Geschäftsplan für ein DIN SPEC-Projekt nach dem PAS-Verfahren zum Thema **„Festlegung eines Quantencomputer-resistenten Verschlüsselungsverfahrens“**

Status:
Zur Erarbeitung der DIN SPEC (PAS) nach Annahme am 06. Juli 2020

Anmeldungen zur Mitarbeit sowie Kommentare zum Geschäftsplan sind erbeten und bis zum 17.06.2020 an jessica.frost@din.de zu übermitteln[1]

Die Empfänger dieses Geschäftsplans werden gebeten, mit ihren Kommentaren **jegliche relevanten Patentrechte**, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Berlin, 13.07.2020 (Version 2)

[1] Anmeldungen zur Mitarbeit und Kommentare zum Geschäftsplan, die nach Ablauf der Frist eingehen, müssen nicht berücksichtigt werden. Über die Einarbeitung der fristgerecht eingegangenen Kommentare entscheidet das Konsortium (Gremium) nach seiner Konstituierung.

Inhaltsverzeichnis

1. Status/Version des Geschäftsplans

- **Zur Kommentierung durch die Öffentlichkeit (Version 1)**

  Dieser Geschäftsplan dient zur Information der Öffentlichkeit über das geplante Projekt. Interessenten haben die Möglichkeit, sich an dem Projekt zu beteiligen und/oder den Geschäftsplan zu kommentieren. Hierfür ist eine entsprechende E-Mail an jessica.frost@din.de zu richten.

  Über die tatsächliche Durchführung des Projekts entscheidet die Geschäftsleitung von DIN im Nachgang an die Veröffentlichung dieses Geschäftsplans.

  Kommt das Projekt zustande, werden alle Akteure, die sich fristgerecht zur Mitarbeit angemeldet oder den Geschäftsplan kommentiert haben, zum Kick-Off eingeladen.

- **Zur Erarbeitung der DIN SPEC nach Annahme am 06.07.2020**

  Änderungsvermerk zur Vorgängerversion 1:

  - Status des Geschäftsplans auf Titelblatt und in Abschnitt 1 geändert
  - Versionsnummer geändert
  - Abschnitt 2: Tabelle der teilnehmenden Organisationen ergänzt
  - Abschnitt 4: Aussage zur Kick-Off-Sitzung angepasst
  - Abschnitt 7: Daten zur Konsortialleitung ergänzt

2. Initiator[2] und weitere Konsortialmitglieder

- Initiator:

Person/Organisation	Kurzbeschreibung
Dr. Rachid El Bansarkhani, QuantiCor Security GmbH	QuantiCor Security GmbH ist ein Unternehmen (KMU), das Quantencomputer-resistente Sicherheitslösungen entwickelt. Es besteht aus einem Team von IT-Sicherheitsexperten, die auf dem Gebiet der Post-Quanten Kryptografie spezialisiert sind. Außerdem hat es verschiedene renommierte Preise für seine Quantencomputer-resistenten Sicherheitslösungen

[2] Die in diesem Dokument gewählte männliche Form der geschlechtsbezogenen Begriffe wie z. B. „der Initiator“ gelten selbstverständlich auch für alle weiblichen Personen. Lediglich aufgrund der besseren Verständlichkeit des Textes wurde einheitlich die männliche Form gewählt.

	gewonnen, wie z. B. den Accenture Innovation Award und den Hauptpreis beim deutschen Gründerwettbewerb für Digitale Innovationen.

- Potenzielle zusätzliche Teilnehmer:

Die DIN SPEC wird durch einen Konsortium (temporäres Gremium) erarbeitet, der jedem Interessenten offen steht. Die Mitwirkung von weiteren Experten ist sinnvoll und wünschenswert. Es bietet sich an, dass sich beispielsweise

- Hochschulen/Universitäten
- Forschungseinrichtungen
- Cyber Security-Unternehmen
- IT-Dienstleister
- Beratungsunternehmen
- Bundesbehörden (z. B. BSI – Bundesamt für Sicherheit in der Informationstechnik)
- usw.

an der Erarbeitung der DIN SPEC beteiligen.

- Organisationen[3], die sich zur Mitwirkung angemeldet haben:

Dr. Rachid El Bansarkhani	QuantiCor Security GmbH
Dr. Michael Riecker	Protiviti GmbH
Dr. Juliane Krämer	Technische Universität Darmstadt
Matthias Springer	TÜV NORD CERT GmbH
Jessica Frost	DIN

- Organisationen[3], die diesen Geschäftsplan angenommen haben (Konsortialmitglieder):

Person	**Organisation**
Dr. Rachid El Bansarkhani	QuantiCor Security GmbH
Dr. Michael Riecker	Protiviti GmbH
Dr. Juliane Krämer	Technische Universität Darmstadt
Matthias Springer	TÜV NORD CERT GmbH
Hans-Peter Fischer	KPMG AG Wirtschaftsprüfungsgesellschaft

3. Ziele des Projekts

3.1. Allgemeines

Quantencomputer stellen die nächste Generation der Rechnertechnologie dar. Die Gesetze der Quantenphysik erlauben es ihnen auf eine außergewöhnliche, heute noch nicht absehbare, Rechenleistung zurückzugreifen. Alle in der Praxis eingesetzten asymmetrischen Kryptosysteme können aufgrund der Anfälligkeit für Quantencomputer-Angriffe infolge Shors-Quantenalgorithmus gebrochen werden. Gegenwärtige Verschlüsselungstechnologien können demnach mittels Quantencomputer außer Kraft gesetzt werden und bieten somit keinen ausreichenden Schutz mehr. Das Ausmaß der Gefahr ist dramatisch, denn verschlüsselte Daten können schon heute gespeichert werden, um diese zu einem späteren Zeitpunkt mittels Quantencomputer zu entschlüsseln. Davon betroffen sind die verschiedensten Bereiche der Wirtschaft und Gesellschaft, wie z. B. die im Internet ausgetauschten Informationen, der E-Mail Verkehr, Online-Banking und Online-Shopping. Dies betrifft insbesondere auch das Internet der Dinge (IoT), dem intelligente IoT-Geräte zugrunde liegen, die sicherheitskritische Informationen miteinander austauschen. Von den Folgen dieser Bedrohung sind alle Unternehmen und Lebensbereiche direkt betroffen. Wenn das Beispiel von medizinischen Informationen oder Patientendaten herangezogen wird, die mindestens ein Leben lang (mehr als 100 Jahre) gesichert werden müssen, so kann ein Angreifer vergangene und gegenwärtig verschlüsselte Daten sammeln, um diese dann mittels Quantencomputer zu brechen. Diese Daten können im Interesse des Angreifers missbraucht werden.

Da klassische Public Key Verschlüsselungsverfahren keinen Schutz gegen Quantencomputer-Angriffe bieten können, sind neue Sicherheitsmechanismen notwendig. Die sogenannten Quantencomputer-resistenten Sicherheitstechnologien dienen hierbei als Kandidaten und können die traditionellen Verschlüsselungsmechanismen ersetzen.

Quantencomputer-resistente Verschlüsselungsverfahren basieren auf Berechnungsproblemen, die auch von Quantencomputern nicht gebrochen werden können. Gitter-, Code-, Hash-, Multivariate und Isogenie-basierte Kandidaten spielen hierbei eine wichtige Rolle.

In den letzten Jahren haben sich einige Verschlüsselungsverfahren hervorgetan, die als Quantencomputer-resistente Alternativen in Frage kommen. Bisher wurden lediglich die Hash-basierten Signaturverfahren standardisiert.

Ziel der DIN SPEC ist es, einen Quantencomputer-resistenten Verschlüsselungs- bzw. Schlüsselkapselungsmechanismus (KINDI-KEM) zu standardisieren, welcher auf Gitterproblemen basiert. Im Speziellen basiert das Verfahren auf dem gitterbasierten Verschlüsselungsmechanismus LARA, der mittels einer Falltürkonstruktion realisiert wird und die zu verschlüsselnden Daten im Fehlerterm verbirgt. Das Verfahren bietet Schutz

vor Angriffen durch Quantencomputer. Dies hat viele Vorteile und ist ein wichtiger Schritt für den Einsatz in Unternehmensanwendungen. Die feste Vorgabe von Bausteinen, Schnittstellen, Formaten, Parametern und Funktionen erlaubt es, das jeweilige Verfahren sicher zu implementieren und zu nutzen. Generell gilt es Verschlüsselungs- und Signaturverfahren zu standardisieren, um Implementierungsfehler zu beseitigen. Die Spezifikation gibt somit vor, wie die Verschlüsselungsverfahren zu nutzen sind und verringert dadurch die Fehler auf der Seite der Anwender und Unternehmen.

3.2. Geplanter Anwendungsbereich

Diese DIN SPEC definiert einen Quantencomputer-resistenten Verschlüsselungs- bzw. Schlüsselkapselungsmechanismus (KINDI-KEM), welcher auf Gitterproblemen basiert. Bei diesem Verfahren werden Daten im Fehlerterm verborgen. Dazu werden die dafür nötige Funktionsweise und relevanten Sicherheitsmerkmale festgelegt. Weiterhin werden Parametersätze festgelegt, die verschiedene Sicherheits- und Effizienzlevel angeben. Das Sicherheitslevel umfasst die Bit-Sicherheit des Verfahrens und das Effizienzlevel umfasst die Größen der Schlüssel und Schlüsseltexte.

3.3. Verwandte Aktivitäten

Das Thema der geplanten DIN SPEC ist bisher nicht Gegenstand einer Norm. Es existieren jedoch die folgenden, themenverwandten Gremien, Normen und/oder Regelwerke, die im Zuge des Projekts berücksichtigt und ggf. einbezogen werden:

- ETSI ISG QKD
- Normenausschuss Sicherheitstechnische Grundsätze (NASG)
- Normenausschuss Informationstechnik und Anwendungen (NIA)
- DIN EN ISO/IEC 19790, Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für kryptografische Module
- ISO/IEC 23837-1, Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements (in Erarbeitung)
- ISO/IEC 23837-2, Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods (in Erarbeitung)
- RFC 8391, XMSS: eXtended Merkle Signature Scheme
- RFC 8554, Leighton-Micali Hash-based Signatures

4. Arbeitsprogramm

Im Zuge des Projekts soll eine DIN SPEC nach dem PAS-Verfahren (vgl. www.din.de/go/spec) erarbeitet werden. Die DIN SPEC darf nicht in Widerspruch zum Deutschen Normenwerk stehen.

Das Kick-Off fand **am 06.07.2020 per Webkonferenz** statt. Die Projektlaufzeit beträgt ca. zwölf Monate.

Das Kick-Off dient der Konstituierung des Konsortiums, der Abstimmung bzw. Klärung weiterer organisatorischer Punkte sowie ggf. der Aufnahme der inhaltlichen Arbeiten.

Die Veröffentlichung eines Entwurfs zur Kommentierung durch die Öffentlichkeit ist nicht vorgesehen.

Insgesamt werden zwei Projektmeetings (Kick-off und Arbeitsmeeting) und drei Webkonferenzen durchgeführt, um die jeweils bis dahin erarbeiteten Inhalte vorzustellen, abzustimmen und ggf. zu verabschieden. Die Erarbeitung der Inhalte kann durch einzelne Konsortialmitglieder oder Arbeitsgruppen erfolgen.

Die Terminierung der weiteren Projektmeetings und/oder Webkonferenzen erfolgt durch das Konsortium in Abstimmung mit DIN.

Die DIN SPEC wird in Deutsch erarbeitet (Sitzungssprache, Berichte, usw.). Die DIN SPEC wird in Englisch verfasst.

ANMERKUNG In der Kalkulation wurde nur eine Sprachfassung berücksichtigt. Die Erarbeitung weiterer Sprachfassungen verursacht zusätzliche Kosten und muss deswegen gesondert vereinbart werden. Wenn eine weitere Sprachfassung gewünscht wird, kann die Übersetzung auch durch Beuth/DIN erfolgen. Diese wäre nach Verabschiedung des Manuskripts zur Veröffentlichung der DIN SPEC zusätzlich zu beauftragen.

5. Ressourcenplanung

Jedes Konsortialmitglied trägt seine im Rahmen des Vorhabens anfallenden Aufwendungen selbst.

Die Mitgliedschaft im Konsortium und die Teilnahme an den Projektmeetings ist kostenfrei, da die Kosten, die DIN aufgrund der Durchführung des Projekts entstehen, durch Mittel aus dem DIN-Connect-Projekt „Festlegung eines Quantencomputer-resistenten Verschlüsselungsverfahrens“ – gefördert durch DIN – finanziert werden.

6. Regeln der Zusammenarbeit im DIN SPEC-Konsortium

Das Projekt unterliegt den PAS-Verfahrensregeln. Alle Interessenten und Konsortialmitglieder sind dazu aufgefordert, sich unter http://www.din.de/go/spec über die Verfahrensregeln in Kenntnis zu setzen.

Die Konstituierung des Konsortiums erfolgt im Zuge des Kick-Offs. Der Kick-Off findet erst statt, nachdem der Geschäftsplan veröffentlicht und die Durchführung des Projekts durch die DIN-Geschäftsleitung genehmigt wurde. Das Konsortium muss sich aus mindestens drei Konsortialmitgliedern unterschiedlicher Organisationen[3] zusammensetzen. Es ist nicht notwendig, dass diese unterschiedliche interessierte Kreise repräsentieren. Durch Zustimmung zum Geschäftsplan erklären die Interessenten ihre Bereitschaft zur Mitarbeit im Konsortium und werden dadurch formell zu Konsortialmitgliedern mit den einhergehenden Rechten und Pflichten. Teilnehmer des Kick-Offs, die den Geschäftsplan nicht annehmen, erhalten nicht den Status eines Konsortialmitglieds und sind von weiteren Entscheidungen des Kick-Offs sowie vom weiteren Projekt ausgeschlossen.

Entsendet eine Organisation (z. B. ein Verband) einen nicht-hauptamtlichen Mitarbeiter in das Konsortium, muss dieser von der Organisation autorisiert und DIN der Nachweis vorgelegt werden.

Jedes Konsortialmitglied erhält ein Stimmrecht und verfügt über jeweils eine Stimme. Entsendet eine Organisation mehrere Experten in das Konsortium, besitzt die Organisation, ungeachtet der Anzahl der entsendeten Teilnehmer, eine Stimme. Eine Übertragung von Stimmen auf andere Konsortialmitglieder ist nicht möglich. Bei Abstimmungen gilt einfache Mehrheit der abgegebenen Stimmen, wobei Stimmenthaltungen grundsätzlich nicht mitgezählt werden.

Das konstituierte Konsortium ist in der Regel geschlossen. Über die Aufnahme zusätzlicher Mitglieder entscheiden die bisherigen Konsortialmitglieder.

Im Zuge des Kick-Offs wählen die Konsortialmitglieder einen Konsortialleiter. Dieser leitet das Konsortium inhaltlich und führt die Entscheidungsfindung (Abstimmungen, Beschlüsse) herbei. Der Konsortialleiter wird hierbei durch den DIN-Projektmanager unterstützt, wobei DIN stets eine inhaltlich neutrale Position einnimmt. Darüber hinaus trägt der DIN-Projektmanager dafür Sorge, dass die Verfahrens- und Gestaltungsregeln von DIN bei der Erstellung der DIN SPEC eingehalten werden. Sollte der Konsortialleiter seine Funktion nicht mehr wahrnehmen können, werden vom DIN-Projektmanager Neuwahlen initiiert.

[3] Organisationen sind teilnehmende juristische Personen, die die Experten in das DIN SPEC-Konsortium entsenden und einer Unternehmensstruktur i.S.v. § 15 Aktiengesetz oder § 271 Absatz 2 Handelsgesetzbuch zuzurechnen sind.

Die Organisation und Leitung des Kick-Offs erfolgt durch den DIN-Projektmanager in Abstimmung mit dem Initiator. Die übrigen Projektmeetings und/oder Webkonferenzen werden vom DIN-Projektmanager in Abstimmung mit dem Konsortialleiter organisiert.

Wenn Konsortialmitglieder bei der Verabschiedung der DIN SPEC bzw. des Entwurfs nicht anwesend sein können, sind diese über alternative Wege (z. B. schriftlich, elektronisch) in die Abstimmung einzubeziehen.

Alle Konsortialmitglieder, die für die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt haben, werden als Verfasser namentlich und mit der zugehörigen Organisation im Vorwort aufgeführt. Alle Konsortialmitglieder, die gegen die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt oder sich enthalten haben, dürfen nicht im Vorwort genannt werden.

Über eine nachträgliche Erweiterung des Konsortiums entscheiden die bisherigen Konsortialmitglieder. Dabei ist insbesondere zu berücksichtigen, dass

a) die Erweiterung förderlich ist, die Projektdauer zu verkürzen bzw. ein drohender Verzug der geplanten Projektdauer vermieden bzw. abgewendet werden kann;
b) die Erweiterung nicht zu einer drohenden Verlängerung der Projektdauer führt;
c) das neue Konsortialmitglied keine neuen oder ergänzenden Sachverhalte abseits des im Geschäftsplans festgelegten und bewilligten Anwendungsbereiches thematisiert;
d) das neue Konsortialmitglied ergänzendes Fachwissen mitbringt, damit die neuesten Erkenntnisse der Wissenschaft und der jeweilige Stand der Technik eingebracht werden;
e) das neue Konsortialmitglied sich aktiv an der Manuskriptarbeit beteiligt durch Einbringen konkreter, aber nicht abstrakter Vorschläge und Beiträge.
f) das neue Konsortialmitglied für eine verstärkte Anwendung der DIN SPEC sorgt.

Um die sachgerechte Vervielfältigung und Verbreitung der Ergebnisse der Standardisierungsarbeit zu ermöglichen, räumen die Konsortialmitglieder DIN die Nutzungsrechte an den ihnen erwachsenden Urheberrechten an den Ergebnissen der Standardisierungsarbeit ein. Die Einräumung der Urhebernutzungsrechte hindert die Mitglieder des Konsortiums nicht daran, ihr eingebrachtes Wissen, ihre Erfahrungen und Erkenntnisse weiterhin zu nutzen, zu verwerten und weiterzuentwickeln.

Die Konsortialmitglieder sind angehalten, DIN über relevante Patentrechte, die in Zusammenhang mit diesem DIN SPEC Projekt stehen, zu informieren.

Nachträgliche Änderungen am Anwendungsbereich (Abschnitt 3.2) oder an der Ressourcenplanung (Abschnitt 5) erfordern neben einer 2/3-Mehrheit aller abgegebenen Stimmen zusätzlich die Zustimmung von DIN.

7. Kontaktpersonen

- Konsortialeiter:
  Dr. Rachid El Bansarkhani
  QuantiCor Security GmbH
  Heinrich-Hertz Straße 6
  64295 Darmstadt
  Tel: 017643619123
  E-Mail: rac.eb@quanticor-security.de

- Stellvertretender Konsortialleiter:
  Matthias Springer
  TÜV NORD CERT GmbH
  Manufacturing Technology
  Langemarckstr. 20
  45141 Essen
  Tel.: +49 (0)201 825-3299
  E-Mail: mspringer@tuev-nord.de

- Projektmanager:
  Jessica Frost
  DIN Deutsches Institut für Normung e. V.
  Saatwinkler Damm 42/43
  13627 Berlin
  Tel.: + 49 30 2601 – 2925
  Fax: + 49 30 2601 – 4 - 2925
  E-Mail: jessica.frost@din.de

- Initiator:
  Dr. Rachid El Bansarkhani (Kontaktdaten siehe oben)

Anhang: Zeitplan (vorläufig)

DIN SPEC-Projekt	2020												2021		
	Mrz	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Dez	Jan	Feb	Mrz
Initiierung													
1. Antrag und Prüfung													
2. Erstellung des Geschäftsplans													
3. Veröffentlichung des Geschäftsplans													
Erstellungsphase													
4. Kick-Off / Konstituierung des Konsortiums													
5. Erstellung der DIN SPEC													
6. Verabschiedung DIN SPEC im Konsortium													
Veröffentlichung													
7. Prüfung und Freigabe durch DIN													
8. Veröffentlichung der DIN SPEC													
Meilensteine				**B**	**K**		**W**		**B**	**W**		**W**	**B**		**M / V**					

B Zwischenbericht
K Kick-Off
M Projektmeeting
W Webkonferenz
V Verabschiedung der DIN SPEC