Beschaffungsamt
des Bundesministeriums
des Innern

KOMPETENZSTELLE
für nachhaltige Beschaffung

Vergabeunterlagen

zum Vergabeverfahren

Rahmenvereinbarung zur sicherheitstechnischen Prüfung von Apps

Az. B 15.34 - 3608/17/VV : 1

Ausgabe 2

Alle Änderungen zur ersten Ausgabe der Vergabeunterlage sind gelb hinterlegt.

Diese Vergabeunterlagen setzen sich wie folgt zusammen:

Aufforderung zur Angebotsabgabe (siehe beiliegendes Anschreiben)

Bewerbungsbedingungen

A Allgemeine Bewerbungsbedingungen

B Besondere Bewerbungsbedingungen und Regeln für dieses Verfahren

Vertragsunterlagen

C Beschreibung der Leistung

D Preise

E Vertragsbedingungen

Auf den folgenden Seiten sind diese einzelnen Bestandteile beschrieben.

Inhaltsverzeichnis

Bewerbungsbedingungen

A Allgemeine Bewerbungsbedingungen

Bitte beachten Sie die beigefügte Anlage „Allgemeine Bewerbungsbedingungen“. Hierin sind die grundlegenden Anforderungen und Rahmenbedingungen von Vergabeverfahren des Beschaffungsamtes des BMI formuliert.

Soweit in den folgenden Abschnitten, den „Besonderen Bewerbungsbedingungen“, abweichendes formuliert ist, geht dies den „Allgemeinen Bewerbungsbedingungen“ vor.

B Besondere Bewerbungsbedingungen und Regeln für dieses Verfahren

B 1. Liste der Dokumente, die mit dem Angebot zu übersenden sind:

- Anlage „Angebotsformular“ (**Ausschlusskriterium**, beiliegender Vordruck)
- Anlagen „aussagekräftige Beschreibungen“ (vom Bieter zu beantwortende Kriterien/Fragen
- Spezifikation des Prüfverfahrens pro Betriebssystem (Kap. 3.4)
- Preisblatt (EXCEL-Tabelle)
- Entwurf **Rahmenvereinbarung**
- Anlage „Kriterienkatalog“

B 2. Gegenstand der Vergabe

Folgende Leistungen sind zu erbringen:

- Einrichtung und Betrieb eines Webportals zur Nutzer- und Auftragsverwaltung
- Einrichtung und Betrieb eines Webportals zur Bereitstellung von Prüfberichten (beide Funktionalitäten können in einem Webportal zusammengefasst werden)
- Durchführung von App-Prüfungen

B 2.1 Vertragslaufzeit und Terminplanung

Nach dem Zuschlag müssen innerhalb von drei Monaten die Webportale eingerichtet sein und der Auftragnehmer bereit zur Durchführung von App-Prüfungen sein.

Nach der erfolgreichen Einrichtung der Webportale und der Bereitstellung der Prüfkapazität wird die Rahmenvereinbarung mit einer Laufzeit von 48 Monaten wirksam.

Der Vertrag kann zwei Mal um jeweils ein Jahr verlängert werden.

Der Auftraggeber teilt dem Auftragnehmer spätestens drei Monate vor Vertragsablauf mit, ob von dieser Möglichkeit Gebrauch gemacht wird.

B 3. Verfahrenshinweise und formale Regelungen

Das Verfahren wird im Rahmen eines Verhandlungsverfahrens mit vorgeschaltetem Teilnahmewettbewerb durchgeführt. Der Teilnahmewettbewerb dazu beginnt und alle erfolgreichen Bewerber erhalten hiermit die Vergabeunterlagen.

Das Verhandlungsverfahren ist mehrstufig aufgebaut. In einer ersten Angebotsphase geben die Bieter ein indikatives Angebot ab. Anschließend erfolgen Gespräche mit den Bietern.

Die Angebote können in einem nächsten Schritt überarbeitet und angepasst werden.

B 3.1 Ansprechpartner

Für alle Fragen, die mit der vorliegenden Vergabeunterlage im Zusammenhang stehen, ist die Vergabestelle alleinige Ansprechpartnerin:

Beschaffungsamt des Bundesministeriums des Innern
[redacted]
Brühler Straße 3
53119 Bonn
Telefon: +49 (0) 22899/610-[redacted]
Telefax: +49 (0) 22899/10-610-[redacted]

B 3.2 Bieterfragen / Bieterinformationen

Soweit Sie im Zeitraum der Angebotserstellung Aufklärungsbedarf zu den Vergabeunterlagen sehen, informieren Sie bitte unverzüglich die Vergabestelle hierüber. Entsprechende Fragen sind bei diesem elektronischen Vergabeverfahren ausschließlich über die e-Vergabe-Plattform unter Verwendung der folgenden Struktur (Tabellenform) zu senden:

lfd. Nr.	Dokument	Seite	Kap.	Text / Frage	Antwort

Die Antworten der Vergabestelle (Bieterinformationen) werden zusammen mit den entsprechenden Fragen (anonymisiert) über die e-Vergabe-Plattform elektronisch an alle Bieter gesandt.

Eventuelle Erläuterungen oder Hintergrundinformationen, die von einem Bieter zusammen mit den Fragen übersendet wurden und als solche gekennzeichnet sind, werden grundsätzlich nicht an alle Bieter versendet.

Die Bieterinformationen werden Bestandteil der Vergabeunterlage.
Die Frist für Bieterfragen ist zu beachten (s. Abschnitt 2.1 der Anlage „Teil A - Allgemeine Bewerbungsbedingungen“).

B 3.3 Nebenangebote

Es ist nicht zulässig, Nebenangebote (einschl. Varianten / Alternativangebote) abzugeben. Sollten Sie dennoch Nebenangebote einreichen, werden diese Nebenangebote von der Wertung ausgeschlossen.

B 3.4 Mehrere Hauptangebote

Es ist nicht zulässig, mehrere Hauptangebote abzugeben. Sollten Sie dennoch mehrere Hauptangebote einreichen, wird nur das zeitlich zuletzt eingereichte Angebot (Datum der Vergabeplattform) berücksichtigt.

B 4. Eignung

Die Bieter haben dem Auftraggeber alle (nach dem Teilnahmewettbewerb) eingetretenen Umstände mitzuteilen, die Einfluss auf ihre Eignung haben könnten.

Eine solche Veränderung kann zum Ausschluss führen, wenn dadurch der Wettbewerb beeinträchtigt oder das Ergebnis der im Teilnahmewettbewerb durchgeführten Eignungsprüfung in Frage gestellt wird.

B 5. Anforderungen an die Angebote

Um die Angebote bewerten zu können, ist eine aussagekräftige Beschreibung der angebotenen Leistung durch den Bieter notwendig.

Hierzu sind in der Vergabeunterlage Teil C und der Anlage „Kriterienkatalog“ durchnummerierte Anforderungen, Fragen und geforderte Angaben zur den beschriebenen Leistung formuliert. Diese leiten sich unmittelbar aus den Leistungsanforderungen ab.

In der Anlage „Teil C - Leistungsbeschreibung“ sind diese detailliert dargestellt.

Mittels einer vom Bieter zu erstellenden Anlage „*Angebotene Leistung*“ sind bezüglich der ausgeschriebenen Leistung mit gleicher Struktur und Nummerierung diese Fragen zu beantworten, Angaben zu machen und Lösungen zu entwerfen.

Die in der Vergabeunterlage Teil C und der Anlage „Kriterienkatalog“ nachgefragten Aspekte werden als „Kriterien“ benannt; sie sind gemäß ihrer Relevanz unterschiedlich gewichtet. Die Antworten der Bieter bzw. deren Angaben und Lösungsentwürfe zu diesen gewichteten Kriterien werden der Angebotswertung

zugrunde gelegt und gehen nach der in Abschnitt B 7.1 beschriebenen Bewertungsmethode in die Leistungskennzahl ein (siehe auch Anlage „Teil C - Leistungsbeschreibung“).

Bei der Beantwortung der Fragen bzw. bei der Ausarbeitung der Angaben und Lösungsentwürfe sind folgende Vorgaben zwingend zu beachten:

- Die Fragen jedes Abschnitts sind in der vorgegebenen Reihenfolge und unter Bezugnahme auf die entsprechenden Gliederungspunkte zu beantworten.

- Das Angebot muss Antworten zu allen Fragen enthalten.

- Fragen, die ohne Antwort bleiben, gehen mit der ungünstigsten Bewertung bezüglich des entsprechenden Kriteriums ein. Dies birgt die Gefahr eines Angebotsausschlusses!

- Im Falle von Ausschlusskriterien (Mindestforderungen) sind als Antwort ausschließlich die Antworten „ja“ oder „nein“ zulässig. Weitere Angaben oder Erläuterungen werden grundsätzlich als Einschränkungen in den Antworten der Bieter angesehen und führen damit automatisch zum Ausschluss des Angebots.

- Für den Fall, dass bei den Bewertungskriterien ein zu erwartender Antwortumfang angegeben wird, kann davon abgewichen werden, solange diese der besseren Darstellung des Angebots zweckdienlich ist. Bei extremen, nicht begründbaren Abweichungen kann dies zu Abwertung für das entsprechende Kriterium führen, insbesondere wenn der Prüfaufwand für die Vergabestelle unzumutbar hoch wird und / oder die Gleichbehandlung der Bieter nicht mehr gewahrt bleibt.

- Verweise auf Literatur oder auf Broschüren dürfen nur als ergänzende Informationen erfolgen. Diese Verweise können nicht die geforderten Antworten, Angaben und Lösungsentwürfe ersetzen.

- Von Seiten der Vergabestelle kann nicht geprüft werden, ob die Antwort evtl. an anderer Stelle oder in einer nicht direkt benannten Anlage zum Angebot gegeben worden ist! Es kann von der Vergabestelle somit nicht ausgeschlossen werden, dass in solchen Fällen die Bewertung nur auf Basis eines unsortierten bzw. eingeschränkten Sachverhaltes erfolgt.

- Fragen müssen in geschlossener Form beantwortet werden: Querverweise auf Antworten zu anderen Fragen werden bei der Bewertung eines Kriteriums von der Vergabestelle grundsätzlich als nicht zu bewertende, nicht relevante Zusatzinformation angesehen.

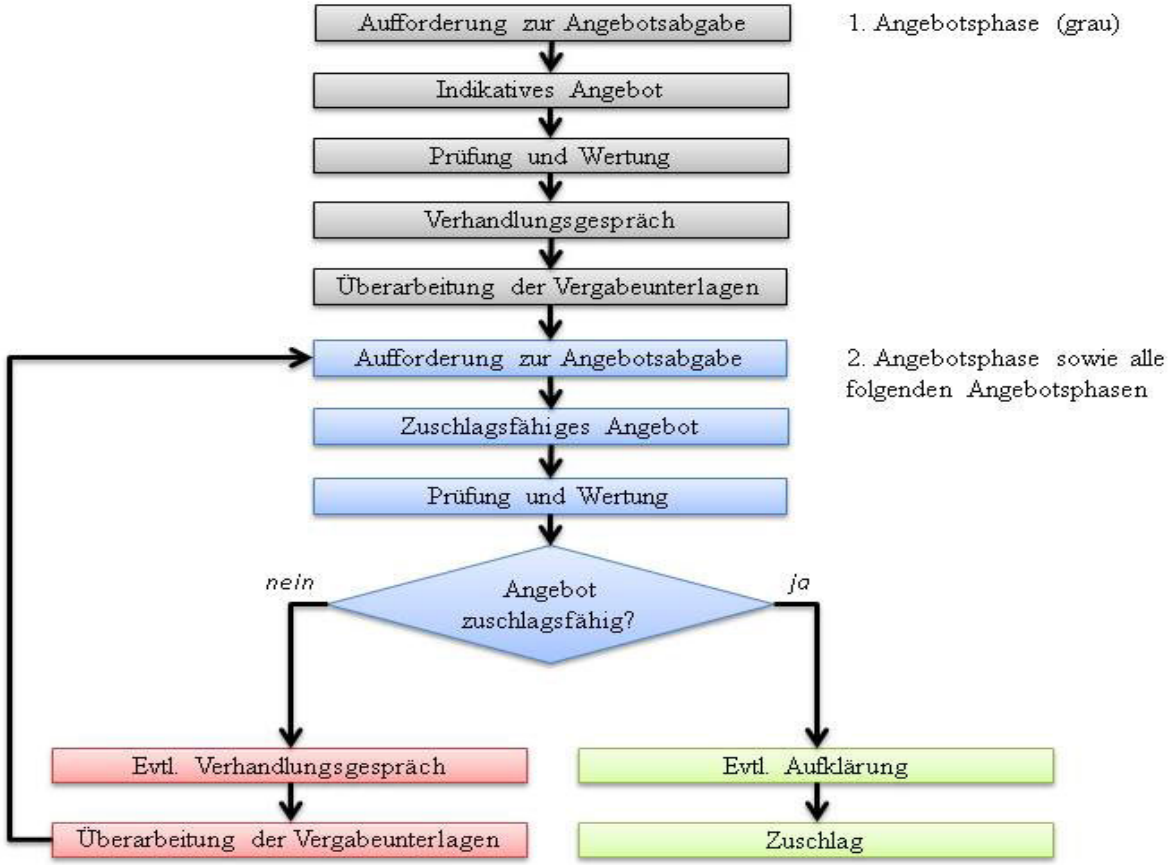
- In den Vergabeunterlagen vorgesehene Optionen müssen vom Bieter angeboten werden. Die Preise für diese Optionen müssen durch den Bieter in das Preisblatt eingetragen werden. Diese Preise gehen in die Ermittlung der Preiskennzahl ein und werden somit in die Bewertung der Wirtschaftlichkeit des Angebotes einbezogen. Dem Auftraggeber wird ein einseitiges bedarfsabhängiges Wahlrecht für die Inanspruchnahme der Optionen eingeräumt.

Das Angebot und alle dazugehörigen Unterlagen sind in deutscher Sprache abzufassen.

Die Anlage „Angebotsformular“ muss einschließlich aller nachgefragten Preise vollständig ausgefüllt werden.

B 6. Verfahrensablauf der Angebotsauswertung

Das Verhandlungsverfahren ist, wie in dem unten dargestellten Ablauf zu ersehen, mehrstufig aufgebaut.



Nach Ablauf der Angebotsfrist wird in einem ersten Schritt geprüft, ob Angebote gemäß VOL/A formal ausgeschlossen werden müssen. Soweit eine Aufklärung eines formalen Mangels grundsätzlich nicht möglich ist (z.B. fehlende Unterschrift oder verspäteter Eingang), kommt ein derartiges Angebot nicht für einen Zuschlag in Frage.

In einem zweiten Schritt erfolgt eine fachlich inhaltliche und preisliche Prüfung. Soweit in diesem Prüfungsschritt Zweifel an der Richtigkeit von Aussagen oder Interpretationsschwierigkeit bestehen, wird zunächst von der Richtigkeit der Angabe bzw. von der für den Bieter günstigsten Auslegung ausgegangen.

Soweit Mindestpunktzahlen hinsichtlich der Bewertung definiert und Ausschlusskriterien formuliert sind, werden diese geprüft. Angebote, die diesbezüglich nicht die Anforderungen erfüllen, kommen für einen Zuschlag nicht in Frage.

Dieser Prüfungsschritt endet mit einem Ranking der für einen Zuschlag in Frage kommenden Angebote.

In einem weiteren Schritt können im Rahmen von Bietergesprächen/ Verhandlungsgesprächen leistungsbezogene, preisliche und vertragliche Aspekte thematisiert werden.

Die Gespräche finden im Beschaffungsamt des BMI in Bonn statt.

Hierzu sollen die vorgesehene Projektleitung und weitere Schlüsselpersonen des Bieters für Aufklärungsfragen und Verhandlungen zur Verfügung stehen. Sie beginnen zunächst mit einer kurzen Angebotspräsentation. Der Bieter erhält hierzu eine gesonderte Einladung mit Tagesordnung.

Im Anschluss an ein Verhandlungsgespräch erhalten alle Bieter eine erneute Angebotsaufforderung für die nächste. Angebotsphase. Sofern in dieser . Angebotsphase ein zuschlagsfähiges Angebot (siehe B 7) vorliegt, wird hierauf der Zuschlag erteilt.

Andernfalls wird eine weitere Verhandlung durchgeführt. Im Anschluss daran erfolgt eine weitere Angebotsaufforderung. Die daran beteiligten Bieter erhalten zeitgerecht eine Information über den Zeitplan sowie eine überarbeitete Vergabeunterlage.

B 6.1 Ausschlusskriterien bei nicht-indikativen (verbindlichen) Angeboten

Wird ein mit „Ausschlusskriterium“ gekennzeichnetes Kriterium nicht erfüllt, so wird das Angebot von der Wertung ausgeschlossen. Das Manko kann auch nicht durch Übererfüllung an anderer Stelle kompensiert werden.

B 6.2 Geforderte Optionen (Optionale Leistungen)

Die geforderten Optionen müssen durch den Bieter angeboten und im Preisblatt mit Preisen versehen werden.

Die Preise für diese Optionen gehen in die Ermittlung der Preiskennzahl ein und werden somit in die Bewertung der Wirtschaftlichkeit des Angebotes einbezogen.

Dem Auftraggeber wird ein einseitiges Wahlrecht für die Inanspruchnahme der angebotenen Optionen eingeräumt. Er entscheidet nach Bedarf, ob die Optionen beauftragt werden.

B 7. Zuschlagskriterien

Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt. Das wirtschaftlichste Angebot ist das Angebot, bei dem die Preiskennzahl und die Leistungskennzahl im günstigsten Verhältnis zu einander stehen. Die Ermittlung erfolgt auf Grundlage der folgenden Zuschlagskriterien.

Die Ermittlung des wirtschaftlichsten Angebotes findet auf Basis der festgestellten Leistungskennzahlen (L) und der feststehenden Preiskennzahlen (P) statt. Es wird für

jedes Angebot die Kennzahl für das Preis-Leistungs-Verhältnis (Z) durch Division gebildet [Z=P/L] und daraus eine Rangfolge der Angebote hergestellt. Leistungskennzahl und Preiskennzahl werden nicht zueinander gewichtet.

B 7.1 Ermittlung der Leistungskennzahl L

Die Leistungskennzahl L spiegelt den Erfüllungsgrad der angebotenen Leistung bezogen auf die Anforderungen an die Leistung wieder.

Zur Ermittlung von L werden die in der Leistungsbeschreibung geforderten Leistungsmerkmale in einem Kriterienkatalog gegliedert und letztlich im Rahmen der Angebotsauswertung gewichtet summiert.

L wird auf Basis der Anlage „Kriterienkatalog“ ermittelt. Füllen Sie dazu die Anlage „Kriterienkatalog“ aus. Beantworten Sie die Fragen und reichen Sie die Anlage mit Ihrem Angebot ein.

Auf Grundlage der Antworten, Angaben und Konzepte der Bieter zu den Kriterien werden entsprechend dem Grad der Zielerreichung jeweils zwischen 0 (Minimum) und 4 (Maximum) Punkte für das zugehörige Einzelkriterium vergeben.

Wird die geforderte Leistung (Bewertungs-Einzelkriterien) vollständig angeboten, d. h. zu 100% oder mehr erfüllt, wird dieses Bewertungskriterium mit vier Punkten bewertet.

4	Anforderung voll erfüllt

Wird ein Bewertungskriterium nicht vollständig erfüllt, verbleibt das Angebot in der Wertung und wird nach folgender Regel bewertet.

3	Anforderung mit kleinen Schwächen erfüllt, die ohne erkennbaren Einfluss auf die Nutzung sind

2	Anforderung teilerfüllt, mit deutlichen Einschränkungen aber noch nutzbar, die mit erheblichen Einfluss auf die Nutzung sind und gerade noch akzeptiert werden

1	Anforderung teilerfüllt, aber auch nicht mehr mit Einschränkungen nutzbar.

0	nicht erfüllt oder keine Angaben.

Bei der Punktevergabe werden ausschließlich die Schlüssigkeit, Wirtschaftlichkeit und Realisierbarkeit der von den Bietern in ihren Antworten gemachten Angaben bzw. vorgelegten Konzepte in Bezug auf die Anforderungen bewertet.

Die Kriterien sind mit einem Gewicht versehen. Das Gewicht aller Kriterien summiert sich auf 100 %. Durch Multiplikation der jeweils erzielten Bewertungspunkte mit der angegebenen Gewichtung des jeweiligen Kriteriums wird die von Ihnen für jedes Kriterium erreichte Leistungspunktzahl berechnet; die Punktzahlen werden anschließend addiert, um die Leistungskennzahl für das Angebot zu ermitteln.

Für den Zuschlag kommen nur Angebote in Betracht, bei denen alle Ausschlusskriterien erfüllt sind und die bei der Leistungsbewertung den geforderten Mindesterfüllungsgrad von 65% jeder Kriteriengruppe einhalten. Der Mindesterfüllungsgrad entspricht der Mindestpunktzahl im Verhältnis zur maximal erreichbaren Punktzahl.

B 7.2 Ermittlung der Preiskennzahl

Die Preiskennzahl wird auf Basis der dargestellten Preisstruktur (Anlage „Preisblatt“) ermittelt. Die Preiskennzahl ist identisch mit dem Gesamtpreis in der Anlage „Angebotsvordruck“.

Ein Anspruch des erfolgreichen Bieters auf einen Umsatz in Höhe der Preiskennzahl entsteht nicht.

Vertragsunterlagen

C Leistungsbeschreibung

C 1. Allgemeine Beschreibung

C 1.1 Ausgangssituation und Handlungsbedarf

In der Bundesverwaltung besteht der Bedarf zur sicheren Nutzung von Smartphones und Tablets. Diese Nutzung sieht u.a. die abhörsichere Sprachkommunikation und die sichere Speicherung und Verarbeitung von digitalen Inhalten vor. Hierzu werden verschiedene Anwendungen, sogenannte „Applikationen“, kurz „Apps“, auf den Geräten installiert und betrieben. Zur Gewährleistung der Sicherheit, Verfügbarkeit und Integrität der übertragenen, verarbeiteten und gespeicherten Daten entsteht neben anderen Sicherheitsmaßnahmen die Notwendigkeit, die auf den Smartphones und Tablets verwendeten Apps hinsichtlich ihrer IT-Sicherheit einer geeigneten Prüfung zu unterziehen. Es sollen nur solche Apps zum Einsatz kommen dürfen, die bestimmten IT-Sicherheitsanforderungen entsprechen.

Es besteht derzeit ein Rahmenvertrag mit einem Prüfdienstleister, über den Apps einer Prüfung unterzogen werden können. Diese neue (hier ausgeschriebene) Rahmenvereinbarung soll 3 Monate nach Zuschlag die bestehende Rahmenvereinbarung ablösen. Die Leistungsbeschreibung setzt auf den bisherigen Erkenntnissen auf und das Prüfverfahren soll weiterentwickelt und ausbaut werden.

C 1.2 Kurzbeschreibung der Ziele der Dienstleistung

Ziel des Vorhabens ist die Bereitstellung eines rahmenvertraglich definierten Dienstes zur sicherheitstechnischen Prüfung von Apps nach transparenten Prüfkriterien. Dieser Dienst soll so gestaltet sein, dass eine hohe Zuverlässigkeit der Prüfergebnisse gegeben ist. Aufgrund der Prüfergebnisse und nach Maßgabe des BSI sollen geprüfte Apps zudem ein abgestuftes Ranking erhalten und als „grün“ = „unbedenklich“, „gelb“ = „eingeschränkt verwendbar unter Auflagen“, oder „rot“ = „darf nicht verwendet werden“ klassifiziert werden. Apps mit Schad- oder Malwarefunktionalität sind gesondert als solche auszuweisen, sie erhalten ebenfalls ein „rot“. Die so um eine Einstufung der App erweiterten Prüfergebnisse sollen in einer Form bereitgestellt werden, die ein einfaches Abrufen und Verwenden ermöglicht und einen schnellen Überblick über die sicherheitstechnischen Eigenschaften der geprüften Apps sowie der ggf. zu beachtenden Auflagen erlaubt.
Zur Nutzer- und Auftragsverwaltung ist ein Webportal einzurichten und zu betreiben. Zur Bereitstellung der Prüfberichte ist ebenfalls ein Webportal einzurichten und zu betreiben. Beide Webportale können zu einem Webportal zusammengefasst werden.

C 2. Leistungsumfang

C 2.1 Grundsätzliche Rahmenbedingungen

Apps, die zur Verarbeitung von Verschlusssachen (VS – Nur für den Dienstgebrauch) auf einer zugelassenen Plattform eingesetzt werden sollen, müssen vor einer Freigabe hierfür in jedem Fall einer intensiven erweiterten sicherheitstechnischen Betrachtung unterzogen werden.

Dienstlich verwendete Apps, auch wenn sie nicht der Verarbeitung von Verschlusssachen dienen, verarbeiten Daten, die in ihrer Gesamtheit als sicherheitsrelevant, zumindest aber als sensitiv zu betrachten sind. Die Funktionalität dieser Apps darf zudem die Sicherheit der anderen Apps, der Plattform und des Gesamtsystems nicht gefährden. Daher müssen dienstlich verwendete Apps einer IT-Sicherheitsüberprüfung unterzogen werden können; hierzu soll im Sinne dieser Leistungsbeschreibung eine Rahmenvereinbarung zwischen dem BSI und einem vertrauenswürdigen Prüfdienstleister abgeschlossen werden.
Bei der Prüfung der Apps sind die mobilen Betriebssystem-Plattformen Android, iOS und BlackBerry 10 zu berücksichtigen.

Die Prüfungen müssen fachlich fundiert und mit hinreichender Prüftiefe ausgeführt werden. Dabei sind Aspekte wie Datensicherheit, Datenschutz und Sicherheit der Kommunikationsverbindungen zu berücksichtigen. Apps mit erkannter Schad- oder Malwarefunktion sind als solche gesondert zu kennzeichnen. Für jede Prüfung ist ein Prüfbericht zu erstellen, der alle wesentlichen Ergebnisse übersichtlich darstellt und als Bewertung (Votum) ein abgestuftes Sicherheits-Ranking enthält („Sicherheits-Ampel“). Darüber hinaus kann eine Empfehlung abgegeben werden, z.B. wenn eine andere gleichartige App aus Sicht der Prüfer eine bessere Alternative darstellt. Apps, die Schadfunktionen enthalten und Apps, deren Sicherheitsampel ein rot enthält, dürfen nicht auf dienstlichen Geräten verwendet werden. Apps, deren Sicherheits-Ampel grün oder gelb zeigt, dürfen verwendet werden. Bei gelb sind entsprechende Auflagen bei der Verwendung zu beachten. Die Entscheidung, welche der grün oder gelb eingestuften Apps verwendet werden dürfen, und wie Auflagen ggf. umzusetzen sind, trifft jede die App einsetzende Behörde eigenverantwortlich. Unabhängig von der Bewertung gemäß Sicherheitsampel kann das BSI einzelne Apps black- oder whitelisten, d.h. die Berechtigung zur Verwendung auf dienstlichen Geräten entziehen oder erteilen. Wird eine App durch das BSI black gelistet, darf sie nicht mehr auf dienstlichen Geräten verwendet werden.

Die Prüfung einer dienstlich erforderlichen App wird jeweils durch den IT-Verantwortlichen (in der Regel der IT-Admin) einer Behörde (Prüfantragsteller) beim Auftragnehmer (Prüfdienstleister) beantragt. Dieser führt die Prüfung durch, nachdem das BSI über den Prüfantrag informiert wurde und diesen freigegeben und damit den Prüfauftrag erteilt hat.
Mit der Prüfantragstellung bestätigt der IT-Verantwortliche zugleich die dienstliche Notwendigkeit der Prüfung der App.

Der IT-Verantwortliche vertritt die Smartphone- und Tablet-Nutzer (User) seiner Behörde und ist Ansprechpartner für den Prüfdienstleister. Der IT-Verantwortliche verteilt geprüfte und grün oder gelb bewertete Apps an die Smartphone- und Tablet-

Nutzer seiner Behörde über ein MDM-/MAM-System oder auf anderen geeigneten Wegen. Der gesamte Workflow der App-Prüfung ist in der folgenden Abbildung schematisch dargestellt:

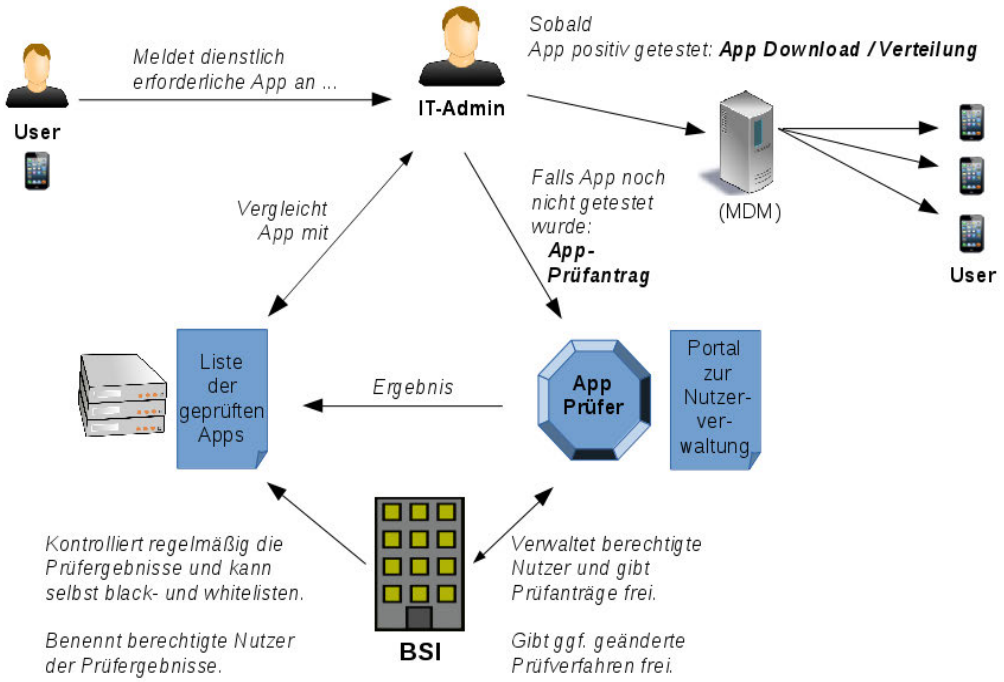


Abb. 1: Workflow App-Prüfung

Darüber hinaus kann das BSI selbst Prüfaufträge erteilen, oder anderen Stellen hierzu die Berechtigung erteilen.

C 2.2 Gegenstand der Rahmenvereinbarung

Ziel der abzuschließenden Rahmenvereinbarung ist die Bereitstellung eines Dienstes zur sicherheitstechnischen Überprüfung und Bewertung („Sicherheits-Ampel“) von Apps, die Bereitstellung eines Webportals zur Nutzer- und Auftragsverwaltung, sowie die Bereitstellung der Prüfberichte über ein Webportal. Die Prüfberichte sollen der gesamten Bundesverwaltung sowie weiteren vom BSI benannten berechtigten Nutzern zur Verfügung stehen. Dies können z.B. andere Stellen aus der gesamten öffentlichen Verwaltung oder auch für das BSI tätige Firmen sein. Das BSI kann Prüfberichte nach eigenem Ermessen anderen dritten Stellen zur Verfügung stellen, oder diesen Stellen die Berechtigung zum Zugriff auf die Prüfberichte erteilen.

Eine generelle, allgemeine Veröffentlichung der Prüfberichte ist nicht vorgesehen.
Im Einzelfall behält das BSI sich allerdings vor, für die Öffentlichkeit relevante Warnungen auf Basis der Prüfergebnisse zu veröffentlichen.

C 3. Anforderungen

C 3.1 Übermittlung von Prüfaufträgen

[A1] Der Auftragnehmer muss Prüfanträge von verschiedenen Prüfantragstellern entgegennehmen können. Es kommen dabei Einrichtungen des Bundes, Bundesministerien und deren nachgeordnete Behörden, sowie vom BSI zu bestimmende Dritte als Prüfantragsteller in Betracht. Ansprechpartner bzw. Antragsteller sind die IT-Verantwortlichen des jeweiligen Hauses oder vom BSI benannte andere Stellen. Ein Prüfantrag enthält neben der Identität des Prüfantragstellers mindestens Angaben über

- die zu prüfende App (eindeutige Bezeichnung),
- das Betriebssystem, für das die App bestimmt ist (Name, Version), und
- den Zeitraum, in dem Aktualisierungen der App, die auf den Markt kommen, fortlaufend geprüft werden sollen,
- sowie die Bestätigung der dienstlichen Notwendigkeit der beantragten Prüfung, die bei Prüfantragstellung durch das Portal abzufragen ist.

[A2] Ein Prüfantrag wird jeweils für eine App eines bestimmten Betriebssystems erteilt. Falls eine App für mehrere Betriebssysteme geprüft werden soll, müssen dementsprechend mehrere Prüfanträge gestellt werden. Eine Versionskennung für die zu prüfende App kann, muss aber nicht, angegeben werden. Falls eine Versionskennung angegeben wird, dann gilt der Antrag für die angegebene Version der App. Fehlt diese Angabe, dann gilt der Antrag für die jeweils aktuellste Version der App. Die Angabe über den Zeitraum muss dem Prüfantragsteller die Möglichkeiten bieten,

- Aktualisierungen *nicht* prüfen zu lassen,
- den Zeitraum mit möglichst feiner Granularität zu spezifizieren, und
- den gesamten Geltungszeitraum der Rahmenvereinbarung anzugeben.

[A3] Ein Prüfantrag kann darüber hinaus auch Angaben über bestimmte Parametrisierungen enthalten (Optionen bei der Installation oder in den Einstellungen der App), die im Falle einer konfigurierbaren App gezielt geprüft werden sollen. Der Auftragnehmer muss evtl. Parametrisierungen berücksichtigen, ggf. sind diese beim Prüfantragsteller zu erfragen.

[A4] Der Auftragnehmer hat ein Webportal einzurichten und zu betreiben, über das elektronisch die Übermittlung der Prüfanträge stattfindet, die Prüfaufträge verwaltet werden, und über das auch die Nutzerverwaltung erfolgt. Das Portal ist auf einem Server mit Standort in Deutschland zu hosten. Der Server selbst, das zugehörige Netzwerk sowie der Zugang zum Server sind nach den anerkannten Regeln der IT-Sicherheit abgesichert zu betreiben. Das entsprechende Sicherheits- bzw. Realisierungskonzept ist mit dem BSI abzustimmen.

Nach Ende der Rahmenvereinbarung muss das Webportal für mindestens 12 weitere Monate zur uneingeschränkten Nutzung zur Verfügung stehen. Dem BSI ist zudem die Möglichkeit zu eröffnen, bei Bedarf das Portal komplett zu übernehmen und in Eigenregie weiter zu betreiben.

[B1] Das Webportal soll mandantenfähig (jeder Nutzer arbeitet in seinem eigenen Nutzerkontext) und möglichst nutzerfreundlich und intuitiv bedienbar sein. Zeigen Sie anhand von mind. 3 Screenshots einschließlich Erläuterungen wie die Nutzeroberfläche aussieht, bedient wird und welche Eintragungen durch den Benutzer vorzunehmen sind.

Dazu muss die erste Abbildung (Screenshot des Webportals) den Login-Bildschirm darstellen. Aus den 2 (oder mehr) weiteren Abbildungen muss zumindest hervorgehen, welche Reiter, Menüs oder auch Optionen für den Endanwender zur Verfügung stehen. Erläutern Sie welche Felder, Schaltflächen und andere Bedienelemente dem Nutzer zur Verfügung gestellt werden um Prüfanträge einzutragen, und deren Status abzufragen .

Eingereichte Prüfanträge bedürfen der Freigabe durch das BSI. Wird der Prüfantrag durch das BSI bestätigt und damit freigegeben, so wird dadurch aus dem Prüfantrag ein Prüfauftrag. Der Prozess hierzu (Workflow) muss durch den Bieter grafisch dargestellt werden (Programmablaufplan, Nassi-Shneiderman-Diagramm oder vergleichbare Darstellung) und ist möglichst einfach zu gestalten, die genaue Realisierung ist mit dem BSI abzustimmen. Die Freigaben sind über das Portal zu verwalten. Das Portal soll zu Zwecken der Kontrolle durch das BSI und zu Abrechnungszwecken Sortier- und Suchfunktionen über alle Prüfanträge, Prüfaufträge und alle erbrachten Prüfleistungen bereitstellen. Die Sortierfunktionen sollen zumindest eine Sortierung nach Datum, spezifizierbaren Zeiträumen, nach Kosten der Prüfung, nach freigegebenen / abgelehnten Prüfungen, sowie nach Prüfantragsteller ermöglichen.

Endgültige Ausgestaltung und Design des Webportals sind im Anschluss an die Zuschlagserteilung gemeinsam mit dem Bedarfsträger BSI festzulegen.

[A5] Prüfaufträge, die über einen längeren Zeitraum gelten (App-Aktualisierungen), müssen - ggf. unter Rücksichtnahme von geeigneten Fristen - gekündigt werden können.

[A6] Falls ein Prüfbericht über eine App/Betriebssystem-Kombination bereits vorliegt, muss der Auftragnehmer eingehende Prüfanträge für diese Kombination ablehnen und den Prüfantragsteller auf den schon vorliegenden Bericht verweisen. Kosten dürfen dabei nicht in Rechnung gestellt werden, wenn der vorliegende Prüfbericht im Rahmen dieser Rahmenvereinbarung erstellt wurde. Dies gilt nicht, wenn sich das zur Anwendung kommende Prüfverfahren zum Beauftragungszeitpunkt von dem des vorliegenden Berichts zugrundeliegenden Prüfverfahrens erheblich unterscheidet. In diesem Fall muss das BSI als Prüfauftraggeber über die Unterschiede informiert werden, und die Möglichkeit erhalten, im Anschluss den Prüfauftrag endgültig zurückzuziehen oder zu erteilen.

[A7] Falls sich ein Prüfauftrag über eine App/Betriebssystem-Kombination bereits in der Bearbeitung befindet, muss der Auftragnehmer weitere Prüfanträge für diese Kombination mit entsprechendem Hinweis ablehnen. Kosten dürfen dabei nicht in Rechnung gestellt werden.

[A8] Prüfanträge dürfen nur von authentifizierten und autorisierten Prüfantragstellern gestellt werden können.

[B2] Das BSI legt fest, wer zur Prüfantragstellung berechtigt ist. Berechtigte Prüfantragsteller sollen durch das BSI über eine geeignete Schnittstelle (z.B. JSON, XML oder CSV) über einen abgesicherten Zugang des Webportals einfach hinzugefügt und wieder entfernt werden können, Änderungen sollen umgehend wirksam werden. Stellen Sie im Rahmen Ihres Angebots dar, welche Schnittstelle Ihr Webportal nutzt und wie der Zugang abgesichert ist. Prüfanträge bedürfen vor Beginn der Prüfung einer Freigabe durch das BSI.

Die Prozesse zur Festlegung, zur Verwaltung und zur Entfernung berechtigter Prüfantragsteller durch das BSI sollen einfach, nutzerfreundlich und intuitiv über das Webportal möglich sein. Zeigen Sie, wie das Webportal diese Anforderungen erfüllt indem Sie die Menüstruktur, die für diese Prozesse notwendigen Arbeitsschritte und die Übersicht über die Prüfantragsteller erläutern und / oder grafisch darstellen.

Aus diesen Erläuterungen und / oder Darstellungen muss ersichtlich sein, wie viele Arbeitsschritte für diese Prozesse und welche Eingaben durch den

Nutzer notwendig sind, sowie welche Menüs zu diesem Zweck genutzt werden.

C 3.2 Durchführung von Prüfaufträgen

[A9] Prüfantragsteller und BSI müssen über den Bearbeitungsstatus der Prüfaufträge informiert werden, bzw. diesen über das Webportal sichten können. Auch ein telefonischer Support für einfache Statusanfragen muss an Werktagen (Mo. bis Fr.) zwischen 9 und 17 Uhr erreichbar sein.

[A10] Prüfaufträge müssen spätestens innerhalb einer Frist von 10 Werktagen abschließend bearbeitet worden sein, d.h. nach Ablauf dieser Frist muss der vollständige Prüfbericht vorliegen. Die Frist beginnt mit der durch das BSI erteilten Freigabe des Prüfantrages, d.h. also mit Auftragserteilung. Kann der Auftragnehmer dieser Anforderung in bestimmten Einzelfällen (z.B. besonders komplexe App) nicht nachkommen, so müssen der Prüfantragsteller und das BSI innerhalb dieser Frist entsprechend informiert werden.

[B3] Die durchschnittliche Bearbeitungsdauer von Prüfaufträgen soll möglichst kurz sein, ohne dass dies zu Qualitätseinbußen führen darf.

[A11] Der Auftragnehmer muss von seiner Prüfkapazität her in der Lage sein, mindestens 20 Aufträge gleichzeitig bearbeiten zu können.

[A12] Im Rahmen von Prüfaufträgen, die auch App-Aktualisierungen umfassen, hat der Auftragnehmer eine Frist von 5 Werktagen für die abschließende Bereitstellung des Prüfberichts für die aktualisierte Version einzuhalten. Die Frist beginnt an dem Tag, an dem die aktualisierte Version der App auf dem Markt erscheint. Eine gesonderte erneute Freigabe des Prüfantrages durch das BSI ist hier nicht erforderlich. Kann der Auftragnehmer dieser Anforderung in bestimmten Einzelfällen (z.B. besonders komplexe App) nicht nachkommen, so müssen der Prüfantragsteller, alle am Portal bekannten Nutzer der App und das BSI innerhalb dieser Frist entsprechend informiert werden.

[B4] Die durchschnittliche Bearbeitungsdauer bei Prüfungen von App-Aktualisierungen soll möglichst kurz sein, ohne dass dies zu Qualitätseinbußen führen darf.

[A13] Es müssen Apps, die für die Betriebssysteme Android, iOS und BlackBerry 10 bestimmt sind, einer Prüfung unterzogen werden können.

[A14] Für die Durchführung von Prüfungen darf nur Personal eingesetzt werden, das mindestens nach Ü1 gemäß Sicherheitsüberprüfungsgesetz (SÜG) überprüft ist. Dies gilt auch für evtl. Unterauftragnehmer. Eine Ausgliederung von Prüfleistungen an einen Unterauftragnehmer bedarf grundsätzlich der vorhergehenden Zustimmung des Auftraggebers. Ist von vornherein vom Auftragnehmer geplant, einen Unterauftragnehmer in die Durchführung von Prüfungen mit einzubeziehen, so ist dies bereits im Angebot explizit anzugeben.

Im Auftragsfall muss der Nachweis darüber, dass das Prüfpersonal des Auftragnehmers Ü1 überprüft ist, spätestens zum Zeitpunkt der Auftragsausführung dem Bedarfsträger BSI vorliegen.

C 3.3 Umfang der Prüfberichte

[A15] Für jede geprüfte App ist ein eigener Prüfbericht zu erstellen, dies gilt auch bei der Prüfung von App-Aktualisierungen.

[A16] Das Prüfverfahren des Auftragnehmers muss so konzipiert sein, dass Prüfberichte inhaltlich mindestens folgende Angaben / Felder enthalten:

1. Eindeutige Prüfbericht-ID
2. Kennung der Spezifikation des Prüfverfahrens / der Prüfverfahren (siehe C 3.2), das dem vorliegenden Prüfbericht zugrunde liegt
3. Eindeutiger Name der geprüften App mit vollständiger Versionskennung
4. Name der die App beinhaltenden Datei, Größe der Datei in Bytes, Hashwert der Datei, verwendeter Hash-Algorithmus
5. Name des Betriebssystems mit Versionskennung, für das die App bestimmt ist
6. Name des App-Herstellers
7. Datum, Uhrzeit und Zeitzonenangabe des Zeitpunkts des Abschlusses der Prüfung
8. Kurze Beschreibung der App / Zusammenfassung der App-Funktionalität (Freitext, 200-500 Zeichen)
9. Angaben darüber, ob die App konfigurierbar ist oder nicht (Optionen bei der Installation oder in den Einstellungen der App); falls sie konfigurierbar ist, eindeutige Angaben darüber, für welche Parametrisierungen der konfigurierbaren Parameter der Prüfbericht gilt
10. Name des Staates, dessen Recht laut AGB / Nutzungsbedingungen der

App für den Endnutzer gelten soll

11. Liste der Datengruppen, die von der App verarbeitet werden. Das Erheben, Kopieren, Weiterleiten, und Speichern von Daten wird auch ohne weitere Verarbeitungsschritte in diesem Zusammenhang als „Verarbeitung“ betrachtet. Einträge dieser Liste müssen mindestens folgende Angaben umfassen:
    11.1. Angabe des Zwecks, zu dem die Daten der jeweiligen Datengruppe erhoben und/oder verarbeitet werden.
    11.2. Einordnung der Daten, die typischerweise in dieser Datengruppe vorkommen, in „personenbezogen“ oder „nicht-personenbezogen“ i.S.v. §3 BDSG
    11.3. Angabe über die Erhebungsart (z.B. Lesen eines Sensors, Nutzereingabe, Auslesen des App-eigenen Speichers, Auslesen gemeinsamen Speichers im Endgerät)
    11.4. Angabe über das Sicherheitsniveau, mit dem die Daten verarbeitet werden (z.B. offene oder verschlüsselte Datenablage, Ablage im Shared Memory, App läuft im Browser-Kontext etc.)
    11.5. Angabe darüber, wie häufig die Daten verarbeitet werden
    11.6. Angabe darüber, ob die Daten auch anderen Apps zugänglich gemacht werden
    11.7. Angabe darüber, ob die Verarbeitung der Daten mit dem Zweck der App insgesamt vereinbar ist oder nicht (hier sind auch Werbung, Tracking und Analytics zu berücksichtigen)
    11.8. Angabe darüber, ob die App ihren Zweck insgesamt auch ohne die Verarbeitung dieser Daten, ohne Funktionalitäts- oder Komfortverlust, erfüllen könnte
12. Liste der verwendeten Funktionen, auf die die App tatsächlich zugreift (APIs, Bibliotheken, usw.), der Abhängigkeiten und der Berechtigungen. Einträge dieser Liste müssen mindestens folgende Angaben umfassen:
    12.1. Eindeutige Kennung der Funktionalität
    12.2. Angabe darüber, ob die Verwendung der Funktion / die Abhängigkeit / die Berechtigung mit dem Zweck der App vereinbar ist oder nicht
    12.3. Angabe darüber, ob die App auch ohne die Verwendung der Funktion / die Abhängigkeit / die Berechtigung ihren Zweck, ohne Funktionalitäts- oder Komfortverlust, erfüllen könnte
    12.4. Angabe darüber, ob im Falle der Verwendung von Bibliotheken Schwachstellen über diese bekannt sind
13. Liste der Netzwerk-Kommunikationskanäle, über die die App kommuniziert. Einträge dieser Liste müssen mindestens folgende Angaben enthalten:
    13.1. Beschreibung des Kanals

13.2. Land, in dem sich die Gegenstelle befindet

13.3. Angabe darüber, ob die Gegenstelle ein Server ist oder nicht. Falls es ein Server ist

13.3.1. DNS Name

13.3.2. IP Adresse

13.3.3. Name und Rechtsform des Betreibers

13.3.4. Name des Staates, dessen Recht bei der Inanspruchnahme des vom Server beanspruchten Dienstes laut Angaben des Betreibers zur Anwendung kommen soll

13.4. Angabe darüber, welcher Kommunikationsendpunkt diesen Kanal initiieren kann (Endgerät, Gegenstelle, oder beide)

13.5. Angaben über das zur Anwendung kommende Transportprotokoll (z.B. TCP Port 8088)

13.6. Angaben über die Sicherheitseigenschaften des Kanals hinsichtlich

13.6.1. Integrität

13.6.2. Vertraulichkeit

13.6.3. Authentifikation des Endgeräts

13.6.4. Authentifikation der Gegenstelle

13.7. Angabe darüber, welche Datengruppen über diesen Kanal in Richtung Gegenstelle verschickt werden oder auf indirekte Weise von der Gegenstelle aufgrund der Kommunikation induziert werden können. Diese Angabe kann in Form von Verweisen auf die betroffenen Einträge der Liste in Feld 11 erfolgen.

13.8. Angabe darüber, ob besondere Verfahren (wie z.B. OAuth) durch die App genutzt werden

14. Hinsichtlich etwaiger Sicherheitsfunktionen der App (z.B. Datenverschlüsselung, gesicherte Datenübertragung, Zertifikatshandling etc.) Angaben darüber, ob die verwendeten Sicherheitsfunktionen dem aktuellen Stand der Technik entsprechend umgesetzt sind (z.B. Standards und Normen, Einhaltung von Vorgaben aus Technischen Richtlinien des BSI, Mindeststandards des BSI etc.).

15. Hinweis auf evtl. fehlende oder falsch implementierte Sicherheitsfunktionen, ggf. auch serverseitig.

16. Zusammenfassende Liste von identifizierten Schwachstellen und evtl. Schadfunktionen

17. Andere Auffälligkeiten (z.B. Auffälligkeiten beim Zeitverhalten oder Hinweise auf Programmabstürze etc.)

18. Gesamtwertung und Votum über die App incl. Sicherheits-Ampel

19. Erläuterungen (Freitext; ggf. Empfehlung einer aus Sicht des

Auftragnehmers besser geeigneten vergleichbaren bereits getesteten App)

[A17] Falls Angaben über Kommunikationsendpunkte (Feld 13) nicht ermittelt werden können (z.B. TOR, Reverse Proxy), müssen sie mit entsprechendem Hinweis als „konnte nicht ermittelt werden“ gekennzeichnet werden.

[A18] Angaben, die im Laufe einer Prüfung nicht ermittelt wurden, da sie nicht zutreffen oder nicht relevant sind, müssen im Prüfbericht mit „nicht zutreffend“ markiert werden.

[A19] Angaben, die aus anderen Gründen nicht ermittelt wurden, müssen mit „unbekannt“ gekennzeichnet werden.

[B5] Im Feld „Erläuterungen“ soll begründet werden, warum die betreffenden Angaben bezüglich der Ausschlusskriterien A17, A18 und A19 nicht zutreffen oder warum sie nicht ermittelt werden konnten.

[A20] Wurden keine Schwachstellen (Feld 16) oder andere Auffälligkeiten (Feld 17) ermittelt, so ist dort „keine“ einzutragen.

[A21] Beim zu ermittelnden Votum (Feld 18) über die App („Sicherheitsampel“) ist durch den Prüfer das gesamte Prüfergebnis zu bewerten, zum Zweck der App und ihren Eigenschaften / Sicherheitseigenschaften in Relation zu setzen, und daraus abgeleitet die Einstufung „unbedenklich“ (grün), „eingeschränkt verwendbar unter Auflagen“ (gelb) oder „darf nicht verwendet werden“ (rot) zu vergeben. Lautet das Votum „eingeschränkt verwendbar unter Auflagen“ (gelb), so sind die empfohlenen zu beachtenden Auflagen konkret zu benennen. Das Votum darf nicht rein automatisiert generiert werden.

[B6] Der konkrete Aufbau der Prüfberichte ist nicht vorgegeben, es soll jedoch durch den Bieter ein Gestaltungsvorschlag erstellt werden. Erörtern Sie diesen Gestaltungsvorschlag und die Struktur des Prüfberichts. Fügen Sie hierzu auch Abbildung, Screenshot etc. bei.

Wo immer möglich, sollen Prüfergebnisse erläutert und bewertet werden. Eine unkommentierte Auflistung von Informationen, die sich dem Leser nicht unmittelbar erschließen, ist zu vermeiden.

Grundsätzlich ist auf eine übersichtliche Darstellung wert zu legen. Die Prüfberichte sollen in einem gängigen Datei-Format (.pdf, .doc(x), .xls(x) oder vergleichbar) erstellt werden.

Das finale Design des Prüfberichts sowie Änderungen daran bedürfen der Freigabe durch das BSI.

[B7] Die o.g. Anforderungen für die Felder 1 – 18 sind Mindestanforderungen; zusätzliche nützliche Informationen werden bei der Bewertung positiv berücksichtigt. Dies betrifft z.B. weitergehende Informationen zur Datensicherheit, Kommunikationssicherheit, Privatsphäre, Sicherheit zur Laufzeit etc.

C 3.4 Spezifikation des Prüfverfahrens

Regulär durchzuführende Prüfungen (App-Prüfung (Standard))

Die Spezifikation des Prüfverfahrens ist Grundlage der Prüfungen und damit des Prüfberichtes. Sie muss hinreichend genau beschreiben, wie die einzelnen Angaben eines Prüfberichts ermittelt werden. Die jeweilige Spezifikation ist anhand der folgenden Kriterien zu beschreiben.

[A22] Der Spezifikation muss eine eindeutige Kennung zugewiesen werden. Diese Kennung ist in Feld 2 aller Prüfberichte anzugeben. Der Auftragnehmer muss die Spezifikation reaktiv und proaktiv auf dem aktuellen Stand der Technik und der sicherheitstechnischen Erkenntnislage halten, und entsprechend fortentwickeln. Änderungen am Prüfverfahren erfordern eine entsprechende Anpassung der zugrundeliegenden Spezifikation. Im Falle einer Anpassung muss der Spezifikation eine neue Kennung zugewiesen werden. Die alte Version der Spezifikation muss dennoch weiter zur Verfügung stehen. Prüfberichte auf Grundlage von Prüfungen, die nach Maßgabe der alten Spezifikation durchgeführt wurden, werden nicht berührt. Änderungen in Prüfverfahren und Spezifikation bedürfen der vorhergehenden Zustimmung des BSI.

Sofern das BSI dem Auftragnehmer neue Erkenntnisse oder Anforderungen hinsichtlich der Sicherheit von Apps mitteilt, ist der Auftragnehmer verpflichtet, diese Erkenntnisse zeitnah in den Prüfspezifikationen zu berücksichtigen.

[A23] Da verschiedene Betriebssysteme unterschiedliche Funktionalitäten zur Verfügung stellen, wird vorausgesetzt, dass sich Prüfverfahren von Betriebssystem zu Betriebssystem erheblich unterscheiden. Demnach müssen separate Spezifikationen pro Betriebssystem erstellt werden. Diese Spezifikationen, sowie die entsprechenden Prüfverfahren, müssen sich unabhängig voneinander entwickeln können.

[A24] Die Spezifikation des verwendeten Prüfverfahrens muss in Textform vorliegen und vollständig sein. Als vollständig gilt eine Spezifikation nur dann, wenn

alle Angaben, die potenziell in den Feldern eines Prüfberichts vorkommen können, mit Ausnahme der mit „Freitext“ gekennzeichneten Felder, in der Spezifikation erläutert werden. Die Spezifikation des Prüfverfahrens pro Betriebssystem muss als Anlage dem Angebot beiliegen. Dies entbindet jedoch nicht von der Erläuterung der Spezifikation / der Prüfverfahren im Rahmen der jeweiligen Bewertungskriterien.

[A25] Prüfverfahren und Prüftiefe sind an die Art und Struktur der zu prüfenden App und des jeweiligen Betriebssystems anzupassen, dies gilt insbesondere für die grundsätzlich obligatorische manuelle Prüfung.

[A26] Apps, die dem Zweck der Realisierung von Sicherheitsfunktionen dienen (z.B. Secure Container) oder die in ihrer Funktion besondere Sicherheitsfunktionen anbieten (z.B. Messenger-Dienste) oder aus deren Verwendungszweck sich ein besonderer Sicherheitsbedarf ergibt (z.B. Banking-App, Browser oder Cloud-Dienst), sind mit hierfür angemessen großer Prüftiefe zu untersuchen. Dies schließt die Fähigkeit zum teilweisen oder vollständigen Reverse-Engineering mit ein.

[A27] Die Prüfmethoden müssen dem Stand der Technik entsprechen. Dies umfasst:

- die umfassende statische Analyse inklusive Auflösen von Java Reflection, zumindest in Bezug auf Apps für das OS Android,
- die dynamische Analyse, die sowohl in einer virtuellen Umgebung als auch auf „echter“ Hardware durchgeführt werden soll,
- die statische / dynamische Analyse muss (zumindest bei Apps für die Betriebssysteme iOS und Android) weitgehend automatisiert erfolgen soweit möglich,
- die manuelle Durchführung von Prüfaufgaben soweit erforderlich

Bei der Analyse ist auf eine möglichst große Code Coverage zu achten; diese ist soweit möglich auch je Analyse anzugeben. Eine symbolische Code Ausführung ist durchzuführen wo erforderlich.

Hinweis: ein rein automatisches Prüfverfahren wird als nicht ausreichend angesehen und gilt nicht als positive Beantwortung.

[B8] Der Prüfumfang einer App-Prüfung, die dabei eingesetzten Verfahren, und die erzielten Prüftiefen sollen je Betriebssystem dargelegt werden.

Dabei soll insbesondere auch auf die Aspekte:

- Nutzung statischer und dynamischer Prüfverfahren,
- automatisierte und manuelle Prüfungen,
- verwendete Prüfumgebungen (z.B. isolierte Umgebung, Simulation, reale Hardware etc.),
- Staffelung der Prüftiefen

eingegangen werden. Die Ausführungen sollen nicht mehr als 6 DIN A4 Seiten (also ca. 7500 Zeichen) je Betriebssystem umfassen, und eine Einschätzung der Angemessenheit, Ausgewogenheit, Zuverlässigkeit und Nachvollziehbarkeit des jeweiligen Prüfverfahrens ermöglichen.

[B9] Der im Mittel pro App-Prüfung angesetzte Zeitaufwand der Prüfer in Personenstunden ist darzulegen. Es wird geschätzt, dass eine App-Prüfung im Mittel mit einem Zeitaufwand von 12 Personenstunden verbunden ist, die Prüfung einer App-Aktualisierung mit 6 Personenstunden.

Abweichungen nach oben oder nach unten sind zu begründen. Sofern Prüfleistungen an Subunternehmen ausgegliedert werden sollen, ist dies explizit anzugeben.

[A28] Die Angaben der Felder 1-18 des Prüfberichtes (siehe Kapitel C 3.3) müssen ermittelt werden.

Dabei muss die Spezifikation des jeweiligen Prüfverfahrens folgende Aspekte umfassen:

[B10] *Umgang mit Parametervielfalt:* Das Prüfverfahren soll die Parametrierbarkeit von Apps (Optionen bei der Installation oder in den Einstellungen der App) angemessen berücksichtigen (Feld 9) und den Raum der Parameterwerte hinreichend abdecken. Insbesondere soll der damit ggf. verbundene Interpretationsspielraum in sicherheitstechnischer Sicht möglichst gering gehalten werden. Die Abhängigkeit des Prüfergebnisses von der Parameterkomplexität bzw. die Größe des Parameterraumes ist ggf. anzugeben. Der Auftragnehmer soll selbst sinnvolle Parametrisierungen vornehmen (z.B. eine optionale Verschlüsselung einschalten), im Zweifelsfalle ist mit dem Auftraggeber Rücksprache zu halten.

[B11] *Datengruppen:* Alle vom Prüfverfahren unterstützten Datengruppen sollen spezifiziert werden (Feld 11), also z.B. Systemdaten, Identifizierungsdaten, Sensordaten, Nutzerdaten etc. Die Spezifikation soll eine Einteilung von Daten in Gruppen vorsehen, die einerseits ausreichend Granularität bietet zur Generierung von ausreichend aussagekräftigen und differenzierten Prüfberichten, anderseits den Aufwand der Auswertung der Prüfberichte

begrenzt. Datengruppen dürfen sich teilweise überlappen, d.h. das gleiche Datum darf in mehreren Datengruppen vorkommen.

[B12] *BDSG-Einschätzung:* Die von der App im Endgerät verwendeten oder erhobenen Daten sollen daraufhin betrachtet werden, ob sie als personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG) einzuordnen sind.

[B13] *Erhebungsarten:* Alle auf den Endgeräten vorkommenden Erhebungsarten (z.B. Nutzung Kamera, Mikrofon, Gyrosensor, GPS etc.) sollen möglichst vollständig erfasst werden (Feld 11.3).

[B14] *Verwendete Funktionen:* Das Prüfverfahren soll Funktionen, Abhängigkeiten und Berechtigungen (Feld 12) angemessen berücksichtigen, also z.B. verwendete Frameworks und APIs auflisten, untersuchen und bewerten, Berechtigungen anhand der Berechtigungssklassifikation untersuchen und bewerten (Systemberechtigungen, über- oder unterpriviligierte Funktionsaufrufe etc.). Evtl. Schnittstellen der App zu anderen Apps sind auf Absicherung zu untersuchen. Einstiegspunkte in die App sind aufzulisten. Für jede berücksichtigte Funktionalität soll die Spezifikation eine Kurzbeschreibung aufweisen.

[B15] *Netzwerk-Kommunikationskanäle:* Alle von der zu prüfenden App verwendeten Kommunikationskanäle sollen ermittelt, untersucht und sicherheitstechnisch bewertet werden (Feld 13).

[B16] *Sicherheitsfunktionen:* Es soll geprüft werden, ob sicherheitstechnische Funktionen der App (Feld 14) dem aktuellen Stand der Technik entsprechend umgesetzt wurden und ob erwartete oder erforderliche Sicherheitsfunktionen fehlen (Feld 15). Dabei soll auch die Einhaltung einschlägiger Standards und Normen sowie die Erfüllung von Forderungen und Vorgaben aus Technischen Richtlinien und Mindeststandards des BSI geprüft werden. Die Prüfung soll dokumentiert werden.

[B17] *Schwachstellen / Schadfunktionen / Sicherheitsziele:* Die zu prüfende App soll eingehend auf Schwachstellen und Schadfunktionen, sowie die Einhaltung von Sicherheitszielen untersucht werden (Feld 16). Es soll eine Auflistung der gefundenen Schwachstellen erstellt werden, evtl. Schadfunktionen sind dabei besonders zu kennzeichnen.

[B18] *Gesamtwertung und Votum:* Die Gesamtwertung und das Votum über die App (Sicherheits-Ampel) sollen durch den Prüfer vorgenommen werden (Feld 18). Es ist darzulegen, wie Gesamtwertung und Votum gebildet werden.

[B19] Sofern die Prüfverfahren / die Spezifikationen über die Mindestanforderungen der Felder 1 – 18 hinausgehende Kriterien berücksichtigen und Informationen zur Verfügung stellen (siehe auch Bewertungskriterium B7), sind diese nach Art, Umfang und Zugewinn näher darzulegen.

Erweiterte Prüfung mit max. Prüftiefe
(Erweiterte Prüfung (nach Aufwand))

[A29] Im Einzelfall und bei Bedarf muss der Auftragnehmer in der Lage sein, eine Prüfung von Apps mit maximaler Prüftiefe durchzuführen . Des Weiteren muss der Auftragnehmer in der Lage sein, Apps welche im Verbund mit einem oder mehreren bestimmten korrespondierenden Server arbeiten, auf bekannte Angriffsverfahren hin zu untersuchen und hierzu diese Angriffsverfahren nachstellen zu können. Dies muss ggf. die Simulation eines Angriffs auf die Client-Server-Kommunikation beinhalten und auch serverseitige Schwachstellen aufzeigen (z.B. fehlerhafte OAuth-Implementierung).
Die rechtlichen Rahmenbedingungen für eine solche Server-Prüfung sind im Einzelfall mit dem BSI und ggf. dem Betreiber des Servers abzustimmen.

Für eine solche Prüfung mit maximaler Prüftiefe ist ein separater Auftrag des BSI nach vorhergehender Aufwandsabschätzung erforderlich, der nicht gemäß der App-Prüfungspauschale, sondern nach Aufwand abgerechnet wird.

[B20] Die Möglichkeiten und Verfahren des Auftragnehmers hinsichtlich der Prüfung mit maximaler Prüftiefe sind darzulegen. Die Ausführungen sollen nicht mehr als 2 DIN A4 Seiten umfassen (also ca. 2500 Zeichen).

C 3.5 Übermittlung, Verwaltung und Verwendung von Prüfberichten

[A30] Die Prüfberichte müssen von einem gesicherten Bereich eines vom Auftragnehmer zu betreibenden Webportals abrufbar sein. Der Zugang darf nur nach erfolgter Authentifikation und Authentisierung erfolgen. Das Portal ist auf einem Server mit Standort in Deutschland zu hosten. Der Server selbst, das zugehörige Netzwerk sowie der Zugang zum Server sind nach den anerkannten Regeln der IT-Sicherheit abgesichert zu betreiben. Das entsprechende Sicherheits- bzw. Realisierungskonzept ist mit dem BSI abzustimmen.

[B21] Das Webportal zur Bereitstellung / Verwaltung von Prüfberichten soll nach Möglichkeit dasselbe sein, über das auch die Übermittlung der Prüfanträge stattfindet, die Prüfaufträge verwaltet werden, und über das auch die Nutzerverwaltung erfolgt (siehe Kapitel C 3.1)

[B22] Alle auf dem Webportal registrierten berechtigten Nutzer sollen in der Lage sein, eine Auflistung aller bereits geprüften Apps einzusehen, und abhängig von Identität und Berechtigung auf Prüfberichte zuzugreifen. Hierzu soll das Webportal mandantenfähig sein, d.h. der Benutzerkontext soll entsprechend berücksichtigt werden. Einzelne Nutzer sollen weder erkennen können, durch welchen anderen Nutzer App-Prüfungen veranlasst wurden, noch welche Apps andere Nutzer einsetzen. Das Portal soll Sortierfunktionen bereitstellen, die eine Sortierung nach Name der App, Betriebssystem, Datum des Prüfberichts, Bewertung der App (Votum) etc. ermöglichen.

[B23] Jeder Nutzer soll für sich auf dem Portal eine Liste „eigener“ Apps anlegen und verwalten können, um das Sicherheitsniveau (Sicherheits-Ampel, evtl. Black- oder Whitelisting durch das BSI) der von ihm verwendeten Apps stets im Blick zu haben. Auf die jeweils aktuelle, zuletzt geprüfte Version einer App ist hinzuweisen. Die berechtigten Nutzer und deren Zugriffsrechte sollen vom BSI über eine geeignete Schnittstelle (z.B. JSON, XML oder CSV) über einen geeigneten abgesicherten Zugang einfach hinzugefügt und wieder entfernt werden können, Änderungen sollen umgehend wirksam werden.

[B24] Das Webportal soll möglichst selbsterklärend, nutzerfreundlich und intuitiv bedienbar sein. Die letztendliche Ausgestaltung des Portals ist mit dem BSI abzustimmen.

[A31] Dem BSI ist das Recht einzuräumen, Prüfberichte nach eigenem Ermessen aus dem Webportal herunter zu laden und im Rahmen seines gesetzlichen Auftrags frei zu verwenden, d.h. auch Dritten zur Verfügung zu stellen. Auch ist dem BSI das Recht einzuräumen, diesen Stellen die Berechtigung zum Zugriff auf die Prüfberichte zu erteilen.

Eine generelle, allgemeine Veröffentlichung der Prüfberichte ist nicht vorgesehen. Dem BSI ist jedoch das Recht einzuräumen, im Einzelfall für die Öffentlichkeit relevante Warnungen auf Basis der Prüfergebnisse zu veröffentlichen. Nutzungsrechte an den Prüfberichten sind der gesamten öffentlichen Verwaltung sowie weiteren vom BSI benannten berechtigten Nutzern einzuräumen. Dies können z.B. auch für das BSI tätige Firmen sein.

[A32] Dem BSI muss ein individueller, gesondert abgesicherter Zugriff auf das Webportal gewährt werden. Mit diesem Zugriff muss es möglich sein, geprüften Apps über das Ergebnis der Prüfung und des Votums hinaus („Sicherheits-Ampel“) den Status „whitelisted“ oder „blacklisted“ zuzuweisen. Ein solcher ggf. vom BSI vergebener Status ersetzt das Votum gemäß Sicherheits-Ampel. Dieser Status muss den übrigen Teilnehmern zusätzlich zur Sicherheits-Ampel und augenfällig eingeblendet werden. Ein geänderter Status (Sicherheitsampel oder durch das BSI vergebener Status) ist allen am Portal registrierten Nutzern der betreffenden App („Liste eigener Apps“, s.o.) per Mail durch das Portal bzw. durch den Auftragnehmer umgehend mitzuteilen.

[B25] Das Webportal kann eine Export-Funktionalität bieten, die einen Import von Apps bzw. von Verweisen auf Apps, die den Status „grün“ oder „gelb“ gemäß Sicherheits-Ampel oder „whitelisted“ nach BSI-Bewertung aufweisen, durch möglichst verschiedene MDM Systeme ermöglicht. Die Export-Funktion kann, muss aber nicht, den Vertrieb von solchen Apps unterstützen.

[A33] Nach Ende der Rahmenvereinbarung muss das Webportal für mindestens 12 weitere Monate zur uneingeschränkten Nutzung zur Verfügung stehen. Dem BSI ist zudem die Möglichkeit zu eröffnen, bei Bedarf das Portal komplett zu übernehmen und in Eigenregie weiter zu betreiben.

[A34] Die Prüfberichte müssen bezüglich ihrer Darstellung barrierefrei sein. Weitergehende Informationen und Randbedingungen hat das Informationstechnikzentrum Bund (ITZBund) auf seinen Seiten.... veröffentlicht..

Mit BaNu http://www.banu.bund.de/DE/Home/home_node.html stellt das ITZBund eine kostenlose Webanwendung zur Verfügung, mit der Sie selbst prüfen können, ob Ihre Internetangebote, PDF- und Office Dokumente oder Client-Anwendungen nutzungsfreundlich- und barrierefrei sind.

D Preise

Zu den nachgefragten Angebotsteilen sind die Einzelpreise in das Preisblatt als „Festpreise“ einzutragen.

Die Einzelpreise müssen alle Nebenkosten beinhalten.

Die errechnete Preiskennzahl (Gesamtpreis) ist in das Angebotsformular zu übernehmen.

Ein Anspruch auf einen Umsatz in Höhe der Preiskennzahl besteht nicht, er kann über bzw. auch unterschritten werden.

E Vertragsbedingungen

E 1. Allgemeine Geschäftsbedingungen des Beschaffungsamtes des BMI (AGB)

Es gelten mit Vertragsschluss die Allgemeinen Geschäftsbedingungen des Beschaffungsamtes des BMI vom 27.07.2016 (siehe beigefügte **„Anlage AGB“)**

E 2. Rahmenvereinbarung

Siehe Anlage 3

E 3. Anlagen die diesen Vergabeunterlagen beiliegen

1. Anlage „Angebotsformular“
2. Rahmenvereinbarung
3. Anlage “Kriterienkatalog”
4. Anlage “Preisblatt”