Bundesamt
für Sicherheit in der
Informationstechnik

Projekt 481

Pflege und Weiterentwicklung der Kryptobibliothek Botan (Weiterentwicklung Botan)

Leistungsbeschreibung
und Besondere Bewerbungsbedingungen

Version 1.0

Datum: 13.07.2021

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

A Leistungsbeschreibung

1 Übersichtsinformationen zum Projekt

1.1 Auftraggeber

Als die Cyber-Sicherheitsbehörde des Bundes gestaltet das Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Das BSI wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Derzeit sind dort ca. 1.400 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Das BSI ist die zentrale, unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit. Das BSI schützt die Netze des Bundes; es richtet sich jedoch zugleich auch an gewerbliche und private Anbieter wie Nutzer von Informationstechnik. Das breite Aufgabenspektrum des BSI ist im BSI-Gesetz geregelt.

1.2 Ausgangslage und Handlungsbedarf

Ausgangslage

Kryptografische Primitive und Protokolle sind die Grundlage der IT-Sicherheit im Allgemeinen und der vom BSI zugelassenen bzw. zertifizierten IT-Sicherheitsprodukte, z.B. zum Zwecke der Zulassung, im Speziellen. Eine verlässliche und vertrauenswürdige Implementierung dieser Primitive und Protokolle ist somit von hoher Wichtigkeit. Im Rahmen des abgeschlossenen BSI-Projekts "197 - Sichere Implementierung einer allgemeinen Kryptobibliothek" ist daher ein BSI Entwicklungszweig inklusive detaillierter Kryptodokumentation für die Kryptobibliothek Botan entstanden. Dabei wurden die zu diesem Zeitpunkt gängigen Kryptoprimitive und Protokolle gemäß den technischen Standards und Richtlinien des BSI geprüft bzw. implementiert und dokumentiert.

Der BSI Entwicklungszweig von Botan hat ein Angebot für Unternehmen geschaffen, Botan als geprüfte und dokumentierte Kryptobibliothek in IT-Sicherheitsprodukten zu verwenden. Als prominentes Beispiel kann hier der E-Mail Client Thunderbird der Mozilla Foundation genannt werden, der seit 08/2020 Botan (Hauptentwicklungszweig) als grundlegende Kryptobibliothek einsetzt.

In der aktuellen Version des BSI Entwicklungszweigs von Botan finden sich bereits erste Ansätze quantencomputerresistente Verfahren zu etablieren. Hierzu wurde das Signaturverfahren XMSS+ in einer frühen Phase des mittlerweile verabschiedeten IETF RFC 8391 in Botan implementiert. Vor dem Hintergrund der BSI-Studie "Entwicklungsstand Quantencomputer", der vom BSI herausgegebenen Handlungsempfehlungen mit dem Titel "Migration zu Post-Quanten-Kryptografie" und der um quantencomputerresistente Verfahren ergänzten BSI technische Richtlinie TR-02102-1, haben sich die Migrationsbemühungen des BSI in Richtung Post-Quanten-Kryptografie intensiviert. Dies ist allerdings im derzeitigen BSI Entwicklungszweig von Botan noch nicht abgebildet. Insbesondere sind beispielsweise die derzeit vom BSI empfohlenen Post-Quanten Verfahren noch nicht im BSI Entwicklungszweig implementiert (oder es handelt sich bei der Implementierung um eine frühere Version des Verfahrens).

Im Rahmen des vom BMBF geförderten Projekts "Kryptobibliothek Botan für Langlebige Sicherheit" (KBLS, https://www.rohde-schwarz.com/de/loesungen/cybersicherheit/about-us/research/kbls_254244.html) werden voraussichtlich die Verfahren CRYSTALS-Kyber und CRYSTALS-Dilithium aus dem NIST Post-Quanten Standardisierungsprozess in Botan implementiert. Die im KBLS-Projekt getroffene Auswahl ist unabhängig von den aktuellen BSI Empfehlungen. Hier sind jedoch potentiell Synergieeffekte erkennbar. So könnten die

o.g. Verfahren beispielsweise über einen Prüf- und Dokumentationsschritt in den BSI-Entwicklungszweig von Botan übernommen werden.

Handlungsbedarf

Das BSI hat mit dem BSI Entwicklungszweig von Botan eine sichere Kryptobibliothek geschaffen. Um dies auch in Zukunft gewährleisten zu können, muss der BSI Entwicklungszweig aktualisiert und weiterentwickelt werden. Insbesondere müssen die aktuell vom BSI empfohlenen quantencomputerresistenten kryptografischen Verfahren sowie die vom BSI geforderte Umsetzung einer hybriden Schlüsseleinigung in TLS implementiert werden. Im Folgenden wird der Handlungsbedarf genauer beschrieben.

Während der Hauptentwicklungszweig der Botan-Bibliothek derzeit in der Version 2.17.3 (s. https://github.com/randombit/botan) vorliegt, befindet sich der BSI-Entwicklungszweig auf Stand der Version 2.4.0 (s. https://github.com/Rohde-Schwarz/botan). Eine Angleichung der Entwicklungsstände und entsprechende Überarbeitung der Kryptodokumentation ist dringend geboten, um die Attraktivität der Botan-Bibliothek als geprüfte und dokumentierte Kryptobibliothek für den Einsatz in IT-Sicherheitsprodukten zu erhalten.

Der Handlungsbedarf beschränkt sich jedoch nicht nur auf eine Aktualisierung und Angleichung an den Status quo. Neben dem NIST-Standardisierungsprozess "Post-Quantum Cryptography Standardization", aus dem vsl. 2022-2024 erste Standards hervorgehen werden, und den bereits finalisierten Standards zu hashbasierten Signaturverfahren (IETF RFC 8391, IETF RFC 8554, NIST SP 800-208) hat auch das BSI seine Migrationsbemühungen in Richtung Post-Quanten-Kryptografie intensiviert (s. Ausgangslage). Im Hochsicherheitsbereich geht das BSI derzeit von der Arbeitshypothese aus, dass Anfang der 2030er Jahre ein kryptografisch relevanter Quantencomputer verfügbar sein wird. Diese Aussage ist nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen, sondern stellt einen Richtwert für die Risikobewertung dar. Die Integration von Post-Quanten-Kryptografie in IT-Sicherheitsprodukte ist jedoch ein komplexes Unterfangen mit noch wenig vorliegenden Erfahrungswerten. Zudem steht man mit der Implementierungssicherheit von quantencomputerresistenten kryptografischen Verfahren noch am Anfang. Daher ist es notwendig ein konkretes Angebot für Hersteller von IT-Sicherheitsprodukten in Form einer nach gegenwärtigem Kenntnisstand geprüften Kryptobibliothek für den Einsatz und die Verwendung von Post-Quanten-Kryptografie zu schaffen, um den vom BSI gewünschten breiten Einsatz quantencomputerresistenter Kryptografie zu fördern.

1.3 Auftragsgegenstand und Projektziele

Ziel des Projekts ist die Weiterentwicklung und Pflege des BSI-Entwicklungszweigs der Kryptobibliothek Botan. Das Projekt verfolgt vier zentrale Ziele:

- Angleichung des BSI Entwicklungszweigs an die (im Zeitraum der Projektdurchführung) aktuelle Botan Version (Hauptentwicklungszweig) in Abstimmung mit dem BSI.
- Erweiterung der Botan-Bibliothek um Verfahren der Post-Quanten-Kryptografie (orientiert an NIST, IETF, TR-02102-1). Die Auswahl der Verfahren wird vom BSI getroffen und umfasst die Verfahren FrodoKEM, Classic McEliece, CRYSTALS-Kyber, CRYSTALS-Dilithium, XMSS, LMS, und Sphincs+.
- Implementierung einer hybriden Schlüsseleinigung im TLS 1.3 Stack (sofern bis dahin verfügbar) der Botan-Bibliothek (orientiert sich an IETF und BSI TLS-Mindeststandard).
- Prüfung der vom BSI empfohlenen und implementierten Bestandteile (u.a. auf Seitenkanalresistenz) und entsprechende Überarbeitung der Kryptodokumentation.

1.4 Projektstrukturplan

Im Rahmen der Leistungserbringung sind folgende Arbeitspakete (AP) vorgesehen.

- AP 1: Auftakt
- AP 2: Initiale Angleichung
  - AP 2.1: Analyse und Spezifikation
  - AP 2.2: Angleichung der Version
  - AP 2.3: Testspezifikation und Tests AP 2
  - AP 2.4: Überarbeitung der Kryptodokumentation zu AP 2
  - AP 2.5: Auslieferung AP 2
- AP 3: Entwicklungsbegleitende Angleichung
  - AP 3.1: Analyse und Spezifikation
  - AP 3.2: Angleichung der Version
  - AP 3.3: Testspezifikation und Tests AP 3
  - AP 3.4: Überarbeitung der Kryptodokumentation zu AP 3
  - AP 3.5: Auslieferung AP 3
- AP 4: Weiterentwicklung Post-Quanten Verfahren
  - AP 4.1: Analyse und Spezifikation
  - AP 4.2: Implementierung: Post-Quanten Verfahren
  - AP 4.3.: Testspezifikation und Tests AP 4
  - AP 4.4: Erstellung der Kryptodokumentation zu AP 4
  - AP 4.5: Auslieferung AP 4
- AP 5 (OPTIONAL): Weiterentwicklung hybride Schlüsseleinigung in TLS
  - AP 5.1: Analyse und Spezifikation
  - AP 5.2: Implementierung: hybride Schlüsseleinigung in TLS
  - AP 5.3.: Testspezifikation und Tests AP 5
  - AP 5.4: Erstellung der Kryptodokumentation zu AP 5
  - AP 5.5: Auslieferung AP 5
- AP 6: Abschlusspräsentation
- AP 7: Wartung und Pflege

AP 5 ist eine optionale Leistung. Diese muss vom Bieter angeboten werden, der Auftraggeber verzichtet jedoch ggf. generell auf deren Beauftragung. Die Beauftragung des AP 5 ist abhängig davon, ob bis dahin die Basisfunktionalität von TLS 1.3 in Botan implementiert ist, die zur Durchführung dieses APs benötigt wird. Falls AP 5 zum geplanten Zeitpunkt nicht beauftragt werden kann, besteht die Möglichkeit, die restlichen Arbeitspakete (AP 6 und AP 7) vorzuziehen und AP 5 im Anschluss zu beauftragen.

Das optionale AP 5 kann vom Auftraggeber bis zum Abschluss von AP 7 beauftragt werden.

2 Beschreibung der Arbeitspakete

Der Auftragnehmer hat die in den folgenden Arbeitspaketen dargestellten Leistungen zu erbringen.

2.1 Arbeitspaket 1: Auftaktbesprechung

Zu Beginn des Projekts findet beim Auftraggeber (AG) in Bonn eine Auftaktbesprechung zwischen AG und allen wesentlich am Projekt beteiligten Mitgliedern des Projektteams des AN, jedoch maximal sechs Personen, statt. Gemäß der zum Auftakt geltenden COVID-19 Verordnungen kann diese Besprechung als Videokonferenz erfolgen. Diese ist vom AN zu organisieren. Es wird vorausgesetzt, dass sich die Teilnehmer vor der Besprechung umfassend mit dem Projekt auseinandergesetzt haben.

In der Auftaktbesprechung wird vom AN das Vorgehen zu allen Arbeitspaketen im Detail vorgestellt. Verbleibende offene Fragen werden zwischen AG und AN diskutiert und verbindlich geklärt. Die Planung wird gegebenenfalls weiter konkretisiert und die Regeln der Zusammenarbeit verabschiedet.

Ferner sind die Kommunikationswege zu etablieren und die Erreichbarkeit der beteiligten Personen seitens AN und AG abzustimmen. Aufgrund der COVID-19 Situation ist ein fester Kommunikationsweg über ein vom AN organisiertes Videokonferenzsystem einzurichten.

Kam es bei der Auftragserteilung zu zeitlichen Verschiebungen (vgl. Kapitel 6.2.1.4, Zuschlagskriterium „Zahlungs- und Meilensteinplan“) so werden die daraus ggf. resultierenden Terminverschiebungen verbindlich zwischen AN und AG abgestimmt. Der aktualisierte Zahlungs- und Meilensteinplan ist vom AN mit dem Besprechungsprotokoll vorzulegen.

2.2 Arbeitspaket 2: Initiale Angleichung

2.2.1 Arbeitspaket 2.1: Analyse und Spezifikation

In der Analyse-Phase ist zum einen der aktuelle Stand des Botan-Hauptentwicklungszweiges zu sichten und die Differenzen zum aktuellen BSI-Entwicklungszweig zu identifizieren.

Aufbauend auf oben beschriebener Analyse ist in Abstimmung mit dem BSI ein Pflichtenheft zu erstellen, welches die Realisierung der nachfolgenden Unter-Arbeitspakete in AP 2 spezifiziert. Darin ist zu spezifizieren, welche Aspekte aus dem Hauptzweig in den BSI-Entwicklungszweig eingepflegt werden sollen.

2.2.2 Arbeitspaket 2.2: Angleichung der Version

In diesem Arbeitspaket sind die in AP 2.1 spezifizierten Angleichungen des BSI-Entwicklungszweiges an den Hauptentwicklungszweig vorzunehmen. Der AN hat dabei insbesondere auch zu prüfen und berücksichtigen, gegen welche SCA-Szenarios (v.a. Laufzeitangriffe) die Verfahren durch eine geeignete Implementierung geschützt werden können (siehe z.B. AIS 46[1]). Die genaue Vorgehensweise muss dann mit dem BSI abgestimmt werden. Zusätzlich muss eine Implementierung der notwendigen Ein- und Ausgabekodierungen erfolgen.

Als Programmiersprache ist C++ zu wählen. Sämtliche Software, die im Rahmen des Projekts entsteht, muss unter der selben Lizenz wie der aktuelle Botan BSI-Entwicklungszweig stehen.

1 Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Anwendungshinweise-und-Interpretationen/anwendungshinweise-und-interpretationen_node.html

Die Funktionen der Kryptobibliothek sollen mit möglichst geringem Aufwand z.B. von Mitarbeitern des BSI evaluiert werden können. Bei der Programmierung ist mindestens Folgendes umzusetzen:

- Vermeidung komplexer Verschachtelungen von Funktionen (z.B. über mehr als fünf Ebenen hinweg).
- Vermeidung komplexer Verschachtelungen von Datenstrukturen.
- Sofern Verschachtelungen erforderlich sind, sollen diese auf möglichst wenige Sourcefiles verteilt werden.
- Nach Möglichkeit sollen Teilfunktionen („Module“) durch separate Kompilation der entsprechenden Sourcefiles in Testprogramme eines Evaluators/Entwicklers einfügbar sein.

2.2.3 Arbeitspaket 2.3: Testspezifikation und Tests AP 2

Für die in AP 2 vorgenommenen Angleichungen ist ggf. die vorhandene Testspezifikation (siehe https://github.com/Rohde-Schwarz/botan/blob/master/doc/bsi/testspecification.pdf) anzupassen bzw. zu erweitern und mit dem BSI abzustimmen. Hierbei sind sowohl Positivtests, die das spezifizierte Verhalten des Testobjekts validieren, als auch Negativtests, die die Behandlung von Ausnahme- und Fehlersituationen belegen, durchzuführen. Die Resistenz aller implementierten Verfahren gegen Seitenkanalangriffe ist bei der Testung in angemessener Form zu berücksichtigen, die genaue Vorgehensweise ist mit dem BSI abzustimmen.

Außerdem muss der Software-Reviewprozess beschrieben und nach Absprache mit dem BSI eine statische und dynamische Softwareanalyse durchgeführt werden. Dazu zählt ein Codereview durch das Entwicklungsteam und die Analyse mit automatisierten Tools.

Alle durchgeführten Tests und Analysen und deren Ergebnisse sind in einem Testreport zu dokumentieren.

2.2.4 Arbeitspaket 2.4: Überarbeitung der Kryptodokumentation

Für die in AP 2 vorgenommenen Angleichungen muss die Kryptodokumentation von Botan (in englischer Sprache) entsprechend überarbeitet werden. Dies beinhaltet sowohl eine Beschreibung der Architektur (Grob- und Feinspezifikation), als auch der Schnittstellen. Umfang und Dokumentationstiefe müssen dabei den Anforderungen an eine VS-NfD-Evaluation entsprechen, siehe beiliegendes Dokument „Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD, BSI Version 1.4, August 2020“.
Die in der Bibliothek implementierten kryptografischen Abläufe und Verfahren müssen dazu gemäß beiliegendem Dokument „Detailspezifikation kryptographischer Abläufe und Mechanismen, BSI, Version 1.0, Januar 2015“ dokumentiert werden.
Zusätzlich sind ausführlich kommentierte Anwendungsbeispiele zu erstellen.

2.2.5 Arbeitspaket 2.5: Auslieferung AP 2

Die in AP 2 angeglichene Botan-Version wird im BSI-Entwicklungszweig auf dem GitHub Account (https://github.com/BSI-Bund) bereitgestellt. Im Zuge dessen ist der BSI-Entwicklungszweig vom Rohde & Schwarz GitHub Account auf den BSI GitHub Account umzuziehen.

Der AN muss sich aktiv darum bemühen, dass die Ergebnisse des Projekts in die OpenSource-Entwicklung von Botan entsprechend den geltenden Lizenzbestimmungen zurückfließen. Dies gilt insbesondere für identifizierte Schwachstellen und Sicherheitslücken. Das Ziel ist hier, dass der BSI-Entwicklungszweig und der Hauptentwicklungszweig möglichst deckungsgleich sind.

2.3 Arbeitspaket 3: Entwicklungsbegleitende Angleichung

2.3.1 Arbeitspaket 3.1: Analyse und Spezifikation

Falls während der Projektlaufzeit nach Abschluss der initialen Angleichung (AP 2) noch Aktualisierungen am Stand des Botan-Hauptentwicklungszweiges vorgenommen werden, sind diese zu sichten und die Differenzen zum aktuellen BSI-Entwicklungszweig zu identifizieren.

Aufbauend darauf ist mit dem BSI abzustimmen, ob bzw. welche Änderungen aus dem Hauptzweig in den BSI-Entwicklungszweig eingepflegt werden sollen, und in einem Pflichtenheft festzuhalten. Insbesondere eine mögliche TLS 1.3 Implementierung im Hauptentwicklungszweig ist hierbei von Interesse.

Alle Angleichungen in diesem Arbeitspaket geschehen grundsätzlich nach Abruf durch das BSI.

2.3.2 Arbeitspaket 3.2: Angleichung der Version

In diesem Arbeitspaket sind die in AP 3.1 spezifizierten Angleichungen des BSI-Entwicklungszweiges an den Hauptentwicklungszweig vorzunehmen. Der AN hat dabei insbesondere auch zu prüfen und zu berücksichtigen, gegen welche SCA-Szenarios (v.a. Laufzeitangriffe) die Verfahren durch eine geeignete Implementierung geschützt werden können (siehe z.B. Anlagen zu [AIS 46]). Die genaue Vorgehensweise muss dann mit dem BSI abgestimmt werden. Zusätzlich muss eine Implementierung der notwendigen Ein- und Ausgabekodierungen erfolgen.

Als Programmiersprache ist C++ zu wählen. Sämtliche Software, die im Rahmen des Projekts entsteht, muss unter der selben Lizenz wie der aktuelle Botan BSI-Entwicklungszweig stehen.

Die Funktionen der Kryptobibliothek sollen mit möglichst geringem Aufwand z.B. von Mitarbeitern des BSI evaluiert werden können. Bei der Programmierung muss mindestens Folgendes umgesetzt werden:

- Vermeidung komplexer Verschachtelungen von Funktionen (z.B. über mehr als fünf Ebenen hinweg).
- Vermeidung komplexer Verschachtelungen von Datenstrukturen.
- Sofern Verschachtelungen erforderlich sind, sollen diese auf möglichst wenige Sourcefiles verteilt werden.
- Nach Möglichkeit sollen Teilfunktionen („Module“) durch separate Kompilation der entsprechenden Sourcefiles in Testprogramme eines Evaluators/Entwicklers einfügbar sein.

2.3.3 Arbeitspaket 3.3: Testspezifikation und Tests AP 3

Für die in AP 3 vorgenommenen Angleichungen ist ggf. die vorhandene Testspezifikation anzupassen bzw. zu erweitern und mit dem BSI abzustimmen. Hierbei sind sowohl Positivtests, die das spezifizierte Verhalten des Testobjekts validieren, als auch Negativtests, die die Behandlung von Ausnahme- und Fehlersituationen belegen, durchzuführen. Die Resistenz aller implementierten Verfahren gegen Seitenkanalangriffe ist bei der Testung in angemessener Form zu berücksichtigen, die genaue Vorgehensweise ist mit dem BSI abzustimmen.

Außerdem muss der Software-Reviewprozess beschrieben und nach Absprache mit dem BSI eine statische und dynamische Softwareanalyse durchgeführt werden. Dazu zählt ein Codereview durch das Entwicklungsteam und die Analyse mit automatisierten Tools.

Alle durchgeführten Tests und Analysen und deren Ergebnisse sind in einem Testreport zu dokumentieren.

2.3.4 Arbeitspaket 3.4: Überarbeitung der Kryptodokumentation

Für die in AP 3 vorgenommenen Angleichungen muss die Kryptodokumentation von Botan (in englischer Sprache) entsprechend überarbeitet werden. Dies beinhaltet sowohl eine Beschreibung der Architektur (Grob- und Feinspezifikation), als auch der Schnittstellen. Umfang und Dokumentationstiefe müssen dabei den Anforderungen an eine VS-NfD-Evaluation entsprechen, siehe beiliegendes Dokument „Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD, BSI Version 1.4, August 2020“.
Die in der Bibliothek implementierten kryptographischen Abläufe und Verfahren müssen dazu gemäß beiliegendem Dokument „Detailspezifikation kryptographischer Abläufe und Mechanismen, BSI, Version 1.0, Januar 2015“ dokumentiert werden.
Zusätzlich sind ausführlich kommentierte Anwendungsbeispiele zu erstellen.

2.3.5 Arbeitspaket 3.5: Auslieferung AP 3

Die in AP 3 angeglichene Botan-Version wird im BSI-Entwicklungszweig auf dem GitHub Account bereitgestellt.

Der AN muss sich aktiv darum bemühen, dass die Ergebnisse des Projekts in die OpenSource-Entwicklung von Botan entsprechend den geltenden Lizenzbestimmungen zurückfließen. Dies gilt insbesondere für identifizierte Schwachstellen und Sicherheitslücken. Das Ziel ist hier, dass der BSI-Entwicklungszweig und der Hauptentwicklungszweig möglichst deckungsgleich sind.

2.4 Arbeitspaket 4: Weiterentwicklung Post-Quanten Verfahren

2.4.1 Arbeitspaket 4.1: Analyse und Spezifikation

In der Analyse-Phase sind die aktuellen Spezifikationen bzw. Standards der zu implementierenden Post-Quanten-Verfahren zu analysieren. Bei den zu betrachtenden Post-Quanten-Verfahren handelt es sich um die Verfahren FrodoKEM, Classic McEliece, CRYSTALS-Kyber, CRYSTALS-Dilithium, XMSS, LMS, Sphincs+.[2] Insbesondere ist bei den bereits im BSI-Entwicklungszweig implementierten Verfahren (Classic) McEliece und XMSS die Differenz zur aktuellen Spezifikation bzw. zum Standard der Verfahren zu identifizieren. Ebenfalls sind die im Rahmen des KBLS-Projekts entstandenen Implementierungen der Verfahren CRYSTALS-Kyber und CRYSTALS-Dilithium in Botan zu sichten.

Aufbauend auf der im vorigen Absatz beschriebenen Analyse ist in Abstimmung mit dem BSI ein Pflichtenheft zu erstellen, welches die Realisierung der nachfolgenden Unter-Arbeitspakete in AP 4 spezifiziert. Insbesondere ist zu spezifizieren, welche der oben genannten Post-Quanten-Verfahren gänzlich neu implementiert werden müssen beziehungsweise bei welchen der Verfahren eine bestehende Implementierung übernommen (ggf. mit Anpassungen) werden kann.

2.4.2 Arbeitspaket 4.2: Implementierung: Post-Quanten Verfahren

In diesem Arbeitspaket sind die in AP 4.1 spezifizierten Post-Quanten-Verfahren zu implementieren bzw. vorhandene Implementierungen in den BSI-Entwicklungszweig einzupflegen und ggf. anzupassen. Der AN hat dabei insbesondere auch zu prüfen und zu berücksichtigen, gegen welche SCA-Szenarios (v.a. Laufzeitangriffe) die Verfahren durch eine geeignete Implementierung geschützt werden können (siehe z.B. Anlagen zu

2 Aktuelle Spezifikationen finden sich unter https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions bzw. https://tools.ietf.org/html/rfc8391 bzw. https://tools.ietf.org/html/rfc8554 bzw. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

[AIS 46]). Die genaue Vorgehensweise muss dann mit dem BSI abgestimmt werden. Zusätzlich muss eine Implementierung der notwendigen Ein- und Ausgabekodierungen erfolgen.

Als Programmiersprache ist C++ zu wählen. Sämtliche Software, die im Rahmen des Projekts entsteht, muss unter der selben Lizenz wie der aktuelle Botan BSI-Entwicklungszweig stehen.

Die Funktionen der Kryptobibliothek sollen mit möglichst geringem Aufwand z.B. von Mitarbeitern des BSI evaluiert werden können. Bei der Programmierung muss mindestens Folgendes umgesetzt werden:

- Vermeidung komplexer Verschachtelungen von Funktionen (z.B. über mehr als fünf Ebenen hinweg).
- Vermeidung komplexer Verschachtelungen von Datenstrukturen.
- Sofern Verschachtelungen erforderlich sind, sollen diese auf möglichst wenige Sourcefiles verteilt erfolgen.
- Nach Möglichkeit sollen Teilfunktionen („Module“) durch separate Kompilation der entsprechenden Sourcefiles in Testprogramme eines Evaluators/Entwicklers einfügbar sein.

2.4.3 Arbeitspaket 4.3: Testspezifikation und Tests AP 4

Für die in AP 4 vorgenommene Weiterentwicklung ist die vorhandene Testspezifikation entsprechend zu erweitern und mit dem BSI abzustimmen. Hierbei sind sowohl Positivtests, die das spezifizierte Verhalten des Testobjekts validieren, als auch Negativtests, die die Behandlung von Ausnahme- und Fehlersituationen belegen, durchzuführen. Die Resistenz aller implementierten Verfahren gegen Seitenkanalangriffe ist bei der Testung in angemessener Form zu berücksichtigen, die genaue Vorgehensweise ist mit dem BSI abzustimmen.

Außerdem muss der Software-Reviewprozess beschrieben und nach Absprache mit dem BSI eine statische und dynamische Softwareanalyse durchgeführt werden. Dazu zählt ein Codereview durch das Entwicklungsteam und die Analyse mit automatisierten Tools.

Alle durchgeführten Tests und Analysen und deren Ergebnisse sind in einem Testreport zu dokumentieren.

2.4.4 Arbeitspaket 4.4: Erstellung der Kryptodokumentation zu AP 4

Für die in AP 4 vorgenommene Weiterentwicklung muss die Kryptodokumentation von Botan (in englischer Sprache) entsprechend überarbeitet werden. Dies beinhaltet sowohl eine Beschreibung der Architektur (Grob- und Feinspezifikation), als auch der Schnittstellen. Umfang und Dokumentationstiefe müssen dabei den Anforderungen an eine VS-NfD-Evaluation entsprechen, siehe beiliegendes Dokument „Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD, BSI Version 1.4, August 2020“.
Die in der Bibliothek implementierten kryptografischen Abläufe und Verfahren müssen dazu gemäß beiliegendem Dokument „Detailspezifikation kryptographischer Abläufe und Mechanismen, BSI, Version 1.0, Januar 2015“ dokumentiert werden.
Zusätzlich sind ausführlich kommentierte Anwendungsbeispiele zu erstellen.

2.4.5 Arbeitspaket 4.5: Auslieferung AP 4

Die in AP 4 vorgenommene Weiterentwicklung von Botan wird im BSI-Entwicklungszweig auf dem BSI GitHub Account bereitgestellt.

Der AN muss sich aktiv darum bemühen, dass die Ergebnisse des Projekts in die OpenSource-Entwicklung von Botan entsprechend den geltenden Lizenzbestimmungen zurückfließen. Dies gilt insbesondere für identifizierte Schwachstellen und Sicherheitslücken. Das Ziel ist hier, dass der BSI-Entwicklungszweig und der Hauptentwicklungszweig möglichst deckungsgleich sind.

2.5 Arbeitspaket 5 (OPTIONAL): Weiterentwicklung hybride Schlüsseleinigung in TLS

2.5.1 Arbeitspaket 5.1: Analyse und Spezifikation

In der Analyse-Phase sind die in Standards oder Entwürfen zu Standards vorgeschlagenen Varianten zur Umsetzung einer hybriden Schlüsseleinigung in TLS 1.3 zu analysieren und auf Ihre Umsetzbarkeit in Botan hin zu untersuchen.

Aufbauend auf der im vorigen Absatz beschriebenen Analyse ist in Abstimmung mit dem BSI ein Pflichtenheft zu erstellen, welches die Realisierung der nachfolgenden Unter-Arbeitspakete in AP 5 spezifiziert. Insbesondere ist ein konkretes Verfahren zur hybriden Schlüsseleinigung in TLS 1.3 zu spezifizieren.

2.5.2 Arbeitspaket 5.2: Implementierung: hybride Schlüsseleinigung in TLS

In diesem Arbeitspaket ist das in AP 5.1 spezifizierte Verfahren zur hybriden Schüsseleinigung in TLS 1.3 zu implementieren. Der AN hat dabei insbesondere auch zu prüfen und zu berücksichtigen, gegen welche SCA-Szenarios (v.a. Laufzeitangriffe) oder Protokollfehler/-schwächen (z.B. Orakel-Attacken) die Implementierung geschützt werden kann (siehe z.B. Anlagen zu [AIS 46]). Die genaue Vorgehensweise muss dann mit dem BSI abgestimmt werden. Zusätzlich muss eine Implementierung der notwendigen Ein- und Ausgabekodierungen erfolgen.

Als Programmiersprache ist C++ zu wählen. Sämtliche Software, die im Rahmen des Projekts entsteht, muss unter der selben Lizenz wie der aktuelle Botan BSI-Entwicklungszweig stehen.

Die Funktionen der Kryptobibliothek sollen mit möglichst geringem Aufwand z.B. von Mitarbeitern des BSI evaluiert werden können. Bei der Programmierung muss mindestens Folgendes umgesetzt werden:

- Vermeidung komplexer Verschachtelungen von Funktionen (z.B. über mehr als fünf Ebenen hinweg).
- Vermeidung komplexer Verschachtelungen von Datenstrukturen.
- Sofern Verschachtelungen erforderlich sind, sollen diese auf möglichst wenige Sourcefiles verteilt erfolgen.
- Nach Möglichkeit sollen Teilfunktionen („Module“) durch separate Kompilation der entsprechenden Sourcefiles in Testprogramme eines Evaluators/Entwicklers einfügbar sein.

2.5.3 Arbeitspaket 5.3: Testspezifikation und Tests AP 5

Für die in AP 5 vorgenommene Weiterentwicklung ist die vorhandene Testspezifikation entsprechend zu erweitern und mit dem BSI abzustimmen. Hierbei sind sowohl Positivtests, die das spezifizierte Verhalten des Testobjekts validieren, als auch Negativtests, die die Behandlung von Ausnahme- und Fehlersituationen belegen, durchzuführen. Die Resistenz aller implementierten Verfahren gegen Seitenkanalangriffe ist bei der Testung in angemessener Form zu berücksichtigen, die genaue Vorgehensweise ist mit dem BSI abzustimmen.

Außerdem muss der Software-Reviewprozess beschrieben werden und es ist eine statische und dynamische Softwareanalyse nach Absprache mit dem BSI durchzuführen. Dazu zählt ein Codereview durch das Entwicklungsteam und die Analyse mit automatisierten Tools.

Alle durchgeführten Tests und Analysen und deren Ergebnisse sind in einem Testreport zu dokumentieren.

2.5.4 Arbeitspaket 5.4: Erstellung der Kryptodokumentation zu AP 5

Für die in AP 5 vorgenommene Weiterentwicklung muss die Kryptodokumentation von Botan (in englischer Sprache) entsprechend überarbeitet werden. Dies beinhaltet sowohl eine Beschreibung der Architektur (Grob- und Feinspezifikation), als auch der Schnittstellen. Umfang und Dokumentationstiefe müssen dabei den Anforderungen an eine VS-NfD-Evaluation entsprechen, siehe beiliegendes Dokument „Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD, BSI Version 1.4, August 2020".
Die in der Bibliothek implementierten kryptografischen Abläufe und Verfahren müssen dazu gemäß beiliegendem Dokument „Detailspezifikation kryptographischer Abläufe und Mechanismen, BSI, Version 1.0, Januar 2015" dokumentiert werden.
Zusätzlich sind ausführlich kommentierte Anwendungsbeispiele zu erstellen.

2.5.5 Arbeitspaket5.5: Auslieferung AP 5

Die in AP 5 vorgenommene Weiterentwicklung von Botan wird im BSI-Entwicklungszweig auf dem BSI GitHub Account bereitgestellt.

Der AN muss sich aktiv darum bemühen, dass die Ergebnisse des Projekts in die OpenSource-Entwicklung von Botan entsprechend den geltenden Lizenzbestimmungen zurückfließen. Dies gilt insbesondere für identifizierte Schwachstellen und Sicherheitslücken. Das Ziel ist hier, dass der BSI-Entwicklungszweig und der Hauptentwicklungszweig möglichst deckungsgleich sind.

2.6 Arbeitspaket 6: Abschlusspräsentation

Insbesondere die folgenden Projektergebnisse werden bei einer halbtägigen Abschlussveranstaltung vom Auftragnehmer vor Fachpublikum (BSI-Mitarbeiter/-innen) in Form von Folien präsentiert.

- Implementierte Neuerungen im Botan BSI-Entwicklungszweig
- Verwendete Methoden zur SCA-Analyse und Resultate
- Eventuelle Schwierigkeiten, die bei der Implementierung der Post-Quanten-Verfahren und der hybriden Schlüsseleinigung zu bewältigen waren

Die Präsentationsunterlagen (Foliensatz in MS PowerPoint) händigt der AN dem AG mindestens zehn Arbeitstage vor dem Präsentationstermin zur Kommentierung und weiteren Verwendung im elektronischen Originalformat aus.

Die Abschlusspräsentation findet im BSI in Bonn statt. Aufgrund der aktuellen Gesundheitskrise durch Covid-19 ist es möglich, dass die Abschlusspräsentation (AP 6) – je nach aktueller Situation – lediglich digital durchgeführt werden kann. Die Präsentation soll dann als Videokonferenz erfolgen und ist vom AN zu organisieren.

2.7 Arbeitspaket 7: Wartung und Pflege

Nach Abschluss der Angleichungs- und Weiterentwicklungsphase schließt sich die fortgeführte Wartungs- und Pflegephase an. Um auf neue wissenschaftliche Entwicklungen, Änderungen im NIST-Standardisierungsprozess, eventuelle neue Sicherheitsbedrohungen oder neue Sicherheitsanforderungen seitens des BSI reagieren zu können, muss die Kryptobibliothek fortlaufend überprüft und gegebenenfalls nachgebessert, angepasst und erweitert werden.
Dabei gibt es im Wesentlichen drei zu unterscheidende Fälle:

1. Die Bibliothek muss aufgrund von Änderungen an den umgesetzten Standards bzw. Änderungen in laufenden Standardisierungsprozessen, neuen wissenschaftlichen Erkenntnissen zu einzelnen Kryptoverfahren, neuen Einsatzszenarien etc. verändert oder ergänzt werden.

Für die fortlaufende Überprüfung in diesem Fall, sind mindestens die Entwicklungen im NIST-Standardisierungsprozess "Post-Quantum Cryptography" und die Veröffentlichungen auf dem "Cryptology ePrint Archive" (https://eprint.iacr.org/) zu verfolgen.

Treten für dieses Projekt relevante Änderungen auf, so ist das BSI unmittelbar per E-Mail zu informieren. Hier wird eine möglichst zeitnahe Umsetzung (bis maximal acht Wochen nach Beauftragung) gefordert. Müssen dabei Teile der Kryptobibliothek verändert oder neu implementiert werden, so sind ergänzend die entsprechenden Tests (analog zu den vorherigen Arbeitspaketen) nachzuweisen und die Dokumentation (analog zu den vorherigen Arbeitspaketen) zu ändern bzw. zu erweitern.

2. Es wird eine kritische Sicherheitslücke in einem der beteiligten Standards oder in einer (von Funktionalität und Umfang her ähnlichen) anderen Kryptobibliothek gefunden.

   Für die fortlaufende Überprüfung in diesem Fall, sind mindestens die Entwicklungen im NIST-Standardisierungsprozess "Post-Quantum Cryptography", die Veröffentlichungen auf dem "Cryptology ePrint Archive" (https://eprint.iacr.org/), die Common Vulnerabilities and Exposures Datenbank (https://cve.mitre.org/) und die Meldungen im offiziellen Botan Repository (https://github.com/randombit/botan) zu verfolgen.

   Treten für dieses Projekt relevante Sicherheitslücken auf, so ist das BSI unmittelbar per E-Mail zu informieren. In diesem Fall muss Botan auf diese Sicherheitslücke hin analysiert und getestet werden, wobei das Untersuchungsergebnis dokumentiert werden muss. Gegebenenfalls ist die Sicherheitslücke anschließend nach Absprache mit dem BSI zu schließen. Ein solcher anlassbezogener Sicherheitstest und die anschließende Fehlerbehebung müssen je nach Dringlichkeit kurzfristig (bis maximal vier Wochen nach Beauftragung) durchgeführt worden sein.

3. In der Bibliothek selbst (Architektur, Schnittstellen, Implementierung, etc.) wird ein Fehler gefunden, der sicherheitskritisch ist oder die Benutzung stark beeinträchtigt.

   Für die fortlaufende Überprüfung in diesem Fall, sind mindestens die Common Vulnerabilities and Exposures Datenbank (https://cve.mitre.org/) und die Meldungen im offiziellen Botan Repository (https://github.com/randombit/botan) zu verfolgen.

   Treten für dieses Projekt relevante sicherheitskritische Fehler auf, so ist das BSI unmittelbar per E-Mail zu informieren. In diesem Fall muss kurzfristig (in einem Zeitraum von maximal vier Wochen nach Beauftragung) der Fehler dokumentiert und behoben werden, was durch verschiedene Tests (analog zu den vorherigen Arbeitspaketen) zu belegen und anschließend (analog zu den vorherigen Arbeitspaketen) zu dokumentieren ist.

Als Programmiersprache ist C++ zu wählen. Sämtliche Software, die im Rahmen des Projekts entsteht, muss unter der selben Lizenz wie der aktuelle Botan BSI-Entwicklungszweig stehen.

Die Funktionen der Kryptobibliothek sollen mit möglichst geringem Aufwand z.B. von Mitarbeitern des BSI evaluiert werden können. Bei der Programmierung muss mindestens Folgendes umgesetzt werden:

- Vermeidung komplexer Verschachtelungen von Funktionen (z.B. über mehr als fünf Ebenen hinweg).
- Vermeidung komplexer Verschachtelungen von Datenstrukturen.
- Sofern Verschachtelungen erforderlich sind, sollen diese auf möglichst wenige Sourcefiles verteilt werden.
- Nach Möglichkeit sollen Teilfunktionen („Module“) durch separate Kompilation der entsprechenden Sourcefiles in Testprogramme eines Evaluators/Entwicklers einfügbar sein.

Alle Pflege- und Wartungsarbeiten an der Kryptobibliothek geschehen grundsätzlich auf Abruf durch das BSI.

3 Zahlungs- und Meilensteinplan, Projektplan und Vergütung

Die nachfolgenden Kapitel geben einen Überblick über die Vergütung und den zeitlichen Projektverlauf.

3.1 Vergütung

Die Vergütung erfolgt abhängig von den einzelnen Arbeitspaketen / der Art der Leistung entweder als Festpreis oder nach Aufwand bis zu einer maximalen Obergrenze (siehe die verbindlichen Vorgaben in Kapitel 3.2, Tabelle 1, Spalte „Art der Vergütung“).

3.1.1 Vergütung nach Festpreis

Die Vergütung der AP 1, AP 6 erfolgen nach Festpreis.

3.1.2 Vergütung nach Aufwand

AP 2.1 – AP 5.5 sowie AP 7 werden nach Aufwand bis zu einer jeweiligen maximalen Obergrenze vergütet. Hierzu sind die tatsächlich angefallenen Aufwände bei Rechnungsstellung zu belegen.

Gemeinkosten, Reisekosten sowie sonstige Kosten werden nicht gesondert vergütet und müssen daher bereits in den veranschlagten Tagessätzen enthalten sein.

Je Kalendertag wird pro Person nicht mehr als ein Tagessatz vergütet. Der vereinbarte Tagessatz kann nur dann in Rechnung gestellt werden, wenn mindestens acht Zeitstunden geleistet wurden. Werden weniger als acht Zeitstunden pro Tag geleistet, sind diese anteilig (viertelstundengenau) in Rechnung zu stellen.

Angefallene Aufwände, die nicht zuvor mit dem Auftraggeber abgestimmt wurden, können nicht vergütet werden.

Während der Leistungserbringung können die Obergrenzen der einzelnen Unterarbeitspakete (z.B. AP 2.1 – AP 2.5) unter Beachtung der maximalen Obergrenze des übergeordneten AP (z.B. AP 2) in Abstimmung mit dem AG untereinander verschoben werden.

3.1.2.1 Vergütung nach Aufwand mit vom AN kalkulierter Obergrenze (AP 2, AP 4 und AP 5 - Optional)

Die jeweilige maximale Obergrenze der AP 2.1 – AP 2.5, AP 4.1 – AP 4.5 sowie der optionalen AP 5.1 – AP 5.5 ergibt sich aus den vom Auftragnehmer kalkulierten Personentagen und den angebotenen Tagessätzen (siehe Kapitel 6.2.1.4, Zuschlagskriterium Nr. 2.3).

3.1.2.2 Vergütung nach Aufwand mit vorgegebenem Abrufkontingent (AP 3 und AP 7)

Der AG legt für die AP 3.1 – AP 3.5 ein gemeinsames Abrufkontingent in Höhe von 20 Personentagen und für das AP 7 ein Abrufkontingent in Höhe von 60 Personentagen fest. Die jeweilige maximale Obergrenze ergibt sich bei diesen APs somit aus der jeweils vorgegebenen Kontingentgröße und den im Angebot anzugebenden Tagessätzen (siehe Kapitel 6.2.1.4, Zuschlagskriterium Nr. 2.3).

Abrufe aus diesem Kontingent erfolgen durch den Auftraggeber in Textform. Der Auftragnehmer erstellt für den jeweiligen Abruf eine Kalkulation der Personentage. Erst nach Freigabe dieser Kalkulation durch den Auftraggeber gilt der Abruf als getätigt. Sollte das Leistungsziel ohne Erfüllung zusätzlicher Leistungen/Per-

sonentage nicht erreicht werden können, ist dies unverzüglich nach Kenntnisnahme dem Auftraggeber zu kommunizieren. Nach Prüfung durch den Auftraggeber erfolgt ggf. eine Aufstockung der für den betroffenen Abruf zur Verfügung stehenden Personentage.

Sollte im Rahmen eines Abrufs der tatsächliche Aufwand die vereinbarte Anzahl von Personentagen unterschreiten, werden die freien Ressourcen wieder dem verbleibenden Kontingent zugerechnet.

3.2 Projektverlauf, Zahlungs- und Meilensteinplan

Für die Fertigstellung des Projektes wird vom AG ein Zeitrahmen von maximal 36 Kalendermonaten verbindlich vorgegeben. Der Termin der Auftaktbesprechung kennzeichnet den offiziellen Projektstart. Die Auftaktbesprechung ist seitens des AN in Abstimmung mit dem AG spätestens vier Kalenderwochen nach Auftragserteilung anzusetzen.

Das AP 4 muss spätestens 21 Monate nach dem offiziellen Projektstart abgeschlossen werden.

Die Arbeitspakete 1 und 2 sind zuerst zu bearbeiten, da die verbleibenden darauf aufbauen. Bei den Arbeitspaketen 3, 4 und 5 ist eine (teilweise) parallele Bearbeitung möglich. In deren Anschluss finden die Arbeitspakete 6 und 7 statt. Falls das optionale Arbeitspaket 5 nicht zum geplanten Zeitpunkt beauftragt werden kann, ist es möglich, dieses während der Laufzeit von AP 7 zu beauftragen (vgl. Kapitel 1.4).

Für das AP 7 – Wartung und Pflege – wird vom AG eine Laufzeit von 12 Monaten verbindlich vorgegeben.

Jedes der Arbeitspakete wird einem Meilenstein zugeordnet. Ein Meilenstein gilt als erreicht, sobald die ihm zugeordneten AP erbracht und vom AG abgenommen wurden. Grundsätzlich können nur vollständig erbrachte Arbeitspakete abgenommen werden. Bei Festpreis-Arbeitspaketen ist eine Rechnungslegung erst nach Erreichen eines Meilensteins zulässig. Entgegen der Regelung zu den Festpreis-Arbeitspaketen können vom AG abgenommene Teilleistungen aus den nach Aufwand vergüteten Arbeitspaketen (siehe Kapitel 3.1.2) quartalsweise in Rechnung gestellt werden.

Arbeitspaket (AP) / Meilenstein (MS)	**(Kurz-) Bezeichnung**	**Termin nach Projektstart [Kalendermonate]**		**Beginn**	**Ende**	**Art der Vergütung**	**Höhe des Festpreises / der maximalen Obergrenze**	
		Beginn	Ende				zzgl. USt.	inkl. USt.
AP 1	Auftaktbesprechung	0	0	*Datum*	*Datum*	Festpreis	*Betrag* €	*Betrag* €
MS 1	Meilenstein 1	---	0	---	*Datum*	---	*Betrag* €	*Betrag* €
AP 2	Initiale Angleichung	1	7	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
AP 2.1	Analyse und Spezifikation	1	1	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
AP 2.2	Angleichung der Version	2	7	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
AP 2.3	Testspezifikation und Tests AP 2	3	7	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
AP 2.4	Überarbeitung der Kryptodokumentation zu AP 2	3	7	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
AP 2.5	Auslieferung AP 2	---	7	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €
MS 2	Meilenstein 2	---	7	---	*Datum*	---	*Betrag* €	*Betrag* €
AP 3	Entwicklungsbegleitende Angleichung	8	23	*Datum*	*Datum*	Aufwand	*Betrag* €	*Betrag* €

Arbeitspaket (AP) / Meilenstein (MS)	(Kurz-) Bezeichnung	Termin nach Projektstart [Kalendermonate]		Beginn	Ende	Art der Vergütung	Höhe des Festpreises / der maximalen Obergrenze	
		Beginn	Ende				zzgl. USt.	inkl. USt.
AP 3.1	Analyse und Spezifikation	8	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 3.2	Angleichung der Version	8	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 3.3	Testspezifikation und Tests AP 3	8	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 3.4	Überarbeitung der Kryptodokumentation zu AP 3	8	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 3.5	Auslieferung AP 3	---	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
MS 3	Meilenstein 3	---	23	---	*Datum*	---	*Betrag €*	*Betrag €*
AP 4	Weiterentwicklung Post-Quanten Verfahren	8	20	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 4.1	Analyse und Spezifikation	8	9	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 4.2	Implementierung: Post-Quanten Verfahren	9	19	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 4.3	Testspezifikation und Tests AP 4	11	20	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 4.4	Erstellung der Kryptodokumentation zu AP 4	11	20	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 4.5	Auslieferung AP 4	---	20	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
MS 4	Meilenstein 4	---	20	---	*Datum*	---	*Betrag €*	*Betrag €*
AP 5 (optional)	Weiterentwicklung hybride Schlüsseleinigung in TLS	21	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 5.1	Analyse und Spezifikation	21	21	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 5.2	Implementierung: hybride Schlüsseleinigung in TLS	22	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 5.3	Testspezifikation und Tests AP 5	22	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 5.4	Erstellung der Kryptodokumentation zu AP 5	22	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
AP 5.5	Auslieferung AP 5	---	23	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*
MS 5	Meilenstein 5	---	23	---	*Datum*	---	*Betrag €*	*Betrag €*
AP 6	Abschlusspräsentation	24	24	*Datum*	*Datum*	Festpreis	*Betrag €*	*Betrag €*
MS 6	Meilenstein 6	---	24	---	*Datum*	---	*Betrag €*	*Betrag €*
AP 7	Wartung und Pflege	25	36	*Datum*	*Datum*	Aufwand	*Betrag €*	*Betrag €*

Arbeits-paket (AP) / Meilen-stein (MS)	**(Kurz-) Bezeichnung**	**Termin nach Projektstart [Kalender-monate]**		**Beginn**	**Ende**	**Art der Vergütung**	**Höhe des Festpreises / der maximalen Obergrenze**	
		Beginn	Ende				zzgl. USt.	inkl. USt.
MS 7	Meilenstein 7	---	36	---	*Datum*	---	*Betrag* €	*Betrag* €
Gesamtprojekt		0	36	*Datum*	*Datum*	---	*Betrag* €	*Betrag* €

Tabelle 1: Zahlungs- und Meilensteinplan. Der hier dargestellte und nicht vollständig befüllte Zahlungs- und Meilensteinplan dient als Übersicht über den derzeit vom AG als sinnvoll erachteten Projektverlauf. Bei den Angaben in der Spalte „Termin nach Projektstart (Beginn, Ende)“ handelt es sich um unverbindliche Schätzwerte des AG. Im Rahmen des Angebotes ist ein konkreter und verbindlicher Zahlungs- und Meilensteinplan in der oben stehenden Darstellungsform vorzulegen. (siehe Kapitel 6.2.1.4, Zuschlagskriterium „Zahlungs- und Meilensteinplan“). Dabei sind die Spalten „Beginn“, „Ende“ sowie „Höhe des Festpreises /der maximalen Obergrenze“ zu befüllen. Die verbindlichen Vorgaben aus Kapitel 3.1 und 3.2 sind zwingend zu beachten.

4 Rahmen- und Ausführungsbedingungen

In diesem Kapitel sind die Rahmen- und Ausführungsbedingungen für die Projektdurchführung festgelegt. Deren Einhaltung wird durch Abgabe eines Angebotes automatisch von den Bietern bestätigt (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

4.1 Personal des Auftragnehmers

Für die Erbringung der Leistung sind vom AN mindestens 2 Personen einzusetzen (inkl. Projektleitung und Beauftragte/r für das Qualitätsmanagement).

4.1.1 Direktionsrecht und Disziplinargewalt

Auftraggeber und Auftragnehmer werden durch organisatorische Maßnahmen gewährleisten, dass die jeweils von Ihnen abgestellten Personen für die Leistungserbringung ausschließlich dem Direktionsrecht und der Disziplinargewalt des jeweiligen Arbeitgebers unterstehen. Weisungen erfolgen ausschließlich im Rahmen der vereinbarten Aufgabenverteilung.

4.1.2 Qualifikationen, Erfahrungen und sonstige Anforderungen

Die zur Erbringung der Leistungen eingesetzten Personen müssen vereinbarungsgemäß, unabhängig davon jedoch mindestens dem Vertragszweck und der Aufgabenstellung entsprechend, qualifiziert sein. Unabhängig davon wird der Auftragnehmer gewährleisten, dass die für die Leistungserbringung vorgesehenen Personen über die Qualifikation verfügen, die mindestens seinen diesbezüglichen Angaben sowie den Anforderungen des Auftraggebers im Vergabeverfahren entspricht.

Für die einzelnen vorgesehenen Rollen gelten die nachfolgend aufgelisteten Mindestanforderungen. Deren Erfüllung ist im Angebot mit geeigneten Referenzen zu belegen (siehe Kapitel 6.2.1.4), wobei die Referenzen sich höchstens auf die letzten drei Jahre ab Veröffentlichung der Auftragsbekanntmachung beziehen dürfen. Ausgenommen hiervon sich Zeugnisse. Eine Referenz kann hierbei auch mehrere Anforderungen abdecken.

a) Projektleitung (PL):

- Erfolgreiche Leitung von mindestens einem Projekt in der Entwicklung von Software mit Schwerpunkt Informationssicherheit und Kryptografie, welches mit der hier zu vergebenden Leistung vergleichbar ist (Dauer, Umfang, Inhalt) oder darüber hinaus geht.
- Praktische Erfahrung im Bereich der Entwicklung von Software mit Schwerpunkt Informationssicherheit und Kryptografie durch maßgebliche Mitwirkung an mindestens einem Projekt / Auftrag in diesem Themenbereich.

b) Beauftragte/r für das Qualitätsmanagement (BQM)

- Praktische Erfahrung im Qualitätsmanagement im Bereich Informationssicherheit und Kryptografie durch maßgebliche Mitwirkung an mindestens einem Projekt / Auftrag in diesem Themenbereich.

c) Entwickler/in

- Praktische Erfahrung im Bereich der Entwicklung von Software mit Schwerpunkt Informationssicherheit und Kryptografie durch maßgebliche Mitwirkung an mindestens einem Projekt / Auftrag in diesem Themenbereich.
- Nachweis umfassender Kenntnisse der Programmiersprachen C und C++ durch mindestens ein Projekt, welches der hier zu vergebenden Leistung vergleichbar ist (Dauer, Umfang, Inhalt) oder darüber hinaus geht.

d) mindestens eine Person des Projektteams / Teamqualifikation

Die folgenden Mindestanforderungen können von verschiedenen Personen des Projektteams abgedeckt werden.

- Sehr gute Kenntnisse und praktische Erfahrungen im Bereich der Kryptografie sowie insbesondere sehr gute Kenntnisse der zu implementierenden Verfahren, die durch die Angabe von relevanten Publikationen oder früher bereits durchgeführten Entwicklungsprojekten nachgewiesen werden müssen.
- Sehr gute Kenntnisse und Erfahrungen in der Entwicklung von IT-Sicherheitslösungen einschließlich der Entwicklung und Integration der enthaltenen kryptografischen Verfahren.
- Praktische Erfahrung im Bereich der Entwicklung von Open-Source-Software durch maßgebliche Mitwirkung an mindestens einem Projekt / Auftrag in diesem Themenbereich.

e) alle Personen der Personengruppe Entwickler/innen

Die folgenden Mindestanforderungen können von verschiedenen Personen des Projektteams abgedeckt werden.

- Nachweis umfassender Kenntnisse der Programmiersprachen C und C++ durch mindestens ein Projekt, welches der hier zu vergebenden Leistung vergleichbar ist (Dauer, Umfang, Inhalt) oder darüber hinaus geht.
- Sehr gute Kenntnisse und Erfahrungen in der Entwicklung von IT-Sicherheitslösungen einschließlich der Entwicklung und Integration der enthaltenen kryptografischen Verfahren.

f) alle Personen des Projektteams (inkl. PL und BQM)

- Hochschulabschluss in einem MINT-Fach, d.h. aus den Bereichen Mathematik, Informatik, Naturwissenschaft oder Technik.
- Alternativ zu dem oben genannten Hochschulabschluss können objektiv belegbare, äquivalente und für das Projektvorhaben ausreichende und adäquate Qualifikationsnachweise (z.B. Erfahrungsjahre) eingereicht werden.

4.1.3 Personaleinsatz und -austausch

Der Auftragnehmer hat zwingend mindestens das Personal einzusetzen, das er im Rahmen seines Angebots (Anlage: „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“) als konkret einzusetzendes Personal mit Qualifikationsprofilen angeboten hat. Unabhängig davon hat er nur solches Personal einzusetzen, das für die jeweils zu erbringende Leistung hinreichend qualifiziert ist. Für jede Person, die eingesetzt wird, hat der Auftragnehmer spätestens eine Woche vor dem geplanten Einsatz ein Qualifikationsprofil einzureichen, es sei denn, es liegt betreffend der jeweiligen Person ein solches Qualifikationsprofil beim Auftraggeber bereits vor. Ein Austausch von Personal ist nur nach vorheriger Zustimmung durch den Auftraggeber zulässig.

Der Auftraggeber wird seine Zustimmung im Fall eines berechtigten Grundes und wenn ein gleich- oder höherwertiger Ersatz angeboten wird erteilen. Ein berechtigter Grund liegt beispielsweise vor, wenn der Austausch aufgrund Krankheit oder Ausscheiden der betreffenden Person aus dem Unternehmen oder vergleichbarer Umstände, bedingt ist. Die Umstände sind vom Auftragnehmer darzulegen und plausibel zu machen. Kein berechtigter Grund ist der Einsatz der betreffenden Person in einem anderen Projekt oder ein Umzug des Standorts des Unternehmens. Die Gleichwertigkeit des Ersatzes orientiert sich anhand des für die auszutauschende Person vormals eingereichten Qualifikationsprofils, soweit ein solches vorliegt, andernfalls nach billigem Ermessen.

Eine höhere Qualifikation der Ersatzperson begründet keinen Anspruch auf Erhöhung der Vergütung.

Die durch den Austausch und die Einarbeitung der Ersatzperson entstehenden Kosten gehen zu Lasten des Auftragnehmers.

Das eingetauschte Personal ist unverzüglich auf Kosten des Auftragnehmers vollumfänglich einzuarbeiten. Soweit möglich arbeitet die ausscheidende Person die Ersatzperson ein.

4.2 Projektorganisation und Erreichbarkeit

Durch den Auftragnehmer ist ein qualifizierter Projektleiter zur Verfügung zu stellen, der sich mit dem Projektleiter des Auftraggebers abstimmt und die durchzuführenden Arbeiten auf Seiten des Auftragnehmers koordiniert.

Der Projektleiter muss während der üblichen Arbeitszeiten (Montag bis Freitag, jeweils mindestens von 9:30 bis 15:30 Uhr) regelmäßig telefonisch oder per E-Mail erreichbar sein. Sollte der Projektleiter verhindert sein, muss jeweils ein Vertreter benannt werden.

Seitens des Auftraggebers wird das Projekt vom Referat KM 21 geleitet. Ansprechpartner werden bei Erteilung des Zuschlags mitgeteilt.

4.3 Projektsprache

Die Projektsprache ist grundsätzlich Deutsch. Abweichungen sind in der folgenden Tabelle aufgeführt:

fachlische Abstimmung zwischen Auftragnehmer und BSI (persönliche Treffen, telefonisch, schriftlich):	Deutsch oder Englisch
Berichtswesen, Besprechungsprotokolle:	Deutsch oder Englisch
Alle Ergebnisdokumente (z.B. Testspezifikation, Kryptodokumentation):	Englisch

4.4 Besprechungen

Die Auftaktbesprechung sowie die Abschlusspräsentation finden im BSI in Bonn statt, können aber aufgrund der aktuellen Gesundheitskrise durch Covid-19 ggf. auch per Videokonferenz durchgeführt werden.- Diese sind vom AN zu organisieren.

Bei Bedarf sind zusätzliche Telefon- oder Videokonferenzen einzuplanen. Darüber hinaus stattfindende Meetings zur Diskussion von Zwischenergebnissen finden nach Absprache beim Auftragnehmer oder per Videokonferenz statt.

Zu jedem Arbeitstreffen und jeder Telefonkonferenz hat der Auftragnehmer ein schriftliches Protokoll anzufertigen, in dem die Beschlüsse und Ergebnisse festgehalten werden. Das Protokoll ist dem Auftraggeber spätestens drei Arbeitstage nach Stattfinden des jeweiligen Arbeitstreffens bzw. der Telefonkonferenz zur Freigabe vorzulegen.

Struktur und Format der Besprechungsprotokolle werden im Rahmen der Auftaktbesprechung festgelegt.

Jegliche Videokonferenz ist datenschutzfreundlich, d.h. konform zu den Hinweisen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[3], zu gestalten.

4.5 Berichtswesen

Im Rahmen des Berichtwesens erhält der Auftraggeber vom Auftragnehmer alle 14 Tage einen tabellarischen, fortlaufend zu erweiternden und aussagekräftigen Kurzbericht per E-Mail über den Verlauf. Mögliche Probleme im Projektverlauf sind sofort anzuzeigen und dem Auftraggeber gegenüber besonders hervorzuheben. Die vertraglichen Regelungen in Ziffer 9 des Projektvertrages bleiben unberührt.

Struktur und Format der regelmäßigen Berichte werden im Rahmen der Auftaktbesprechung festgelegt.

4.6 Formale Anforderungen an Projektdokumente

Der Auftragnehmer übermittelt die Projektdokumente (Projektergebnisse, Besprechungsprotokolle, Berichte) in elektronischer Form entweder im OpenDocument Dateiformat und im Portable Document Format (PDF) an den Auftraggeber. Ausnahmen von diesen Dateiformaten sind erst nach Absprache mit dem Auftraggeber möglich. Wurde sich auf die Erstellung von Microsoft Word Dokumenten geeinigt, so ist in diesen grundsätzlich auf die Referenzierung von OLE-Objekten (Object Linking and Embedding) zu verzichten.

Alle Projektdokumente sind übersichtlich strukturiert und enthalten (wenn sinnvoll) ein Inhaltsverzeichnis, eine Zusammenfassung, eine Dokumenten-Version, eine Änderungshistorie mit Erstellungs- und Bearbeitungs-Datum sowie der Liste der Autoren, so dass Erstellung und Änderung des jeweiligen Dokuments nachvollziehbar sind.

Die sprachliche Qualität ist von großer Bedeutung. Im Durchschnitt sind pro Textseite maximal vier sprachliche Fehler; das heißt grammatikalische Fehler oder Rechtschreibfehler zulässig.

4.7 Umgang mit Sicherheitslücken

Jegliche im Rahmen des Projekts identifizierte Sicherheitslücken in Software sind offen zu legen. Die Offenlegung geschieht nach dem Coordinated Vulnerability Disclosure (CVD) Prinzip. D.h. die potentiell betroffenen Elternprojekte sind unverzüglich über eine identifizierte Schwachstelle zu informieren. Alle weiteren Schritte sind verantwortungsvoll mit den entsprechenden Elternprojekten zu koordinieren.

3 https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Kommunikations-node.html

4.8 Einsatz von Unterauftragnehmern

Der Auftragnehmer kann zur Leistungserbringung Unterauftragnehmer nur einsetzen oder eingesetzte Unterauftragnehmer nur auswechseln, wenn der Auftraggeber dem ausdrücklich vorher zustimmt. Die Zustimmung kann nicht aus sachwidrigen Gründen verweigert werden.

Die Einarbeitung des neuen Unterauftragnehmers erfolgt auf Kosten des Auftragnehmers. Für die im Angebot des Auftragnehmers benannten Unterauftragnehmer gilt die Zustimmung des Auftraggebers als erteilt.

Die Weitergabe von Projektteilen an nicht zugelassene Unterauftragnehmer ist verboten.

4.9 Formale Anforderungen an die Rechnungsstellung

Gemäß § 3 i.V.m. § 11 der E-Rechnungsverordnung (E-RechV) sind Rechnungen ab dem 27.11.2020 zwingend in elektronischer Form auszustellen und zu übermitteln. Hierbei ist grundsätzlich der Datenaustauschstandard XRechnung in der jeweils aktuellen Fassung zu verwenden (§ 4 E-RechV).

Ggf. erforderliche Anlagen sind in den Rechnungsdatensatz einzubetten und dürfen keine aktiven Inhalte (z.B. Makros) enthalten.

Rechnungsformate, welche nicht den Anforderungen der europäischen Norm für die Rechnungsstellung (EN-16931) entsprechen sowie Rechnungen, die nicht über die Rechnungseingangsplattform des Bundes (https://xrechnung.bund.de) zugestellt wurden, können nicht berücksichtigt werden.

Nähere Informationen zu den formalen Anforderungen sind dem in den Vergabeunterlagen enthaltenen Dokument „Rechnungseingangsplattformen des Bundes“ (Version 1.6 vom 08.07.2020) zu entnehmen.

B Besondere Bewerbungsbedingungen

5 Bedingungen für die Zuschlagserteilung

In diesem Kapitel sind die Bedingungen für die Zuschlagserteilung festgelegt, die bei der Erstellung eines Angebots gemäß Kapitel 6 zu berücksichtigen sind.

5.1 Gesetzliche Ausschlussgründe, Eignung und Ausführungsbedingungen

Öffentliche Aufträge werden nur an fachkundige und leistungsfähige (geeignete) Unternehmen vergeben, die nicht nach den §§ 123 oder 124 GWB ausgeschlossen worden sind (§ 122 Abs. 1 GWB, § 31 Abs. 1 UVgO).

Die zwingenden Ausschlussgründe (§ 123 GWB) und die fakultativen Ausschlussgründe (§ 124 GWB) können unter den folgenden Quellen nachgelesen werden:

- https://www.gesetze-im-internet.de/gwb/__123.html
- https://www.gesetze-im-internet.de/gwb/__124.html

Mit der Abgabe des Angebots versichern die Bieter, dass keine der in §§ 123, 124 GWB genannten Gründe im Hinblick auf ihre Person oder Unternehmen vorliegen, soweit nicht eine Erklärung zu den §§ 123, 124 GWB eingereicht wurde (siehe Kapitel 6.2.4). Das BSI schließt ein Unternehmen jedoch zu jedem Zeitpunkt des Vergabeverfahrens von der Teilnahme aus, wenn es Kenntnis davon erhält, dass ein Ausschlussgrund nach § 123 GWB vorliegt. Ein Ausschluss kommt gleichermaßen bei Kenntnis über einen Ausschlussgrund nach § 124 GWB in Betracht. Die Möglichkeit der Selbstreinigung nach § 125 GWB bleibt unberührt.

Das BSI prüft, ob die Bieter die festgelegten Eignungskriterien (siehe Kapitel 6.2.1.3) und etwaig festgelegte Mindestanforderungen erfüllen (§ 122 Abs. 2 GWB[4], § 31 Abs. 2 UVgO). Wird eine Mindestanforderung an die Eignung nicht erfüllt, ist das Angebot auszuschließen. Im Übrigen prüft das BSI auf Grundlage der Eignungskriterien, ob die vorgelegten Belege den Schluss zulassen, dass der Bieter den Auftrag ordnungsgemäß erfüllen kann.

Ausführungsbedingungen betreffen die Vertragsausführung und stellen vom BSI festgelegte Bedingungen dar, die vom Auftragnehmer einzuhalten sind. Der Transparenz halber ist von den Bietern bereits im Vergabeverfahren zu versichern, dass sie im Rahmen der Auftragsausführung die vom BSI vorgesehenen Bedingungen einhalten werden (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

5.2 Wirtschaftlichstes Angebot

Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt. Grundlage dafür ist eine Bewertung des BSI, ob und inwieweit das Angebot die vorgegebenen Zuschlagskriterien erfüllt. Das wirtschaftlichste Angebot bestimmt sich nach dem besten Preis-Leistungs-Verhältnis. Zu dessen Ermittlung können neben dem Preis oder den Kosten auch qualitative, umweltbezogene oder soziale Aspekte berücksichtigt werden (§ 127 Abs. 1 GWB, § 43 Abs. 1 und 2 UVgO).

Für die Ermittlung der Wirtschaftlichkeit eines Angebotes wendet das BSI die „erweiterten Richtwertmethode“ über die Faktoren „Bewertungspreis“ (siehe Kapitel 5.2.1) und „Leistung“ (siehe Kapitel 5.2.2) an.

4 Jeweils in Verbindung mit den Regelungen der §§ 42 ff. VgV oder §§ 7, 21 ff VSVgV.

5.2.1 Bewertungspreis

Der Bewertungspreis umfasst die folgenden Komponenten (siehe auch Kapitel 6.1):

Bewertungspreis = Angebotsnettopreis + anfallende (Einfuhr-/)Umsatzsteuer ohne Rücksicht auf die Steuerschuldnerschaft

Der Angebotsnettopreis umfasst dabei sämtliche Einzelpositionen (siehe Kapitel 3.2, Tabelle 1).

5.2.2 Leistung

Die „Leistung“ der einzelnen Angebote wird vom BSI anhand der festgelegten qualitativen Zuschlagskriterien (siehe Kapitel 6.2.1.4) bewertet.

Bei den qualitativen Zuschlagskriterien wird zwischen Ausschlusskriterien (A-Kriterien) und Bewertungskriterien (B-Kriterien) differenziert.

Während bei einem A-Kriterium lediglich geprüft wird, ob die Ausführungen des Bieters die definierten Mindestanforderungen erfüllen (Prüfergebnis: Ja oder Nein), werden die Ausführungen des Bieters bei einem B-Kriterium anhand einer durchgängigen Wertungsskala von 0 bis 4 Bewertungspunkten (BP) bewertet:

BP	Zielerreichungsgrad
0	Es sind keine Angaben vorhanden oder in Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI nur in unzureichendem Maße entsprechen wird.
1	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI in ausreichendem Maße entsprechen wird.
2	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI weitgehend entsprechen wird.
3	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI voll entsprechen wird.
4	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI in besonderem Maße entsprechen wird.

Zur Orientierung werden bei jedem B-Kriterium die Voraussetzungen angegeben, die erfüllt sein müssen, damit das Angebot bzgl. dieses Kriteriums vom BSI mit 0 BP, 1 BP oder 4 BP bewertet wird.

Bei den B-Kriterien muss das Angebot jeweils mindestens 1 BP ($\mathbf{BP_{min}} = 1$) erzielen (Mindestanforderung).

Erfüllt ein Angebot bei mindestens einem A-Kriterium oder bei mindestens einem B-Kriterium nicht die definierte Mindestanforderung, so wird dieses Angebot von der Wertung ausgeschlossen.

Bei den verbleibenden Angeboten ergeben sich die für die erweiterte Richtwertmethode maßgeblichen Leistungspunkte (**LP**) aus dem Produkt der bei den einzelnen B-Kriterien erzielten BP und der vom BSI für die jeweiligen B-Kriterien vorgegebenen Gewichtungsfaktoren (**GF**, siehe Kapitel 6.2.1.4).

5.2.3 Erweiterte Richtwertmethode mit dem Entscheidungskriterium „Leistungspunkte“

Bei der erweiterten Richtwertmethode wird in einem ersten Schritt für jedes der Angebote eine individuelle Kennzahl, welche aus dem Quotient zwischen den erzielten Leistungspunkten (siehe Kapitel 5.2.2) und dem Bewertungspreis (siehe Kapitel 5.2.1) besteht, ermittelt.

Ausgehend vom Angebot mit der höchsten Kennzahl wird in einem nächsten Schritt ein Schwankungsbereich von 10 % definiert. Alle Angebote, die mit Ihrer Kennzahl unterhalb dieses Schwankungsbereiches liegen, können bei der Zuschlagserteilung nicht berücksichtigt werden.

Bei den verbleibenden Angeboten erfolgt die Zuschlagserteilung auf das Angebot mit der höchsten Leistungspunktzahl. Ist die Leistungspunktzahl identisch, erfolgt der Zuschlag auf das preislich günstigere Angebot.

6 Erstellung des Angebotes

Ein vollständiges Angebot besteht aus folgenden Unterlagen:

- Angebotsformular (siehe Kapitel 6.1)
- Anlagen zum Angebotsformular
  - Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen (siehe Kapitel 6.2.1).

    Wird im Rahmen einzelner Eignungskriterien und / oder Zuschlagskriterien explizit die Einreichung weiterer Dokumente (z.B. Kopie einer offiziellen Bescheinigungen oder eines amtlichen Nachweises, etc.) gefordert, so sind diese nach Möglichkeit an der entsprechenden Stelle in diese Anlage zu integrieren. Ist eine Integration nicht möglich, so bilden diese eine eigenständige Anlage.
  - ggf. Bietergemeinschaftserklärung (siehe Kapitel 6.2.2)
  - ggf. Unterauftragnehmerverpflichtungserklärungen (siehe Kapitel 6.2.3)
  - ggf. Angaben zu vorliegenden Ausschlussgründen und zur Selbstreinigung im Sinne von § 125 GWB (siehe Kapitel 6.2.4)
  - ggf. weitere individuelle Anlagen des Bieters (siehe Kapitel 6.2)

Die Anzahl der geforderten Anlagen ist dabei abhängig von der Bieterkonstellation (siehe Kapitel 6.2.2), der geplanten Einbindung von Unterauftragnehmern (siehe Kapitel 6.2.3) sowie dem Vorliegen von gesetzlichen Ausschlussgründen (siehe Kapitel 6.2.4).

Das BSI ist rechtlich verpflichtet, die eingereichten Angebote mindestens drei Jahre ab dem Tag der Zuschlagserteilung aufzubewahren. Reichen Sie daher alle für die Angebotswertung relevanten Informationen in archivierbarer Form ein. Verzichten Sie z.B. in der Anlage „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“ auf die Angabe von URLs bzw. auf deren Verweisung.

Bitte fügen Sie nach Möglichkeit alle Anlagen zum Angebotsformular zu einer „Gesamtdatei“ (PDF) zusammen (jedoch ohne das Angebotsformular, vgl. Kapitel 6.1).

6.1 Angebotsformular

Das in den Vergabeunterlagen enthaltene Angebotsformular ist gemäß den dort aufgeführten Vorgaben auszufüllen.

Ist die Steuerschuldnerschaft aufgrund von § 13b USTG auf den Auftraggeber übergegangen (reverse charge), so weisen Sie im Angebot einen Steuersatz von 0 % aus. In diesem Fall wird die von Auftraggeber abzuführende Umsatzsteuer bei der Bewertung des Angebotes berücksichtigt (siehe Kapitel 5.2.1).

Verschiedene Eingabefelder des Angebotsformulars werden nach Abgabe und Öffnung des Angebotes maschinell ausgelesen. Verzichten Sie daher auf die Einreichung eines eingescannten Auftragsformulars und auf die Zusammenfassung des Angebotsformulars mit den zugehörigen Anlagen zu einer „Gesamtdatei“.

Hinweis bzgl. Covid-19:
Bitte geben Sie im Angebotsformular für AP 1 und AP 6 stets den Preis für eine Präsenzveranstaltung an.

6.2 Anlagen zum Angebotsformular

Die nachfolgenden Unterkapitel geben einen Überblick über die einzelnen Anlagen sowie über deren inhaltliche Anforderungen.

Falls aus Sicht des Bieters erforderlich, so kann das Angebot um weitere Anlagen ergänzt werden.

Alle zum Angebot gehörenden Anlagen sind auf Seite 2 des Angebotsformulars aufzuführen.

6.2.1 Anlage: Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen

Die von jedem Bieter individuell zu erstellende Anlage „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“ fungiert neben dem Angebotsformular als zentraler Bestandteil des Angebotes.

Halten Sie sich bei der Erstellung dieser Anlage an die Vorgaben in den Kapiteln 6.2.1.1 bis 6.2.1.4 sowie an die vorgegebene Reihenfolge. Achten Sie darauf, die geforderten Angaben unmittelbar bei den einzelnen Kriterien aufzuführen.

Achtung: Verzichten Sie auf nicht geforderte Angaben, insbesondere zu den vertraglichen Regelungen (siehe Ziffer 4.2 der Allgemeinen Bewerbungsbedingungen).

Die vollständige Abdeckung des in der Leistungsbeschreibung geforderten Leistungsumfangs inkl. der Einhaltung sämtlicher in Kapitel 4 der Leistungsbeschreibung definierten Rahmen- und Ausführungsbedingungen wird durch Abgabe eines Angebotes automatisch bestätigt (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

6.2.1.1 Einzelbieter / Mitglieder der Bietergemeinschaft

Erstellen Sie vom Einzelbieter bzw. vom jedem Mitglied der Bietergemeinschaft ein aussagekräftiges Firmenprofil. Die Darstellung muss in tabellarischer Form erfolgen und folgende Punkte umfassen:

- Offizielle Bezeichnung
- Rechtsform
- Firmensitz und Standorte
- Struktur und Organisation
  - z.B. Abbildung des Organigramms
- Geschäftsfelder
  - Auflistung der einzelnen Geschäftsfelder
  - Benennung der Geschäftsfelder, die für den hier zu vergebenden Auftrag relevant sind (auftragsbezogene Geschäftsfelder)
  - ggf. nähere Ausführungen / Erläuterungen zu den auftragsbezogenen Geschäftsfeldern
- Anzahl der Mitarbeiter in den auftragsbezogenen Geschäftsfeldern
- Gesamtumsatz in den letzten drei Geschäftsjahren (Angabe pro Jahr), sofern entsprechende Angaben verfügbar sind.
- Umsatz in den auftragsbezogenen Geschäftsfeldern in den letzten drei Geschäftsjahren (Angabe pro Jahr), sofern entsprechende Angaben verfügbar sind.

Gehen Sie im Falle einer Bietergemeinschaft zudem auf die Aufteilung der zu erbringenden Leistung auf die einzelnen Mitglieder der Bietergemeinschaft ein.

6.2.1.2 Unterauftragnehmer

Werden wesentliche Teile der angebotenen Leistung von einem oder mehreren Unterauftragnehmern erbracht (siehe Ziffer 2.1 des Angebotsformulars), so sind diese Unternehmen inkl. der von ihnen durchzuführenden Leistungen genau zu benennen. Erstellen Sie von jedem Unterauftragnehmer zudem ein aussagekräftiges Firmenprofil inkl. der folgenden Angaben:

- Offizielle Bezeichnung

- Rechtsform
- Firmensitz und Standorte
- auftragsbezogene Geschäftsfelder
- Anzahl der Mitarbeiter in den auftragsbezogenen Geschäftsfeldern
- durchzuführende Leistungen

Wird die Leistung ohne Mitwirkung von einem oder mehreren Unterauftragnehmern erbracht, so geben Sie an dieser Stelle Ihres Angebotes bitte lediglich „Kein Unterauftragnehmer“ an.

Die Weitergabe von wesentlichen Projektteilen an nicht genannte Unterauftragnehmer ist verboten.

6.2.1.3 Eignungskriterien

Nr.	Kriterien
1	Referenzen Legen Sie geeignete Referenzen der beteiligten Unternehmen vor. Referenzen sind geeignet, wenn die der Referenz zu Grunde liegenden Projekte hinsichtlich der fachlichen und technischen Leistungsfähigkeit im Wesentlichen ähnliche Anforderungen an die Unternehmen gestellt haben wie die ausgeschriebene Leistung. Dies ist bei der vorliegenden Ausschreibung insbesondere gegeben, bei Erfahrungen in der Neu- und Weiterentwicklung von Projekten im Bereich Kommunikations- und Informationssicherheit oder von Verschlüsselungs- und Signatursystemen und deren Komponenten. Die genannten Referenzen müssen insbesondere die Fähigkeit der beteiligten Unternehmen auf dem Gebiet der Forschung und Entwicklung sowie die Ausarbeitung und Umsetzung innovativer Lösungen belegen. Im Wege der Referenzen ist daher nachzuweisen, dass die beteiligten Unternehmen bereits Erfahrungen in den folgenden Erfahrungsbereichen gesammelt haben: 1. Entwicklung von Open-Source-Software (OSS) für die Betriebssysteme Linux oder Windows 2. Erstellung von Konzepten im Bereich der IT-Sicherheitskomponenten und -systeme 3. Erfahrungen im Bereich der IT-Sicherheit, insbesondere Schutz vor Angriffen von Dritten 4. Erfahrung in der Umsetzung und Implementierung von Kryptoalgorithmen und -protokollen, insbesondere unter Berücksichtigung angemessener Gegenmaßnahmen gegen Seitenkanalattacken beziehungsweise Protokollangriffen 5. Umsetzung/Realisierung eines innovativen Test- oder Pilotbetriebs 6. Behandlung von Sicherheitslücken in Standards oder Software-Komponenten Gehen Sie bei der Erstellung des Referenznachweises auf die folgenden Punkte ein: • Auftraggeber inkl. Fachbereich • (detaillierte) Darstellung des Auftragsgegenstands / der Tätigkeit • Umfang / Betroffener Erfahrungsbereich • Dauer • Auftragsvolumen Die Darstellung sollte zwei DIN A4-Seiten pro Referenzprojekt nicht überschreiten. Es werden keine Referenzschreiben früherer Auftraggeber benötigt. Mindestanforderungen: Für jeden Erfahrungsbereich (Nr. 1 bis 6) ist mindestens eine geeignete Referenz vorzulegen, wobei eine Referenz den Nachweis für mehrere Erfahrungsbereiche darstellen kann.

Nr.	Kriterien
2	**Technische Ausrüstung** Geben Sie einen kurzen Überblick über das technische Equipment, welches Ihnen zur Verfügung steht und von Ihnen zur Erbringung der hier ausgeschriebenen Leistung eingesetzt wird. Mindestanforderung: Der Bieter ist aus Sicht des BSI in der Lage, die hier zu vergebende Leistung mit Hilfe der beschriebenen technischen Ausrüstung erfolgreich zu erbringen. Der Auftragnehmer verfügt insbesondere mindestens über die folgende technische Ausrüstung: • Datenschutzfreundliches Videokonferenzsystem • Webserver für Downloads
3	**Qualitätsmanagement** Bitte stellen Sie das Qualitätsmanagement Ihres Unternehmens dar. Machen Sie bitte auch Angaben zu Zertifizierungen, die Ihr Unternehmen erworben hat. Mindestanforderung: Es ist ein Qualitätsmanagement etabliert und dokumentiert und kann nachgewiesen werden.

6.2.1.4 Qualitative Zuschlagskriterien

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
1	**B**	**KG1: Inhaltliche Auseinandersetzung mit der Leistung**	**-**	**50**	**50**	**200**
1.1	B	Aufgabenverständnis Weisen Sie Ihr Aufgabenverständnis nach, indem Sie die Ausgangssituation, die Zielsetzung des Projektes und die erwarteten Ergebnisse mit eigenen Worten erläutern. Benennen Sie die Ihrer Ansicht nach wichtigsten Punkte zu diesem Fachthema. Bewertungsskala (durchgängig von 0 bis 4 BP): • 0 BP: Die Ausführungen fehlen oder die Ausgangssituation, die Projektziele und / oder das erwartete Ergebnis sind unzureichend beschrieben. Die Ausarbeitung lässt keine umfassende Auseinandersetzung bzw. kein hinreichendes Verständnis der Thematik erkennen. Das Ziel des Projektes wurde nicht verstanden. • 1 BP: Die Ausgangssituation, die Projektziele und das erwartete Ergebnis sind ausreichend beschrieben. Die Ausarbeitung lässt eine Auseinandersetzung bzw. ein Verständnis der Thematik erkennen. Das Ziel des Projektes wurde hinreichend verstanden. • 4 BP: Die Ausgangssituation, die Projektziele und das erwartete Ergebnis sind zutreffend beschrieben. Die Ausarbeitung lässt eine umfassende Auseinandersetzung bzw. ein tieferes Verständnis der Thematik erkennen. Das Ziel des Projektes wurde vollumfänglich verstanden.	1	10	10	40
1.2	B	Umsetzung Seitenkanalanalyse bei Post-Quanten Verfahren in AP 4 Beschreiben Sie Ihre geplante Vorgehensweise bei der Analyse der Seitenkanalresistenz von Post-Quanten Verfahren. Gehen Sie dabei insbesondere darauf ein, wie Sie der Tatsache begegnen, dass in diesem Bereich noch nicht so viel Erfahrung und Resultate vorliegen, wie bei klassischen kryptografischen Verfahren. Bewertungsskala (durchgängig von 0 bis 4 BP): • 0 BP: Die Ausführungen fehlen, sind lückenhaft oder aus fachlicher Sicht unstimmig. • 1 BP: Die Ausführungen sind vollständig und stimmig. Aus Sicht des BSI können die beiden genannten Designziele auf dem beschriebenen Wege erfolgreich erreicht werden.	1	20	20	80

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		• 4 BP: Die Ausführungen sind vollständig und stimmig. Sie lassen eine tiefe Durchdringung des Themas erkennen und zeigen unter Berücksichtigung aller möglichen Nutzerszenarien eine optimale Umsetzung der beiden genannten Designziele.				
1.3	B	Vorgehensweise Tests Beschreiben Sie die Werkzeuge (Softwaretools, Methodiken, etc.), die Sie für die jeweiligen Arbeitspakete „Testspezifikation und Tests“ verwenden wollen. Bewertungsskala (durchgängig von 0 bis 4 BP): • 0 BP: Die Ausführungen fehlen, sind lückenhaft oder aus fachlicher Sicht unstimmig. • 1 BP: Die Ausführungen sind vollständig und stimmig. Die beschriebenen Werkzeuge scheinen geeignet, um die Ziele der jeweiligen Arbeitspakete „Testspezifikation und Tests“ in hinreichender Weise zu erreichen. • 4 BP: Die Ausführungen sind vollständig und stimmig. Sie lassen eine tiefe Durchdringung der Problematik erkennen. Die beschriebenen Werkzeuge scheinen geeignet, um die Ziele der jeweiligen Arbeitspakete „Testspezifikation und Tests“ in jeglicher Hinsicht zu erreichen.	1	10	10	40
1.4	B	Projektrisiken Welche Projektrisiken sehen Sie? Wie werden Sie mit diesen umgehen? Bewertungsskala (durchgängig von 0 bis 4 BP): • 0 BP: Die Ausführungen fehlen, die Darstellung der genannten Risiken ist unzureichend oder die Lösungsansätze für identifizierte Risiken sind nicht vorhanden oder undifferenziert. • 1 BP: Es wurde eine Risikoanalyse durchgeführt. Die Darstellung der genannten Risiken ist plausibel. Geeignete Lösungsansätze für identifizierte Risiken sind vorhanden, aber wenig differenziert. • 4 BP: Es wurde eine Risikoanalyse durchgeführt. Die Darstellung der genannten Risiken ist fundiert. Geeignete Lösungsansätze für identifizierte Risiken sind vorhanden und differenziert.	1	10	10	40
2	**A / B**	**KG 2: Projektorganisation und Kosten**		**10**	**10**	**40**
2.1	B	Personalprofile und Rollen Erstellen Sie von sämtlichen Personen des angebotenen	1	10	10	40

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		Projektteams ein Personalprofil. Mindestens die Projektleitung (PL) sowie die stellvertretende Projektleitung (sPL) sind namentlich zu benennen. Geben Sie im Profil der PL auch die Kontaktdaten (E-Mail, Telefon) an. Ordnen Sie die einzelnen Personen den beteiligten Unternehmen (Anbieter / Mitglieder der Bietergemeinschaft / Unterauftragnehmer) zu. Erläutern Sie in den Personalprofilen die Kenntnisse und Erfahrungen der einzelnen Personen anhand Ihrer Bildungsabschlüsse und/oder anhand von konkreten Projekten / Aufträgen / Publikationen, an denen die einzelnen Personen maßgeblich beteiligt waren. Gehen Sie dabei explizit auf den fachlichen Schwerpunkt dieser Projekte /Aufträge / Publikationen ein (Verweis auf bei den Eignungskriterien aufgeführte Referenzen der beteiligten Unternehmen möglich) und erläutern Sie die Tätigkeiten, die von der jeweiligen Person im Rahmen dieser Projekte / Aufträge / Publikationen erbracht wurden und welche Erfahrungen die jeweilige Person dabei sammeln konnte, die für das hier zu vergebende Projekt / die Abdeckung der definierten Mindestanforderungen relevant sind. Es muss für das BSI klar ersichtlich sein, welche konkreten Mindestanforderung aus Kapitel 4.1.2 mit den beschriebenen Projekten / Aufträgen /Publikationen abgedeckt werden. Die hier genannten Projekte / Aufträge / Publikationen, an denen die hier angebotenen Personen des Projektteams maßgeblich beteiligt waren, müssen nicht mit dem derzeitigen Arbeitgeber (Bieter / Mitglied der Bietergemeinschaft / Unterauftragnehmer) im Zusammenhang stehen. Die gesamte Darstellung sollte pro Person zwei DIN-A4 Seiten nicht überschreiten. Ordnen Sie zudem in einer tabellarischen Übersicht die angebotenen Personen / die Personalprofile konkreten Rollen / Tätigkeiten im Sinn von Projektleitung, Entwickler, Techniker, wissenschaftlicher Mitarbeiter, technischer Berater, etc zu. Anmerkung: die im vorherigen Satz vom BSI exemplarisch genannten Rollen dienen lediglich der Anschauung und wurden nicht auf das hier zu vergebende Projekt abgestimmt. Bewertungsskala (durchgängig von 0 bis 4 BP): • 0 BP: Die Ausführungen fehlen oder das angebotene Personal erfüllt nicht die in Kapitel 4.1.2 definierten Mindestanforderungen. • 1 BP: Das angebotene Personal erfüllt die in Kapitel 4.1.2 definierten Mindestanforderungen.				

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		• 4 BP: Die Qualifikation des angebotenen Personals übertrifft die in Kapitel 4.1.2 definierten Mindestanforderungen deutlich. Diese höhere Qualifikation hat erheblichen positiven Einfluss auf das Niveau der Auftragsausführung				
2.2	A	Kalkulation der Festpreise Stellen Sie für das AP 1 und AP 6, welche nach Festpreis vergütet werden (siehe Kapitel 3.1 und 3.2), Ihre Kostenkalkulation dar. Mindestanforderung: Das Angebot enthält eine tabellarische Übersicht, aus der für jedes einzelne AP, welches gemäß Kapitel 3.1 und 3.2 nach Festpreis vergütet wird, die folgenden Angaben entnommen werden können: • An der Durchführung des jeweiligen AP beteiligte Personen / Rollen (siehe Zuschlagskriterium „Personalprofile und Rollen“) • Tagessätze (zzgl. USt.) der jeweiligen Personen / Rollen (inkl. Gemeinkosten, etc.) • Kalkulierte Personentage pro Person / Rolle • Die aus den zuvor angegebenen Tagessätzen und kalkulierten Personentagen resultierenden Personalkosten • Ggf. anfallende Reisekosten • Ggf. anfallende Materialkosten. Setzen sich diese aus mehreren größeren Einzelpositionen zusammen, so sind diese in einer separaten Tabelle aufzuschlüsseln. • Höhe der Festpreise (zzgl. USt.) der einzelnen AP (resultierend aus den aufgeführten Personal-, Reise- und Materialkosten). • Achtung: Aufgrund der Corona-Pandemie ist es möglich, dass die Auftaktbesprechung, sowie der Projektabschluss lediglich digital stattfinden können. Demnach muss zusätzlich zu der Kalkulation für eine Präsenzveranstaltung, eine Kalkulation für eine Videokonferenz eingereicht werden. In diesem Fall entfallen mindestens die Reisekosten des Auftragnehmers. Die bei den einzelnen AP vorgesehenen Personen / Rollen sowie die jeweils veranschlagten Personentage erscheinen unter Berücksichtigung der sonstigen Ausführungen im Angebot plausibel und stehen nicht im Widerspruch zu den in Kapitel 4.1.2 geforderten Mindestqualifikationen des für die Leistungserbringung einzusetzenden Per-	-	-	-	-

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		sonals.				
2.3	A	Kalkulation der maximalen Obergrenzen Stellen Sie Ihre Kalkulation der angebotenen jeweiligen Obergrenzen dar. Mindestanforderung: Das Angebot enthält eine tabellarische Übersicht, aus der für jedes einzelne AP, welches gemäß Kapitel 3.1.2 nach Aufwand vergütet wird, die folgenden Angaben entnommen werden können: • An der Durchführung des jeweiligen AP beteiligte Personen / Rollen (siehe Zuschlagskriterium „Personalprofile und Rollen“) • Tagessätze (zzgl. USt.) der jeweiligen Personen / Rollen. Gemeinkosten, Materialkosten, Reisekosten sowie sonstige Kosten werden nicht gesondert vergütet und müssen daher bereits in den veranschlagten Tagessätzen enthalten sein. • Kalkulierte Personentage (PT) pro Person / Rolle **Achtung:** Für die AP 3.1 – AP 3.5 wurde vom BSI ein gemeinsames Kontingent von 20 PT und bei AP 7 ein Kontingent von 60 PT festgelegt, d.h. die Summe der kalkulierten Personentage muss diesem Kontingent genau entsprechen. • Höhe der jeweiligen maximalen Obergrenzen (zzgl. USt.) der einzelnen AP (resultierend aus den aufgeführten Tagessätzen und Personentagen) Die bei den einzelnen AP vorgesehenen Personen / Rollen sowie die jeweils veranschlagten Personentage erscheinen unter Berücksichtigung der sonstigen Ausführungen im Angebot plausibel und stehen nicht im Widerspruch zu den in Kapitel 4.1.2 geforderten Mindestqualifikationen des für die Leistungserbringung einzusetzenden Personals.	-	-	-	-
2.4	A	Zahlungs- und Meilensteinplan Erstellen Sie anhand der Vorgaben in Kapitel 3.1 und 3.2 einen verbindlichen Zahlungs- und Meilensteinplan in tabellarischer Form mit folgenden Spalten (analog zur Darstellung in Tabelle 1 in Kapitel 3.2): • Arbeitspaket / Meilenstein • (Kurz-) Bezeichnung • Beginn • Ende	-	-	-	-

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		• Art der Vergütung • Höhe des Festpreises / der maximalen Obergrenze ◦ zzgl. USt. ◦ inkl. USt. Die verbindlichen Vorgaben des AG (z.B. Art der Vergütung) sind dabei zwingend zu beachten. Stellen Sie den Ablauf des Projektes zudem als Gantt-Diagramm dar. Die zeitliche Planung ist im Angebot unter der Annahme zu erstellen, dass die Auftragserteilung erst unmittelbar vor Ablauf der Bindefrist des Angebotes erfolgt. Bei der späteren Leistungserbringung sind sämtliche in Kapitel 3.2 definierten verbindlichen zeitlichen Vorgaben (inkl. „maximaler zeitlicher Abstand zwischen Auftragserteilung und Projektstart“ sowie „maximale Projektlaufzeit“) jedoch auch dann einzuhalten, wenn das Vergabeverfahren früher als geplant erfolgreich abgeschlossen werden kann. In diesem Fall ist die zeitliche Planung des erfolgreichen Bieters in Abstimmung mit dem BSI entsprechend anzupassen (vgl. Kapitel 2.1). Die Dauer der einzelnen AP kann von jedem Bieter individuell kalkuliert werden, d.h. Abweichungen von den unverbindlichen Schätzwerten des AG (siehe Kapitel 3.2, Tabelle 1, Spalte „Termin nach Projektstart [Kalendermonate], Beginn, Ende“) sind durchaus möglich. Mindestanforderung: • Der Meilensteinplan bildet alle AP / Leistungen, die in Kapitel 3.2, Tabelle 1 dargestellt sind, ab. Enthält Kapitel 3.2 verbindliche Vorgaben bzgl. der Bearbeitungsreihenfolge der einzelnen AP / Leistungen, so wurden diese eingehalten. • Wurde die Reihenfolge einzelner AP in Kapitel 3.2 nicht verbindlich vorgegeben und weicht die im Angebot enthaltene Planung bei diesen AP / Leistungen von der in Kapitel 3.2, Tabelle 1 dargestellten Reihenfolge ab, so wurde diese Abweichung detailliert begründet. Die abweichende Planung erscheint aus Sicht des BSI zweckmäßig. • Im Angebot ist jeweils ein konkretes Datum für die Fertigstellung der einzelnen Arbeitspakete sowie für das Erreichen der einzelnen Meilensteine angegeben. Diese erscheinen aus Sicht des BSI realistisch und plausibel. • Die verbindlichen zeitlichen Vorgaben aus Kapitel 3.2 (z.B. maximaler Zeitrahmen für die Leis-				

Nr.	Kriterien-art	Kriteriengruppen (KG) / Kriterien	BP_{min}	GF	LP_{min}	LP_{max}
		tungserbringung) wurden eingehalten. Wurde die in Kapitel 3.2, Tabelle 1 dargestellte Meilensteinplanung zwecks Einführung zusätzlicher Zahlungszeitpunkte um weitere Meilensteine ergänzt, so wurden dabei die in Kapitel 3.2 definierten Vorgaben bzgl. Abnahmefähigkeit der Leistungen und Zulässigkeit der Rechnungslegung beachtet.				
3	**A**	**KG 3: Nutzungsrechte**				
3.1	A	Aufbau auf bestehenden Entwicklungen Baut die angebotene Leistung auf bestehenden Entwicklungen (proprietäre oder Open Source Software bzw. Hardware) auf, die der Bieter oder ein Dritter unabhängig von dem hier zu vergebenden Auftrag entwickelt hat (Eigenentwicklungen), so sind diese bzw. die verwendeten Softwarelizenzen im Angebot gemäß Ziffer 10.4 des Projektvertrages aufzulisten. Mindestanforderung: Das Angebot enthält eine stichpunktartige Aufzählung, aus der die oben geforderten Angaben entnommen werden können. Diese sind auch im Hinblick auf die sonstigen Angaben im Angebot schlüssig. Sofern nicht auf bestehenden Entwicklungen aufgebaut wird und es sich um eine vollständige Neuentwicklung handelt, ist dies ebenfalls anzugeben.	-	-	-	-
		Gesamt:		**60**	**60**	**240**

6.2.2 Anlage: Bietergemeinschaftserklärung

Wird das Angebot von einer Bietergemeinschaft abgegeben, so ist dem Angebot eine entsprechende Erklärung beizufügen (siehe standardisiertes Formular in den Vergabeunterlagen). Diese Erklärung ist von allen Mitgliedern der Bietergemeinschaft zu signieren (siehe Ziffern 3.4.2 und Ziffer 6.2 der Allgemeinen Bewerbungsbedingungen).

6.2.3 Anlage: Unterauftragnehmerverpflichtungserklärung(en)

Sollen wesentliche Teile der angebotenen Leistung von einem oder mehreren Unterauftragnehmern für den Bieter erbracht werden, so ist dem Angebot pro Unterauftragnehmer eine entsprechende Verpflichtungserklärung beizufügen (siehe standardisiertes Formular in den Vergabeunterlagen). Diese sind von den Unterauftragnehmern zu signieren (siehe Ziffern 3.4.2 und Ziffer 6.3 der Allgemeinen Bewerbungsbedingungen).

6.2.4 Anlage: Angaben zu vorliegenden Ausschlussgründen und zur Selbstreinigung im Sinne von § 125 GWB

Liegt mindestens ein zwingender oder fakultativer gesetzlicher Ausschlussgrund bei dem Bieter, bei einem Mitglied der Bietergemeinschaft oder bei einem Unterauftragnehmer vor (siehe Kapitel 5.1), so ist dem Angebot eine entsprechende Erklärung als Anlage beizufügen. Diese muss mindestens die folgenden Angaben enthalten:

- Abschließende Auflistung aller vorliegenden Ausschlussgründe im Sinne von den § 123 und § 124 GWB
- Detaillierte Erläuterungen zu den vorliegenden Ausschlussgründen. Insbesondere enthalten die Erläuterungen Angaben zur Art der Straftat, zur Höhe des fraglichen Betrages, zum Datum einer rechtskräftigen Gerichtsentscheidung / bestandskräftigen Verwaltungsentscheidung, zur Dauer des festgelegten Ausschlusszeitraums sowie zu den eingegangenen Verpflichtungen im Sinne von § 123 Abs. 4 Satz 2 GWB.
- Getroffene Maßnahmen zur Selbstreinigung im Sinne von § 125 GWB.

Die Anlage ist zu signieren (siehe Ziffern 3.4.2 der Allgemeinen Bewerbungsbedingungen).

C Abkürzungsverzeichnis [5]

AG	Auftraggeber
AN	Auftragnehmer
AP	Arbeitspaket
BMWi	Bundesministerium für Wirtschaft und Energie
BP	Bewertungspunkte
BP_{min}	Mindestpunktzahl (Bewertungspunkte)
BQM	Beauftragte/Beauftragter für Qualitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
GP	Gewichtungspunkte
KG	Kriteriengruppe
LP	Leistungspunkte
LP_{max}	Maximalpunktzahl (Leistungspunkte)
LP_{min}	Mindestpunktzahl (Leistungspunkte)
MS	Meilenstein
PDF	Portable Document Format
PL	Projektleitung
sPL	stellvertretende Projektleitung
SÜG	Sicherheitsüberprüfungsgesetz
Ü2	Erweiterte Sicherheitsüberprüfung
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch

5) Das Abkürzungsverzeichnis erhebt keinen Anspruch auf Vollständigkeit. Auch kann dieses standardisierte Verzeichnis ggf. Abkürzungen und Begriffe zu inhaltlichen Punkten enthalten, die nicht Gegenstand der hier vorliegenden Leistungsbeschreibung sind (z.B. SÜG).