plattform durch externe Konfigurationsdateien berücksichtigt werden.
  Die Anbindung des Stores für „Externes Krypto-Material“ (z.B. HSMService) für die Verwendung des kryptographischen Materials erfolgt im Falle von Java über die JCE/JCA

Architektur, bei anderen Programmiersprachen über etwaige verfügbare Standardmechanismen bzw. über Schnittstellen, die von Auftraggeber und Bieter gemeinsam definiert werden.

- **Kryptographische Bindungen (MUSS)**: Das qualifizierte Signaturzertifikat des Benutzers stellt die Wurzel, der im E-ID System für den Benutzer erstellen kryptographischen Schlüssel dar. Weiteres Schlüsselmaterial, das von der Ausweisplattform verwendet wird, (Zertifikate etc.) muss generell so bereitgestellt werden, dass eine kryptographische Bindung zum ursprünglichen qualifizierten Signaturzertifikat durchgeführt wird und somit eine Überprüfbarkeit des Zusammenhangs der kryptographischen Schlüssel möglich ist.
- **Weiterverwendung von kryptographischen Schlüsseln (MUSS)**: Im Sinne der Benutzerfreundlichkeit und Sicherheit muss bestehendes kryptographisches Material so weit wie möglich (sicherheits-)technisch weiterverwendet werden. Der Grund dafür ist, dass es zu verhindern gilt, dass etwaige Authentifizierungsmechanismen für die Verwendung von kritischen Schlüsseln in den mobilen Apps mehrfach bei der Initialisierung eingegeben werden müssen.
  Als Beispiel dafür werden Schlüssel genannt, die bereits in der „iOS Secure Enclave“ oder dem „Android KeyStore“ für die Verwendung im E-ID-System vorhanden ist. Die Verwendung dieses Schlüsselmaterials muss mit dem E-ID System abgestimmt werden, Erweiterungen/Änderungen des E-ID System können in Abstimmung mit dem Bieter auch vom Auftraggeber durchgeführt werden, um eine sichere und benutzerfreundliche Verwendung zu ermöglichen.
- **Kontinuierliche Weiterentwicklung der Sicherheitsfunktionen (MUSS):** Es müssen alle relevanten (im Sinne des Gewinns an Sicherheit und Relevanz für die Prozesse) und bestmöglichen zum Zeitpunkt der Umsetzung bekannten Sicherheitsfunktionen und kryptographischen Methoden von mobilen Betriebssystemen zum Einsatz kommen (Beispiele: Certificate Pinning, Verwendung von Key-Attestation wo möglich, Rooting Detection, sofern diese nicht schon von der App des Nutzers übernommen werden). Im Rahmen der Wartung muss garantiert werden, dass eine Weiterentwicklung dieser Sicherheitsfunktionen (z.B. bei Verfügbarkeit von neuen Methoden) in Abstimmung mit dem Auftraggeber und im Einklang mit den Sicherheitskonzepten der E-ID Komponenten durchgeführt wird. Dies gilt ebenso für die Backend-Services der Plattform aber insbesondere – aufgrund der sehr starken Dynamik – für die mobilen Komponenten der Plattform.
- **Sicherheitsanforderungen Benutzeridentifikation (MUSS)**: Die kryptographischen Konzepte und Sicherheitsfunktionen für die Bereitstellung, Überprüfung und Identifikation des Benutzers und des Prüfers bei der Übergabe des Ausweises müssen im Rahmen des Projekts unter Berücksichtigung der gesetzlichen Rahmenbedingungen, der Sicherheitsanforderungen und des bestehenden E-ID Systems berücksichtigt werden (dies gilt speziell für die Fälle in denen Prüfer/Benutzer oder einer der beiden Offline sind. Generell müssen dabei dedizierte Risiken und daraus abgeleitete Anforderungen im Projekt erarbeitet werden und Standard-Sicherheitsanforderungen im Rahmen der Kommunikation zwischen zwei Partnern berücksichtigt werden. Diese sind wie folgt abstrakt dargestellt:
  - Vertrauensstellungen zu Kommunikationspartnern
  - Vertraulichkeit der übertragenen Information
  - Authentizität und Integrität der übertragenen Informationen
  - Authentizität von Empfänger und Sender
  - Replay-Schutz
- **Standards, Protokolle für Ausweisaufbewahrung- und Weitergabe (MUSS)**: Etwaige Standards und Best-Practice Ansätze der Wissenschaft und Industrie im Umfeld Ausweise müssen vom Bieter auf Ihre Anwendbarkeit für das Projekt evaluiert werden (z.B. ISO/IEC 7810, Self Souvereign Identity, etc.). Die Verwendung von Protokollen abseits solcher Standards ist ggf. notwendig, muss aber mit dem Auftraggeber abgestimmt werden.

## 7.4 Detailanforderungen zur Außenkommunikation über dokumentierte Schnittstellen sowie Anbindung E-ID System

Die gesamte Kommunikation nach außen muss über dokumentierte Schnittstellen erfolgen.




**Anbindung E-ID-System**

- Ausweisdaten aus Registern der Verwaltung müssen primär über das E-ID-System geladen werden.
- Dafür stellt das E-ID-System eine technische Schnittstelle zur Verfügung, über die alle Register angesprochen werden können.
- Neue Ausweise deren Daten ausschließlich über das E-ID-System geladen werden, müssen rein konfigurativ der Ausweisplattform hinzugefügt werden können.

- **Dashboard/Mein-E-ID**: Etwaige Management-Funktionen für den Nutzer (DSGVO-Auskunft, Einsicht in Transaktionsdaten, Verwaltung von Ausweisen, Widerruf von Ausweisen etc.) müssen im zentralen Dashboard (Mein E-ID) zur Verfügung gestellt werden (Web/App?). Die Bereitstellung von Funktionen der Ausweisplattform (Verwaltung der Ausweise bzw. weiteren Funktionen der Ausweisplattform) muss mit dem Auftraggeber abgestimmt werden und eine Entscheidung getroffen werden welche Funktionen davon im Dashboard/Mein E-ID Service bzw. unabhängig davon angebunden werden.
- **Integration der Service Provider (MUSS)** ggf. erweiterte Identitätskonzepte müssen in Abstimmung zwischen Bieter und Auftraggeber abgestimmt und umgesetzt werden.
- **Identitätsmerkmale (MUSS)**: Es müssen die bestehenden rechtlichen und technischen Anforderungen (siehe dazu: https://www.bmdw.gv.at/Ministerium/Das-BMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen.html) für die Bereitstellung der Identitätsdaten (Konzept zum bereichsspezifischen Personenkennzeichen - bPK) berücksichtigt werden bzw. ggf. in Abstimmung mit dem Auftraggeber erweitert werden (technisch und ggf. auch rechtlich).

## 7.5 Detailanforderungen zur Integration in die App „Digitales Amt“

- Die Ausweisplattform muss in die App „Digitales Amt“ integriert werden.
- Dabei sind die bestehenden Sicherheitsmechanismen (Öffnen über Fingerprint/FaceID) mitzuverwenden.
- Vor einer Überprüfung sind die zu übermittelnden Daten anzuzeigen und die Datenübermittlung bei jedem Anwendungsfall durch eine Benutzerinteraktion (bspw. Fingerprint/FaceID) unter Einhaltung der Vorgaben insbesondere aus Kapitel 2.3.1, freizugeben.
- Der Bieter muss hierzu eine Programmbibliothek zur Verfügung stellen.

- **Berechtigungen von mobilen Betriebssystemen (MUSS**): Etwaige Berechtigungen, die von den mobilen Komponenten der Ausweisplattform benötigt werden, müssen explizit vom Auftraggeber freigegeben werden. Für jede Berechtigung muss eine detaillierte Begründung abgegeben werden und diese in Abstimmung mit UI/UX Komponenten in der bestehenden App dem Benutzer erläutert werden.
- **Backup bei mobilen Apps (MUSS)**: Die Verwendung von Backup-Mechanismen von mobilen Betriebssystemen müssen mit dem Auftraggeber abgestimmt werden und können nur nach der expliziten Freigabe des Auftraggebers verwendet werden.
- **App Store (MUSS)**: Die mobilen Komponenten müssen so umgesetzt werden, dass eine Veröffentlichung im Google Play Store bzw. Apple App Store möglich ist. Etwaige Mechanismen, die für die Durchführung der Reviews (vor allem beim Apple App Store) nötig sind, müssen vom Bieter im Einklang mit der App „Digitales Amt“ berücksichtigt und beigestellt werden (Test-Benutzer und Konten, Videos zur Darstellung gegenüber dem Reviewer etc.).
- **Fehlerkonzept (MUSS)**: Die Übergabe von Fehlern an die App des Nutzers muss in Analogie zu dem bestehenden Fehlerkonzept umgesetzt werden, bzw. die bestehenden Fehlerkonzepte erweitert werden.
- **Testkonzept (MUSS)**: Testkonzepte für die Digitale Amt App, sowie Möglichkeiten für automatisierte Tests müssen in der Umsetzung berücksichtigt werden (z.B. Build-Variante der App in der kryptographische Schlüssel nicht über biometrische Merkmale geschützt werden, und damit für die Durchführung von automatisierten Tests lokal und in Device-Clouds ermöglicht wird). Test-Suites für kryptographische Protokolle, die vor allem auf Device-Clouds getestet werden, stehen bereits im Rahmen der E-ID Systems zur Verfügung und müssen dementsprechend erweitert werden. Die regelmäßige Überprüfung dieser Funktionen – vor allem beim Release von Geräten mit hohem Marktanteil – muss gewährleistet sein.
- **Push Notifications (MUSS)**: Eine etwaige Integration von Push-Notifications muss berücksichtigen, dass die App „Digitales Amt“ bereits für 2 Klassen von Push-Notifications verwendet wird (Vertrauensdiensteanbieter - VDA für Signaturerstellung bzw. Nachrichten an die App selbst). Weitere Integrationen von Push-Notifications müssen kompatibel zu diesen Systemen sein bzw. die bestehenden Komponenten benutzen. Dies muss mit dem Auftraggeber abgestimmt werden.
- **Umsetzung der App-Komponenten (MUSS)**: Die Umsetzung der mobilen Komponenten muss im Allgemeinen „native“ erfolgen. Abweichungen davon müssen vom Auftraggeber explizit freigegeben werden. Ausgenommen davon sind Schnittstellen, die für die Integration in die Digitale Amt App notwendig sind (z.B. Capacitor Plug-Ins).
- **Kryptographie: siehe Kapitel 7.3**
- **Datenschutz: siehe Kapitel 7.2**
- **Sicherheit**: Allgemeine Anforderungen zum Thema Sicherheit: siehe Kapitel 7.1.1

## 7.6 Detailanforderungen zur Überprüfung mit weiteren Apps

- Die Überprüfung von Ausweisen muss auch mit weiteren Apps möglich sein, z.B.
  - Apps auf einem anderen Gerät:
    - App des Organs der öffentlichen Sicherheit
    - Apps für Unternehmen
    - App für sonstige Mitarbeiter der Verwaltung
  - Apps, die direkt am Gerät installiert sind und im Sinne von Kapitel 2.3.3 als Service Provider agieren.
- Der Bieter hat hierfür eine Programmbibliothek zur Verfügung zu stellen die von Dritten in weitere Apps integriert werden kann

## 7.7 Detailanforderungen zu Infrastruktur & Verfügbarkeit

Die on-premises Plattform und deren Betrieb müssen folgende Anforderungen berücksichtigen bzw. ermöglichen

- Im BRZ stehen zwei parallele Rechenzentren mit Standort-übergreifendem Loadbalancing zur Verfügung

- Die Plattform muss auf einem der 3 in Folge beschriebenen Infrastrukturmodelle klassisch auf virtuellen Servern oder innerhalb einer Container Plattform oder auch gemischt betrieben werden können.
- Voraussetzung für die Nutzung der Infrastruktur-Plattformen des Auftraggebers ist die Einbringung der Software in die zentrale Continuous Integration/Continuous Deployment Pipeline des Auftraggebers, welche als ausschließliche Quelle für ein Deployment dient. In der CI/CD Pipline finden Tests für Software Bibliotheken hinsichtlich Aktualität und Lizenztyp, sowie generelle Softwaretests gegen Schadsoftware und Prüfung auf Secure Coding Regeln statt.
- Es ist das vom Auftraggeber geforderte Stagingkonzept – Test/Qualitätsicherung/Produktion – so umzusetzen, dass die CI/CD-Pipeline automatisiert die korrekte Stage deployed.
- Der Auftraggeber setzt als klassische Server-Virtualisierungs-Plattform VMWare auch in der Ausprägung Fault Tolerance ein.
- Der Auftraggeber setzt als Container Plattform eine RedHat Open Shift Plattform ein, die einerseits Basiscontainer (RHEL OS, OpenJDK8/OpenJDK11 tomcat, apache), aber auch Customcontainer eines Dienstleisters tragen kann.
    - Die Erstellung des/der Customcontainer auf Basis eines BRZ Standard-OS-Containers in das BRZ-Environment sind seitens des Bieters mit einzupreisen.
- Der Bieter muss innerhalb dieser Rahmenbedingungen sowie der u.g. Details ein Lösungsdesign zur Abdeckung der Schutzbedarfsklasse „HOCH“ (gemäß ISO 27001) in Bezug auf die Verfügbarkeit darstellen.

- Das Lösungsdesign des Bieters muss ein Sizing für 3 Systemstages (Test, Qualitätssicherung und Produktion) vorsehen, wobei die Test-Stage nicht die Verfügbarkeit „HOCH“ gewährleisten muss.
- Im Lösungsdesign muss ein Schnitt der SW-Lösung mit dem dazugehörigen Deployment Diagramm und den erforderlichen Schnittstellen inkl. Typ und Protokoll dargestellt werden.
- Es ist jedenfalls auf eine Trennung zwischen Authentication/Presentation, Application und Data Layer zu achten. Von dieser Anforderung darf nur begründet und nach vorheriger Rücksprache mit dem Auftraggeber abgewichen werden.

## 7.8 Detailanforderungen zur Betriebsführung

**Grundlegendes** – siehe dazu auch Rahmenvereinbarung Kapitel 14.1

Die Plattform muss beim Auftraggeber oder bei Abrufberechtigten on-premises OHNE Anbindung an eine Cloud betrieben werden können

- Weder die Plattform noch Teile davon dürfen Verbindung zu anderen als den in den Schnittstellen definierten und für die jeweilige Instanz konfigurierten Services/Servern aufnehmen. Insbesondere sind Verbindungen mit Cloudservices des Anbieters oder Dritter zu unterbinden.

Die Ausweisplattform muss so betrieben werden können, dass es sich um technisch unabhängige Instanzen bei unterschiedlichen Serviceprovidern handeln kann.

First- und Second-Level Support werden durch das BRZ sichergestellt.

**Technische Anforderungen** – siehe dazu auch Rahmenvereinbarung Kapitel 14.2
Im Hinblick auf den Betrieb sind folgende technische Anforderungen zu erfüllen:

- Die Installation der Software muss ohne Rootrechte bzw. ohne Domainadministrationsrechten möglich sein.
- Der Betrieb der Software muss ohne Systemadministrationsrechten auskommen.
- Der Auftragnehmer muss sein Fehlerhandling in ein übergreifendes Fehlerkonzept zwischen App „Digitales Amt“, E-ID und Ausweisplattform integrieren um eine effiziente Fehleranalyse anhand abgestimmter Fehlercodes zu gewährleisten.

- Die Ausweisplattform muss sich in das zentrale Monitoring-System der BRZ basierend auf Splunk einfügen. Teil der Leistungen des Auftragnehmers ist die Unterstützung bei der Integration.
- Um die Übergabe in den Betrieb zu gewährleisten, sind seitens des Auftragnehmers folgende Dokumente zu erstellen und dem Auftraggeber zu übergeben:
  - Installation Guide für eine Bieter-unabhängige Installation der Software
  - User/Admin Guide für den Bieter-unabhängigen Betrieb der Software
  - Aktualisierung der Grunddokumente durch Release Notes.

  Diese Inhalte sind erstmalig mit der Übergabe und mit jeder Release wiederkehrend in einer Form zu übergeben, die eine Nutzung unabhängig von Bieter-seitigen Plattformen oder Systemen ermöglicht.
- Vor allem bei den mobilen Plattformen muss mindestens eine Major Release für Android/IOS aufgrund der jährlichen Major-Betriebssystem-Updates berücksichtigt werden. Support von mobilen Betriebssystemversionen und Browser-Versionen muss jenem des E-ID Systems entsprechen.
- Das bestehende Logging Konzept muss sowohl für mobile Komponenten als auch Backend-Komponenten umgesetzt und gegebenenfalls erweitert werden, damit die Anforderungen der DSGVO durchgängig erfüllt werden.

**Supportvarianten** – siehe dazu auch Rahmenvertrag Kapitel 14.3.1

Der Bieter muss einen 3rd Level Support in 2 Qualitäten darstellen und auspreisen:

- **Standard**
  Supportzeiten: werktags 07:00 bis 17:00 Uhr
  Reaktionszeit für Fehler der Klassen 1 und 2: 2 Stunden
  Fehlerbehebungszeit für Fehler der Klasse 1: 12 Stunden
  Fehlerbehebungszeit für Fehler der Klasse 2: 24 Stunden
- **Erweitert**
  Supportzeiten: zusätzlich zu Standard werktags 17:00-07:00
  Reaktionszeit für Fehler der Klassen 1 und 2 in der erweiterten Supportzeit: 4 Stunden
  Fehlerbehebungszeit für Fehler der Klasse 1: 12 Stunden
  Fehlerbehebungszeit für Fehler der Klasse 2: 24 Stunden

  Bereitschaftszeiten 17:00 bis 07:00 Uhr,
  Reaktionszeit für Fehler der Klassen 1 und 2: 4 Stunden.

Definition Reaktionszeit: siehe Rahmenvereinbarung Kapitel 14.3.4
Definition Fehlerbehebungszeit: siehe Rahmenvereinbarung Kapitel 14.3.5

Der Anlauf und Fortlauf der Reaktions- und Fehlerbehebungszeiten ist außerhalb der Supportzeiten gehemmt.

Der Auftragnehmer liefert zur Unterstützung des First Level Supports Anwendungsfall-, Szenarien- und Ausweis-spezifischen Input in Form von Content/Modulen für den Chat Bot der Bürgerhotline.

**Fehlerannahme** – siehe dazu auch Rahmenvereinbarung Kapitel 14.3.2
Zur Koordination aller laufenden Dienstleistungen wird der Auftragnehmer eine Telefonnummer (Hotline) und eine E-Mail-Adresse oder einen kostenlosen Zugriff auf ein Trouble Ticket-System bekannt geben, sodass der Auftraggeber in der Lage ist, Störungen und Probleme mit der Software zu melden und Auskünfte einzuholen. Der Auftragnehmer wird für die Dauer der Wartungspflicht ein Trouble Ticket-System führen, das jede Wartungshandlung mit Datum, jede Änderung des Versionsstandes der Software und jede Störungsbehebung mit Datum, ausgefallener bzw. gewarteter Software, Fehlerklasse, Dauer des Ausfalls, Fehlermeldungen von Hardware oder Software (sofern dokumentiert verfügbar), Ursache der Störung, Art der Behebung und Name des Wartungstechnikers beinhaltet. Auf dessen Basis wird der

Auftragnehmer dem Auftraggeber einen monatlichen Bericht per E-Mail an eine vereinbarte Adresse übersenden oder via Web einen Online-Zugriff für den Auftraggeber auf das System zur Verfügung stellen.

Im Falle einer Fehlermeldung hat der qualifizierte Service-Techniker des Auftragnehmers innerhalb der oben angegebenen Reaktionszeiten zu reagieren (durch Rückruf oder auf elektronischem Wege).

**Fehlerklassen** – siehe dazu auch Rahmenvereinbarung Kapitel 14.3.3

Auftretende Fehler werden gemäß den folgenden **Fehlerklassen** klassifiziert:

- Fehlerklasse 1 - „kritisch“ – Die zweckmäßige Nutzung eines Teiles des der Ausweisplattform oder des IT-Gesamtsystems ist nicht möglich oder unzumutbar eingeschränkt. Der Fehler hat schwerwiegenden Einfluss auf die Geschäftsabwicklung oder Sicherheit der Ausweisplattform. Das sind vor allem Fehler, die eine weitere Verarbeitung ausschließen.
  - Funktionsbezogene Beispiele: Systemstillstand ohne Wiederanlauf, Datenverlust/Datenzerstörung, falsche Ergebnisse bei zeitkritischer Massenverarbeitung von Daten, beim Aufruf eines Ausweises in der App, stürzt diese ab.
  - Maßnahmen: Der Auftragnehmer beginnt während der Wartungsbereitschaftszeit spätestens innerhalb der vereinbarten Reaktionszeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal und sorgt soweit möglich kurzfristig für eine Fehlerbehebung z. B. durch Umkonfiguration von Software, Behebung von Softwarefehlern durch Patches. Darüber hinaus meldet der Auftragnehmer den Fehler umgehend und mit hoher Priorität an einen vom Auftragnehmer verschiedenen Hersteller.
- Fehlerklasse 2 - „schwer“ – Die zweckmäßige Nutzung eines Teiles des IT-Systems oder des IT-Gesamtsystems ist ernstlich eingeschränkt. Der Fehler hat wesentlichen Einfluss auf die Geschäfts-abwicklung oder Sicherheit, lässt aber eine Weiterarbeit zu.
  - Funktionsbezogene Beispiele: falsche oder inkonsistente Verarbeitung, spürbare Unterschreitung der vereinbarten Leistungsdaten des IT-Systems, Häufung von kurzfristigen Störungen des IT-Betriebes, beim Aufruf eines Ausweises werden veraltete oder falsche Attribute angezeigt.
  - Maßnahmen: Der Auftragnehmer beginnt während der Wartungsbereitschaftszeit innerhalb der vereinbarten Reaktionszeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal, sorgt zumindest für eine Umgehung und sorgt soweit möglich für eine Korrektur der Fehlerursache z. B. durch Austausch von Hardwarekomponenten, Umkonfiguration von Software, Behebung von Softwarefehlern durch Patches.
- Fehlerklasse 3 - „leicht“ – Die zweckmäßige Nutzung eines Teiles des IT-Systems oder des IT-Gesamtsystems ist leicht eingeschränkt. Der Fehler hat unwesentlichen Einfluss auf die Geschäftsabwicklung oder Sicherheit, lässt jedoch eine weitere Verarbeitung uneingeschränkt zu.
  - Funktionsbezogene Beispiele: Plattform reagiert auf die Anfragen außerhalb der erwarteten Antwortzeiten/ falsche Fehlermeldung.
  - Maßnahmen: Der Auftragnehmer beginnt in angemessener Zeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal und sorgt soweit möglich für eine Korrektur der Fehlerursache z. B. durch Umkonfiguration von Software, Behebung von Softwarefehlern im Rahmen der Releasepolitik.
- Fehlerklasse 4 - „trivial“ – Die zweckmäßige Nutzung des IT-Systems oder des IT-Gesamtsystems ist ohne Einschränkung möglich. Der Fehler hat keinen oder nur geringfügigen Einfluss auf die Geschäftsabwicklung oder Sicherheit. Das sind vor Allem Schönheitsfehler oder Fehler, die von Mitarbeitern des Auftraggebers selbst umgangen werden können.
  - Funktionsbezogene Beispiele: Zu ignorierende Logmeldungen/Dokumentationsfehler/Schreibfehler.

- Maßnahmen: Der Auftragnehmer sorgt ohne besondere Priorität im Rahmen geplanter vorbeugender Wartung oder der Releasepolitik für die Fehlerbehebung.

Die Zuordnung zu den Fehlerklassen erfolgt einvernehmlich. Im Zweifelsfall hat der Auftragnehmer vor einvernehmlicher Klärung zunächst Maßnahmen auf Basis der Klassifizierung des Auftraggebers zu setzen, um Nachteile für den Auftraggeber zu vermeiden. Die Beweislast für das Vorliegen eines Fehlers geringerer Klasse als vom Auftraggeber behauptet, liegt beim Auftragnehmer.

**Software Wartung** – siehe dazu auch Rahmenvereinbarung Kapitel 14.4
Der Auftragnehmer erbringt die folgenden Software-Wartungsleistungen:

- Security patches – Der Auftragnehmer muss bei Auftreten eines CVE (Common Vulnerabilities and Exposures) in einer der, in der Lösung eingesetzten, SW-Komponenten (3rd Party Software, OpenSource Produkte, SW-Libraries, etc.) den Auftraggeber in Kenntnis setzen und über den Zeitplan und die Schritte zur Behebung informieren.
- Der Auftragnehmer liefert quartalsmäßige Minor Releases für Bug fixes und kleine funktionale Anpassungen und Major Releases im Drei-Jahres-Zyklus für technologische Anpassungen und funktionale Erweiterungen des Backendsystems. Bei Bereitstellung von Client Software ist ein Major Release Zyklus von 1 Jahr vorzusehen. Der Bieter muss darstellen wie er die Major und Minor Release Zyklen umsetzen möchte.
- Content-Aktualisierung der Chat Bot Module bei funktionalen Änderungen.
- Aktualisierung der Transaction-ID und Fehlercode Tabellen.

**Vertragsstrafe** – siehe dazu auch Rahmenvereinbarung Kapitel 14.6
Der Auftragnehmer hat die vorgegebenen Reaktions- und Fehlerbehebungszeiten einzuhalten. Falls der Auftragnehmer die in den vorgenannten Punkten vorgegebenen Zeiten aus welchem Grunde auch immer nicht einhält, wird eine vom Nachweis eines Schadens unabhängige Vertragsstrafe fällig, sofern der Auftragnehmer nicht nachweisen kann, dass er den Verzug nicht verursacht hat.

Bei Überschreitung der Reaktionszeit beträgt die Vertragsstrafe Euro 100,-- pro Stunde Verzug. Die Vertragsstrafe ist pro Fall der Überschreitung der Reaktions- bzw. Behebungszeit mit 5% des im Angebot ausgewiesenen kumulierten Wartungsentgelts für Softwarewartung für sämtliche zu diesem Zeitpunkt abgerufene Lizenzen begrenzt. Alle in einem Wartungsjahr angefallenen Vertragsstrafen aufgrund der Überschreitung der Fehlerbehebungs- bzw. Reaktionszeiten sind insgesamt mit 30% des im Angebot ausgewiesenen kumulierten Wartungsentgelts für Softwarewartung für sämtliche zu diesem Zeitpunkt abgerufene Lizenzen begrenzt.