



Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Bundesministerium des Innern,
für Bau und Heimat
Referat DV 2
Alt-Moabit 140
10557 Berlin

Dr. Felix Bleckmann
Bundesamt für Sicherheit in der
Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582-6372
Fax +49 228 99 10 9582-6372

referat-di12@bsi.bund.de
www.bsi.bund.de

DE-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Bewertung Hotel Check-in Pilot

Bezug: Erlasse 0779_21 DV 2, 0780_21 DV 2, 0785_21 DV 2 vom 30.04.2021

Geschäftszeichen: DV2-17003/18#32

Berichterstatter/in: RD Dr. Jens Bender

Datum: 11.05.2021

Seite 1 von 8

Sachstand:

In §28 (5) des Bundesmeldegesetzes (BMG) wird geregelt, wie die besondere Meldepflicht in Beherbergungsstätten auf elektronischem Wege erfüllt werden kann. Folgende drei Möglichkeiten sind dort fest vorgesehen:

1. Auslösung eines kartengebundenen Zahlungsvorgangs mit einer starken Kundensicherheitsauthentifizierung im Sinne des § 1 Absatz 24 des Zahlungsdienstleistungsaufsichtsgesetzes, bei dem die zweckgebundene Zuordnungsnummer des eingesetzten Zahlungsmittels erhoben wird.
2. Erbringung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes.
3. Verwendung des Personalausweises nach § 18a des Personalausweisgesetzes, der eID-Karte nach § 13 des eID-Karte-Gesetzes oder des Aufenthaltstitels nach § 78 Absatz 5 des Aufenthaltsgesetzes zum Vor-Ort-Auslesen.

Auf Basis einer Experimentierklausel ist darüber hinaus seit Kurzem der Einsatz anderer Verfahren übergangsweise möglich. Dazu muss das BSI bei einer vorherigen Prüfung des Verfahrens ein vergleichbares Sicherheitsniveau zu den oben genannten drei Verfahren feststellen. Ein Vergleich mit dem klassischen Verfahren (papierbasierter Meldeschein) ist durch die Experimentierklausel nicht vorgesehen.

Das „Pilotvorhaben SSI-Hotel-Check-In“ des BKAmts soll genau diese Experimentierklausel nutzen. Das BSI hat daher intensiv die fortschreitenden Arbeiten am „Systemkonzept“ zum SSI-Piloten begleitet, das die Grundlage für eine Prüfung des BSI sein soll.



Seite 2 von 8

Das BSI wurde am 30.04.2021, basierend auf entsprechenden Anträgen der Hotelketten Motel One GmbH, Lindner Hotels AG und Steigenberger Hotels AG, vom BMI gebeten eine Einschätzung bzgl. der Sicherheit des SSI-Piloten vorzulegen. Als Grundlage liegt dem BSI Version 0.98 des Systemkonzepts („DIGITALE IDENTITÄTEN: PILOTVORHABEN HOTEL CHECK-IN“) vom 28.04.2021 vor, die den Anträgen beigelegt ist.

Stellungnahme:

Am 31.03.2021 wurde dem BSI ein erster Draft des Systemkonzepts „DIGITALE IDENTITÄTEN: PILOTVORHABEN HOTEL CHECK-IN“ vorgelegt. Dieses Konzept wurde seitdem in regelmäßigen Meetings (zwei pro Woche) des Konsortiums mit BSI, sowie einigen zusätzlichen Meetings in kleineren Runden intensiv diskutiert und fortentwickelt.

Die Prüfung des BSI erfolgte ausschließlich auf Basis dieser vorliegenden Dokumentation. Eine Prüfung der Umsetzung bzw. eine Prüfung der Einhaltung des Konzeptes ist nicht erfolgt. Entsprechend der Anforderung des BMG bezieht sich die Bewertung des BSI ausschließlich auf die „vergleichbare Sicherheit“ der Identifizierungsleistung („Basis-ID“) des Systems, nicht auf weitere Attribute wie etwa eine Arbeitgeberbestätigung („Company-ID“).

Basierend auf den im beiliegenden Systemkonzept enthaltenen Informationen erfüllt der SSI-Pilot technisch NICHT das von § 29 BMG geforderte zu den in Satz 1 Nummer 1 bis 3 genannten Verfahren vergleichbare Sicherheitsniveau. Ebenso erfüllt diese Lösung technisch nicht das Vertrauensniveau ‚substantiell‘ oder ‚hoch‘ nach BSI-TR-03107 bzw. nach der eIDAS VO.

Mit strikten (teilweise schon im Systemkonzept berücksichtigten) Einschränkungen den Nutzungszeitraum, die Gültigkeit, die Personengruppe, die Endgeräte, sowie die beteiligten Unternehmen betreffend, ist es aber möglich den Sicherheitsrisiken entgegenzuwirken und daher denkbar den SSI-Piloten im Rahmen des Hotel Check-ins zu testen. Die folgenden notwendigen Einschränkungen sind bereits im Systemkonzept berücksichtigt:

- Die Gesamtaufzeit des Piloten ist auf sechs Monate zu begrenzen. Eine Verlängerung auf Basis einer Neubewertung eines fortentwickelten Systems ist dabei nicht ausgeschlossen.
- Der Nutzerkreis, welcher sich im Rahmen des Piloten in einer Beherbergungsstätte identifizieren darf, ist auf die Mitarbeiter der vier Unternehmen Bosch, Deutsche Bahn, Deutsche Lufthansa & BWI zu beschränken, welche im folgenden Pilotunternehmen genannt werden. Die Mitarbeiter müssen den Pilotunternehmen bekannt sein und müssen durch die Unternehmen geeignet in den



Seite 3 von 8

Piloten eingewiesen werden. Die „Basis-ID“ darf nur an Mitarbeiter der Pilotunternehmen ausgestellt werden.

- Änderungen an den am Betrieb des Piloten beteiligten Unternehmen sind auszuschließen. Gleichermassen müssen die im Systemkonzept genannten Rollen ausschließlich, wie im Konzept beschrieben, durch die dort genannten Unternehmen wahrgenommen werden.
- Die Nutzung ist auf gemanagte Firmenhandys der beteiligten Pilotunternehmen zu beschränken. Dies beinhaltet insbesondere den Anschluss an ein Mobile Device Management (MDM), welches die Installation unbekannter Apps auf den für den Piloten genutzten Geräten ausschließt. Bei Geräten mit getrennten privaten und geschäftlichen Bereichen bezieht sich dies nur auf den geschäftlichen Bereich.
- Es muss technisch sichergestellt werden, dass die in öffentlichen App-Stores verfügbare Variante der Wallet-App nicht für den Piloten genutzt werden kann, sondern ausschließlich die über das oben genannten MDM verteilte Version. Dies kann z.B. durch gesonderte Versionen der App für den Piloten und deren Prüfung durch den Aussteller der „Basis-ID“ erfolgen.
- Die Teilnehmer des Piloten müssen für die Verbindung zum Blockchain-Netzwerk die im Anhang des beiliegenden Systemkonzepts enthaltene Genesis-File als Vertrauensanker verwenden.
- Die teilnehmenden Pilot-Hotels müssen für die Verifikation der „Basis-ID“ die im Anhang des beiliegenden Systemkonzepts enthaltene Credential-Definition verwenden.

Darüber hinaus sind folgende Einschränkungen notwendig:

- Der Pilot ist auf die Beherbergungsstätten der Hotelketten Steigenberger Hotels, Linder Hotels, sowie MotelOne zu beschränken, welche im folgenden Pilot-Hotels genannt werden. Technisch kann das Lesen der Daten aus der SSI-Wallet nicht auf diese Hotelketten beschränkt werden, daher ist rechtlich sicherzustellen, dass die Rechtswirkung gemäß BMG auf diese Pilot-Hotels beschränkt ist.
- Die Teilnahme zusätzlicher Pilotunternehmen oder Pilot-Hotels an dem Piloten ist auszuschließen.
- Die Ausgabe der „Basis-ID“ ist auf nur eine „Basis-ID“ pro Person zu beschränken.
- Die „Basis-ID“ muss eine möglichst kurze Gültigkeit (6 Wochen) haben.
- Ein Penetrationstest des Gesamtsystems (ohne Berücksichtigung der Hotel-eigenen Weiterverarbeitung sowie des eID Servers, der für die Online-Ausweisfunktion verwendet wird) ist bis Ende Juni 2021 durchzuführen und die Ergebnisse im Projekt umgehend zu berücksichtigen. Ist dies nicht bis Ende Juni 2021 der Fall, so ist die Gültigkeit der „Basis-ID“ auf vier Wochen zu begrenzen.



Seite 4 von 8

- Eine Absicherung der von der Wallet-App im Rahmen der Authentisierung verwendeten kryptographischen Geheimnisse über hardwareunterstützte Überschlüsselung ist bis Ende Juli 2021 umzusetzen. Ist dies nicht bis Ende Juli 2021 der Fall, so ist die Gültigkeit der Basis-ID auf vier Wochen zu begrenzen. Sind die Ergebnisse des Pentests bis zu diesem Datum nicht vorhanden oder berücksichtigt, ist die Gültigkeit der Basis-ID auf zwei Wochen zu begrenzen.
- Jegliche Veränderung/Anpassung des Piloten gegenüber dem Systemkonzept, sowie den hier genannten Auflagen macht eine Neubewertung erforderlich.

In der jetzigen Ausgestaltung ist der Pilot nicht für einen über den Piloten hinausgehenden Betrieb geeignet. Für letzteres müssten insbesondere die folgenden Punkte geklärt und umgesetzt werden:

- Der Prozess für das Hinzufügen/Ändern von Rollen bzw. Projektteilnehmern muss klar definiert werden und das damit erreichte Sicherheitsniveau bewertet werden. Es muss eine Gesamt-Governance für das System inkl. Anforderungen an die einzelnen Betreiber und sowie regelmäßiger Überprüfung der Anforderungen definiert werden. Es müssen Wege und Verantwortlichkeiten für Sicherheitsvorfälle festgelegt werden.
- Die Confluence-basierte Kommunikation zwischen den Teilnehmern muss gegen eine sichere Lösung ausgetauscht werden.
- Die für die Nutzung der Wallet-App notwendigen kryptographischen Geheimnisse (z.B. das sogenannte „Link-Secret“) müssen vom Smartphone-eigenen Secure Element erzeugt werden und dürfen nur in diesem gesichert verarbeitet werden.
- Sämtliche weiteren für das Identifizierungssystem notwendigen kryptographischen Geheimnisse müssen in gesondert gesicherten elektronischen Speicher- und Verarbeitungsmedien gesichert und verarbeitet werden (aufseiten der Arbeitgeber, der Knotenbetreiber und der Hotels).
- Es dürfen nur Verifier (im Wesentlichen Hotels) zugelassen werden, die im Rahmen der Vertrauensinfrastruktur (im Wesentlichen auf der Blockchain) bekannt sind, um eine Authentisierung der Verifier sicherzustellen. Bevor neue Entitäten (Aussteller von Attributen, Stewards, Verifier) in das System bzw. die Blockchain aufgenommen werden, müssen diese sicher identifiziert werden.
- Es dürfen nur durch das BSI empfohlene kryptographische Algorithmen verwendet werden.

Kurzbeschreibung:

Das vorliegende Systemkonzept beschreibt ein elektronisches Identifizierungssystem auf Basis einer Wallet-App, welche auf dem Mobilgerät des Nutzers installiert wird. In diesem Identifizierungssystem soll die Bindung der Identität an den Nutzer durch zwei Faktoren realisiert



Seite 5 von 8

werden, den Besitz der Wallet-App, sowie das Wissen einer dazugehörigen PIN. Der Besitz wird hierbei über einen kryptographischen Schlüssel ("Link Secret") nachgewiesen, welcher durch die App gespeichert und nur nach Eingabe der PIN verwendet kann. Die Schlüsselspeicherung, sowie die PIN-Verifikation erfolgt hierbei ausschließlich in Software ohne die Verwendung eines gesondert gesicherten elektronischen Speicher- und Verarbeitungsmediums.

Die erstmalige Identifizierung des Nutzers für die Erstellung der Identität in der Wallet erfolgt auf Basis des elektronischen Identitätsnachweises gemäß PAuswG, AufenthG bzw. eIDKG. Die hierbei ausgelesenen Identitätsdaten werden durch die bdr GmbH mit dem Wallet-eigenen „Link Secret“ kryptographisch verknüpft und signiert, wodurch ein "Verifiable Credential" entsteht, welches die elektronische Identität repräsentiert und in der Wallet gespeichert wird. Die bdr GmbH agiert hierbei als Aussteller der elektronischen Identität, welche im Kontext des Piloten "Basis-ID" genannt wird.

Anschließend kann der Nutzer ein weiteres Verifiable Credential („Company-ID“) von seinem Arbeitgeber erhalten, das seine Zugehörigkeit zu diesem nachweist und u.a. die Arbeitgeberadresse enthält. Auch dieses wird in der Wallet-App (auf Softwareebene) hinterlegt. Die Prozesse für die Ausstellung der Company-ID sind nicht Bestandteil dieser Bewertung.

Im Rahmen eines Check-ins werden die vom Hotel angeforderten Attribute (nach Eingabe der PIN) von der Wallet-App um einen sogenannten Zero-Knowledge-Proof für die nicht übermittelten Attribute (z.B. Nachweis des Besitzes des „Link Secret“) ergänzt und zusammen an das Hotel übermittelt. Das Hotel selbst verifiziert die übermittelten Daten (bzw. die enthaltenen Signaturen), wobei eine Blockchain als dezentrale Quelle für Vertrauensanker verwendet wird. Welches Verifiable Credential durch das Hotel als „Basis-ID“ anzufragen ist, wird den beteiligten Verifiern (Hotels) zusätzlich auf gesondertem Wege im Rahmen der Unterstützung bei der Installation der notwendigen Systeme bekannt gemacht.

Der Rückruf der „Basis-ID“ ist durch Nutzung des initial genutzten Personalausweises bzw. durch Verwendung eines anfänglich übermittelten Sperrkennworts in einer eigenen Infrastruktur möglich.

Bewertung:

Die für die Durchführung eines Hotel-Check-ins notwendige Authentifizierung des Nutzers anhand der Faktoren Besitz („Link-Secret“) und Wissen („PIN“) erfolgt ausschließlich anhand von Schlüsselmaterial, welches in der Wallet-App gespeichert wird. Die Schlüsselspeicherung sowie die PIN-Verifikation erfolgen hierbei ausschließlich in Software ohne die Verwendung eines gesondert gesicherten elektronischen Speicher- und Verarbeitungsmediums.



Auch die personenbezogenen Daten (enthalten in den Verifiable Credentials „Basis-ID“ und „Company-ID“) werden durch die Wallet-App lediglich auf Software-Ebene verschlüsselt und gegebenenfalls nach der Entsperrung des Smartphones mit dem Start der Wallet-App im Wesentlichen mit Hilfe der sechsstelligen PIN entschlüsselt.

Mit diesen technischen Maßnahmen werden ausgestellte Verifiable Credentials daher nicht ausreichend gegen den Zugriff Fremder geschützt. Dies ermöglicht schon wenig versierten Angreifern das Kopieren und Nutzen von Credentials (z.B. der „Basis-ID“) ohne Mitwissen des Besitzers sowie ohne seine PIN zu kennen.

Im Rahmen des SSI-Piloten wird die Nutzung daher auf Firmenhandys beschränkt, die zumindest über einen gemanagten (geschäftlichen) Bereich verfügen, zusammen mit einigen anderen organisatorischen Maßnahmen, wie einem Verbot das „Link Secret“ auszulesen. Da dies aber nur teilweise zu einer Verbesserung beiträgt, sind neben den im Systemkonzept berücksichtigten Einschränkungen weitere Einschränkungen (siehe oben) notwendig.

Darüber hinaus sind folgende sicherheitsrelevante Punkte zum SSI-Piloten hervorzuheben:

- Durch die Nutzung der Blockchain-basierten Lösung im SSI-Piloten wird die Komplexität und damit einhergehend die grundsätzliche Anfälligkeit für Sicherheitslücken des gesamten Systems bei unklarem Nutzen deutlich erhöht. Viele Ziele können auch auf Basis klassischer PKI-basierter Technologien ebenso umgesetzt werden, die bei Ausweitung des Betriebs auf eine größere Menge an Parteien in jedem Fall zur Sicherstellung der Authentizität von Nachrichten dieser Parteien erforderlich sind.
- Für den Betrieb des Blockchain-Netzwerks und den Identitätsnachweis werden kryptographische Protokolle und Verfahren eingesetzt, welche vom BSI nicht empfohlen werden und welche teilweise nicht standardisiert sind und noch experimentellen Charakter haben. Für diese liegen bisher keine ausreichenden Sicherheitsaussagen und Sicherheitsnachweise vor, welche eine positive Bewertung ermöglichen.
- Der SSI-Pilot verwendet (abgesehen von der Identifizierung mit dem Personalausweis) keine zertifizierten Komponenten. Ebenso werden keine (Hardware-)Komponenten durch direkte Auftragnehmer des Bundes hergestellt.
- Es gab bisher keinen Penetrationstest oder ähnliche Prüfungen von externen Prüfern, die eine ausreichende Resistenz des hier tatsächlich verwendeten Gesamtsystems gegen Angreifer nachweisen. Vor etwa drei Jahren wurde ein Penetrationstest einer Implementierung Komponente (Hyperledger Indy) durchgeführt. Für den Piloten konnte bisher nicht bestätigt werden, dass die dabei



Seite 7 von 8

entdeckten Schwachstellen nun – nach Ablauf von drei Jahren -- behoben sind. Sicherheitslücken in der Implementierung können daher nicht ausgeschlossen werden.

- Die kryptographischen Geheimnisse, welche die teilnehmenden Knoten des Blockchain-Netzwerks sowie deren Rollen identifizieren, sind auch auf Seiten der Knotenbetreiber nur in Software gesichert. Eine Kompromittierung dieser Geheimnisse ermöglicht es, dem Netzwerk beliebige neue Teilnehmer hinzufügen oder die Kontrolle über Netzwerk zu übernehmen, wodurch beliebige „Basis-IDs“ erzeugt werden können.
- Die sogenannten Genesisfiles, die den obersten Vertrauensanker für die Kommunikation zwischen den teilnehmenden Knoten darstellen, werden ebenfalls lediglich in Software sowie in einem lediglich mit Nutzernamen und Passwort geschützten Confluence Wiki gesichert.
- Auch anonyme Verifier (z.B. andere Hotels oder beliebige Dritte) können einen Check-in-Prozess durchführen. Wenn der Nutzer einen QR-Code zu diesem Zweck einscannt, wird ihm lediglich der darin enthaltene Name sowie der Hostname der anfragenden Stelle angezeigt. Eine Verifikation dieser Daten im Backend findet nicht statt. Der Nutzer kann daher nicht sicher beurteilen, ob er mit der richtigen Stelle kommuniziert.
- Die Aktualität der in der „Basis-ID“ enthaltenen Attribute hängt von dem Zeitpunkt ihrer Erzeugung ab. Eine gesetzliche Pflicht zur Anpassung innerhalb der „Basis-ID“ besteht nicht. Eine angemessene Aktualität kann daher nur durch eine beschränkte Gültigkeit der „Basis-ID“ sichergestellt werden

Für die Bewertung des erreichten Sicherheitsniveaus kann nur angenommen werden, dass die verwendeten Algorithmen und Protokolle ein entsprechendes Sicherheitsniveau erfüllen und auch die Implementierung entsprechend gestaltet ist.

Vergleich mit den bestehenden Möglichkeiten nach §29 BMG Satz 1:

Im Gegensatz zu einem kartengebundenen Zahlungsvorgang (entsprechend §29 BMG Satz 1 Nummer 1) ist im SSI-Piloten konstruktionsbedingt kein Tracking bzw. Risikomanagement o.ä. im Hintergrundsystem vorgesehen. Da es sich dabei jedoch im Kontext von kartenbasierten Zahlungsvorgängen um einen wesentlichen Sicherheitsmechanismus handelt, ist der SSI-Pilot nur sehr eingeschränkt mit den genannten kartengebundenen Zahlungsvorgängen vergleichbar. Darüber hinaus ist durch die beim SSI-Piloten rein lokale und softwarebasierte Sicherung der relevanten Geheimnisse und der Prüfung der PIN sowohl Kopierschutz als auch Zugriffsenschutz nicht mit dem eines kartengebundenen Zahlungsvorgangs vergleichbar.



Seite 8 von 8

In Bezug auf seinen vollständig dezentralen Ansatz und die vollständige Nutzerkontrolle folgt der SSI-Pilot ähnlichen Zielen wie der elektronische Identitätsnachweis mit dem Personalausweis. Wie bei der zweiten Möglichkeit (entsprechend §29 BMG Satz 1 Nummer 2) kommt der Sicherung der personengebundenen Daten und des für die Authentisierung notwendigen Geheimnisses im Gerät (bzw. im Ausweis) des Nutzers, sowie der Bindung von Gerät/Smartcard an die PIN eine zentrale Bedeutung zu. Der Personalausweis verfügt allerdings um einen deutlich stärkeren Kopierschutz und Zugriffsschutz (nachweislich resistent gegen Angreifer mit einem hohen Angriffspotential), so dass der SSI-Pilot ein vergleichbares Sicherheitsniveau nicht erreichen kann.

Im Rahmen der dritten Möglichkeit (entsprechend §29 BMG Satz 1 Nummer 3) ist zu beachten, dass diese nicht nur die Vorlage des Ausweises und das Auslesen desselben beinhaltet, sondern auch eine Identifikation der Person auf Basis des Ausweises (vgl. § 18a PAuswG) bzw. (im Fall der UBK) eines anderen Ausweisdokumentes/Passes. Der damit sichergestellte hohe Kopierschutz sowie die starke Personenbindung, erreicht eine deutlich höhere Sicherheit als der SSI-Pilot.

Weiteres Vorgehen:

- Entscheidung über die Freigabe des Verfahrens durch das BMI
- Von der Verwendung des SSI-Piloten im gegenwärtigen Zustand über den aktuellen Piloten hinaus wird seitens des BSI abgeraten.

Mit freundlichen Grüßen
Im Auftrag
gez.

Dr. Silke Bargstädter-Franke
Abteilungspräsidentin