

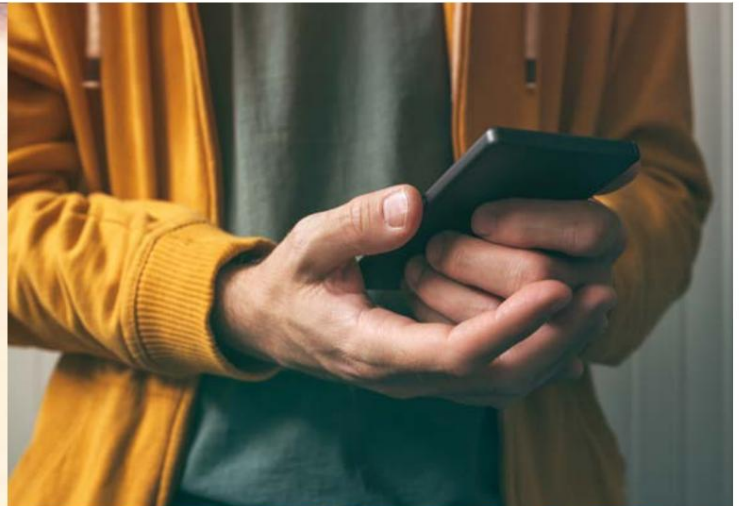
Systeminitiative zur Gestaltung der Zukunft der Mobilität

Der bekannte Reisende

Erschließen Sie das Potenzial der digitalen Identität für sicheres und nahtloses Reisen

In Zusammenarbeit mit Accenture

Januar 2018



Inhalt

3	Vorwort
4	Vorwort
5	Zusammenfassung
7	1. Zunehmender Druck auf die Sicherheit im Reiseverkehr
12	2. Methodik
14	3. Das Known Traveller Digital Identity-Konzept
21	4. Paradigmenwechsel hin zu einer digitalen Identität
23	5. Prinzipien und Kerntechnologien
31	6. Bau eines Prototyps
36	7. Nächste Schritte: Testen und skalieren
38	Empfehlungen
40	Danksagungen
41	Anhang A
42	Endnoten

Vorwort



Cheryl Martin
Geschäftsführer,
Leiter Industrie und
Mitglied des
Vorstand,
Weltwirtschaft
Forum

In der zersplitterten Welt von heute sind Regierungen, Führungskräfte der Reise- und Tourismusbranche und die Öffentlichkeit zunehmend besorgt über Sicherheitsbedrohungen. Anstatt Isolationismus zu fördern und reaktiv auf Sicherheitsschocks zu reagieren, müssen die Beteiligten zusammenarbeiten, um die öffentliche Sicherheit zu schützen und gleichzeitig die Bewegung rechtmäßiger Reisender zu erleichtern. Obwohl Regierungen private Unternehmen zur Optimierung von Reisesicherheitsprozessen einsetzen, müssen sie ihr Engagement vertiefen und die Zusammenarbeit mit verschiedenen Interessengruppen ausbauen, um die Transformation des Reisesicherheitssystems zu maximieren. Im Gegenzug müssen internationale Organisationen, die Einfluss auf Reisevorschriften haben, sowie Fluggesellschaften, Hotels, Finanzdienstleistungen und Technologieanbieter, die Dienstleistungen an Reisende verkaufen, über die typischen Branchenallianzen hinausgehen und mit Regierungen und untereinander zusammenarbeiten.

Neue Technologien – von Biometrie über Distributed Ledger bis hin zu maschinellem Lernen – bieten ein enormes Potenzial zur Transformation und Verbesserung des globalen Reisesicherheitssystems. Allerdings können auch Personen mit böswilliger Absicht die Technologie manipulieren, und Technologie allein wird die aktuellen Sicherheits Herausforderungen nicht lösen. Als internationale Organisation für öffentlich-private Zusammenarbeit bietet das Weltwirtschaftsforum eine Plattform für den offenen Dialog und fungiert als unparteiischer Moderator.

Im Laufe des Jahres 2017 versammelte das Projekt „Shaping the Future of Security in Travel“ Stakeholder zu mehrtägigen Workshops und Arbeitsaufrufen zum Thema digitale Identität, um die Sicherheit im Reiseverkehr weiter voranzutreiben. In diesem Bericht wird das Known Traveler Digital Identity-Konzept als katalytischer Prototyp beschrieben, der den Reise- und Tourismussektor sowie medizinische Dienstleistungen, Bildung und darüber hinaus verändern kann. Wir freuen uns auf die Umsetzung dieses Konzepts durch die Stakeholder im Jahr 2018.

Vorwort



John Moavenzadeh
Leiter Mobilität
Branchen und
Systeminitiative,
Mitglied der
Geschäftsleitung
Ausschuss, Welt
Wirtschaftsforum



Liselotte de Maar
Geschäftsführer,
Reiseindustrie,
Accenture-Strategie,
Niederlande

Grenzüberschreitendes Reisen ist von grundlegender Bedeutung für den globalen Wohlstand und Handel, die Erkundung neuer Kulturen und den Ideenaustausch. Reisen erweitert unseren Horizont und treibt die Wirtschaft voran. Da die Zahl der internationalen Ankünfte bis 2030 voraussichtlich um 50 % steigen wird, müssen wir den enormen Reisestrom trotz zunehmender Sicherheitsbedrohungen, begrenzter Infrastruktur und zahlreicher Kontrollebenen bewältigen.

Derzeit ist eine sichere und reibungslose Reise für Reisende nicht garantiert, und wenn sie nicht gut gehandhabt wird, könnte das Reiseerlebnis und die globale Reisebranche darunter leiden.

Gemeinsam mit seinen Partnern erforschte das Weltwirtschaftsforum Lösungen für nahtlose und sichere Reiseherausforderungen und entwickelte im Rahmen seines Projekts „Shaping the Future of Security in Travel“ das Konzept „Known Digital Traveler Identity“. Durch die Anwendung von Design-Thinking-Strategien und einem auf den Reisenden ausgerichteten Ansatz konnten die Teilnehmer die Reise des Reisenden kartieren und die wichtigsten Schwachstellen für den Reisenden, Regierungsbehörden und Unternehmen bei der Interaktion während des gesamten Reiseprozesses identifizieren. Technologien der Vierten Industriellen Revolution wie Biometrie, Blockchain, Kryptografie und mobile Geräte ermöglichen die Bewältigung der Herausforderungen, mit denen die Beteiligten konfrontiert sind, um eine sicherere und reibungslosere Reise für Reisende zu erreichen.

Dieses Known Traveler Digital Identity-Konzept basiert auf dem Prinzip, dass ein einzelner Reisender die Kontrolle über die Verwendung seiner eigenen Identität und ihrer Komponenten hat. Aufgrund dieser Dezentralisierung der Kontrolle über die Komponenten seiner Identität kann ein Reisender während seiner Reise Beweise für seine Identitätsinformationen – gesichert durch Distributed-Ledger-Technologie und Kryptografie – an staatliche und private Stellen weitergeben. Durch den Zugriff auf verifizierte persönliche biometrische, biografische und historische Reisedaten können Unternehmen unterwegs eine erweiterte Risikobewertung durchführen, die Identität von Reisenden überprüfen und durch biometrische Erkennungstechnologie einen nahtlosen Zugriff ermöglichen. All dies kann erreicht werden, ohne dass personenbezogene Daten in einer zentralen Datenbank gespeichert werden müssen, was ein zu großes Risiko für die Beteiligten darstellen würde, die für den sicheren Umgang mit persönlichen Identitätsinformationen verantwortlich sind.

Ein funktionierender Prototyp des Konzepts, der spezifische Anwendungsfälle demonstriert, wird auf der Jahrestagung des Weltwirtschaftsforums 2018 politischen Entscheidungsträgern, Technologieinnovatoren und Führungskräften aus der Wirtschaft vorgestellt. Zukünftig wird das Projekt darauf abzielen, mit Partnerregierungen ein skalierbares Pilotprojekt der Known Traveler Digital Identity umzusetzen.

Das Weltwirtschaftsforum würdigt und lässt sich von der Führung unserer Partner inspirieren, deren Engagement für dieses Projekt zeigt, dass diese Zukunft möglich ist. Insbesondere möchten wir Marc Garneau, dem kanadischen Verkehrsminister, und dem gesamten Team der kanadischen Regierung dafür danken, dass sie dazu beigetragen haben, sicherzustellen, dass die Forschung und Prototypenentwicklung auf pragmatischen Erfahrungen aus dem öffentlichen Sektor basiert. Gemeinsam hoffen das Weltwirtschaftsforum und Accenture, die an der Gestaltung der Zukunft der Sicherheit im Reiseverkehr arbeiten, dass dieser Bericht und der Prototyp an Dynamik gewinnen und öffentliche und private Parteien dazu ermutigen, dieses Konzept im kommenden Jahr zu testen und zu skalieren.

Zusammenfassung

Das Weltwirtschaftsforum konzentriert sich auf sicheres und reibungsloses Reisen

Prognosen deuten darauf hin, dass der grenzüberschreitende Reiseverkehr in den nächsten zehn Jahren um 50 % zunehmen und bis 2030 1,8 Milliarden internationale Ankünfte erreichen wird.¹ Dieser Anstieg stellt eine Chance für die Luftfahrt-, Reise- und Tourismusbranche dar, die wirtschaftlichen Vorteile, die sie zum BIP und zur Schaffung von Arbeitsplätzen beiträgt, weiter zu nutzen global. Um die wirtschaftlichen Chancen, die dieser Nachfrageanstieg mit sich bringt, voll auszuschöpfen, müssen sich die Beteiligten mit dem Druck auf der Reise des Reisenden auseinandersetzen, insbesondere mit dem erhöhten Risiko und den damit verbundenen Sicherheitsanforderungen sowie der begrenzten Wachstumskapazität der reise- und grenzbezogenen Infrastruktur. Experten gehen davon aus, dass die monetären und wirtschaftlichen Kosten des aktuellen Luftsicherheitssystems in den kommenden Jahrzehnten ein untragbares Niveau erreichen werden. Digitale Innovationen in der Reisesicherheit gepaart mit der Zusammenarbeit mehrerer Interessengruppen werden Lösungen für die Herausforderungen von heute ermöglichen.

Traditionell betrachteten die Menschen die Erleichterung von Passagieren und die Gewährleistung der Grenzsicherheit als Gegensätze. Wie im Bericht „Digitale Grenzen: Eine sichere, nahtlose und personalisierte Reise ermöglichen“ aus dem Jahr 2017 dargelegt, wird die Einbindung neuer Technologien in den Prozess die Art und Weise, wie Industrie und Regierungen den sicheren grenzüberschreitenden Personenverkehr verwalten, dramatisch verändern. Um dies zu erreichen, muss eine kohärente Vision für die Zukunft der Sicherheit im Reiseverkehr Benutzerzentrierung, Digitalisierung und vertrauensvolle Zusammenarbeit umfassen.

Vorherige Forschung

Untersuchungen mit der Internationalen Kriminalpolizeilichen Organisation (INTERPOL) und Interviews mit Leitern der zwölf fortschrittlichsten Programme für vertrauenswürdige und registrierte Reisende zeigten, welche Hindernisse der Verwirklichung dieser Zukunftsvision allein durch solche Programme im Wege stehen. Zu den Herausforderungen gehören die teure und personalintensive Umsetzung, das mangelnde Vertrauen zwischen den teilnehmenden Ländern – was zu doppelten Überprüfungsprozessen führt – und die geringen Akzeptanzraten aufgrund der Kosten und des Aufwands des Antragsverfahrens. Daher sind die Regierungen nur begrenzt in der Lage, Engpässe bei der Kontrolle und dem Grenzmanagement zu reduzieren. Wo Programme für registrierte Reisende eingeführt wurden, um die Aufnahme und Umsetzung zu verbessern, hängt die Bestimmung der ersten Bewertungen weiterhin vom alten System der Risikostufen basierend auf dem Herkunftsland ab.

Digitale Identität als Hebel für Veränderung

Ein Paradigmenwechsel hin zu einem Known Traveller Digital Identity-Konzept wird die Art und Weise, wie legitime Reisende sicher und nahtlos über Grenzen hinweg erleichtert werden, radikal verändern und die in Digital Borders diskutierten Ideen zum Leben erwecken. Das Konzept konzentriert sich auf den Einsatz von von Reisenden verwalteten digitalen Identitäten, die es Regierungen in Zusammenarbeit mit Branchenführern und Passagieren ermöglichen, vorab eine Risikobewertung und Sicherheitsverfahren durchzuführen, um den reibungslosen Grenzübergang von Reisenden zu verbessern. Sicherheitsbeamte werden ihre Aufmerksamkeit und Ressourcen auf die Identifizierung von Bedrohungen lenken und so zu einer verbesserten geopolitischen Sicherheit weltweit beitragen. Das Known Traveler Digital Identity-Konzept bietet zahlreiche Anwendungen für Regierung und Industrie im gesamten Reise- und Tourismussektor und darüber hinaus, um Reisenden personalisiertere und Mehrwertdienste anzubieten.

Neue Technologien zur Erreichung des Paradigmenwechsels

Um die Entwicklung dieses Konzepts zu unterstützen, Viertens Die Technologien der industriellen Revolution werden das Bekannte verändern Digitale Identität von Reisenden vom Konzept zur Realität:

1. Distributed Ledger ermöglicht Vertrauen in das Netzwerk ohne die Kontrolle einer zentralen Behörde
2. Kryptographie ermöglicht ein angemessenes Maß an Sicherheit bei der Autorisierung und Weitergabe von Informationen
3. Biometrie verbindet die physische und digitale Welt und gewährleistet die legitime Nutzung von Identitätsinformationen
4. Mobile Schnittstellen und Geräte ermöglichen es Reisenden, ihre digitale Identität bei sich zu tragen und diese entsprechend zu teilen

Darüber hinaus könnte die zunehmende Einführung und Nutzung elektronischer Reisepässe (ePässe) durch staatliche und nichtstaatliche Stellen die Möglichkeit bieten, neue Möglichkeiten zu eröffnen, um die Reise von Reisenden mit geringem Risiko zu erleichtern und gleichzeitig ein hohes Maß an Sicherheit zu gewährleisten. Wie bei neuen Technologien erwartet, gibt es noch keine ausreichenden Beweise, um die eine „beste“ Lösung zu ermitteln. Jede technologische Entscheidung, die bei der Gestaltung eines solchen innovativen Konzepts getroffen wird, muss im Hinblick auf die zu erwartenden Vor- und Nachteile berücksichtigt werden. Pilottests eines Prototyps, der zum Testen dieser Technologien entwickelt wurde, werden 2018 sowohl im Labor als auch in der realen Umgebung stattfinden.

Institutionelle Beziehungen, um Veränderungen voranzutreiben

Der Drang, Veränderungen herbeizuführen, muss drei Schlüsselwerte beachten. Erstens müssen sich die Regierungen dazu verpflichten, individuelle risikobasierte Bewertungen von Reisenden einzuführen. Auf diese Weise können sie die große Mehrheit der Reisenden mit geringem Risiko effizienter identifizieren und bearbeiten. Eine solche Vorabprüfung spart Zeit, die besser für die Erkennung von Risiken und Bedrohungen genutzt werden kann. Zweitens darf das Streben nach globaler Interoperabilität keinen Vorrang vor der Souveränität der Regierungen bei Entscheidungen über die Sicherheit ihrer Bürger haben. Das Known Traveller Digital Identity-Konzept wahrt das Recht der Regierungen, ihre eigenen Einwanderungs- und Sicherheitsentscheidungen zu treffen und gleichzeitig den Grundsatz der Verhältnismäßigkeit zu wahren. Schließlich muss dem Reisenden die Möglichkeit gegeben werden, von einer passiven Rolle zu einer aktiven Partnerschaft im Sicherheitsprozess überzugehen. Indem sie sich selbst für die Weitergabe ihrer digitalen Identität entscheiden, werden Reisende integraler Bestandteil des Sicherheitsprozesses und erleben die Belohnung einer personalisierteren und reibungsloseren Reise.

Empfehlungen

Das Known Traveler Digital Identity-Konzept ist der erste Schritt, um diesen systemischen Wandel in der Reisesicherheit zu erreichen. Es dient als Katalysator für die notwendigen, nachfolgenden Multistakeholder-Maßnahmen, die uns helfen werden, unser gemeinsames Ziel zu erreichen.

Vision für die Zukunft des Reisens. Zu den Vorschlägen, dies vom Konzept über den Prototyp zur Wirkung zu bringen, gehören:

A. Jetzt handeln: Stakeholder müssen den Prototyp testen

Richtlinien, Prozesse und Technologien, passen sie iterativ an und arbeiten daran, die Einbeziehung technologischer Durchbrüche mit fortlaufendem Fortschritt und Konvergenz auf der Grundlage der derzeit verfügbaren Möglichkeiten in Einklang zu bringen. Zur Ausweitung sollten Pilotprojekte an weiteren Standorten eingeführt werden, die geografisch und wirtschaftlich unterschiedlich sind.

B. Dynamik aufbauen: Dienstleister und Behörden

müssen Systeme entwerfen, die die intrinsischen Werte und Vorlieben des Reisenden berücksichtigen, um Verhaltensänderungen und -akzeptanz zu fördern. Stakeholder sollten nachhaltige und vertrauenswürdige Geschäftsmodelle für die Bereitstellung von Known Traveler Digital Identity-Funktionen und -Infrastruktur formulieren.

C. Einen unterstützenden politischen Rahmen aufrechterhalten: Es

besteht die Notwendigkeit, die Einhaltung globaler Standards und empfohlener Praktiken zu kartieren, zu sozialisieren und zu fördern.

Die Interessengruppen müssen dazu beitragen, die Leitprinzipien für den Einsatz neuer technologischer Entscheidungen und den Einsatz fortschrittlicher Datenanalysen zur Risikobewertung festzulegen.

Cybersicherheit und Privatsphäre müssen jederzeit mit höchster Integrität gewahrt bleiben.



1. Zunehmender Druck auf die Sicherheit im Reiseverkehr

„Innovation ist der Schlüssel zur Verbesserung der globalen Wettbewerbsfähigkeit, Mobilität und Produktivität. Technologische Fortschritte bieten Möglichkeiten, die Sicherheit im Flugverkehr effizienter zu gestalten und gleichzeitig das Reiseerlebnis zu verbessern.“

Marc Garneau, kanadischer Verkehrsminister

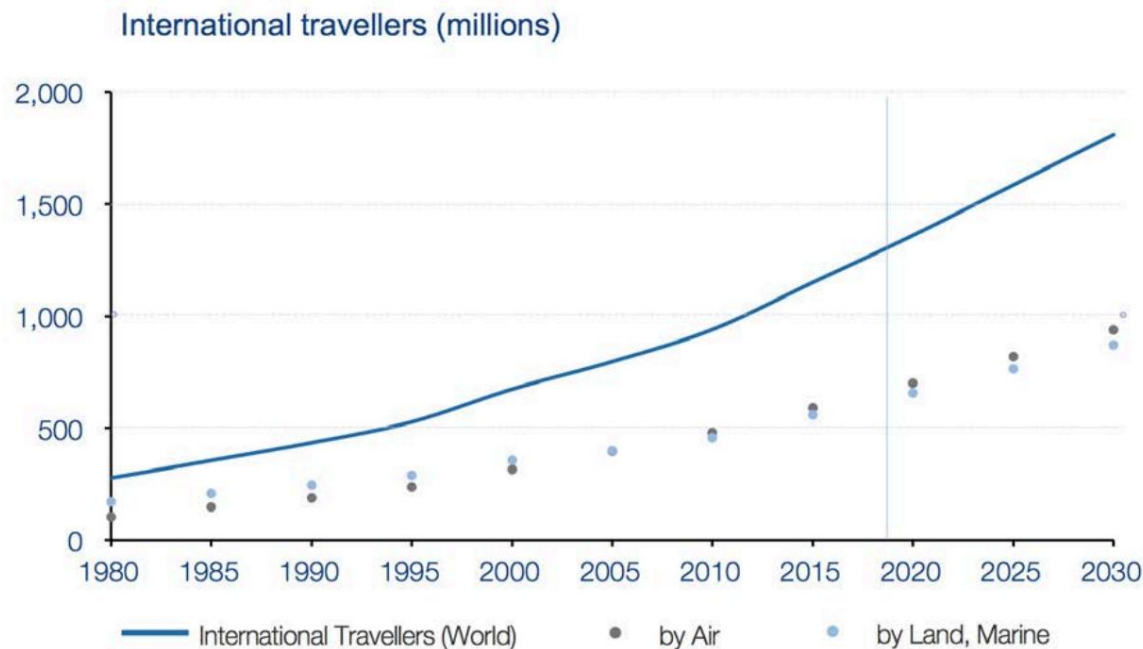
Der Luftfahrt-, Reise- und Tourismussektor steht aufgrund der wachsenden Zahl von Reisenden, steigender Risiko- und Sicherheitsanforderungen sowie begrenzter Infrastrukturskapazitäten unter Druck. Dieser Druck behindert eine sichere und reibungslose grenzüberschreitende Reise und verursacht verschiedene Probleme für Regierungen, Unternehmen und Reisende. Experten gehen davon aus, dass die Kombination dieser Belastungen auf das internationale Reiseerlebnis einen Wendepunkt erreichen und das zukünftige Wachstum der Branche gefährden wird. Insbesondere im Flugverkehr gehen Kommentatoren davon aus, dass die monetären und wirtschaftlichen Kosten des derzeitigen Luftsicherheitssystems in den nächsten 15 bis 20 Jahren ein untragbares Niveau erreichen werden², da die Zahl der Flugreisenden und der Umfang der Luftfracht weiter zunehmen. Allerdings werden digitale Innovationen in der Reisesicherheit erhebliche Veränderungen und Mehrwerte mit sich bringen, und die Branche muss handeln Jetzt.

„Öffentlich-private Partnerschaften haben einen anerkannten Wert bei den kontinuierlichen Bemühungen, die Effizienz der Grenzabfertigung zu verbessern. Diese gemeinsamen Bemühungen sorgen dafür, dass die Regierung von der Forschung und Innovation des Privatsektors profitiert, um sowohl den Kreis vertrauenswürdiger Reisender als auch das Reiseerlebnis insgesamt weiter zu vergrößern.“

Matt Hayden, Stellvertretender stellvertretender Sekretär (kommissarisch), Privatsektorbüro, USA Heimatschutzministerium

Über die unmittelbaren Effizienzgewinne der Digitalisierung des Reiseverkehrs hinaus können neue Technologien genutzt werden, um Änderungen in der Politikgestaltung und den Mechanismen zu ermöglichen, die Regierungsbehörden nutzen, um die sichere Bewegung von Menschen über Grenzen hinweg zu gewährleisten. Das in diesem Bericht vorgestellte Konzept schlägt vor, die verfügbaren Technologien der Vierten Industriellen Revolution zu nutzen, um die Fähigkeit zu demonstrieren, das Grenzübertretterlebnis neu zu gestalten. Diese Neugestaltung verbessert die vor Reiseantritt und risikobasierte Passagierkontrolle, indem Industriepartner und Reisende in den Prozess einbezogen werden, was eine sicherere und reibungslosere Reise ermöglicht.



Abbildung 1: Wachstum der internationalen Ankünfte⁶

Reisen und die Weltwirtschaft

Der Luftfahrt-, Reise- und Tourismussektor sorgt für globale wirtschaftliche Entwicklung und die Schaffung von Arbeitsplätzen und trägt maßgeblich zum Wohlstand auf der ganzen Welt bei. Im Jahr 2016 trug es direkt 2,3 Billionen US-Dollar zum BIP bei und sicherte weltweit 109 Millionen Arbeitsplätze. Wenn man den Anwendungsbereich um die umfassenderen Auswirkungen auf Industrie und Gesellschaft im Allgemeinen erweitert, trug der Sektor im Jahr 2016 7,6 Billionen US-Dollar zum BIP bei und unterstützte 292 Millionen Arbeitsplätze in der Weltwirtschaft. Dies entspricht 10,2 % des weltweiten BIP und etwa 1 von 10 aller Arbeitsplätze.⁷

Zunehmendes Wachstum im internationalen Reiseverkehr

Der unaufhaltsame Anstieg der weltweiten Mobilität von Menschen zeigt keine Anzeichen eines Abklingens.³ Das World Tourism Barometer⁴ verzeichnet, dass die Zahl der Ankünfte internationaler Reisender im Jahr 2016 insgesamt 1,2 Milliarden betrug und bis 2030 voraussichtlich 1,8 Milliarden erreichen wird, was zu einer erwarteten durchschnittlichen Wachstumsrate (CAGR) führt) von etwa 3 % (Abbildung 1). Der Luftfahrt-, Reise- und Tourismussektor, der im Jahr 2016 46 Millionen mehr internationale Reisende verzeichnete als im Jahr 2015, verzeichnete in den letzten sieben Jahren eine Phase anhaltenden, ununterbrochenen Wachstums, was die Widerstandsfähigkeit der Branche unterstreicht.⁵

Steigende Risiko- und Sicherheitsanforderungen

Die Herausforderung für Grenzschutzbehörden bestand schon immer darin, den internationalen Handel und das Reisen für die Mehrheit der Menschen, die aus legitimen Gründen Grenzen überqueren, zu erleichtern und gleichzeitig illegale Bewegungen zu verhindern.⁸ In etwas mehr als einem Jahrhundert hat sich das internationale Reisen von einer Reise, die keine Reise erforderte, gewandelt Reisepass und erforderte eine minimale Sicherheitsüberprüfung zu einem Prozess mit immer mehr Sicherheitsmaßnahmen.⁹ Sicherheit rückt zunehmend in den Fokus internationaler Reisender und Grenzbehörden aufgrund wachsender Unruhen und Unsicherheiten aufgrund geopolitischer Spannungen, komplexer internationaler Sicherheitsrichtlinien und der Bedrohung des Terrorismus und der Zunahme globaler Pandemien.



Infolgedessen steigen die Investitionen in Luftsicherheits- und Grenzmanagementdienste weiter. Beispielsweise haben sich die europäischen Flughafeninvestitionen in weniger als zehn Jahren mehr als verdoppelt und erreichten im Jahr 2011 7,6 Milliarden US-Dollar. Ebenso ist die staatliche Finanzierung der Transportation Security Administration (TSA) der Vereinigten Staaten seit ihrer Gründung erheblich gestiegen und stieg von 2,2 Milliarden US-Dollar im Jahr 2002 auf 2,2 Milliarden US-Dollar im Jahr 2002. Im Jahr 2013 beliefen sich die Ausgaben auf fast 8 Milliarden US-Dollar.¹⁰ In der Zwischenzeit wurde den Ländern geraten, „den Gürtel enger zu schnallen“ und „die Dinge anders zu machen“ – und sogar die Kosten zu senken. Personalkosten stellen für Sicherheits- und Grenzschutzbehörden einen großen Gemeinkostenaufwand dar, und hier wird eine bessere Verteilung der Ressourcen angestrebt.¹¹ Sofern keine wesentlichen Änderungen vorgenommen werden, werden die Kosten für den Betrieb und die Wartung des aktuellen Luftsicherheitssystems wahrscheinlich völlig untragbar werden in den nächsten zwei Jahrzehnten, da die Zahl der Reisenden und der Umfang der Luftfracht weiter zunehmen.¹²

alle auf die Reise von Reisenden aus und verursachen Probleme für Regierungen, Unternehmen und Reisende. Abbildung 2 zeigt die 16 Hauptschritte auf der

Begrenztes Wachstumspotenzial der körperlichen Leistungsfähigkeit

Aufgrund der kontinuierlichen Zunahme des internationalen Reiseverkehrs stoßen die Flughäfen an ihre Kapazitätsgrenzen. Während einige Länder über Spielraum verfügen, um die Zahl der in Betrieb befindlichen Flughäfen zu erhöhen – Indien plant, seine Zahl von 95 im Jahr 2016 auf 250 bis 2020/2013 zu erhöhen

– Die meisten Flughäfen in Asien sind voll ausgelastet oder überlastet.

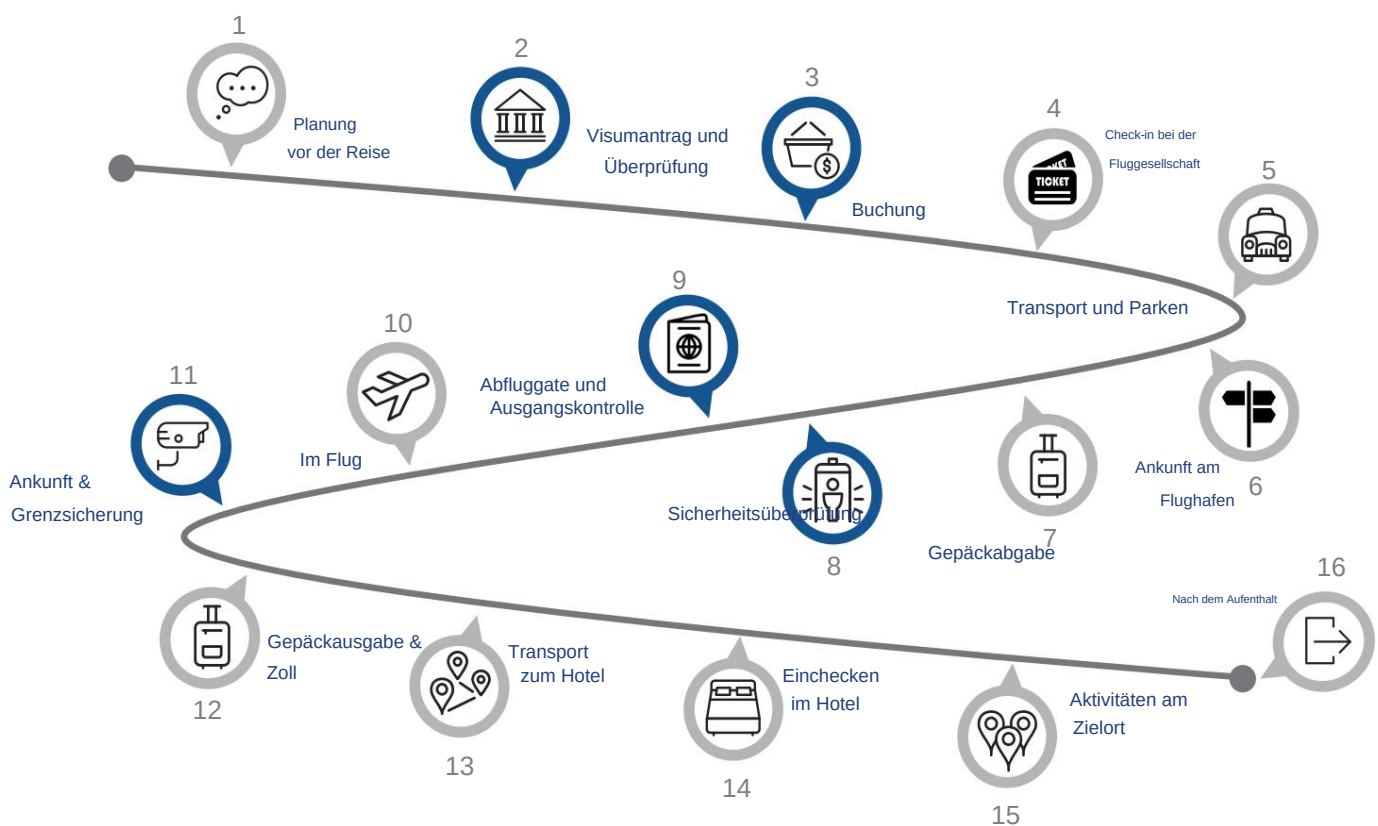
Jedes Jahr kommen schätzungsweise 100 Millionen Passagiere im asiatisch-pazifischen Raum an.¹⁴ An einigen europäischen Flughäfen werden neue Terminals gebaut, um die technische Kapazität und den maximalen Durchsatz zu erhöhen. Allerdings dauert es oft lange, bis diese neuen Terminals in Betrieb gehen, was zu Engpässen und langen Warteschlangen bei der Kontrolle oder Passkontrolle an bestehenden Terminals führen kann.

Regierungen und Flughäfen müssen auch mit Widerstand der Anwohner gegen eine weitere Expansion in bebauten Gebieten rechnen. Da nur begrenzter physischer Raum für Erweiterungen zur Verfügung steht, müssen Flughäfen nach alternativen Möglichkeiten suchen, um mit dem erwarteten Wachstum des internationalen Reiseverkehrs zurechtzukommen.

Schmerzpunkte auf der Reise eines Reisenden

Der rasante Anstieg des internationalen Reiseverkehrs, die steigenden Sicherheitsanforderungen und das begrenzte Wachstumspotenzial wirken sich auf die Reise eines Reisenden aus. Abbildung 2 zeigt die 16 Hauptschritte auf der Reise eines Reisenden¹⁵ – von der Planung vor der Reise bis zu den Aktivitäten nach dem Aufenthalt – wobei fünf als die am meisten belastenden Schritte identifiziert wurden (Tabelle 1). Die genaue Reihenfolge dieser Schritte und das Ausmaß der Unannehmlichkeiten für Regierungen, Unternehmen und Reisende variieren je nach Flughafen und den Prozessen in jedem Land.

Abbildung 2: Reise des Reisenden



Blau markierte Punkte werden als höchste Schmerzpunkte identifiziert, wie in Tabelle 1 erläutert

Tabelle 1: Schmerzpunkte auf der Reise eines Reisenden

Reise des Reisenden	Schmerzstellen
Visumsantrag* und Prüfung	– Unsicherheit über die Anforderungen des Visumverfahrens – Unsicherheit über die Interaktion der Grenzschutzbeamten bei der Einwanderung – Zu viele Dokumente für die Weitergabe an Botschaften – Mangelnde Integration zwischen physischer und digitaler Identität
Buchung	– Bereits bereitgestellte Informationen werden nicht wiederverwendet – Inkonsistente Verwaltung von Identitätsinformationen – Dateneingabefehler können unentdeckt bleiben
Sicherheitsüberprüfung	– Unterschiede in den Kontrollverfahren verursachen bei Passagieren Angst – Kapazitätsengpässe an Sicherheitskontrollen – Mangelndes Wissen über Reisende führt zu einem ressourcenintensiven Ansatz bei der Passagierkontrolle und Stau
Abfluggate und Ausgangskontrolle	– Fragen zum Recht auf Vergessenwerden** – Compliance bei der Ausreise: Grenzbehörden wissen, wer ausgereist ist und wer sein Visum überschritten hat – Einige Länder haben keine klare Ausstiegsstrategie
Ankunft und Grenzsicherung	– Der Prozess zur Feststellung der Zulässigkeit führt zu langen Warteschlangen bei der Einwanderungsbehörde – Die aktuelle Positionierung des Flughafenkontrollprozesses beeinträchtigt das Reiseerlebnis und das Ganze Optimierung des Sicherheitsprozesses – Mangel an Regierungspersonal und technischen Ressourcen, um die Nachfrage nach Dienstleistungen zu decken – Richtlinienbeschränkungen für den Betrieb

*

Dieser Fall bezieht sich auf das traditionelle Visumverfahren, das eine persönliche Prüfung und die Interaktion zwischen Konsular und Auswärtigem Amt umfasst. Heutzutage gibt es viele Beispiele für reibungslosere Verfahren zur Befreiung von der Visumpflicht mit eVisas (z. B. ETA und ESTA).

**

In der neuen EU-Datenschutz-Grundverordnung (DSGVO) seit 2018 ist es einer Person möglich, die Löschung oder Entfernung personenbezogener Daten zu beantragen, wenn kein zwingender Grund für deren weitere Verarbeitung besteht.

Digitale Möglichkeiten in der Reisesicherheit bieten erhebliches Wertpotenzial

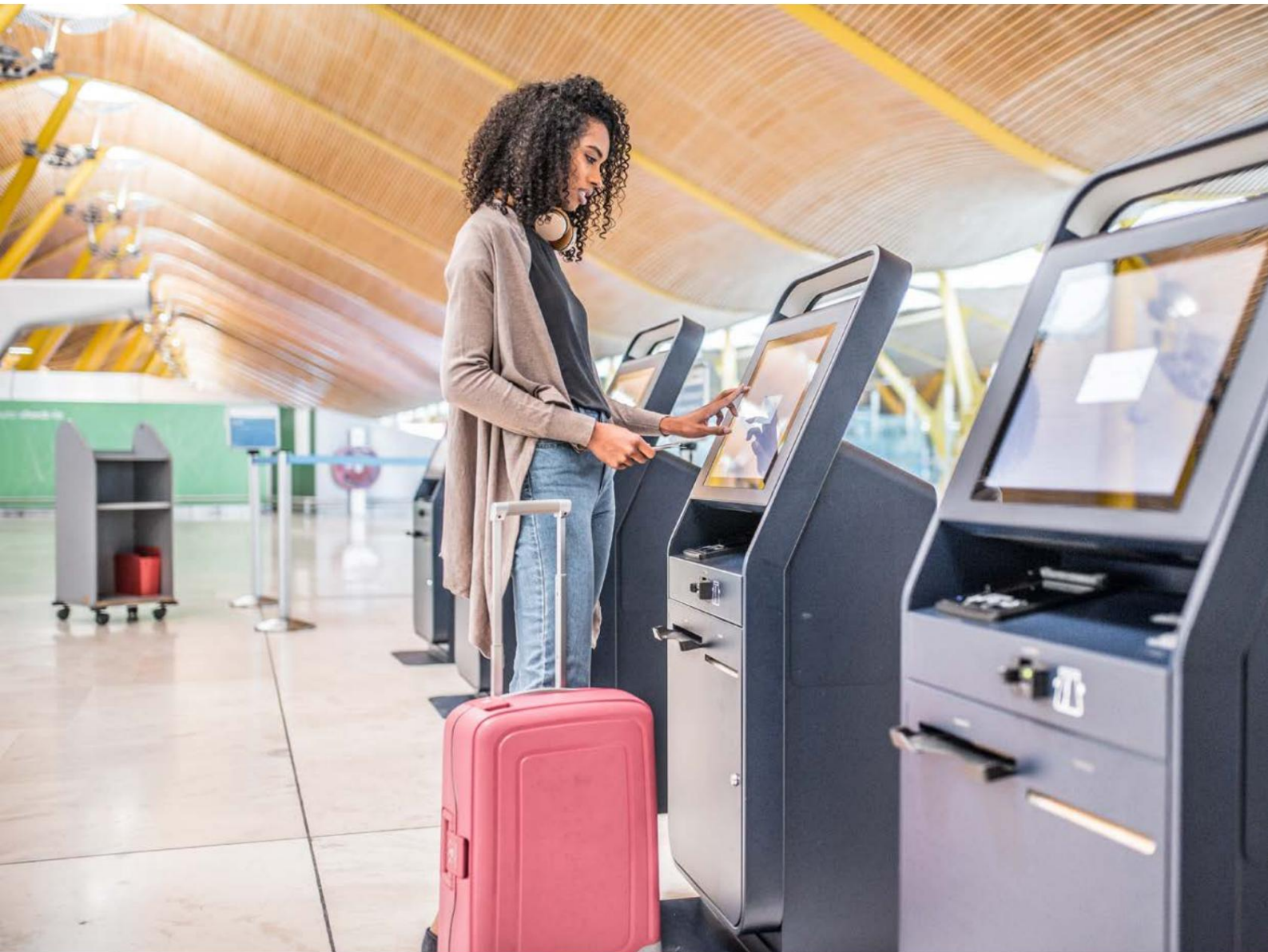
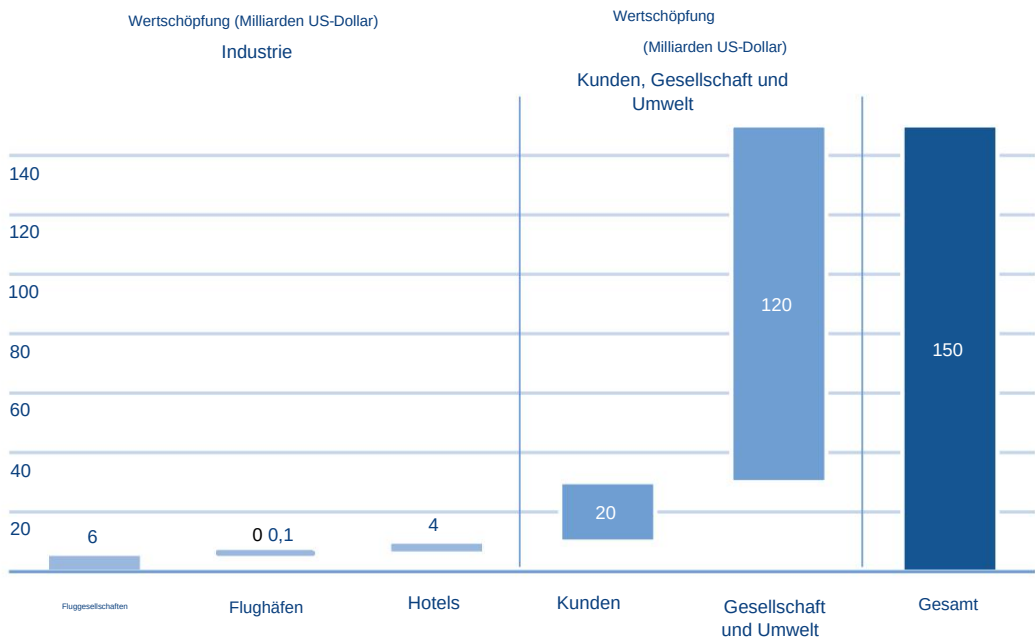
Während eine reibungslose Reise für Reisende zunehmend unter Druck gerät, bleibt Sicherheit ein zentrales Anliegen im gesamten Luftfahrt-, Reise- und Tourismus-Ökosystem.¹⁶ Die vierte industrielle Revolution verbindet die physische und die digitale Welt und revolutioniert gleichzeitig die Art und Weise, wie globale Führungskräfte über Sicherheit und globale Konnektivität denken.¹⁷ Dies hat zu einem Anstieg der Grenzautomatisierungstechnologie geführt und ermöglicht eine effizientere Abfertigung von Reisenden an Aus- und Einreisepunkten. Über die Automatisierung hinaus ermöglichen die Fähigkeiten fortschrittlicher Technologien wie Biometrie und prädiktive Analysen eine völlige Neugestaltung der Prozesse zur Überprüfung von Reisenden. Dadurch wird die Fähigkeit erhöht, Passagiere im Voraus zu überprüfen und Reisende mit geringem Risiko schneller als je zuvor zu überprüfen.

Wie in Abbildung 3 dargestellt, wird zwischen 2016 und 2025 der Wert, der durch den Einsatz digitaler Technologien der Vierten Industriellen Revolution zur Verbesserung der Sicherheit im Reiseverkehr entsteht, bei Fluggesellschaften, Flughäfen und Hotels auf 10 Milliarden US-Dollar geschätzt (7 Milliarden US-Dollar für Effizienzsteigerungen und 3 Milliarden US-Dollar aus Es wird geschätzt, dass der Wert für die Gesellschaft im gleichen Zeitraum 20 Milliarden US-Dollar an Zeit- und Kosteneinsparungen und eine grobe Schätzung von 120 Milliarden US-Dollar an Einsparungen durch die Vermeidung der wirtschaftlichen Kosten eines Großangriffs betragen würde .

„Der Übergang zu einer digitalisierten Gesellschaft stellt eine große Chance dar, Reisenden ein optimales und sicheres Erlebnis zu bieten, das im Einklang mit den anhaltenden Sicherheitsanforderungen und dem Infrastrukturdruk steht. Als Branche müssen wir es begreifen.“

Luis Maroto, Präsident und Chief Executive Officer, Amadeus IT Group

Abbildung 3: Wert, der durch Sicherheit und Schutz auf dem Spiel steht19



2. Methodik

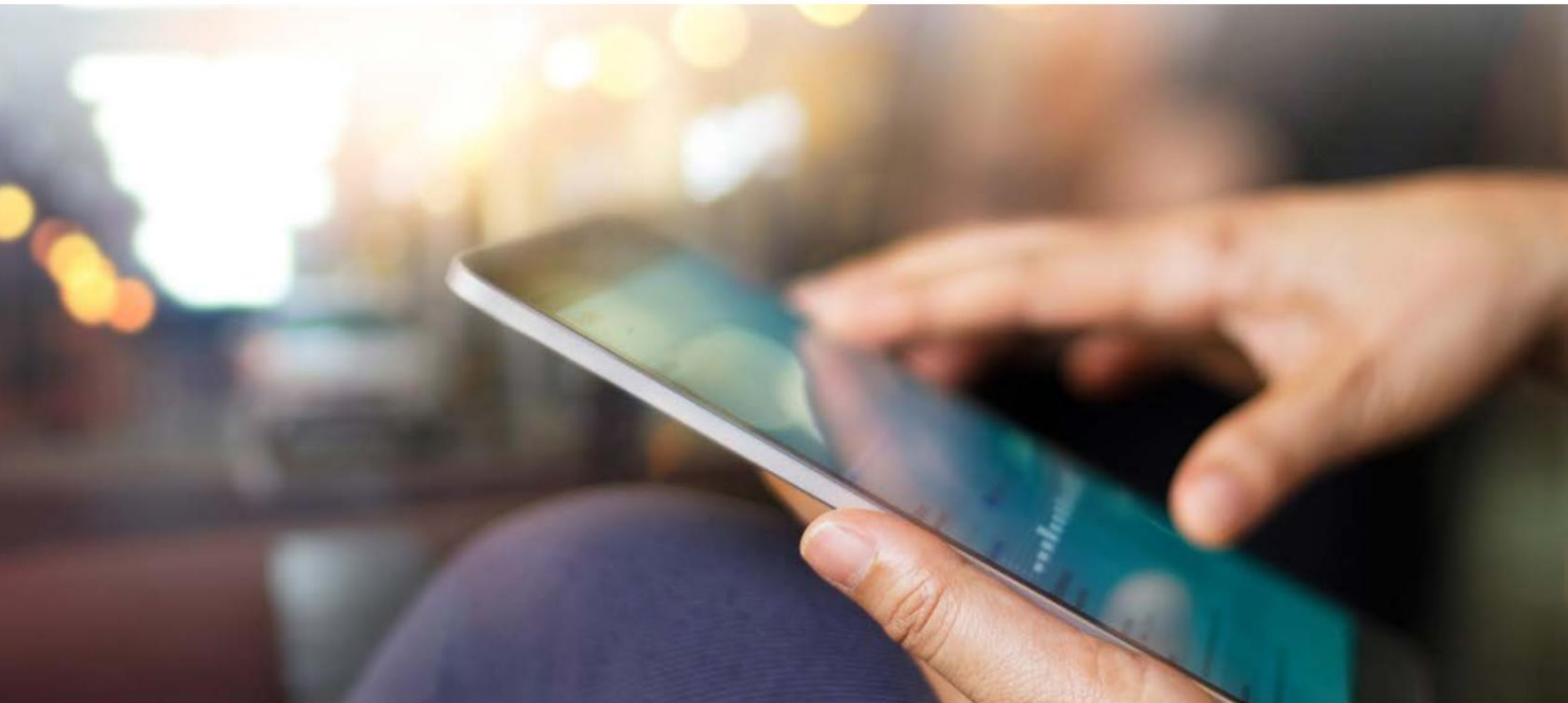
Um dem zunehmenden Druck zu begegnen und zu untersuchen, wie Technologie als Hebel zur Verbesserung sicherer und reibungsloser Reisen genutzt werden kann, folgte das Projekt einem zweistufigen Prozess. Die erste Phase konzentrierte sich auf die Formulierung eines technologischen Interventionskonzepts, das zu Verbesserungen bei Flughafen- und Grenzsicherheitsabläufen führen würde. Die zweite Phase war der Entwicklung eines nachweisbaren Prototyps gewidmet, um das Konzept zum Leben zu erwecken und zu beweisen, dass die Basistechnologien effektiv funktionieren können, um die gewünschten Prozess- und Kooperationsergebnisse zu liefern. Der Prototyp wurde durch schnelle Ideenfindung entwickelt – eine Entwurfsmethodik, die so gewählt wurde, dass eine Vielzahl von Beteiligten die komplexen politischen und institutionellen Hindernisse identifizieren und angehen können, die der Verwirklichung des durch das Konzept dargestellten Potenzials im Wege stehen.

Das Konzept definieren

Im Jahr 2016 wurde eine kohärente Multi-Stakeholder-Vision für die Zukunft der Sicherheit im Reiseverkehr definiert, die sich auf drei Elemente konzentrierte: Neugestaltung des Prozesses, um den Kunden in den Mittelpunkt zu stellen; die Macht digitaler Informationen und neuer Technologien freisetzen; und die Schaffung vertrauensvoller Vereinbarungen, die zur Unterstützung der Zusammenarbeit erforderlich sind. Basierend auf dieser Vision arbeiteten die Beteiligten zusammen, um eine Reihe grundlegender Gestaltungsprinzipien zur Gestaltung des Interventionskonzepts zu entwerfen (T

Tabelle 2: Gestaltungsprinzipien²¹

Vision	PROZESS Kundenzentriertes Erlebnis 	TECHNOLOGIE Digital Information 	ZUSAMMENARBEIT Vertrauensvolle Vereinbarungen 
Wichtige Designprinzipien	• Flexibel vom Design her • Einfach und leicht zu bedienen • Kommunikation in Echtzeit • Optimierte wirtschaftlichen Nutzen • Verbessert effektiv die Sicherheit von Reisenden und Nationen	• Biometrisch basiert • Technologieunabhängig • Modular und skalierbar • International interoperabel • Maschinelles Lernen und KI zur Verbesserung der Genauigkeit	• Transparent • Von der Regierung unterstützt • Mindestens zwei (globale) Stakeholder • Entspricht der internationalen Sicherheit Standards • Inklusivität durch Design (Kultur und Reisepersönlichkeit)



Mit diesen Gestaltungsprinzipien als Leitlinien wurden drei unterschiedliche Interventionskonzepte vorgeschlagen, die sich jeweils auf den Zugang, den Datenaustausch und die Etablierung einer bekannten digitalen Identität des Reisenden konzentrieren (Tabelle 3). Die „Known Traveller Digital Identity“ wurde als vielversprechendste und ehrgeizigste Intervention ausgewählt, da sie den Prinzipien am nächsten kommt und die beste Hoffnung auf eine radikale Umgestaltung des globalen Ansatzes zur Sicherheit im Reisebereich bietet.

Entwicklung des Prototyps

Um von der Absicht zur Wirkung zu gelangen, wird die Demonstration des Konzepts anhand eines Prototyps beweisen, dass die Basistechnologien effektiv funktionieren können, um die gewünschten Prozess- und Kooperationsergebnisse zu liefern. Um die Fähigkeiten zu demonstrieren, die das größte Potenzial haben, konzentriert sich der Prototyp des Known Traveller Digital Identity-Konzepts auf fünf Komponenten der Reise des Reisenden: Anmeldung, Planung vor der Reise, Abreise, Ankunft und Aufbau der Glaubwürdigkeit des Known Traveler-Profiles.

Tabelle 3: Vorgeschlagene Interventionskonzepte und ausgewählte Interventionen²²

	1. Nahtloser Zugriff und Überprüfung	2. Datenaustauschplattform	3. Bekannte digitale Identität des Reisenden (ausgewählte Intervention)
Beschreibung	Identitätsprüfung und Zugangsgewährung mit einem einzigen digitalen Token zum Identitätsnachweis, basierend auf Biometrie, für private Unternehmen im Reiseökosystem. Nach der Verifizierung kann sich der Reisende mit einem einzigen Token im gesamten Partner-Ökosystem identifizieren, ohne einen physischen Ausweis zu benötigen.	Integrierte Plattform zum Austausch von Reisedaten, die eine bessere Risikobewertung durch Regierungen durch den Austausch von Überprüfungsergebnissen (z. B. rotes oder grünes Licht) ermöglicht. Bestehende Mittel zum Identitätsnachweis (ein physischer Reisepass) bleiben unverändert, um das Vertrauen zu stärken.	Eine digitale Identität, die biometrische, biografische und reisehistorische Daten umfasst, ermöglicht es dem Reisenden, Entitäten auf der Reise des Reisenden den Zugriff auf ausgewählte Informationen über ihn zu autorisieren, um eine Risikobewertung, Überprüfung und Zugriff zu ermöglichen.
Vorteile	+ Wertvoll für Pilotversuche mit privaten Unternehmen + Erforderliche Änderungen am aktuellen Ökosystem sind begrenzt + Keine Verfolgung persönlicher Daten von Reisenden, wodurch potenzielle Datenschutzbeschränkungen eingeschränkt werden	+ Ermöglicht Regierungen dies Verbesserung der Risikobewertung und Personalisierung + Erfordert nicht, dass Regierungen einer „digitalen Identität“ vertrauen müssen + Fähigkeit, sich auf potenzielle Hochrisikoreisende zu konzentrieren	+ Ermöglicht es Reisenden, Partner im Sicherheitsprozess zu sein + Respektiert die Souveränität der Länder + Beinhaltet die Fähigkeit zur Durchführung von Verifizierungen und Risikobewertungen + Ermöglicht einen umfassenden, vorab strukturierten Informationsaustausch mit Unternehmen + Risiken, die durch verbesserte Möglichkeiten zur Datennutzung und -analyse anhand anderer Datenbanken identifiziert wurden
Nachteile	- Technologie wird nicht für Risiken eingesetzt Bewertung - Muss mit bestehenden Initiativen harmonisiert werden - Erfordert eine Vereinbarung zwischen zahlreichen privatwirtschaftlichen Unternehmen	- Muss Datenschutz-/Datenschutzprobleme überwinden - Erfordert Vertrauen in das System, zwischen den Regierungen - Risiken im Zusammenhang mit der Existenz zentralisierter Datenbanken	- Erfordert Vertrauen zwischen Entitäten - Datenschutzrisiken müssen angegangen werden - Die Unterstützung der Regierung ist von entscheidender Bedeutung für Erfolg
Bewertung nach Designprinzipien	Verfahren Technologie Zusammenarbeit	Verfahren Technologie Zusammenarbeit	Verfahren Technologie Zusammenarbeit

3. Das bekannte digitale Identitätskonzept für Reisende

Das Known Traveler Digital Identity-Konzept wird von zentraler Bedeutung sein, um eine sicherere und nahtlosere Reise für Reisende zu ermöglichen. Es bietet Strafverfolgungs-, Einwanderungs- und Flugsicherheitsbeamten die Möglichkeit, verifizierte Informationen von Reisenden viel früher auf ihrer Reise anzufordern und zu erhalten.

Der frühere Erhalt ermöglicht eine Neugestaltung des Prozesses, die die Behörden auf eine verstärkte erweiterte Passagierkontrolle und die Freigabe von Reisenden mit geringem Risiko verlagert. Im Gegenzug haben die Beamten mehr Zeit, sich auf die Überprüfung von Passagieren zu konzentrieren, die weniger bekannt sind oder mehr Bedenken äußern.

Das Konzept basiert auf der Idee, dass eine Person die Kontrolle darüber hat, bestimmte Identitätsinformationen (z. B. biometrische, biografische und Reisehistorie) an staatliche und private Akteure während der Reise weiterzugeben, wie z. B. Grenzkontrollbehörden, Autovermietungen, Hotels und Fluggesellschaften, für Risikoprofilierung, Verifizierung und Zugriff (Abbildung 4). Der Reisende kann auswählen, welche Informationen für einen bestimmten Zeitraum entsprechend den Anforderungen der Behörde oder privaten Einrichtung für den Zugriff auf die Dienste weitergegeben werden. Die Identität des Reisenden wird durch biometrische Verifizierung authentifiziert und durch Distributed-Ledger-Technologie und Kryptografie geschützt. Das Konzept ist nicht an ein bestimmtes Produkt gebunden, modular, skalierbar und basiert auf international anerkannten Standards, um Vertrauen in die Technologie zu gewährleisten.

„Umsetzbare Polizeiinformationen, einschließlich biometrischer Daten, zur richtigen Zeit in die richtigen Hände zu bringen, ist die Priorität von INTERPOL. Initiativen wie I-Checkit, die Brücken zwischen dem öffentlichen und dem privaten Sektor bauen, um eine stärkere globale Sicherheitsarchitektur zu entwickeln, haben bewiesen, dass wir das Rad nicht neu erfinden, sondern es nur zweckdienlich machen müssen.“

Jürgen Stock, Generalsekretär, Internationale Kriminalpolizeiliche Organisation, (INTERPOL)

Darüber hinaus verbindet sich die Technologie mit den eigenen Legacy-Systemen der Identitätsanbieter sowie mit nationalen Systemen, die mit dem Public Key Directory (ICAO PKD) der International Civil Aviation Organization verbunden sind, der vertrauenswürdigen globalen Quelle für die digitalen Signaturinformationen von Identitätsanbietern. Stellen Sie die Rückverfolgbarkeit zur vertrauenswürdigen Quelle sicher.

Die Vorteile von ePässen nutzen Die rasche

Einführung des elektronischen Reisepasses (ePass) durch Staaten bietet Möglichkeiten, die Sicherheit des Grenzmanagements zu erhöhen und gleichzeitig das Reisen für Dokumenteninhaber zu erleichtern. Der kontaktlose Chip des Reisepasses enthält biografische Daten des Passinhabers und ein digitales Sicherheitsmerkmal in Form einer digitalen Signatur, die diese Daten versiegelt und deren Integrität und Authentizität gewährleistet. Tatsächlich besteht einer der Hauptvorteile der Ausstellung von E-Pässen darin, dass Grenzbeamte die Integrität und Authentizität dieses Dokuments elektronisch überprüfen können, unabhängig davon, ob es geändert wurde und ob es von der richtigen Behörde ausgestellt wurde oder nicht.

Diese elektronische Validierung erfolgt durch die Prüfung der im kontaktlosen Chip enthaltenen digitalen Signatur, also der Verifizierung der digitalen Zertifikatskette, die der Staat zur Versiegelung der biografischen Daten verwendet. Um die elektronische Validierung eines ePasses durchzuführen, müssten die Grenzbehörden Informationen über die digitale Zertifikatskette anderer Staaten sammeln, die sich aus Sicherheitsgründen regelmäßig ändern. Da mittlerweile mehr als 100 Staaten ePässe ausstellen, wäre die Durchführung dieser Art von Austausch auf bilateraler Ebene komplex, ineffizient und äußerst fehleranfällig. Das ICAO PKD wurde gegründet, um als vertrauenswürdige globale Quelle diesen Austausch zu erleichtern und Staaten eine effiziente und vertrauenswürdige Möglichkeit zu bieten, ihre eigenen digitalen Zertifikatsketteninformationen hochzuladen und die Informationen anderer Länder herunterzuladen. ICAO-PKD-Mitglieder, die die PKD-Validierung an ihren Grenzen nutzen, demonstrieren sowohl ihr Engagement für die Grenzsicherheit als auch die Erleichterung der Durchreise von ePass-Inhabern mit geringem Risiko.

Das Known Traveler Digital Identity-Konzept soll den freiwilligen Austausch von Informationen ermöglichen, wodurch der Einzelne Vertrauen in seine digitale Identität aufbaut. Um einen vertrauenswürdigen „Bekannten Reisenden“-Status aufzubauen, müssen Reisende Bescheinigungen – authentifizierte Ansprüche, die von einer vertrauenswürdigen Stelle deklariert wurden – jedes Mal zu ihrer digitalen Identität als bekannter Reisender hinzufügen, wenn eine vertrauenswürdige Stelle – wie ein Postamt oder eine Regierungs- oder Bildungseinrichtung – überprüft einen Anspruch. In diesem Konzept sind diese Bescheinigungen das Rückgrat des Vertrauens und die Grundlage für die Reputation und letztendlich dafür, wie Sicherheitsentscheidungen getroffen werden können.²³ Beispiele für Bescheinigungen sind der Nachweis der Staatsbürgerschaft in Land X, ein Bildungsabschluss der Hochschule Y und ein Impfnachweis für Viruserkrankung Z. Zukünftig könnte Land A einem Reisenden die Einreise genehmigen, basierend auf einer vorherigen Risikobewertung und der daraus resultierenden Bescheinigung von Land B.

Wichtig ist, dass Reisende, wie derzeit vorgeschlagen, Bescheinigungen in einem Profil bekannter Reisender zusammenfassen und ihren Anspruch auf Compliance, Vertrauen und Legitimität als Reisender zunehmend stärken. Durch den Erwerb weiterer Zertifizierungen bauen die Menschen den Status „Bekannter Reisender“ weiter aus und tragen so zu einer sichereren und reibungsloseren Reise für alle Beteiligten bei (Abbildung 5).

Anwendungsfall für Ankunfts- und Grenzsicherheit

Wenn heute ein Reisender an einer Grenze ankommt, muss die Grenzschutzbehörde die Zulässigkeit – die Erlaubnis zur Einreise in ein Land – schnell und genau bestimmen. Eine Grenzschutzbehörde bestimmt dann die Zulassungsklasse – entweder Bürger, ständiger Wohnsitz, Drittstaatsangehöriger mit einem Visum oder einer Befreiung von der Visumpflicht – oder die Notwendigkeit einer weiteren Prüfung oder den Grund für eine Einreise- (oder Ausreiseverweigerung), z. B. Straftat Aktivitäten, die Überschreitung eines Visums, Zollverstöße oder Täuschung.

Abbildung 4: Visualisierung bekannter Interaktionen mit der digitalen Identität von Reisenden

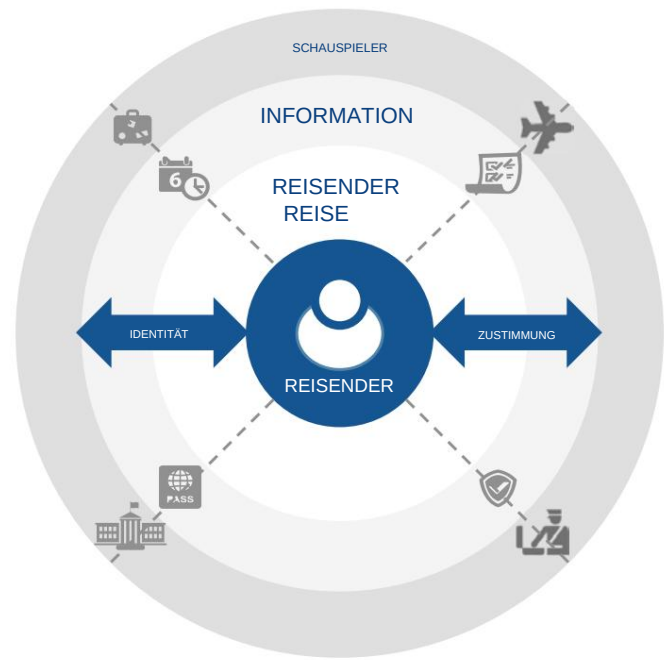


Abbildung 5: Erstellen eines Status als bekannter Reisender

Bauen a Bekannt Reisender Status	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
	Reisende können biometrische Daten sicher austauschen biografische Informationen nach der Registrierung in der TruID-Anwendung	Der Reisende baut seinen Status auf, indem er Bescheinigungen anfordert, z. B. Zertifikate von Uni, Kontoauszug oder Impfung etc.	Der Reisende teilt die für die Beantragung eines Visums erforderlichen Bescheinigungen mit (z. B. L1 für Arbeitszwecke). Basierend auf den übermittelten Informationen erhält der Reisende ein Visum Land X	Bei einer Folge Reise kann sich der Reisende bei der Ankunft aufgrund seines geringen Risikoprofils für eine beschleunigte Bearbeitung auf eine Spur für bekannte Reisende begeben	Der Reisende baut seinen Status jedes Mal weiter auf, wenn Identitätsinformationen hinzugefügt oder weitergegeben werden
Bescheinigungen	Passport Details Picture Match: ✓ Lauren A. Gonzales 5589 74123 23rd April, 2026 United States US Passport Service Female, 24th April 1976 Details Match: ✓	Facial Scan Fingerprint: ✓ Right 4 Fingers: ✓ Left 4 Fingers: ✓ Thumb: ✓ Education: M.Ed Updated 29th Aug 2012 Stamp from University X certifying education credential Bank statement Updated 26th Sep 2017 Stamp from Bank Y certifying bank account credit rating AA Yellow fever vaccine Updated 12th Jan 2010 Stamp from Hospital Z, certifying vaccination for virus XYZ	Visa: India Updated 29th Sep 2017 Stamp from India consulate travel from: Oct-Dec, 2017	TruID Lauren Gonzales Wednesday, October 30 2017 Disembarkation In Progress ZÜRICH AIRPORT Lane 2 TruID Active Updated 29th Sep 2017	TruID Lauren Gonzales Wednesday, October 30 2017 TruID Active Updated 29th Sep 2017 Use at locations marked with the symbols below. Watch Tutorial TruID TruID Contactless not available - Show QR Code



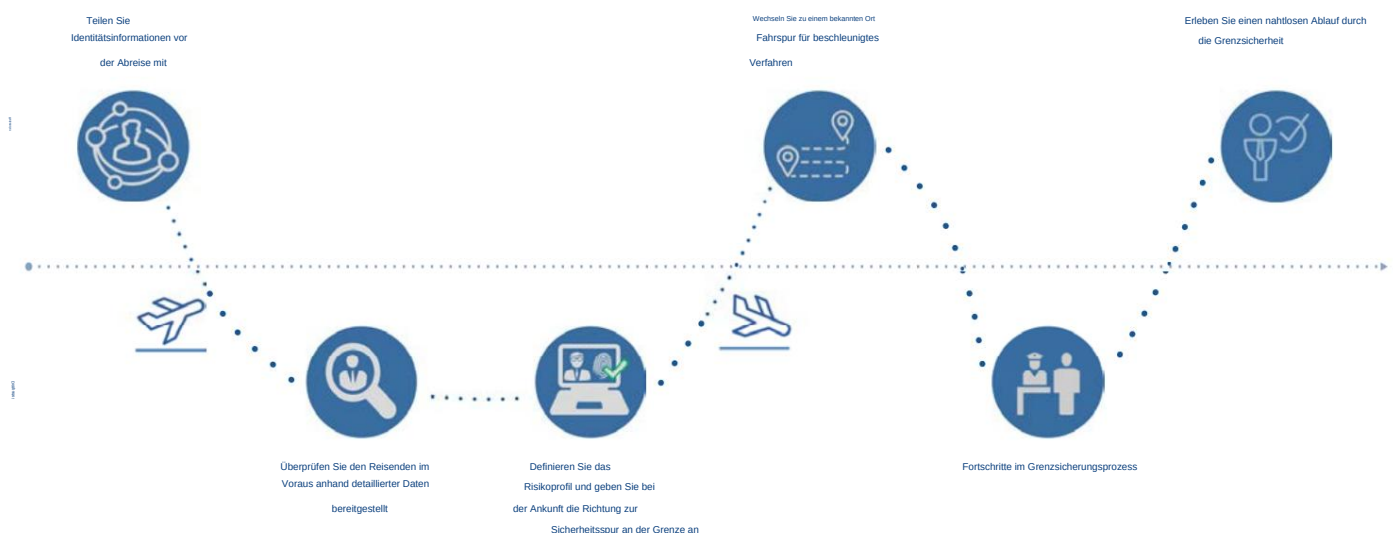
Das Known Traveler Digital Identity-Konzept ermöglicht eine individuelle Überprüfung und Risikobewertung lange vor der Ankunft. Eine verstärkte Vorabkontrolle ermöglicht risikobasierte Einwanderungsspuren, bei denen beispielsweise eine Spur für vorab überprüfte Reisende und eine zweite für diejenigen vorgesehen ist, die ihre Informationen nicht im Voraus angegeben haben. Unternehmen könnten vorab Antworten auf identitätsbezogene Fragen zu Reisenden vor deren Abreise oder Ankunft erhalten. Eine erweiterte Bewertung ermöglicht ein besseres Management sicherheitsrelevanter Risiken an Einreisehäfen (Abbildung 6), da Grenzschutzbehörden die Informationen vor Reiseantritt detaillierter bewerten können. Bei ernsthaften Zweifeln an den Reisegründen einer Person kann ein Grenzbeamter sachdienlichere Fragen stellen, um die Identität zu bestätigen oder neuere Aktivitäten besser zu verstehen. Umgekehrt könnte ein Reisender mit einem geringen Risikoprofil von einer reibungsloseren Reise ohne Abstriche bei der Sicherheit profitieren.

„Die Technologie hat die meisten Aspekte unseres täglichen Lebens drastisch verändert, doch internationale Reisen und die Rahmenbedingungen, die sie ermöglichen, sehen weitgehend genauso aus wie vor 50 Jahren. Die Zusammenarbeit mit Industriepartnern und Kunden ist erforderlich, um einen neuen

Rahmen für die Vorabprüfung legitimer Reisender mit geringem Risiko zu schaffen. Im Gegenzug können Regierungsbehörden mehr Ressourcen für echte Bedrohungen bereitstellen und so das sichere und reibungslose Reisen verbessern, wodurch mehr Menschen die Welt s

Arne M. Sorenson, Präsident und Chief Executive Officer, Marriott International

Abbildung 6: Beispielanwendungsfall bei Ankunft und Grenzsicherung



Datenparameter, die gängige Grenzsicherheitsüberprüfungsprozesse unterstützen

Das Known Traveler Digital Identity-Konzept bietet Strafverfolgungsbehörden die Möglichkeit, vor Reiseantritt ein strukturiertes Datenpaket von einem Reisenden anzufordern. Die folgende Tabelle zeigt die Datenabschnitte, die, wenn sie in das Profil eines bekannten Reisenden eines Passagiers integriert werden, dazu beitragen könnten, die Grenzsicherheitskontrolle zu erleichtern. Wie in den Richtlinien zu erweiterten Passagierinformationen²⁴ stellen die Abschnitte A–C die maximalen Datenfelder dar, die Länder von Fluggesellschaften über Systeme zur erweiterten Passagierinformation anfordern sollten. Abschnitt D stellt zusätzliche Informationen dar, die ein Passagier in sein Profil als bekannter Reisender integrieren könnte, um die Glaubwürdigkeit seines Profils zu verbessern und den Behörden mehr Informationen zu liefern als die maximalen Daten, die derzeit über erweiterte Passagierinformationssysteme erfasst werden.

Abschnitt a	Abschnitt b	Abschnitt C	Abschnitt D
In der Maschine gefundene Kerndatenelemente Lesbare Zone der offiziellen Reise Dokument (OTD)	Zusätzliche Datenelemente, die normalerweise in Flugliniensystemen vorkommen	Zusätzliche Daten, die normalerweise nicht in Flugliniensystemen zu finden sind und die von einer Fluglinie oder im Namen einer Fluglinie erfasst werden können	Zusätzliche Informationen, die der Passagier über das Known Traveler Digital bereitstellen könnte Identität (wie von Strafverfolgungsbehörden empfohlen)
– OTD-Nummer – Ausstellender Staat oder Organisation des OTD – OTD-Typ – Ablaufdatum von OTD - Nachname Vorname) - Staatsangehörigkeit - Geburtsdatum - Geschlecht	– Sitzplatzinformationen – Gepäckinformationen – Status des Reisenden – Ort/Hafen der ursprünglichen Einschiffung – Ort/Hafen der Abfertigung – Ort/Hafen des weiteren Auslandsziels – Positionsnummer des Passagiernamens (oder eindeutige Kennung)	- Visumnummer – Ausstellungsdatum des Visums – Ort der Ausstellung des Visums – Andere für die Reise verwendete Dokumentennummer – Art des anderen verwendeten Dokuments zum Reisen - Hauptwohnsitz - Zieladresse - Geburtsort	- Kontakt Nummer - Kontakt E-mail – Länder, die auf dieser Reise vor der Ankunft besucht wurden - Flugnummer - Reiseverlauf - Zweck der Reise - Reisedauer – Erweiterter Reiseverlauf – Menschen, mit denen man reist – Bargeld wird ins Land gebracht – Jüngste Interaktionen mit der Landwirtschaft oder Viehhaltung – Gesundheitsinformationen (z. B. Impfungen) – Kriminalgeschichte (positive Aussagen) – Führerscheinnummer



Den Wert sicheren und reibungslosen Reisens messen

Stakeholder gehen davon aus, dass das Known Traveler Digital Identity-Konzept durch die digitale Verbesserung der Reisesicherheit einen geschätzten potenziellen Wert von 150 Milliarden US-Dollar freisetzen wird.²⁵ Die Quantifizierung des Werts des Konzepts rechtfertigt die erforderlichen Investitionen und schafft zusätzliche Unterstützung für die Ausweitung seiner Akzeptanz und Nutzung.

Die Analysten können den Wertebaum als Grundlage für die Operationalisierung der Treiber nutzen und die Wertrealisierung quantitativ und qualitativ messen. Der Wertebaum besteht aus zwei Hauptwerttreibern auf Ebene eins: ein nahtloses Erlebnis und sicheres Reisen. Der Werttreiber für nahtlose Erlebnisse ist in Geschwindigkeit, Komfort, Personalisierung und Komplexität unterteilt. Der Werttreiber für sicheres Reisen gliedert sich in Identitätsfeststellung und Autorisierung (Abbildung 7). Die dritte Ebene des Wertebaus bietet eine Aufschlüsselung der Treiber der Ebene zwei, und die vierte Ebene enthält eine Liste nicht erschöpfender Beispieldreiber. Der nahtlose Werttreiber wird hauptsächlich aus der Perspektive von Reisenden und Privatpersonen definiert.

Der sichere Werttreiber ist besonders relevant für die Gesellschaft im Allgemeinen, einschließlich Regierungen und Grenzbehörden.

Das Known Traveler Digital Identity-Konzept befasst sich mit mehreren Schwachstellen auf der Reise des Reisenden und schafft Mehrwert

über verschiedene Werttreiber hinweg, wie im Wertbaum in Abbildung 7 dargestellt.

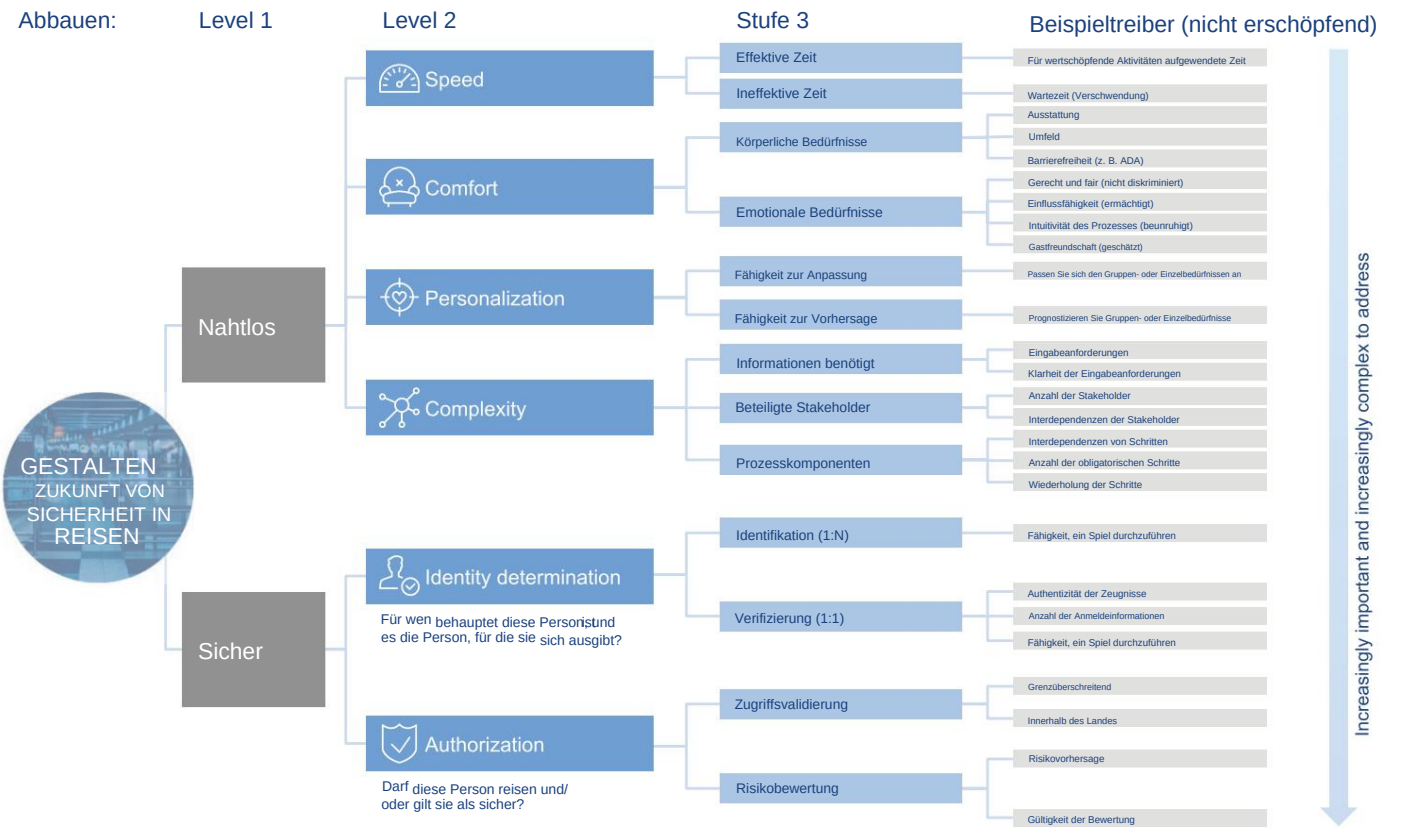
Tabelle 4 zeigt, wie das Konzept die einzelnen Schwachstellen angeht und welche Werttreiber folglich für jeden Schritt der Reise relevant sind. Grau hervorgehobene Schwachstellen sind diejenigen, die durch die Schaffung eines nahtloseren Erlebnisses gemildert werden könnten, die aber zum jetzigen Zeitpunkt keinen großen Nutzen für die gleichzeitige Verbesserung von Sicherheit und Nahtlosigkeit versprechen.

Tabelle 5 zeigt, wie die Werttreiber der Ebene drei quantitativ bzw. qualitativ operationalisiert und gemessen werden können.

Regierungen könnten von Effizienzkosteneinsparungen profitieren, wenn sie von bestehenden auf neue Systeme umsteigen. Dieser Wert kann mithilfe der Tabellen 4 und 5 gemessen werden, um bestimmte wichtige Leistungsindikatoren zu identifizieren und anhand dieser zu messen (z. B. bessere Nutzung der effektiven Zeit, weniger beteiligte Interessengruppen und eine Verringerung der Prozesskomponenten). Beispielsweise kann der Wert des Einsatzes von Gesichtserkennung zur Gewährleistung einer sicheren Reise in Schritt 11 der Reise des Reisenden (Tabelle 4) anhand entsprechender Metriken in den Treibern 11, 12 und 13 (Tabelle 5) gemessen werden.

Ebenso kann der Wert der Gewährleistung einer reibungslosen Reise gemessen werden. In diesem Prozessschritt könnten Kosteneinsparungen erzielt werden, die durch die Messung der Treiber 1, 7 und 9 nachgewiesen werden können.

Abbildung 7: Wert von sicherem und nahtlosem Reisen (13)



Wertschöpfung der Visapolitik

Untersuchungen belegen den Wert eines reibungsloseren Reiseerlebnisses. Die WTO hat beziffert, dass die Verbesserung der Visaerleichterung in der Vergangenheit nach der Umsetzung von Richtlinienänderungen zu einem Anstieg internationaler Reisender in G20-Länder um 5–25 % geführt hat.²⁶

Tabelle 4: Wertversprechen einer bekannten digitalen Identität für Reisende

		Konzept ermöglicht	Wert für sicheres Reisen	Wert für nahtloses Reisen
Vor der Reise				
1	Planung vor der Reise			
2	Visumantrag und -prüfung	– Online-Visum/Reise Genehmigungsantrag	– Verifizierung – Zugriffsvalidierung – Risikobewertung (Echtzeit, wiederholt <24 Stunden vor Abflug)	- Effektive Zeit – Emotionale Bedürfnisse - Fähigkeit zur Anpassung - Informationen benötigt – Einbindung der Stakeholder – Prozesskomponenten
3	Buchung	– Identität automatisch ausfüllen Information	– Verifizierung – Risikobewertung (PNR, allgemeiner Risikoscore)	- Effektive Zeit - Informationen benötigt
4	Einchecken bei der Fluggesellschaft	– Selbst-Check-in	– Verifizierung – Risikobewertung (basierend auf Advance Passagierinformationen)	- Effektive Zeit - Informationen benötigt
Auf Reise				
5	Transport und Parken			
6	Ankunft am Flughafen			
7	Gepäckabgabe	– Selbstabgabe	– Verifizierung	- Effektive Zeit – Emotionale Bedürfnisse
8	Sicherheitsüberprüfung	– Individuelle Sicherheit Bewertung	– Verifizierung – Risikobewertung (endgültig vor der Abreise, einschließlich Verhaltenserkennung und Sicherheitsdurchsetzung)	- Effektive Zeit – Emotionale Bedürfnisse - Fähigkeit zur Anpassung – Fähigkeit zur Vorhersage
9	Abfluggate und Ausgangskontrolle	– Individuelle Sicherheit Bewertung – Selbstausstieg – Selbsteinstieg	– Verifizierung – Risikobewertung (endgültig vor der Abreise, einschließlich Verhaltenserkennung und Sicherheitsdurchsetzung) – Zugriffsvalidierung	- Effektive Zeit – Emotionale Bedürfnisse - Fähigkeit zur Anpassung – Fähigkeit zur Vorhersage
10	Im Flug			
11	Ankunft und Grenzsicherung	– Individuelles Risiko Bewertung	– Verifizierung – Zugriffsvalidierung - Risikobewertung	- Effektive Zeit – Emotionale Bedürfnisse - Fähigkeit zur Anpassung – Fähigkeit zur Vorhersage - Informationen benötigt – Einbindung der Stakeholder – Prozesskomponenten
12	Gepäckausgabe und Zoll	– Sichere Rückforderung	– Verifizierung	– Emotionale Bedürfnisse
13	Transport zum Hotel			
14	Check-in im Hotel	– Selbst-Check-in	– Verifizierung – Risikobewertung (zum Beispiel, wo Industriepartner an Programmen wie I-Checkit teilnehmen können – siehe Hinweissfeld)	- Effektive Zeit
15	Aktivitäten am Zielort			
Nach der Reise				
16	Nach dem Aufenthalt	– Individuelle Risikobewertung – Risikobewertung (Risiko einer Überschreitung der zulässigen Aufenthaltsdauer und ob die Person das Land verlassen und sich bei ihrem Besuch angemessen verhalten hat)		– Emotionale Bedürfnisse – Fähigkeit zur Vorhersage

INTERPOL I-Checkit

I-Checkit ist eine Kontrolllösung, die nationale Grenzsicherungssysteme ergänzt und verbessert und ein wertvolles Beispiel für das Kooperationspotenzial zwischen öffentlichem und privatem Sektor ist. Es ermöglicht vertrauenswürdigen Partnern im privaten Sektor, mit der Strafverfolgungsgemeinschaft zusammenzuarbeiten, um erweiterte Passagierkontrollen in Echtzeit anhand der INTERPOL-Datenbank gestohlener und verlorener Reisedokumente durchzuführen. Angesichts der Leichtigkeit, mit der Terroristen, organisierte Kriminalitätsgruppen und reisende Sexualstraftäter Zugang zu regulierten Reiserouten haben, besteht ein dringender Bedarf für einen weiteren Ausbau von I-Checkit.

Tabelle 5: Empfohlene Leistungskennzahlen (nicht erschöpfend)

#	Treiber	Beschreibung	Messbeispielmetrik	
1	Effektive Zeit	Zeitaufwand für wertschöpfende Aktivitäten (Kunden- oder Geschäftswertschöpfung)	Quantitativ	– Bearbeitungszeit für X Reisende pro Schritt
2	Ineffektive Zeit	Wartezeit (ohne Mehrwert), z. B. aufgrund von Ressourceneffizienz	Quantitativ	– Bearbeitungszeit für X Reisende pro Schritt
3	Körperliche Bedürfnisse	Fähigkeit, körperliche Bedürfnisse hinsichtlich Ausstattung, Umgebung und Zugänglichkeit zu erfüllen	Qualitativ	– Grad der Zufriedenheit (1–5)
4	Emotionale Bedürfnisse	Fähigkeit, auf emotionale Bedürfnisse hinsichtlich eines gerechten und fairen Prozesses einzugehen, Fähigkeit zur Einflussnahme, Intuitivität des Prozesses und Gastfreundschaft	Qualitativ	– Grad der Zufriedenheit (1–5)
5	Fähigkeit zur Anpassung	Fähigkeit, sich an Gruppen- oder Einzelbedürfnisse anzupassen	Qualitativ	– Anzahl der Beschwerden – Schwere der Beschwerden
6	Fähigkeit zur Vorhersage	Fähigkeit, Gruppen- oder Einzelbedürfnisse vorherzusagen	Qualitativ	– Anzahl der Beschwerden – Schwere der Beschwerden
7	Informationen benötigt	Die erforderlichen Informationen werden durch die Anzahl der Eingabebeanforderungen, die Schwierigkeit bei der Einhaltung der Anforderungen und die Klarheit der Eingabebeanforderungen bestimmt	Quantitativ	– Anzahl der Eingabebeanforderungen - Schwierigkeitslevel – Grad der Zufriedenheit
8	Beteiligte Stakeholder Umfasst	Die Anzahl der beteiligten Stakeholder und die gegenseitigen Abhängigkeiten zwischen diesen Stakeholdern	Quantitativ	– Anzahl der Stakeholder – Anzahl der gegenseitigen Abhängigkeiten – Anzahl der Beamten pro Reisendem pro Transaktion oder pro Zeiteinheit
9	Prozesskomponenten Komponenten	Komponenten in einem Prozess, die durch die gegenseitigen Abhängigkeiten der Schritte, die Anzahl der obligatorischen Schritte und die Wiederholung der Schritte bestimmt werden	Quantitativ	– Anzahl der Links – Anzahl der sich wiederholenden Schritte
10	Identifikation	Fähigkeit, ein Individuum zu treffen; Die Person selbst ist ein Symbol für Eins-zu-Viele (1:N) bei der Massenidentifikation	Quantitativ	– % der korrekten Übereinstimmung (TPIR, TNIR) – Zeitaufwand für die Durchführung des Spiels – Kosten pro Spiel
11	Überprüfung	Der bereitgestellte Ausweis dient der Verifizierung dieser Person. unter Berücksichtigung der Authentizität des Berechtigungsnachweises, der Anzahl der Berechtigungsnachweise und der Fähigkeit, eine 1:1-Übereinstimmung durchzuführen	Quantitativ	– % der korrekten Übereinstimmung (TMR, TNMR) – Zeitaufwand für die Durchführung des Spiels – Kosten pro Spiel
12	Zugriffsvalidierung	Die Zulässigkeit wird von einer zuständigen Behörde auf der Grundlage von Informationen bestimmt, die eine Form der Risikobewertung umfassen (z. B. ist der Reisende berechtigt, ein Land oder eine bestimmte Dienstleistung zu betreten/einen Veranstaltungsort zu betreten).	Quantitativ	– % der korrekten Übereinstimmung – Zeitaufwand für die Durchführung der Validierung – Kosten pro Validierung
13	Risikobewertung	Enthält eine Vorhersage des Risikos und der Gültigkeit der Bewertung. Die Risikobewertung basiert auf: (1) interne Bestände; (2) geteilte Identitätsinformationen; und (3) Datenaustausch mit externen Stellen.	Quantitativ	- % Daten verfügbar – % Datenfehler (Fehlalarme, Fehlschläge) – Zeitaufwand für die Bearbeitung – Prozentualer Rückgang der Bußgelder und/oder Kosten für Fluggesellschaften für falsch eingestiegene Passagiere

4. Paradigmenwechsel hin zu einer digitalen Identität

Heutzutage gibt es mehrere digitale Identitätskonzepte. Jedes weist ein unterschiedliches Maß an Benutzerkontrolle auf und unterscheidet sich in dem Ausmaß, in dem es an ein bestimmtes Produkt gebunden ist („Anbieteragnostizismus“). Die Kontrolle durch den Benutzer ermöglicht es Einzelpersonen, die über sie selbst gesammelten Informationen zu verwalten und zu entscheiden, wann und mit wem sie diese teilen (gemäß den Anforderungen der vertrauenden Partei). Der Grad der Anbieterunabhängigkeit eines digitalen Identitätskonzepts zeigt, inwieweit der Zugriff auf die Informationen und die Überprüfung der Identität nicht von einem bestimmten Anbieter oder der Nutzung der Technologien dieses Anbieters abhängt.

Abbildung 8 zeigt die Landschaft aktueller Initiativen zur digitalen Identität.²⁸ Viele ermöglichen keine vollständige Unabhängigkeit oder Kontrolle durch den Benutzer. Bei den Initiativen handelt es sich überwiegend um Punktlösungen – also Korrekturen, die ganz bestimmte Anwendungsfälle adressieren, etwa die Identitätsprüfung im Bankwesen.

Die Möglichkeiten der Wiederverwendung im Reisekontext scheinen zunächst begrenzt zu sein, müssen jedoch möglicherweise weiter untersucht werden. Dennoch,

Das Framework demonstriert einen Wandel in Richtung Selbstkontrolle und Anbieterunabhängigkeit, zwei wichtige Designprinzipien, die in das Known Traveler Digital Identity-Konzept integriert sind.

Bei der Einführung des Known Traveler Digital Identity-Konzepts basiert die Genehmigung zur Reise oder Einreise in ein fremdes Land auf dem einzelnen Reisenden und seinem eingeschätzten Risikoniveau und nicht auf einem pauschalen Risikoniveau, das hauptsächlich auf dem Herkunftsland einer Person basiert. Dem Einzelnen zu ermöglichen, auf Anfrage und nach eigenem Ermessen seine persönlichen Daten an ausgewählte Stellen während der Reise des Reisenden weiterzugeben, ist ein Schlüsselement, um den Übergang zu einem reisezentrierten, sicheren und nahtlosen Reiseerlebnis zu fördern.

Die präventive Weitergabe von Identitätsinformationen ermöglicht die Personalisierung von Dienstleistungen für Reisende und ermöglicht gleichzeitig den Unternehmen, die die Informationen erhalten, diese im Voraus zu nutzen und Verwaltungs- oder Sicherheitsüberprüfungsprozesse für den Reisenden zu beschleunigen.

n-umfassender Überblick über Initiativen zur digitalen Identität (14)

Abbildung 8: Nicht erschöpfender Überblick über Initiativen zur digitalen Identität²⁸



Eine selbstsouveräne Identität

Eine selbstsouveräne Identität ist „Eigentum“ des Einzelnen. Als Eigentümer hat die Person Zugriff auf diese Identität und kann nach eigenem Ermessen auf Bestandteile dieser Identität verweisen und diese teilen. Während bestimmte Bestandteile der Identität von den ausstellenden Behörden festgestellt werden (z. B. Passnummer, Bankdaten), muss die Person der Weitergabe ihrer Identität und aller damit verbundenen Daten zustimmen. Dies wird dadurch erreicht, dass Einzelpersonen ihre eigenen Identitätsdaten sicher auf ihren eigenen persönlichen Geräten speichern und sie denjenigen, die sie validieren müssen, effizient zur Verfügung stellen, ohne auf ein zentrales Repository für Identitätsdaten angewiesen zu sein.²⁹

Von entscheidender Bedeutung für diesen Paradigmenwechsel ist die Aufrechterhaltung eines empfindlichen Gleichgewichts zwischen einer sichereren und reibungsloseren Reise für Reisende und dem Recht des Einzelnen auf Privatsphäre. Viele Menschen stehen der Weitergabe großer Mengen personenbezogener Daten an Behörden heute skeptisch gegenüber. Wir müssen die Gestaltung von Technologien, die den Austausch von Identitätsinformationen oder den Nachweis von Identitätsansprüchen ermöglichen, gründlich prüfen, um sicherzustellen, dass Regierungen Daten mit ausreichender Verhältnismäßigkeit anfordern, empfangen und verwenden. Im Einklang mit den formulierten Gestaltungsprinzipien muss die Sicherheit im Reiseverkehr der Zukunft ein System umfassen, das für den Einzelnen verständlich ist. Den Menschen muss bewusst sein, dass die vorherige Angabe ihrer Identität und Reisedaten nicht nur die Sicherheit beschleunigt und zu einer reibungsloseren Reise führt, sondern auch zu mehr Sicherheit für die breite Öffentlichkeit beiträgt.

Für Advance existieren internationale Richtlinien und Standards Passagierdaten und Passagierdatensätze werden gemeinsam von der entwickelt und gepflegt Weltzollorganisation (WCO), die International Air

Transport Association (IATA) und ICAO. Wie in den Gestaltungsprinzipien hervorgehoben, sollte das Konzept der bekannten digitalen Identität von Reisenden etablierten Best Practices und Anforderungen entsprechen, die es Reisenden ermöglichen, autonom zu handeln und neben detaillierteren – optionalen – Informationen auch ähnliche erweiterte Passagierdaten und Passagiernamendaten mit den Behörden zu teilen früher auf der Reise.

„In den Niederlanden haben wir den Wert von ‚digitalen Grenzen‘ und automatisierten Grenzkontrolltechnologien erkannt. Wir glauben, dass der wahre Sicherheitswert dadurch realisiert werden könnte, dass man mehr über Passagiere weiß, bevor sie reisen, und zwar durch Programme wie RTP-NL, die es Reisenden ermöglichen, bereitwillig „bekannt“ zu werden und von den Behörden bearbeitet zu werden.“

C. Riezebos, Direktor, Abteilung Migrationspolitik, Ministerium für Justiz und Sicherheit, Niederlande

Digitale Identität

Digitale Identität ist die einzigartige Darstellung einer Person, die an einer Online-Transaktion beteiligt ist. Eine digitale Identität ist im Kontext eines digitalen Dienstes immer eindeutig, muss das Subjekt jedoch nicht unbedingt in allen Kontexten eindeutig identifizieren. Mit anderen Worten bedeutet der Zugriff auf einen digitalen Dienst möglicherweise nicht, dass die reale Identität der Person bekannt ist.³⁰ Derzeit identifizieren viele Nationen ihre Bürger und Einwohner eindeutig und stellen ihnen eine Art digitale Identität in Form eines ePasses zur Verfügung. Reisende nutzen ePässe, um in den Gastländern Identitätsansprüche geltend zu machen, sodass andere Länder auf die personenbezogenen Daten (PII) des Reisenden zugreifen können. Diese werden von der ausstellenden Behörde digital signiert und enthalten eine obligatorische Gesichtsbio metrie (Finger und Iris sind optional).



Verhältnismäßigkeit im Datenschutz³¹

Der Grundsatz der Verhältnismäßigkeit verlangt von den Behörden, dass sie bei der Ausübung ihrer Befugnisse ein Gleichgewicht zwischen den eingesetzten Mitteln und dem angestrebten Ziel herstellen. Wenn es um das Recht auf Schutz personenbezogener Daten geht, erfordert die Verhältnismäßigkeit, dass jede Einschränkung dieses Rechts begründet werden muss, sodass nur die personenbezogenen Daten erhoben und verarbeitet werden, die für die Zwecke (und den angestrebten Vorteil) der Verarbeitung angemessen und relevant sind.

5. Prinzipien und Kerntechnologien

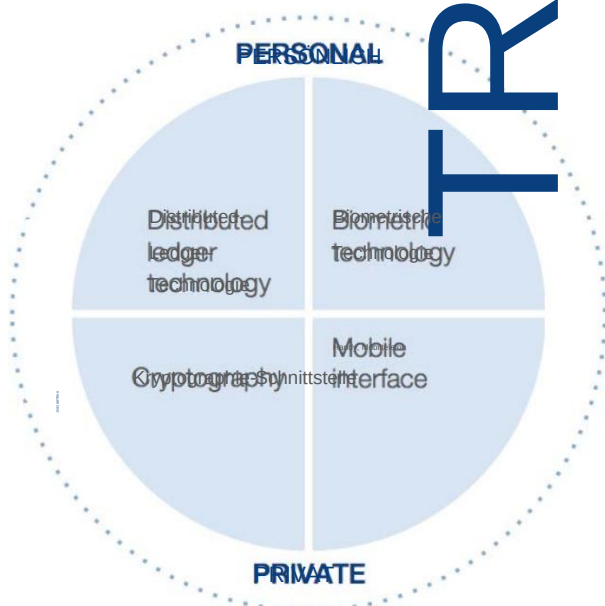
Die technologischen Entwicklungen der vierten industriellen Revolution haben die Konzeptualisierung und Konstruktion eines Konzepts für die digitale Identität bekannter Reisender ermöglicht.

Sie ermöglichen die Verlagerung des „Eigentums“ und der Verwaltung der vielen Komponenten der Identität eines Individuums von der Verwaltung durch zentralisierte Dienste auf die Verwaltung durch Einzelpersonen selbst. Durch die Known Traveler Digital Identity haben Einzelpersonen die Kontrolle über die Verwendung ihrer persönlichen Daten und werden in die Lage versetzt, aktiv zur Sicherheit der Gesellschaft insgesamt beizutragen.³² In diesem Kapitel werden die vier Schlüsselwerte eines Selbst beschrieben – persönlich, tragbar, privat und dauerhaft – souveräne digitale Identität, die diesen Wandel hin zur individuellen Verwaltung der Identität ermöglicht. Darüber hinaus werden die vier Kerntechnologien skizziert, die derzeit als die fortschrittlichsten Optionen zur Ermöglichung der erforderlichen Neugestaltung von Richtlinien und Systemen gelten (Abbildung 9).

Prinzipien der Technologiearchitektur

Das Known Traveller Digital Identity-Konzept ist so konzipiert, dass es den Werten und Prinzipien der Selbstsouveränität entspricht. Die vier Schlüsselwerte – dass es persönlich, tragbar, privat und dauerhaft ist – werden jeweils zu entsprechenden Prinzipien erweitert, wie in Tabelle 6 detailliert beschrieben. Die Tabelle zeigt, wie das Known Traveler Digital Identity-Konzept diese Prinzipien einhält, indem es sich auf die derzeit fortschrittlichsten Technologien stützt, verfügbar – die jeweils in den Demonstrationsprototyp eingebaut werden.

Abbildung 9: Überblick über Werte und Kerntechnologien



Grundlegende Schlüsseltechnologien erklärt

Distributed-Ledger-Technologie, Public-Private-Key-Kryptographie, fortschrittliche Biometrie und eine mobile Schnittstelle ermöglichen den nächsten Schritt in der Entwicklung einer weltweit akzeptablen Known Traveler Digital Identity-Infrastruktur:

1. Distributed Ledger ermöglicht Vertrauen in das Netzwerk ohne die Kontrolle einer zentralen Behörde
2. Kryptographie ermöglicht ein angemessenes Maß an Sicherheit bei der Autorisierung und Weitergabe von Informationen
3. Biometrie verbindet die physische mit der digitalen Welt und gewährleistet die legitime Nutzung von Identitätsinformationen
4. Mobile Geräte ermöglichen es dem Reisenden, seine Sachen mitzunehmen, digitale Identität und entscheiden sich autonom dafür, diese entsprechend zu teilen

Wie bei neuen Technologien erwartet, gibt es noch keine ausreichenden Beweise, um die eine „beste“ Lösung zu ermitteln. Es ist wichtig, jede technologische Entscheidung, die bei der Gestaltung eines solchen innovativen Konzepts getroffen wird, im Hinblick auf die zu erwartenden Vor- und Nachteile zu berücksichtigen. Es müssen mehrere weitere Überlegungen berücksichtigt werden, die nicht speziell an eine einzelne Technologie gebunden sind, die aber ebenso wichtig zu berücksichtigen sind.

Distributed-Ledger-Technologie, Blockchain, Zeiger und Hubs

Herkömmliche Identitätsmanagementsysteme basieren auf zentralisierten Behörden, während das Fehlen eines zentralen Registers für ein selbstverwaltetes digitales Identitätssystem von grundlegender Bedeutung ist.³⁴ Mit der Verlagerung des Identitätsmanagements in die digitale Welt ist es von entscheidender Bedeutung, gemeinsame Anstrengungen zu unternehmen, um die Cybersicherheit zu erhöhen und Reisende zu schützen, um den Datenschutz, um das Vertrauen der Kunden aufrechtzuerhalten, die Serviceakzeptanz durch Benutzer zu fördern und die öffentliche Sicherheit zu verbessern.³⁵ Ein Distributed Ledger ist ein Konsens replizierter, gemeinsam genutzter und synchronisierter digitaler Daten, die geografisch über mehrere Länder oder Institutionen verteilt sind. Es gibt keinen zentralen Administrator oder zentralen Datenspeicher und daher dient das Distributed Ledger als dediziertes Peer-to-Peer-Netzwerk.

Ein nicht-Blockchain-verteiltes Hauptbuch

Die Distributed-Ledger-Technologie weist ein großes Potenzial für eine selbstsouveräne digitale Identität bekannter Reisender auf, da sie von Natur aus verteilt und nachhaltig, unauslöschlich, transparent und überprüfbar, orchestriert und flexibel, konsensbasiert und transaktional ist.³⁶ Alternative zur Blockchain, einer verteilten Nicht-Blockchain Ledger könnte ebenfalls zu den Prinzipien passen. Beispielsweise verfügt Corda von R3 über viele der notwendigen Elemente für selbstsouveräne digitale Identitätssysteme – koordinierte Arbeitsabläufe, digitale Signaturen und Regeln zur Datenentwicklung.³⁷ Ein weiteres Beispiel ist X-Road, die Datenaustauschschicht für Informationssysteme der estnischen Regierung . X-Road schafft eine technologische und organisatorische Umgebung, die einen sicheren internetbasierten Datenaustausch zwischen Informationssystemen ermöglicht.³⁸

Für das Known Traveler Digital Identity-Konzept wird Blockchain zur Implementierung des verteilten Hauptbuchs verwendet, obwohl Alternativen verfügbar sind. Unter Blockchain versteht man die Datenstruktur aus kryptografisch verknüpften Datenblöcken.³⁹ Dies impliziert die Fähigkeit, den Inhalt der Blöcke zuverlässig zu überprüfen, impliziert jedoch keine Verteilung jeglicher Art.⁴⁰ Die Kombination aus einer Blockchain zur kryptografischen Verknüpfung von Datenblöcken und der Distributed-Ledger-Technologie ermöglicht die sichere Übertragung von Informationen ohne die Kontrolle einer zentralen Behörde.

Im Wesentlichen handelt es sich um eine verteilte Datenbank, bei der eine Blockchain als öffentliches Hauptbuch dient, das niemals gelöscht oder neu geschrieben werden kann. Einträge können geändert, aber nicht aus einem Blockchain-basierten Distributed Ledger gelöscht werden. Daten können nur geändert werden, wenn unter den Netzwerkteilnehmern Konsens darüber erzielt wird, dass eine vorgeschlagene Transaktion korrekt und gültig ist. Die Kette ist unveränderlich, da jeder neue Block im Datenspeicher auch einen Hash des vorherigen Blocks in der Kette enthält. Je länger die Kette, desto sicherer und schwerer zu manipulieren.

Tabelle 6: Prinzipien eines selbstsouveränen digitalen Identitätskonzepts³³

Schlüsselwerte	Konzept folgt dem Prinzip	0 gibt den niedrigsten Wert der Technologie an, um das Prinzip einzuhalten, 4 ist hoch			
		Existenz	Kontrolle	Zustimmung	Beharrlichkeit
persönlich (sicher) Die Identitätsinformationen müssen vor unbeabsichtigter Offenlegung geschützt werden	Schutz Das Recht der Nutzer muss geschützt werden, wenn ein Konflikt zwischen den Bedürfnissen des Netzwerks und den Rechten des Einzelnen besteht; Letzteres sollte Priorität haben	2 	4 	1 	1
	Minimierung Die Offenlegung von Ansprüchen muss minimiert werden	3 	1 	1 	2
tragbar Der Identitätseigentümer muss seine Identitätsdaten überall nutzen können und darf nicht an einen einzigen Technologieanbieter gebunden sein	Interoperabilität Identitäten sollten möglichst umfassend nutzbar sein	2 	1 	4 	2
	Transparenz Das System und seine Logik müssen in ihrer Funktionsweise, ihrer Verwaltung und ihrer Aktualität transparent sein	4 	1 	0 	2
	Transportabel Alle Informationen über Identitäten müssen transportierbar sein; Die Identität muss beim Benutzer und nicht bei einem Dritten liegen	3 	1 	3 	4
	Zugriff Benutzer sollten direkten Zugriff auf ihre eigene Identität und alle damit verbundenen Daten haben; Alle Daten müssen ohne Gatekeeper sichtbar und zugänglich sein	3 	2 	3 	3
Privat (Kontrolle) Der Identitätsinhaber muss die Kontrolle darüber haben, wer seine Daten zu welchen Zwecken sehen und darauf zugreifen kann	Existenz Benutzer müssen eine unabhängige Existenz haben; es kann niemals nur digital existieren	0 	0 	4 	0
	Kontrolle Benutzer können ausgewählte Daten an ausgewählte Entitäten übertragen	2 	2 	0 	4
	Zustimmung Nutzer müssen der Nutzung ihrer Identität und der Weitergabe damit verbundener Daten zustimmen	1 	2 	0 	4
Hartnäckig Die Identität lebt mit dem Individuum vom Leben bis zum Tod	Beharrlichkeit Identitäten müssen langlebig sein, zumindest so lange, wie der Benutzer es wünscht, aber sie sollten nicht im Widerspruch zu einem „Recht auf Vergessenwerden“ stehen.	3 	0 	0 	0

Der Aufruf zur Verteilung

Bisher bestand die einzige Möglichkeit zur Speicherung von Identitätsinformationen in einer zentralen Art und Weise mit einem einzigen Kontrollpunkt. Das Problem bei einer zentralen Datenbank, wie sie beispielsweise für die Speicherung von Sozialversicherungsnummern oder Kreditauskünften verwendet wird, besteht darin, dass sie, wenn sie erst einmal kompromittiert wurde, ein enormes Sicherheitsrisiko für viele Menschen darstellt. Zu den jüngsten Beispielen kompromittierter Daten gehören: der Equifax-Verstoß, von dem 140 Millionen Menschen betroffen waren; der Home-Depot-Verstoß, von dem 50 Millionen Kunden betroffen waren, und Yahoo, bei dem Berichten zufolge mehr als 3 Milliarden Kundenkonten gehackt wurden.⁴²

Anstelle der eigentlichen Identitätsdaten enthält die Blockchain Zeiger auf die Daten. Diese Zeiger beziehen sich auf eine Identität und werden in der Blockchain gespeichert, um den Teilnehmern nach Autorisierung den Zugriff auf die Identitätsdaten zu ermöglichen. Zeiger führen zu Hubs, die einen sicheren Datenaustausch und eine sichere Datenspeicherung ermöglichen und die Datenintegrität wahren. Ein Hub ist ein Datenspeicher, der Fragmente von Identitätsdaten an einem bekannten Ort enthält (in diesem Fall könnten gesicherte Datenbanken mit Identitätsinformationen als Hub betrachtet werden). Jedes Objekt in einem Hub ist mit einer Identität signiert und über ein weltweit anerkanntes Anwendungsprogrammierschnittstellenformat zugänglich, das explizit semantischen Datenobjekten zugeordnet ist.⁴³ Identitätsdaten werden nicht in der Blockchain gespeichert. Die Blockchain enthält den Zeiger, der die Entität an die richtige Stelle auf einem Hub leitet, der mit der Identität verknüpft ist. Die Blockchain kann als verteilte Zertifizierungsstelle betrachtet werden, die die Zuordnung von Identitäten zu öffentlichen Schlüsseln verwaltet. Darüber hinaus können intelligente Verträge eine ausgefeilte Logik hinzufügen, die beim Widerruf und bei der Wiederherstellung hilft, was den Verwaltungsaufwand für den Endbenutzer verringert (Abbildung 10).⁴⁴

Da die Distributed-Ledger- und Blockchain-Technologie noch in den Kinderschuhen steckt und das aktuelle Entwicklungstempo rasant ist, beeinflussen oder verändern regelmäßig neue Lösungen die Landschaft. Eine Bewertung verschiedener Technologieoptionen sowie ihrer potenziellen Nachteile bietet detaillierte Einblicke in das aktuelle Verständnis der Technologien. Im Allgemeinen werden drei Arten von Distributed-Ledger-Architekturen unterschieden: öffentliche, konsortiale und private Ledger. Diese Typen variieren je nachdem, wer am Netzwerk teilnehmen darf, wer das Konsensprotokoll ausführt und wer das gemeinsame Hauptbuch führt.

Damit die bekannte digitale Identität des Reisenden selbstsouverän ist, ist ein liberaler Ansatz erforderlich, um die Autonomie des Einzelnen zu maximieren. Daher wird ein erlaubnisbasiertes öffentliches Hauptbuch als am besten geeignet angesehen. Ausgewählte vertrauenswürdige Knoten verfügen über bestimmte Schreibberechtigungen, aber jeder Einzelne und jede Entität darf das verteilte Hauptbuch lesen, was vollständige Transparenz gewährleistet.

Außerdem muss entschieden werden, ob die Speicherung der identitätsbezogenen Daten auf oder außerhalb der Blockchain erfolgt.

Basierend auf den fortschrittlichsten Überlegungen wird die Speicherung von Identitätsinformationen außerhalb der Blockchain als am besten geeignet angesehen, um sowohl die erforderliche Privatsphäre als auch die Skalierbarkeit zu ermöglichen. Abschließend muss über den Einsatz von Smart Contracts nachgedacht werden, um eine granulare Berechtigungsstruktur zu ermöglichen. Derzeit ist unklar, welche Parteien welche Berechtigungen haben sollen.

Abbildung 10: Visualisierung der Technologie

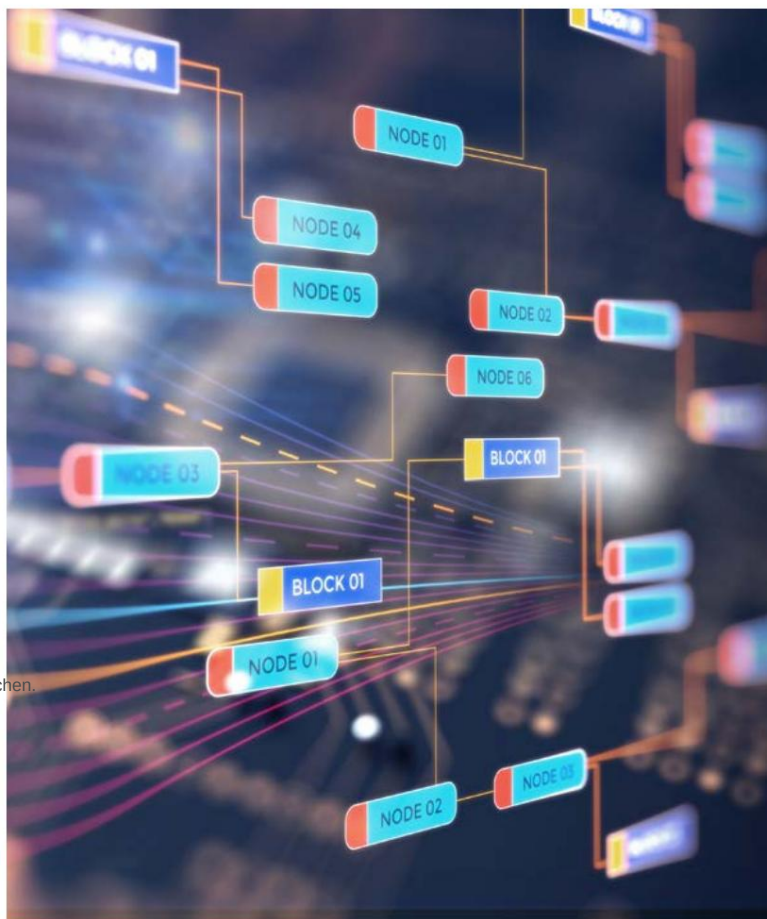
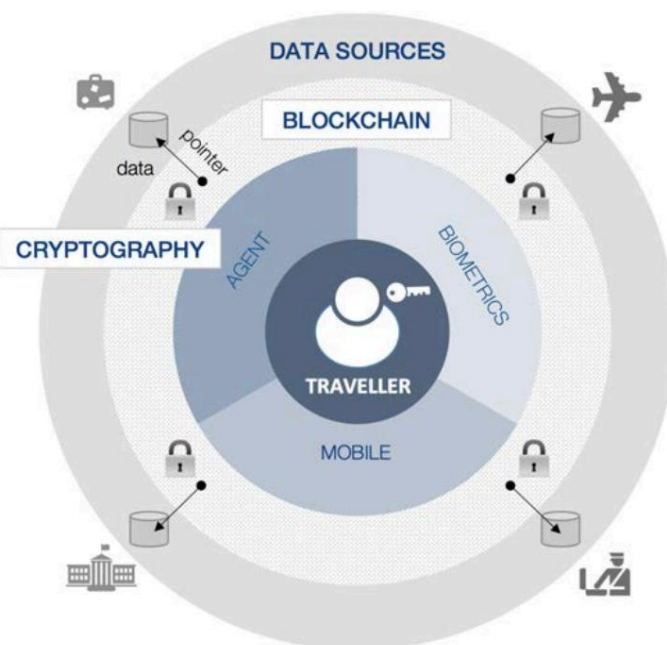


Tabelle 7: Arten von Distributed-Ledger-Architekturen⁴⁵

	Erlaubnisfreies öffentliches Hauptbuch	Zugelassenes öffentliches (Konsortial-)Hauptbuch	Zugelassenes privates Hauptbuch
Begründung	Konsensbasiert Dezentralisiert: eliminiert den Vermittler Peer-to-Peer-Transaktionen Jede Transaktion wird mit jedem angeschlossenen Knoten überprüft und synchronisiert Vollständig dezentrale Sicherheit und Kontrolle	Erlaubnisbasiert Logische Dezentralisierung: Ein paar ausgewählte Knoten, bekannte Entitäten, werden vorgegeben, um das System zu steuern und sicherzustellen Konsens	Erlaubnisbasiert Zentralisiert: umfasst einen Vermittler, bei dem ein Knoten jede Transaktion schreibt und überprüft; Der Knoten kann wählen, wer Lesezugriff hat (Lesezugriff kann öffentlich sein)
Vorteile	+ Völlig offen, jeder hat Zutritt + Anreizmechanismus dazu Ermutigen Sie mehr Teilnehmer, dem Netzwerk beizutreten + Hohe Sicherheit, jede Transaktion ist öffentlich und Benutzer können ihre Anonymität wahren + Volle Transparenz + Zensurresistent + Manipulationssicher	+ Erfordert eine Einladung und muss durch (eine Reihe von Regeln) validiert werden, die vom Netzwerkstarter festgelegt wurden + Ermöglicht eine größere Skalierbarkeit hinsichtlich des Transaktionsdurchsatzes + Ermöglicht schnelle Transaktionen durch höhere Effizienz + Transaktionsdatenschutz möglich	+ Teilnehmer benötigen eine Einladung oder Erlaubnis zum Beitritt + Einschränkungen, wer am Netzwerk teilnehmen darf + Ermöglicht eine größere Skalierbarkeit hinsichtlich des Transaktionsdurchsatzes + Ermöglicht schnelle Transaktionen durch höhere Effizienz + Größere Privatsphäre durch Einschränkungen der Leseberechtigungen
Nachteile	- Hohe Rechenleistung aufgrund mangelnden Vertrauens für den Arbeitsnachweis erforderlich - Aufgrund der Offenheit gibt es bei Transaktionen kaum oder gar keine Privatsphäre - Höhere Kosten	- Geringere dezentrale Sicherheit - Nicht vollständig zensurresistent - Erfordert Vertrauen in bekannte Entitäten	- Geringere dezentrale Sicherheit - Unerwünschte Zensur möglich - Begrenztes Risiko einer Datenmanipulation - Erfordert Vertrauen in eine Entität
Beispiele	Bitcoin, Ethereum	Hyperledger, Ripple	R3 CEV, DAH

Netzwerk für Geldautomaten (ATM).

Ein ATM-Netzwerk ist ein „öffentlich zugelassenes“ Distributed-Ledger-Design. Grundsätzlich kann jeder einen Geldautomaten nutzen (er ist öffentlich), aber nur wer eine Sondergenehmigung hat, kann einen neuen Geldautomaten zum Geldautomatennetz hinzufügen (erlaubt).⁴⁶

Kryptographie mit öffentlichem und privatem Schlüssel

Eine Public-Key-Infrastruktur (PKI) ermöglicht eine sichere digitale Authentifizierung und Signatur.⁴⁷ Bei der Public-Key-Kryptografie werden Informationen mit einem „Schlüsselpaar“ gesichert, das aus einem öffentlichen Schlüssel, der für jedermann sichtbar ist, und einem privaten Schlüssel, der sichtbar ist, besteht ausschließlich dem Identitätseigentümer vorbehalten und nicht für andere zugänglich ist. Mit dem privaten Schlüssel wird zusammen mit gehashten zusätzlichen Metainformationen ein öffentlicher Schlüssel generiert, der die Zeigeradresse erstellt. Diese Adresse ist für die Teilnehmer im Netzwerk sichtbar; Allerdings kann der private Schlüssel nicht aus dem öffentlichen Schlüssel generiert werden, wodurch die Authentifizierung sicher ist. Da die Zeiger auf einer Blockchain gespeichert sind, ist jeder Identifikationsprozess als eigene Root-Autorität dienen – eine Architektur, die als dezentrale Public-Key-Infrastruktur (DPKI) bezeichnet wird. Diese Zeiger erreichen globale Einzigartigkeit, ohne dass eine zentrale Registrierungsstelle erforderlich ist. Dies geht leider auf Kosten der menschlichen Einprägsamkeit. Die Algorithmen, die global eindeutige Identifikatoren generieren können, erzeugen automatisch zufällige Zeichenfolgen, die keine menschliche Bedeutung haben.

Dies verdeutlicht das als Zooko-Dreieck bekannte Axiom über Identifikatoren: „Menschlich sinnvoll, dezentral, sicher – wählen Sie zwei.“⁴⁹ Eine Kombination aller drei gilt vorerst als unmöglich.

Die Sicherheit aller Reisenden hat für alle Beteiligten oberste Priorität. Zu jeder Zeit zu wissen, wer Ihr Kunde ist, ist eine entscheidende Komponente, um das Erreichen dieses Ziels sicherzustellen. Dies muss jedoch im Rahmen der bestehenden Gesetze und Vorschriften zum Schutz personenbezogener Daten und der Privatsphäre erfolgen. Diese äußerst wichtigen Ziele können durch den Einsatz fortschrittlicher Technologien erreicht werden, um Datenschutz und Sicherheit durch Design zu erreichen.

Rob Leslie, Chief Executive Officer, Sedicii

Es gibt mehrere Mechanismen zum Verschlüsseln und Sichern von Identitätsinformationen. Der Einsatz von Zero-Knowledge-Proof-Funktionen (ZKP) gilt als praktikable Option für die Identitätsprüfungstechnologie. ZKP ist ein kryptografischer Algorithmus, der es Benutzern ermöglicht, Informationen zu überprüfen, ohne die Informationen tatsächlich preiszugeben – es wird lediglich überprüft, ob die Informationen tatsächlich mit sehr hoher Wahrscheinlichkeit korrekt sind.

Im Wesentlichen ermöglicht ZKP einem Benutzer, einen Identitätsnachweis zu erhalten, ohne jemals Kenntnis von den tatsächlich nachgewiesenen Informationen zu haben. In Prozessen mit geringer Kritikalität, an denen beispielsweise Regierungen nicht beteiligt sind, können alternative Mechanismen wie Fast Identity Online (FIDO) eingesetzt werden. Universal Authentication Framework (UAF) kann erkundet werden.

ZKP kann die Herausforderung des Datenschutzes personenbezogener Daten mit Blockchains lösen

ZKP ist ein Protokoll, das in kryptografischen Systemen verwendet wird und es einer Partei ermöglicht, nachzuweisen, dass sie etwas weiß – beispielsweise einen Identitätsnachweis –, ohne diesen Nachweis jemand anderem zugänglich machen zu müssen. ZKP sollte nicht mit Verschlüsselung verwechselt werden. Das von einem ZKP zurückgegebene Ergebnis ist binär und verrät lediglich, dass die Entität entweder die Information kennt oder nicht. Zu den Informationen selbst wird nie etwas preisgegeben. Dies ist besonders wichtig, wenn die Informationen sensibel sind oder Kontrollen unterliegen.

Bei der Verwendung von Identitätsdaten in oder mit Blockchains gibt es zwei wesentliche Herausforderungen, denen die ZKP-Technologie begegnen kann. Ein wesentliches Merkmal einer Blockchain besteht darin, dass für deren Ausführung kein zentraler Administrator oder keine Anwendungslogik erforderlich ist. **Dezentralisierung** ist wichtig, da sie garantiert, dass es keinen Single Point of Failure gibt. Allerdings geht die Dezentralisierung mit der Tatsache einher, dass sie sieht, was alle anderen tun. Privatsphäre. Jeder Knoten in der Kette muss jede Transaktion unabhängig überprüfen, und zwar

Zweitens verlangt die Datenschutzgesetzgebung, insbesondere die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, das „Recht auf Vergessenwerden“, was bedeutet, dass personenbezogene Daten auf Anfrage eines EU-Bürgers in einem System gelöscht und gelöscht werden müssen. Wenn dieses Recht auf eine Blockchain angewendet würde, die personenbezogene Daten enthält, würde das Löschen aller Daten in der Blockchain die Kette unterbrechen und einen „Hard Fork“ oder Schlimmeres verursachen, der die Kette vollständig zerstören würde. Daher besteht Bedarf an der Möglichkeit, Blockchains zur Verwaltung personenbezogener Daten zu nutzen, ohne dass personenbezogene Daten auf der Blockchain selbst vorhanden sind. ZKP kann diese Datenschutzherausforderungen angehen und lösen.



Die FIDO UAF-Architektur kann die Authentifizierung unterstützen, ohne dass biometrische Daten mit einem Authentifizierungsserver geteilt werden müssen

Das FIDO UAF-Framework ermöglicht die lokale biometrische Authentifizierung mithilfe der nativen Sicherheitsfunktionen eines Endbenutzergeräts.

Biometrische Daten werden von der FIDO-zertifizierten Anwendung sicher lokal gespeichert, während nur der öffentliche Schlüssel eines Benutzers mit dem FIDO-zertifizierten Server geteilt wird. Diese Technologie würde beispielsweise Gesichts- und Stimmerkennung sowie Iris- oder Fingerabdruckerkennung zur Authentifizierung des Reisenden oder eine Kombination davon ermöglichen, ohne dass ein externes Gerät erforderlich ist. Der Reisende müsste sein eigenes FIDO-zertifiziertes Gerät mitführen. Diese Architektur eignet sich am besten für Prozesse mit geringer Kritikalität, an denen Regierungsbehörden nicht beteiligt sind, beispielsweise beim Austausch zwischen Hotels und Reisenden.

Biometrie

Heutzutage ist die Validierung von Identitätsansprüchen der Grundstein für eine wirksame Luftsicherheit und Grenzverwaltung. Viele Sicherheits- und Grenzschutzbehörden verlassen sich auf textbasierte Informationen, die aus dem vom Reisenden vorgelegten Dokument abgeleitet werden, um Passagierlisten zu validieren, Überwachungslistenkontrollen durchzuführen und diejenigen zu ermitteln, die ihr Visum überschritten haben. Es besteht jedoch keine Gewissheit, dass die Person, die die Dokumente vorlegt, der rechtmäßige Inhaber ist.

Es gibt drei primäre Methoden der digitalen Authentifizierung: etwas, das Sie wissen, ein Passwort, beispielsweise einen PIN-Code; etwas, das Sie haben, eine Smartcard wie ein Hardware-Token-Generator; und etwas, das Sie sind, ein biometrischer Wert wie etwa Fingerabdrücke. Zu den weiteren Authentifizierungsmethoden gehören: Ihr Standort, geografischer Standort; und wie Sie interagieren, Verhaltensbiometrie, zum Beispiel Tastendynamik.

Die One ID-Initiative der IATA

Die One ID-Initiative der IATA zielt darauf ab, einen optimierten, reibungslosen und passagierzentrierten Prozess einzuführen, der es einer Person ermöglicht, ihre Identität online oder persönlich in jedem Prozessschritt der End-to-End-Passagierreise im erforderlichen Umfang geltend zu machen. unter Wahrung der Privatsphäre personenbezogener Daten. Das Konzept basiert auf einer einzigen Erfassung und kontrollierten Verteilung von Passagierdaten an die verschiedenen Stakeholder auf der Basis einer „Authorized-to-know“-Basis. Wenn die Identität eines Passagiers an jedem Berührungspunkt bestätigt werden kann, wird es einfacher, ein personalisierteres Kundenerlebnis zu bieten und gleichzeitig erhebliche Verbesserungen der betrieblichen Effizienz und Sicherheit zu ermöglichen. Um dies zu erreichen, wird eine echte Zusammenarbeit zwischen den Beteiligten von größter Bedeutung sein.

Derzeit ist die Verwendung einer Gesichtsbimetrie das gängige Mittel zur Überprüfung. Aufgrund des technologischen Fortschritts könnte sich die während der gesamten Reise des Reisenden verwendete biometrische Daten in Zukunft ändern. Die in Tabelle 8 aufgeführten Merkmale geben Hinweise zur Beurteilung der Eignung eines biometrischen Merkmals. Zukünftig könnten andere biometrische Daten aus neuen Modalitäten, darunter 3D-Gesicht, DNA, Gang und Elektrokardiogramm, Potenzial für die Verbindung der digitalen und physischen Welt haben und eine sichere und nahtlose Reise für Reisende ermöglichen. Die Akzeptanz der Verwendung dieser biometrischen Daten kann sich abhängig von der Fähigkeit des Benutzers ändern, zu steuern, wann seine Identität authentifiziert wird und welche Informationen mit seiner Identität verknüpft werden.

„Biometrische Authentifizierungstechnologien sind der Schlüssel zur digitalen Transformation im Flugverkehr, da sie den Sicherheitsprozess verbessern und einen personalisierten, nahtlosen Ablauf ermöglichen. Sie haben die Möglichkeit, unser tägliches Leben über das Reisen hinaus zu verändern.“

Nobuhiro Endo, Vorstandsvorsitzender der NEC Corporation

Biometrie an Grenzen

Grenzschutzbehörden können vom Einsatz biometrischer digitaler Identitäten profitieren, um das Passagiererlebnis zu verbessern und gleichzeitig die Sicherheit zu gewährleisten:

- 73 % der Bürger glauben, dass die Verwendung biometrischer Daten zur Überprüfung der Identität jedes Grenzübertritts die Sicherheit erhöhen würde – 62 % der Bürger würden biometrische Daten weitergeben, um die Grenzsicherheit zu verbessern
- 58 % der Bürger geben an, dass sie biometrische Informationen weitergeben würden, um die Grenzabwicklung schneller und effizienter zu gestalten.

Biometrie wird genutzt, um die digitale Identität mit der physischen Welt zu verbinden. Die Authentifizierung von Identitätsansprüchen ist die Grundlage vertrauensbasierter Beziehungen. Moderne Sicherheitssysteme hängen von der erfolgreichen Validierung von Identitäten ab, um Zugriffsrechte und -privilegien basierend auf den mit einer etablierten Identität verbundenen Sicherheitsstufen zu gewähren oder zu verweigern. Die Einführung biometrischer Systeme zur Authentifizierung bietet Reisenden die Möglichkeit, ihre physische Identität mit ihrer digitalen Identität zu verknüpfen⁵⁰ und zu überprüfen, ob eine Person, die einen Anspruch auf eine Identität geltend macht, diesen Anspruch tatsächlich nachweisen kann. One ID, eine von der IATA geleitete Initiative, untersucht den transformativen Einsatz biometrischer Daten, um einen flughafenspezifischen, reibungslosen Prozess zu ermöglichen und ein nahtloseres und personalisierteres Flughafenerlebnis zu ermöglichen.

Bei der Verwendung biometrischer Daten ist es von entscheidender Bedeutung, Privatsphäre und Sicherheit zu gewährleisten, da biometrische Daten im Gegensatz zu einem Passwort nicht geändert werden können, wenn sie kompromittiert werden.⁵¹ Die biometrische Erkennung hat sich als wirksamer als der Mensch erwiesen, da sie in der Lage ist, die individuelle Zulässigkeit schnell und genau zu bestimmen.⁵²



Tabelle 8: Vergleichsbiometrie (0 ist niedrig, 4 ist hoch)54

Biometrisch		Fingerabdruck	Gesicht	Iris	Stimme	Gefäß	Unterschrift
Identifizierung der Person durch		Unterscheidungsmerkmale an Fingerspitzen	Besonderheiten des Gesichts	Markante Merkmale im pigmentierten Teil des Auges, der die Pupille von der weißen Sklera trennt	Physiologische und verhaltensbezogene Aspekte der Stimme	Venenmuster, meist am Handrücken, Aspekte der Stimme Handfläche oder dem Finger	Verhaltensmodalität, die normalerweise nur zur Überprüfung verwendet wird
Genauigkeit: Falsche Akzeptanz- oder Ablehnungsrate in verschiedenen Situationen	Identifikation						
	Überprüfung						
Universalität: Vorhandensein des Merkmals bei allen Mitgliedern der relevanten Population							
Stabilität: Beständigkeit des Merkmals über Alterung, Krankheit und Verletzung hinweg							
Sammelbarkeit: Einfache Beschaffung qualitativ hochwertiger Proben							
Umgehungsresistenz: Anfälligkeit der Modalität für Betrug							
Akzeptanz: Vorbehalte der Benutzer gegenüber der Verwendung einer bestimmten Modalität							
Benutzerfreundlichkeit: Einfache Benutzerschnittstellen mit einem System							
Kosten: Hardware-/Softwarekosten für die Probenentnahme und anschließende Deduplizierung							
Gesamtpunktzahl							

Mobile Schnittstelle

Kurzfristig wird eine mobile Schnittstelle als die bequemste Möglichkeit angesehen, private Schlüssel zu generieren, öffentliche Schlüssel an Emittenten zu senden und digitale Aufzeichnungen mit dem entsprechenden privaten Schlüssel oder dezentralen Identifikator zu führen.⁵⁵ Die mobile Identitätsanwendung sollte Benutzern eine ganzheitliche Sichtbarkeit ermöglichen ihrer digitalen Identitätskomponenten und stellen eine Schnittstelle bereit, über die sie diese an staatliche und private Stellen weitergeben können. Benutzer profitieren von der Kontrolle über mehrere Komponenten ihrer digitalen Identität, da diese Komponenten je nach den Anforderungen des Dienstes, auf den sie zugreifen möchten, über verschiedene Kanäle und Mechanismen verpackt, übertragen und verarbeitet werden können. Die an eine Grenzschutzbehörde weitergegebenen Identitätsinformationen unterscheiden sich stark von den Identitätsinformationen, die an anderen Punkten ihrer Reise benötigt werden – beispielsweise beim Zugang zu Transportdiensten.

Darüber hinaus gibt es Einzelpersonen die Möglichkeit, die Nutzung ihrer digitalen Identität aktiv, autonom und bequem zu verwalten. Diese Verwaltung sollte die Möglichkeit umfassen, Interaktionen mit Diensten zu überprüfen und Benutzern zu helfen

die umfassenderen Auswirkungen der Identitätsweitergabe auf ihre Privatsphäre und persönliche Sicherheit verstehen.

Über die mobile Schnittstelle können Push-Nachrichten mit der Bitte um Zustimmung zur Weitergabe personenbezogener Daten an Empfänger für einen bestimmten Zeitraum empfangen werden. In dieser Hinsicht fungiert das mobile Gerät als Benutzerschnittstelle für die Interaktion mit dem Netzwerk. Eine mobile Schnittstelle kann alles sein, von einem Mobiltelefon über eine Smartwatch bis hin zu einer Augmented-Reality-Brille. Letztendlich gibt es möglicherweise auch andere Möglichkeiten, diese Anfragen entgegenzunehmen – zum Beispiel über Bildschirme, die vor dem Abflug bequem an Flughäfen angebracht sind und eine persönliche Nachricht anzeigen, wenn jemand vorbeikommt.

Es wird nicht erwartet, dass jeder Reisende über ein mobiles Gerät verfügt. Daher sollten Alternativen bereitgestellt werden, die es Einzelpersonen ermöglichen, der Weitergabe ihrer Informationen zuzustimmen. Darüber hinaus gibt es eine große Vielfalt an Arten mobiler Schnittstellen, was eine breite Kompatibilität der Technologie hinter dem Konzept erfordert. Um eine kritische Masse an Anwendern zu erreichen, sind weit verbreitete Technologiestandards am erfolgversprechendsten.

Allgemeine Überlegungen

In Bezug auf Datenschutz, Sicherheit, Governance, Technologie und Protokolle, Richtlinien und Standards müssen noch eine Reihe von Problemen geklärt werden. Die Interessengruppen müssen weiterhin zusammenarbeiten, um Fragen wie die folgenden zu beantworten:

1. Wie können Technologien sich ständig weiterentwickeln?

Wir stellen sicher, dass wir diese Entwicklungen berücksichtigen und die richtigen Entscheidungen hinsichtlich der eingesetzten Technologien treffen.

2. Interoperabilität basiert auf dem Austausch von Protokollen und Daten

Schemata und Governance. Wie können wir die relevanten Stakeholder im Ökosystem einbeziehen und zu vereinbarten Standards gelangen?

3. Wie stellen wir die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sicher? Sind aktuelle kryptografische Ausdrucksmechanismen dieser Aufgabe gewachsen?

4. Wie sieht die Finanzstruktur eines bekannten Reisenden aus?

Wie sieht das digitale Identitätssystem aus? Sind für alle Akteure die richtigen Anreize vorhanden, die Infrastruktur zu erhalten, zu nutzen und anzupassen?

5. Welche Spezifikationen, Protokolle und Implementierungen von

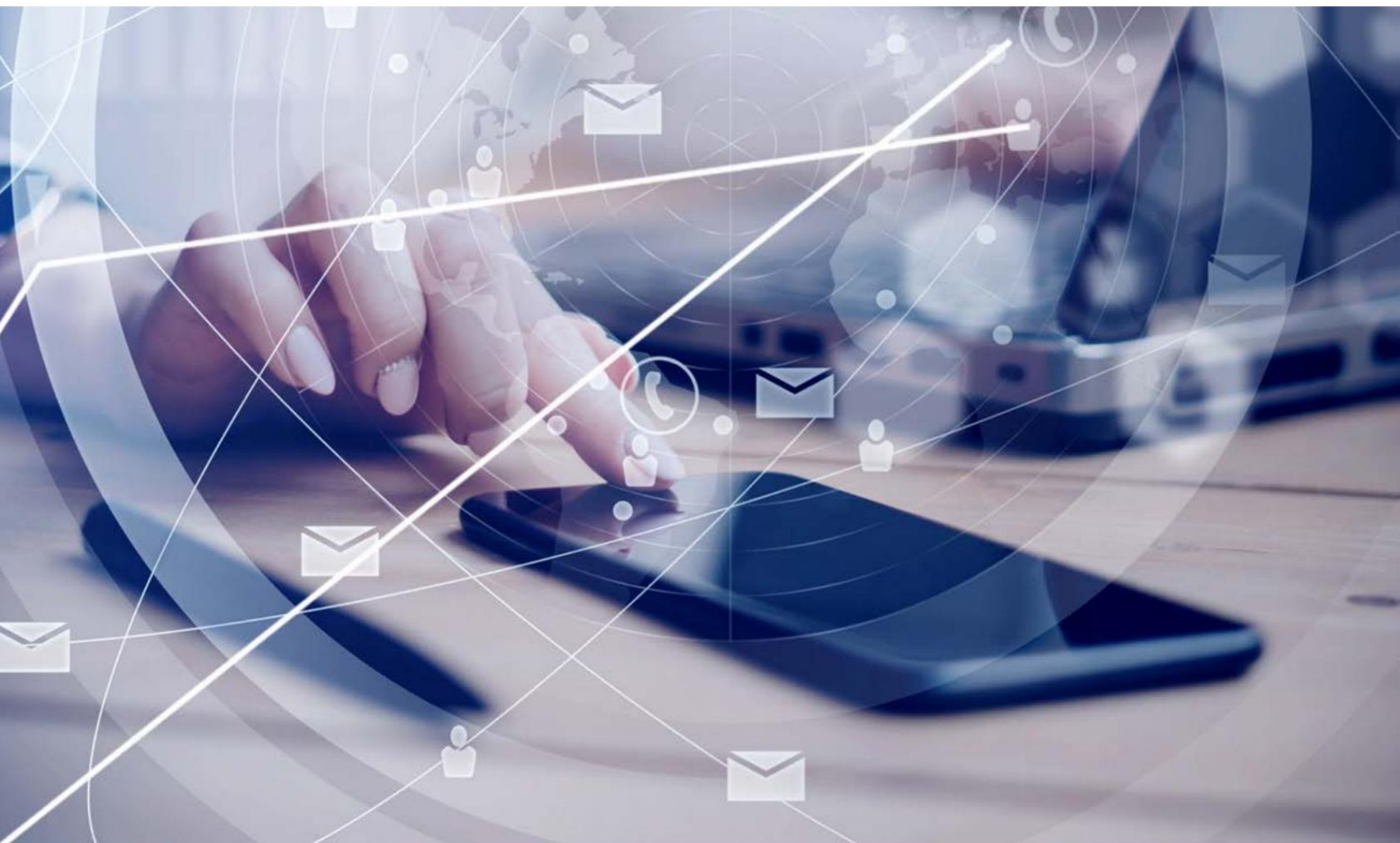
Anwendungen, Diensten, Paketen und Bibliotheken, die die Interoperabilität zwischen Systemen und Anbietern gewährleisten, existieren bereits und welche neuen Aspekte müssen möglicherweise entwickelt werden?

6. Wie definieren wir die vertraglichen Regelungen?

(intelligente Verträge) zwischen Parteien, die verwendet werden, um der digitalen Identität Bestätigungen hinzuzufügen und eine detailliertere Entscheidungsfindung über die Zugangskontrolle zu ermöglichen?

Anwendungsfall von Smart Contracts im uPort-Konzept

Der Zweck eines Proxy-Vertrags als Kernidentifikator besteht darin, dass der Benutzer seinen privaten Schlüssel ersetzen und gleichzeitig einen dauerhaften Identifikator beibehalten kann. Wenn die Kennung des Benutzers der öffentliche Schlüssel wäre, der seinem privaten Schlüssel entspricht, würde er die Kontrolle über seine Kennung verlieren, wenn er das Gerät verlieren würde, auf dem der private Schlüssel gespeichert ist. Im Falle eines Geräteverlusts verwaltet der Controller-Vertrag eine Liste von Wiederherstellungsdelegierten, die dem Benutzer bei der Wiederherstellung seiner Identität helfen können. Diese Delegierten können Einzelpersonen wie ausgewählte Freunde und Familienmitglieder oder Institutionen wie Banken und Kreditgenossenschaften sein. Es ist ein Quorum von Delegierten erforderlich, damit der Benutzer seine Identität wiederherstellen und mit einem neuen Gerät verbinden kann.⁵⁶



Wachsende Bedenken hinsichtlich der Privatsphäre

Im April 2016 verabschiedete das Europäische Parlament die DSGVO, die die Sicherheit und den Datenschutz personenbezogener Daten in der EU verbessern soll und vorsieht, dass die Kontrolle über personenbezogene Daten beim Einzelnen liegt.

6. Bau eines Prototyps

Durch die Erstellung eines Prototyps wird das Konzept zum Leben erweckt. Der Wert eines funktionierenden Prototyps besteht darin, dass er den Beteiligten die Möglichkeit bietet, die im Konzeptentwurf getroffenen Annahmen ernsthaft zu hinterfragen und die Herausforderungen zu identifizieren, die angegangen werden müssen, damit sich das System ändert. Der Prototyp umfasst die fünf Interventionsschritte in der Reise des Reisenden, die den größten potenziellen Mehrwert des Known Traveler Digital Identity-Konzepts aufzeigen.

In diesem Kapitel werden die folgenden Elemente beschrieben:

1. Ein Überblick über fünf wichtige ausgewählte Interventionsschritte in der User Journey. 2. Eine detaillierte Beschreibung jedes Interventionsschritts. 3. Ein konzeptioneller Entwurf für die Technologiearchitektur.

Übersicht über die ausgewählten Interventionsschritte

Abbildung 11 zeigt die wichtigsten zur Demonstration ausgewählten Prozessschritte und veranschaulicht das Potenzial des Konzepts in verschiedenen Szenarien. Die in der Reiseplanungsphase demonstrierten Fähigkeiten veranschaulichen beispielsweise die Fähigkeit von Passagieren, nahtlos einen Reisegenehmigungsantrag über die bei Reisebuchungsaktivitäten erfassten Profilelemente der bekannten digitalen Identität des Reisenden zu initiieren. Es zeigt auch die entscheidende Maßnahme, bei der ein Passagier sein Profil als bekannter Reisender den Grenzbehörden sowohl bei der Ausreise als auch bei der Einreise lange vor dem Reisedatum vorlegt, was eine erweiterte Risikobewertung, Vorabgenehmigung und beschleunigte Bearbeitung vor Ort bei der Grenzkontrolle auslöst.

Tabelle 9 zeigt die wichtigsten Interventionsschritte der Reise des Reisenden in Verbindung mit den Kerntechnologiefunktionen, die den Prozess neu gestalten.

Abbildung 11: Übersicht ausgewählter Interventionsschritte

Abbildung 11: Übersicht ausgewählter Interventionsschritte

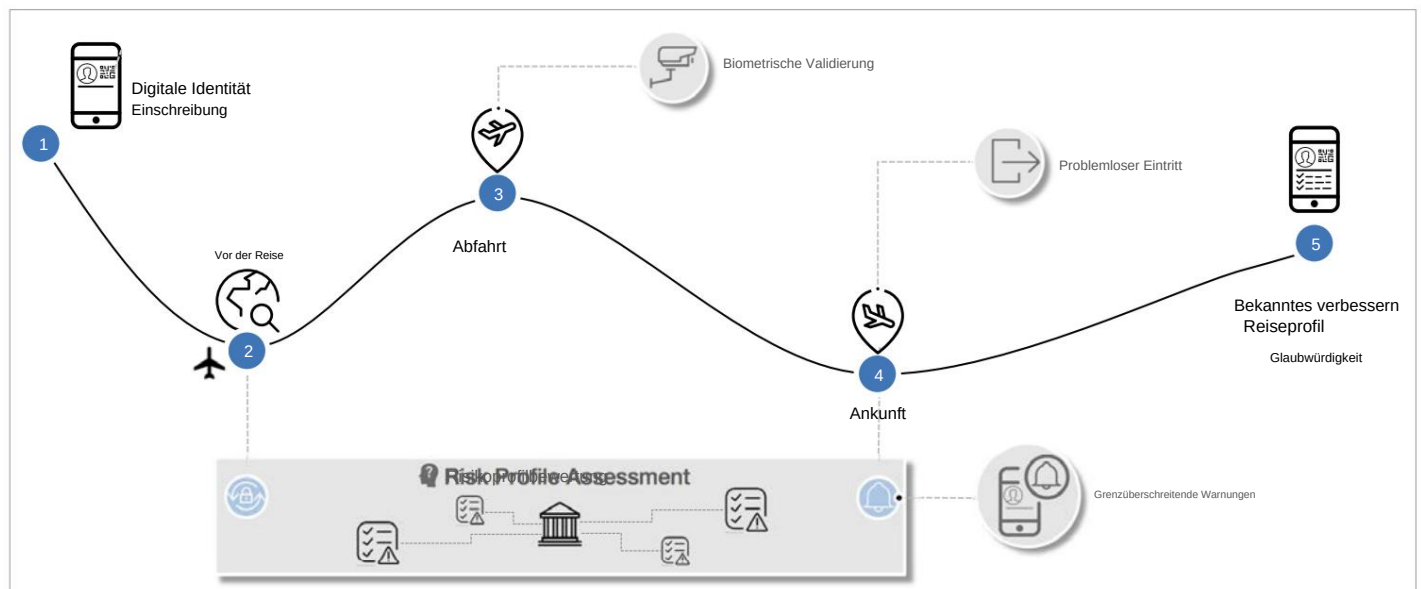


Tabelle 9: Übersicht der für den Prototyp berücksichtigten Interventionsschritte

Einschreibung	Vor der Reise	Abfahrt	Ankunft
Übersicht: Der Reisende lädt die Anwendung herunter und erstellt in der Anwendung ein digitales Identitätsprofil. Hierzu sind biografische und biometrische Informationen erforderlich. Technologiefähigkeit: Registrieren und überprüfen Sie die Identität und erstellen Sie eine digitale Identität, die dem Reisenden gehört.	Übersicht: Reisender bucht Flug bei der Fluggesellschaft. Bei der Eingabe der Identitätsinformationen bei der Buchung wird der Reisende aufgefordert, Informationen mit dem Abflug- und Zielland zu teilen, um die Grenzabwicklung zu beschleunigen. Sollte eine Reisegenehmigung erforderlich sein, wird der Reisende zu einer ETA-/Visumantragsseite weitergeleitet. Technologiefähigkeit: Weitergabe genauer und verifizierter Identitätsinformationen – einschließlich zusätzlicher Informationen wie Hotelreservierungen und vollständiger Reisehistorie – im Voraus, damit Regierungsbehörden vor der Reise eine Risikobewertung und Reisegenehmigung durchführen können.	Überblick: Der Reisende navigiert mithilfe nahtloser Identifikationstechnologie durch den Check-in und die Sicherheitskontrolle, die Ausreisekontrolle und die Tafeln. Technologiefähigkeit: Durch die Weitergabe vertrauenswürdiger biometrischer Identitätsinformationen an den Flughafen entfällt die Notwendigkeit, eine vorzulegen. Reisepass und Bordkarte und ermöglicht den Zugang zu beschleunigten Fahrspuren.	Überblick: Der Reisende durchläuft aufgrund der Vorkontrolle eine beschleunigte Einreisekontrolle. Beschleunigte Fahrspuren nutzen die nahtlose Identifikationstechnologie. Technologiefähigkeit: Durch die Weitergabe vertrauenswürdiger biometrischer Identitätsinformationen an einen Flughafen entfällt die Notwendigkeit, bei der Ankunft einen Reisepass zur Überprüfung der Identität vorzuzeigen. Durch die Vorabprüfung zuvor übermittelter Daten können sich die Behörden auf Reisende mit hohem Risiko konzentrieren.

Abbildung 12: Registrierung der digitalen Identität bekannter Reisender
Detaillierte Beschreibung der Interventionsschritte

Abbildung 12: Registrierung bekannter digitaler Identitäten von Reisenden

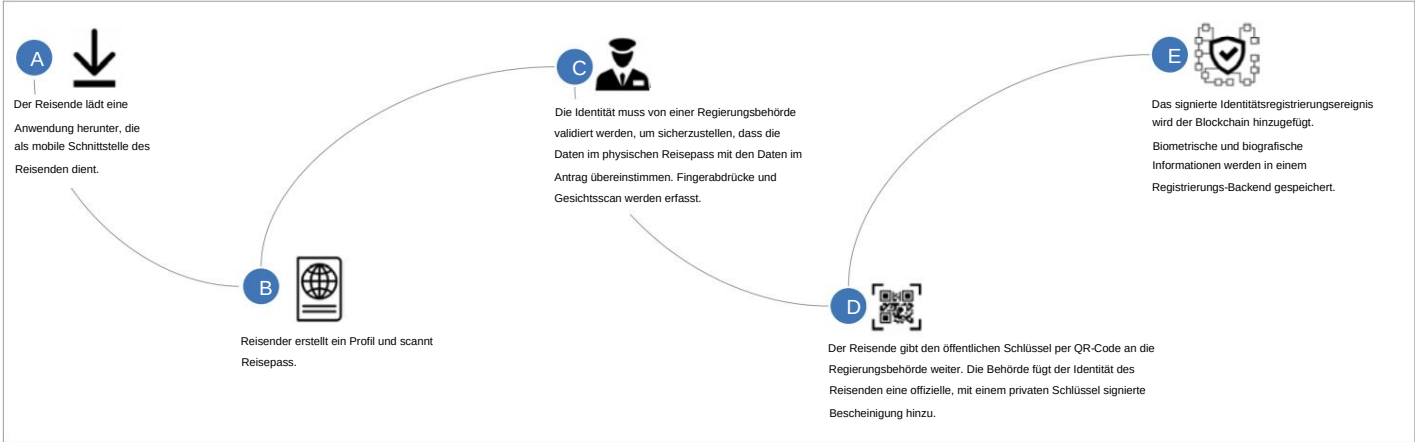


Abbildung 13: Vor der Reise: Buchung, Reisegenehmigung und Vorprüfung

Abbildung 13: Vor der Reise: Buchung, Reisegenehmigung und Vorprüfung

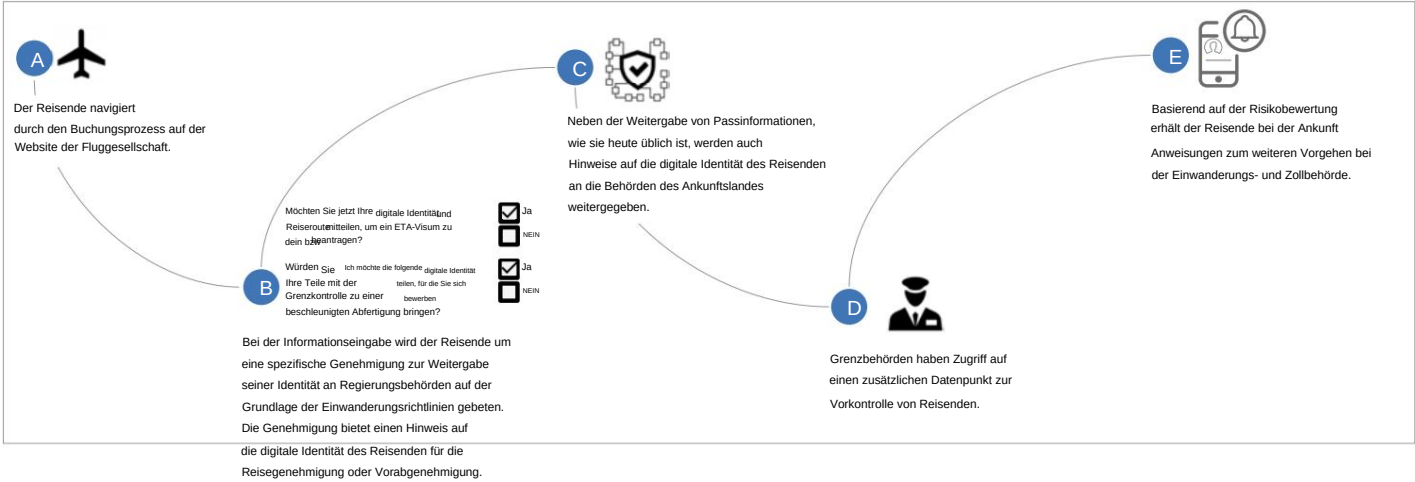


Abbildung 14: Abfahrt

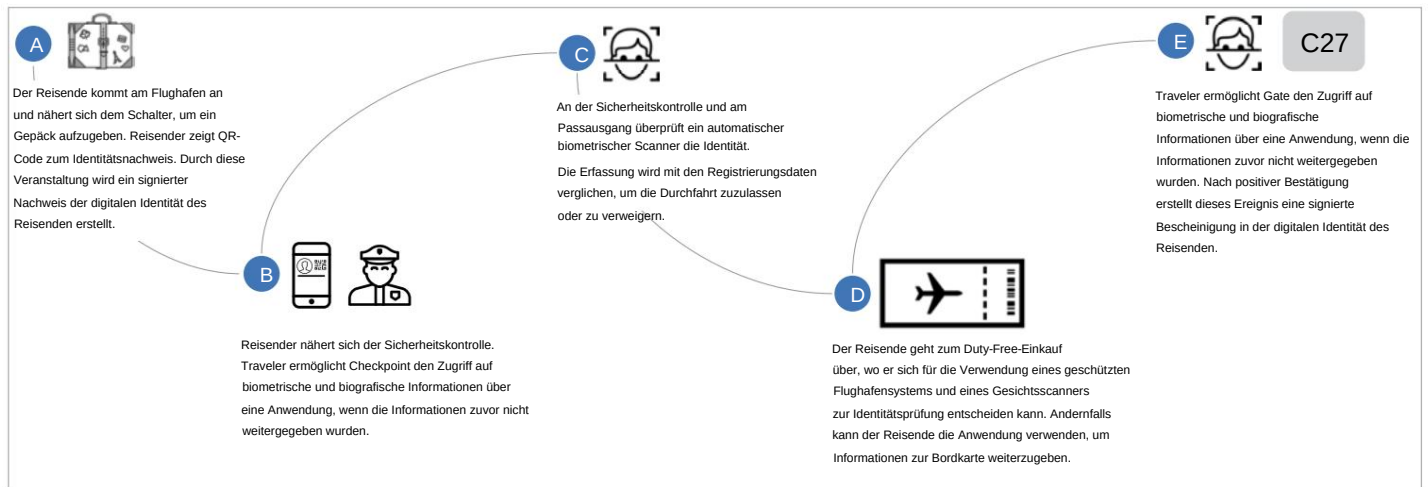


Abbildung 15: Ankunft

Abbildung 15: Ankunft

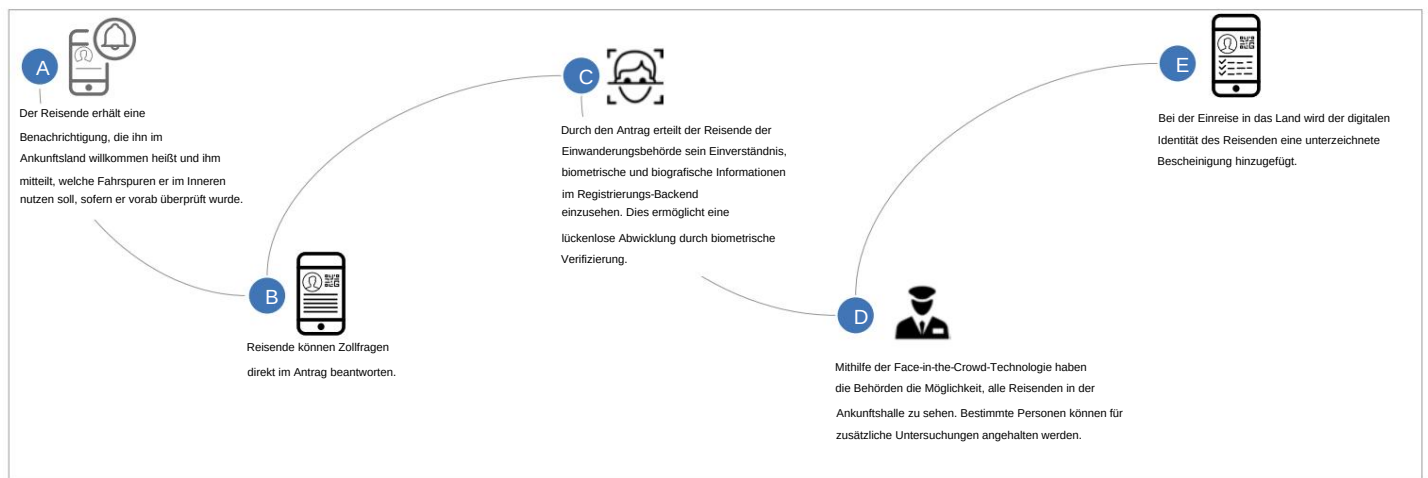
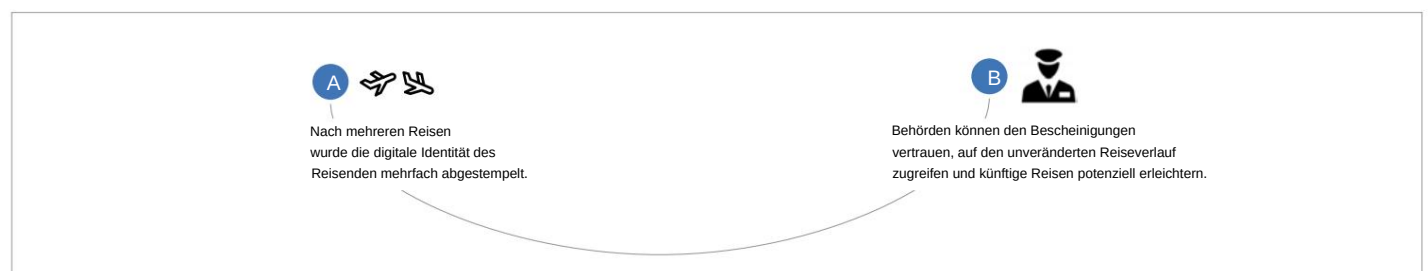


Abbildung 16: Verbesserung der Glaubwürdigkeit bekannter digitaler Identitätsprofile von Reisenden

Abbildung 16: Verbesserung der Glaubwürdigkeit bekannter digitaler Identitätsprofile von Reisenden

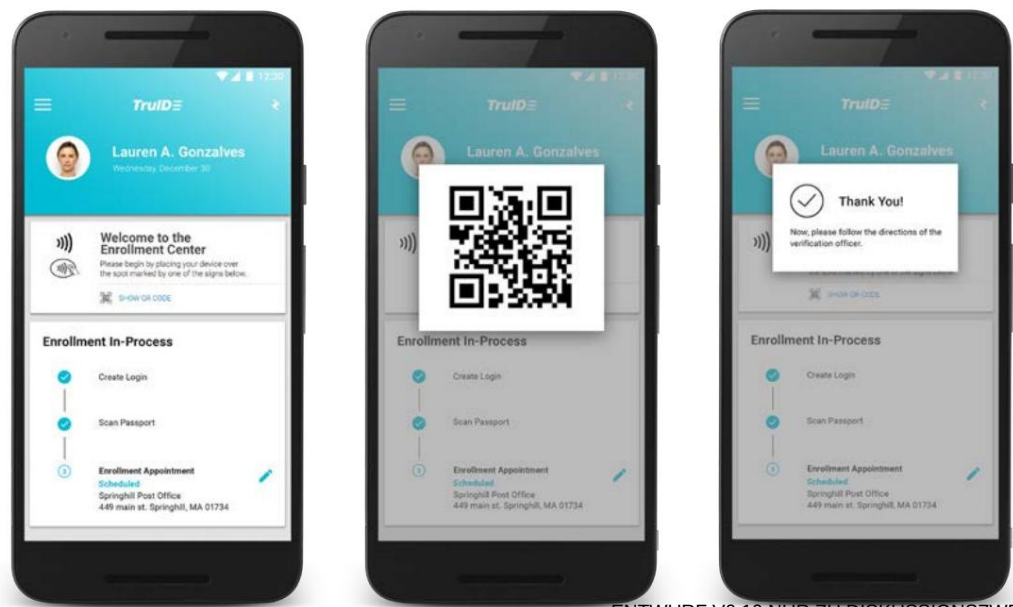


Eine anschauliche mobile Anwendungsoberfläche bietet eine konzeptionelle Reise durch den Registrierungsprozess. Abbildung 17 stellt den Standpunkt des Reisenden dar, während Abbildung 18 den Standpunkt einer Grenzbehörde darstellt. Weitere Details und Wireframes finden Sie in Anhang A.

ENTWURF V0.10 NUR ZU DISKUSSIONSZWECKEN

Abbildung 17: Perspektive des Reisenden auf der mobilen Schnittstelle

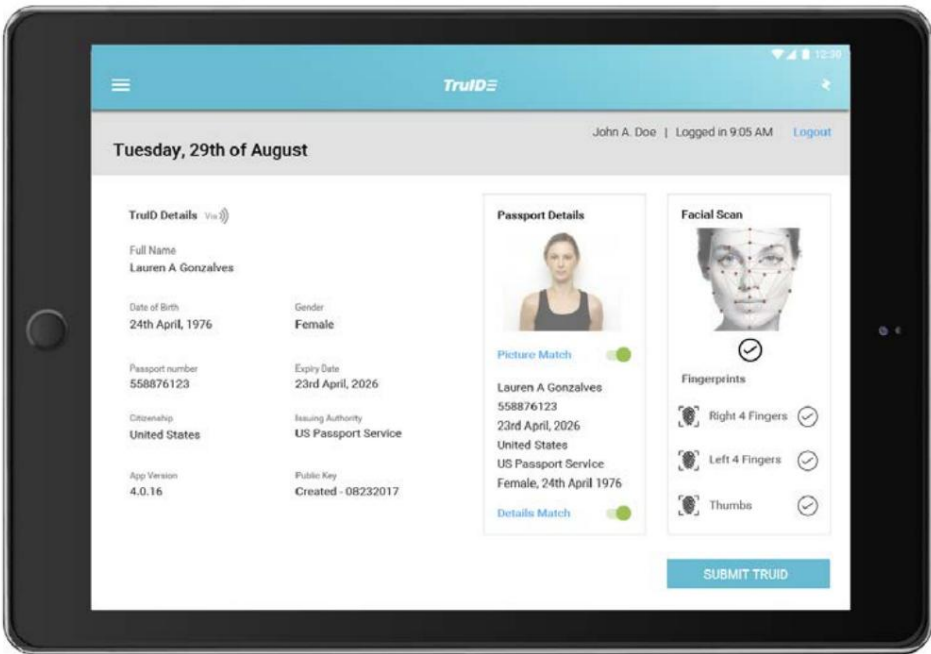
Abbildung 17: Perspektive des Reisenden auf der mobilen Schnittstelle



ENTWURF V0.10 NUR ZU DISKUSSIONSZWECKEN

Nahtlose und sichere Reiselösungen

Abbildung 18: Perspektive der Autorität der mobilen Schnittstelle



Nahtlose und sichere Reiselösungen

Konzeptioneller Entwurf der Technologiearchitektur

Der Prototyp nutzt alle vier Kerntechnologien – Distributed Ledger, Kryptographie, Biometrie und mobile Schnittstelle. Abbildung 19 zeigt den allgemeinen Entwurf des Prototyps. Der Prototyp ist zunächst nicht in der Lage, sich in Live-Produktionssysteme von Interessengruppen im Reiseökosystem (z. B. Regierungen, Grenzbehörden usw.) zu integrieren.

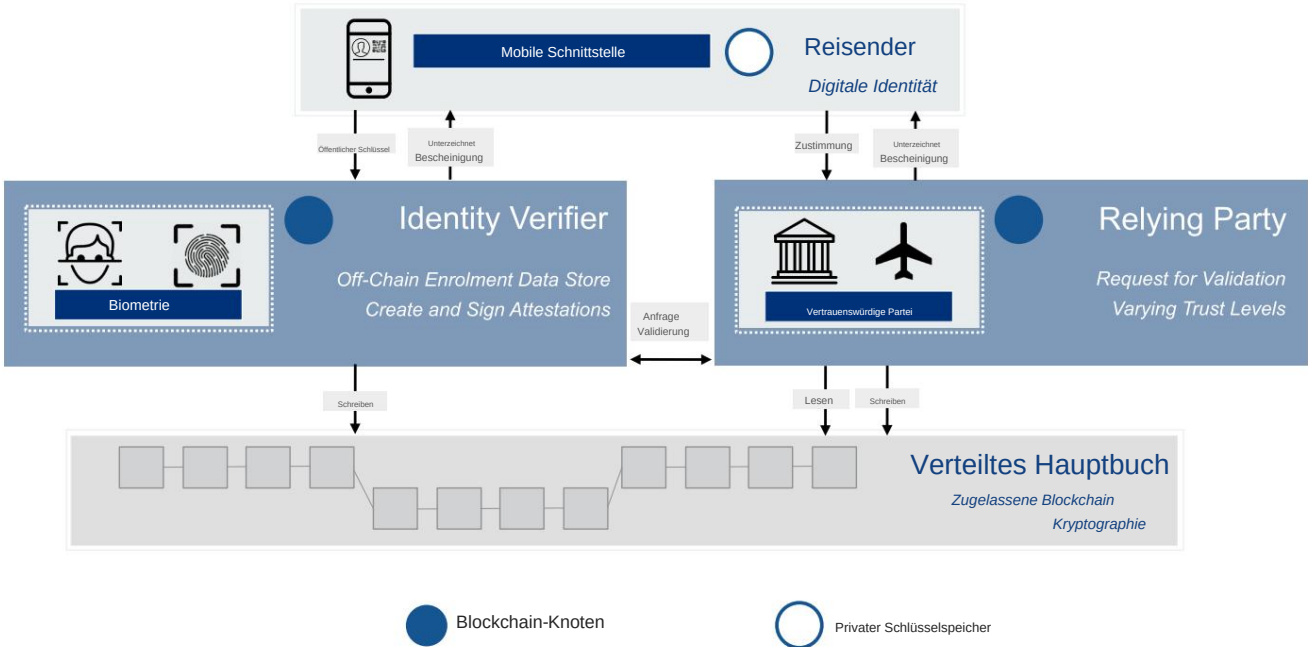
Daher ist es für die Verbindung mit Scheindatenquellen konzipiert, um den End-to-End-Prozess unter Verwendung der vier Kerntechnologien zu demonstrieren. Das Modell kann in Zukunft über die in diesem Prototyp beschriebenen Schritte hinaus auf andere Einheiten ausgeweitet werden (z. B. Hotels, Universitäten usw.).

ENTWURF V0.10 NUR ZU DISKUSSIONSZWECKEN

Die mobile Schnittstelle ist der private Schlüsselspeicher des Reisenden und speichert alle Attestierungen. Die Identität des Reisenden muss zunächst von der zuständigen Regierung (dem Identitätsprüfer) überprüft werden. Nach der Verifizierung wird die digitale Identität des Reisenden in einem Registrierungs-Backend erstellt, ein Identitätsnachweis zum verteilten Hauptbuch hinzugefügt und eine Bescheinigung zur digitalen Identität des Reisenden hinzugefügt. Anschließend kann der Reisende einer vertrauenden Partei die Einwilligung erteilen, seine Bescheinigungen einzusehen und zu validieren. Zu diesem Zweck kann die vertrauende Partei das Distributed Ledger mithilfe des gemeinsamen öffentlichen Schlüssels des Reisenden überprüfen und anschließend Identitätsinformationen vom Identitätsprüfer anfordern. Die vertrauende Partei kann dann Bescheinigungen zur Identität des Reisenden hinzufügen. Der Reisende zeigt den Beteiligten wichtige technologische Hindernisse auf und lädt zum Experimentieren ein, um nach Lösungen zu suchen und das Konzept aus technologischer Sicht zu verbessern. Darüber hinaus wird bei der Neubewertung die Machbarkeit des Prototyps für eine Ausweitung auf das breitere Ökosystem des öffentlichen und privaten Sektors bewertet.

Abbildung 19: Entwurf eines Prototyps auf hoher Ebene

Abbildung 19: Entwurf eines Prototyps auf hoher Ebene



7. Nächste Schritte: Testen und skalieren

Um das Konzept und den Prototyp einer vollständigen Umsetzung näher zu bringen, werden in einer Roadmap die Meilensteine aufgeführt, die die Beteiligten benötigen, um klein anzufangen und schnell zu wachsen (Abbildung 20).

Der Luftfahrt-, Reise- und Tourismussektor ist komplex, wobei jede Region, jedes Land und jede Agentur durch ihre eigenen nuancierten kontextuellen und politischen Implikationen gekennzeichnet ist. Während das Konzept davon ausgeht, dass sich ein globales interoperables System für von Passagieren kontrollierte digitale Identitäten positiv auf die Sicherheit im grenzüberschreitenden Reisen auswirken wird, wird es eine Vision bleiben, sofern es nicht für eine flächendeckende Umsetzung konzipiert und entwickelt wird. Als erster Schritt zur Prüfung der Eignung für Einführung und Wachstum werden nun die notwendigen institutionellen Beziehungen aufgebaut, um einen Machbarkeitsnachweis in einer sicheren „Laborumgebung“ und anschließend in einem Live-Pilotversuch zu testen.

Das erste Ziel besteht darin, den Prototyp mit tatsächlichen Drittsystemen im Ökosystem zu verbinden – nicht mit Live-Systemen, sondern nur mit Testumgebungen. In der Startphase wird das Ökosystem auf eine Reihe privater Akteure wie Technologieanbieter, Hotels und andere Dienstleister sowie Regierungsbehörden ausgeweitet. Sobald sich zeigt, dass das Known Traveler Digital Identity-Konzept in der Laborumgebung funktioniert, können Reisende und andere Interessengruppen das Konzept in einer Live-Pilotstudie testen. Die Pilotstudie sollte in einer Zone mit geringem Risiko, beispielsweise einem bestimmten Bereich eines Flughafens, für einen bestimmten Flug mit vorab überprüften Passagieren getestet werden.

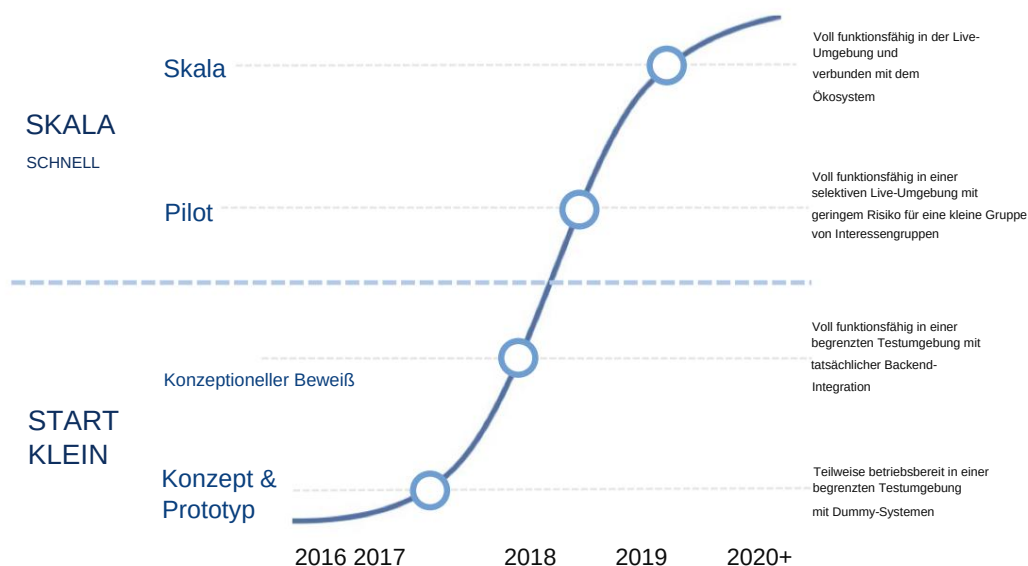
Für den Erfolg der Pilotstudie ist die bewusste Zusammenarbeit verschiedener Partner aus dem öffentlichen und privaten Sektor erforderlich.

„Technologieunternehmen haben große Fortschritte in den Bereichen Data Mining, maschinelles Lernen und künstliche Intelligenz gemacht, die eine verbesserte prädiktive Analyse ermöglichen. In Kombination mit von Passagieren bereitgestellten Informationen können diese Technologien von Regierungen genutzt werden, um ein nahtloseres, passagierzentriertes Erlebnis an Grenzen zu bieten und komplexe Muster in Big Data zu analysieren mit dem Ziel, Grenzsicherheitsrisiken vorherzusagen.“

Rob Torres, Geschäftsführer, Reisen, Google, USA

Es ist wichtig, dass führende Unternehmen des privaten Sektors in den Bereichen fortschrittliche Datenanalyse, Risikovorhersage, Datenschutz und Betrugsprävention ihr Fachwissen und ihre Innovationen mit dem öffentlichen Sektor teilen, um das Potenzial der Technologien zu demonstrieren. Gleichzeitig muss der Erfolg der Pilotstudie angemessen gemessen werden, während Erfolgshindernisse identifiziert und für zukünftige Iterationen angepasst werden. In den Jahren 2018–2019 wird das Weltwirtschaftsforum die Umsetzung eines geografisch begrenzten Pilotprojekts in Zusammenarbeit mit verschiedenen Interessengruppen (z. B. Regierungen, Flughäfen, Fluggesellschaften) erleichtern. Die kanadische Regierung hat gemeinsam mit dem Forum aktiv die Erprobung des Konzepts untersucht.

Abbildung 20: Roadmap, um klein anzufangen und schnell zu skalieren



Um eine Ausweitung zu ermöglichen, ist es von entscheidender Bedeutung, Netzwerkeffekte zu nutzen und die Anwendungsmöglichkeiten des Konzepts zu erweitern, um nicht nur Reisende, sondern auch den öffentlichen und privaten Sektor zur Teilnahme zu bewegen. Führungskräfte auf offizieller und politischer Ebene in verschiedenen Ministerien müssen bei der Unterstützung zusammenarbeiten Umsetzung des Konzepts auf zwischenstaatlicher Ebene und mit internationalen Organisationen wie INTERPOL, ICAO, WCO, dem UN-Hochkommissar für Flüchtlinge und der Internationalen Organisation für Migration. Es bedarf einer starken Zusammenarbeit mit der Reisebranche – einschließlich Fluggesellschaften, Reedereien, Hafenbetreibern, Gastgewerbe und anderen Reise- und Tourismusdienstleistern. Es bedarf außerdem eines vertrauenswürdigen Engagements des Privatsektors, um die effektivste Nutzung neuer und aufkommender digitaler Technologien und die Unterstützung der erforderlichen Transformation sicherzustellen.

Eine bekannte digitale Identität von Reisenden weist ein großes Potenzial für die Nutzung über das Reisen hinaus auf, beispielsweise im Gesundheitswesen, im Bildungswesen, im Bankwesen, in der humanitären Hilfe und bei Abstimmungen. Um das Konzept über gelegentliche grenzüberschreitende Reisen hinaus voranzutreiben, muss das Pilotprojekt die mit der Plattformökonomie verbundenen Netzwerkeffekte nutzen und den Nutzern das potenziell breite Spektrum des Alltags verdeutlichen Anwendungen. Bis 2020 soll das Known Traveler Digital Identity-Konzept über die Reise des Reisenden hinaus ausgeweitet und einem breiten Publikum zugänglich gemacht werden können, wobei eine breite Akzeptanz für den Erfolg des Konzepts von entscheidender Bedeutung ist.

Digitale Identität beim Weltwirtschaftsforum

Das Forum hat kürzlich in Zusammenarbeit mit Accenture eine Initiative gestartet, um ein Rahmenwerk für digitale Identitäten zur Nutzung über das Reisen hinaus zu entwickeln und die digitalen Identitäten von Menschen sowie unbelebten Objekten und Entitäten zu berücksichtigen.

Das Known Traveler Digital Identity-Konzept wird in die umfassenderen digitalen Identitätsstandards und -protokolle passen, die in diesem Forum-Projekt definiert wurden.

Decentralized Identity Foundation Decentralized

Identity Foundation (DIF) ist ein dezentrales Open-Source-Identitätsökosystem, das die dezentrale Identitätsgemeinschaft mit den Protokollen, Tools und Implementierungen ausstattet, die zum Erstellen und Validieren von Identitätsnachweisen erforderlich sind.

DIF fördert die Fähigkeit von Menschen, Organisationen und Maschinen, eine einzige Kennung zu haben, ähnlich den heutigen DNS-Einträgen für Computer. Ein Teil der Arbeit von DIF besteht darin, das Problem der „letzten Meile“ zu lösen, bei dem die Kennung mit dem Menschen (oder ähnlichen Merkmalen einer Sache) verknüpft wird. Mit diesen Funktionen interagieren Benutzer von Blockchain-basierten Systemen als eine einzige, konsistente Identität, mit der alle ihre Aktivitäten (Werte und Informationen) verknüpft und indiziert werden. Benutzer haben durch eine detaillierte Zugriffskontrolle für jede einzelne Information die Kontrolle darüber, wer auf ihre Informationen zugreifen darf. Gegenparteien des Nutzers können überprüfen, ob die Daten nicht manipuliert wurden, und die Bescheinigungen sowie die Herkunft ihrer Daten auswerten.⁵⁷



Empfehlungen

A. Handeln Sie jetzt

Pilotieren und iterativ entwickeln

Um die Machbarkeit des Known Traveller Digital Identity-Konzepts in einer realen Umgebung zu demonstrieren, müssen Interessenvertreter aus dem privaten und öffentlichen Sektor den Prototyp testen, iterative Entwicklungsmethoden anwenden, um seinen Wert zu demonstrieren, kontinuierliches Feedback von Interessenvertretern einholen und sich entsprechend anpassen. Ein iterativer Ansatz wird den notwendigen Paradigmenwechsel unter den Interessengruppen fördern und ein Umfeld für eine groß angelegte Einführung schaffen.

Implementierungspartner sollten den bereitgestellten Rahmen nutzen, um das Wertpotenzial für alle Beteiligten zu bewerten und sich auf Erfolgsmessungen zu einigen. Die Überprüfung des Fortschritts anhand dieser Messungen wird dabei helfen, herauszufinden, welche Komponenten des Konzepts weitere Aufmerksamkeit benötigen, wenn zugehörige Werttreiber eine unterdurchschnittliche Leistung erbringen. Darüber hinaus wird die objektive Demonstration des Werts des Known Traveler Digital Identity-Konzepts für mehrere Interessengruppen die Gründe für die Einführung untermauern.

Sorgen Sie für Inklusivität, um die Skalierbarkeit voranzutreiben

Zwischen den Ländern bestehen große Unterschiede in der Infrastruktur und den Ressourcen für die Grenz- und Reisesicherheit. Um die globale Skalierbarkeit zu beschleunigen, ist es unbedingt erforderlich, die Intervention in verschiedenen Kontexten mit unterschiedlichen Reisegruppen zu testen. Führungskräfte aus Industrie und Regierung sollten Pilotstudien an mehr Standorten initiieren, um sicherzustellen, dass die Tests eine angemessene Auswahl an Ländern, Regionen und Wirtschaftsniveaus umfassen. Um dies zu unterstützen, sollten Partner aus dem öffentlichen und dem privaten Sektor zusammenarbeiten, um ein Toolkit zu entwickeln, das Entscheidungsträgern die Möglichkeit gibt, zusätzliche Pilotprojekte zu starten.

Beobachten Sie kontinuierlich neue Entwicklungen

Für alle Beteiligten im öffentlichen und privaten Sektor ist es wichtig, neue technologische Durchbrüche und politische Überlegungen kontinuierlich zu überwachen und ihre Fähigkeit anzugeben, die Einhaltung der Designprinzipien voranzutreiben. Erwartet wird ein ständiges Spannungsverhältnis zwischen dem, was bereits gebaut wurde, und der „Passung“ mit neuen technologischen Lösungen. Insbesondere politischen Entscheidungsträgern wird empfohlen, bei ihrer Politikgestaltung Agilität beizubehalten, um auf regelmäßigem Lernen aufzubauen, ohne Fortschritt und Konvergenz zu gefährden.



B. Schwung aufbauen

Konzentrieren Sie sich auf reiseorientiertes Design, um die Akzeptanz zu beschleunigen. Reisende stehen im Mittelpunkt des Erfolgs des Known Traveler Digital Identity-

Konzepts. Stakeholder müssen die inneren Werte und Vorlieben des Reisenden für ein zweckmäßiges Konzept verstehen und den Reisenden die Vorteile der Einführung aufzeigen. Bei jeder technologischen oder politischen Entwicklung müssen die Beteiligten einen reisezentrierten Designansatz in Betracht ziehen, der letztendlich das Konzept der Known Traveler Digital Identity für die breitere Luftfahrt-, Reise- und Tourismusbranche attraktiver macht. Dies, gepaart mit gezielten Verhaltensänderungsstrategien, wird den Reisenden einen Anreiz bieten, aktive Partner bei der Gewährleistung der Sicherheit auf Reisen zu werden.

Entdecken Sie neue Geschäftsmodelle

Die Festlegung tragfähiger, nachhaltiger und vertrauenswürdiger Geschäftsmodelle zur Bereitstellung von Known Traveler Digital Identity-Funktionen und Infrastruktur-Upgrades kann den privaten und öffentlichen Sektor dazu bewegen, sich an der Förderung sicherer und nahtloser Reisen zu beteiligen. Es gibt immer mehr Möglichkeiten, digitale Identitätsdaten zu nutzen, nicht nur zur Verbesserung der Sicherheit, sondern auch zur Verbesserung des Serviceangebots. Darüber hinaus haben sich organisch neue Modelle zur Verwaltung und Authentifizierung von Online-Identitäten entwickelt. Innovationen können durch Komfort für den Kunden, Kosteneffizienz für Dienstleister und höhere Kapitalrendite durch neue Einnahmequellen für diejenigen Organisationen des öffentlichen und privaten Sektors vorangetrieben werden, die sich dafür entscheiden oder bereits in Identitätsmanagement investiert haben.

C. Aufrechterhaltung eines unterstützenden politischen Rahmens

Halten Sie Standards und empfohlene Praktiken ein

Um den exponentiellen Wert zu maximieren und eine kritische Masse von Benutzern zu erreichen, erfordert der Known Traveler Digital Identity-Prototyp Interoperabilität über Regionen, politische Umgebungen und Branchen hinweg. Branchenführer und Partner aus dem öffentlichen Sektor müssen einen technologieunabhängigen Ansatz verfolgen und einen anerkannten Rahmen offener Standards und Protokolle fördern. Um die bestehenden Rahmenbedingungen abzubilden, sollten die Beteiligten alle bestehenden Standards zusammenstellen, die die Verwendung persönlicher Identitätsdaten und relevanter Technologien im gesamten Reisesicherheitsumfeld regeln.

Wo Lücken bestehen, müssen die Beteiligten weiterhin die Führung bei neuen Denkanstätzen übernehmen und mit Agenturen zusammenarbeiten, die den Auftrag haben, Standards zu entwickeln und aufrechtzuerhalten, um eine angemessene Entwicklung sicherzustellen.

Entwickeln Sie erweiterte Risikoprofile, um den Sicherheitsprozess zu beschleunigen.

Da der

Reisende dazu neigt, mehr Informationen als Teil seiner digitalen Identität weiterzugeben, stehen Daten für die Analyse auf einer detaillierteren Ebene zur Verfügung und ermöglichen erweiterte Datenanalysen zur Sicherheitsüberprüfung und Personalisierung. Durch das Erkennen von Mustern, das Erkennen von Zusammenhängen und den Einsatz fortschrittlicher Algorithmen können Agenturen detaillierte Erkenntnisse über den Reisenden gewinnen. Ein detailliertes Risikoprofil einer Person ermöglicht es den Behörden beispielsweise, diesen Reisenden zur intensivierten Kontrolle auf eine bestimmte Sicherheitskontrolle zu leiten. Dies kann den Sicherheitsvorgang für die meisten Reisenden beschleunigen, da

Die wahrgenommene Bedrohung wird gezielt von der vorab überprüften Fahrspur mit geringem Risiko entfernt. Das Aufkommen von künstlicher Intelligenz und maschinellem Lernen erweitert die Möglichkeiten, von individuellen Identitätsinformationen zu profitieren. Interessengruppen in der Finanzdienstleistungs-, Versicherungs- und Technologiebranche sind gut positioniert, um Best Practices für die Datenanalyse und Risikomodellierung von Identitäten zu entwickeln, die mit Regierungsbehörden zur Anpassung an deren staatliche Risikobewertungsprozesse geteilt werden könnten.

Priorisieren Sie Datenschutz und Cybersicherheit

Datenschutz- und Cybersicherheitsaspekte stehen weiterhin im Vordergrund aller Interessen aller Beteiligten. Akteure aus dem privaten und öffentlichen Sektor müssen die hohe Integrität der vorgeschlagenen Sicherheitsrahmen und technologischen Konzepte sicherstellen.

Es muss darüber nachgedacht werden, wie das System die gesetzlichen Anforderungen für das Identitätsmanagement in allen Ländern einhält bzw. erfüllt und die Genehmigung von Datenschutzaufsichtsbehörden erhält. Darüber hinaus ist es von entscheidender Bedeutung, dass die Sicherheitsfunktionen denjenigen, die sie in Anspruch nehmen, ordnungsgemäß kommuniziert werden – insbesondere den Reisenden, die den Systemen ihre privaten, persönlichen Daten anvertrauen.

Danksagungen

Das Weltwirtschaftsforum möchte die vielen wertvollen Beiträge zu dieser Arbeit durch Expertenwissen, Interviews und Forschung würdigen. Das Forum würdigt insbesondere die wertvolle Beteiligung der Mitglieder der Arbeitsgruppe „Zukunft der Sicherheit im Reiseverkehr“.

Arbeitsgruppe „Zukunft der Sicherheit im Reiseverkehr“.

Nigel Aston, Senior Adviser, Unternehmensstrategie, Amadeus, Spanien

Isabelle Barnett, Senior-Projektmanagerin, I-Checkit, Internationale Kriminalpolizeiliche Organisation (INTERPOL), Frankreich

Alain Berinstain, Direktor für Politik, Abteilung für Transport von Kanada, Kanada

Nina Brooks, Sicherheitschefin, Airports Council International (ACI), Kanada

Céline Canu, Managerin, Passagier- und Moderationsabteilung, International Air Transport Association (IATA), Kanada

Boubacar Djibo, Direktor, Lufttransportbüro, Internationale Zivilluftfahrt-Organisation (ICAO), Kanada

Melissa Flood, Vizepräsidentin, Social Impact und Public Angelegenheiten, Marriott International, USA

Todd Fox, Vizepräsident, Public Policy, Visa Inc., USA

Matt Hayden, Stellvertretender stellvertretender Sekretär (kommissarisch), Privatmann Sektorbüro, Heimatschutzministerium, USA

Isabel Hill, Direktorin, Nationales Reise- und Tourismusbüro, USA Handelsministerium, USA

Jürgen Keitel, Leiter Globale Angelegenheiten und Entwicklung Offizier, AirAsia, Malaysia

Rob Leslie, Chief Executive Officer, Sedicii, Irland

Muriel Leveque, Vizepräsidentin Safety Group, AccorHotels, Frankreich

Helen Marano, Senior-Vizepräsidentin der Regierung und Branchenangelegenheiten, World Travel and Tourism Council, United Königreich

Noriko Morimura, Global Business Unit, Transport City Infrastrukturabteilung, NEC Corporation, Japan

Jonas Neihardt, Senior-Vizepräsident, Regierungsangelegenheiten, Hilton Worldwide, USA

Michael O'Connell, Leiter des Nationalen Geheimdienstes – IOCCC, UK National Crime Agency, Vereinigtes Königreich

Cheryl Rutenberg, Leiterin, Partnerschaftsentwicklung, Visa Inc., USA

Charlie Sultan, Senior Vice-President, Supplier Services, Concur Technologies, USA

Rob Torres, Geschäftsführer, Travel, Google Inc., USA

Masakazu Yamashina, Senior Vice-President, NEC Corporation, Japan

Serge Yonke Nguewo, Senior Manager, Moderation und IT, Airports Council International (ACI), Kanada

Accenture (Berater und Wissenspartner)

Liselotte de Maar, Geschäftsführerin, Strategie, Reisen Industrie, Accenture, Niederlande

Rajeev Kaul, Geschäftsführer und Master Technology Architekt, Accenture, USA

Unser Dank gilt dem engagierten Team von Accenture, darunter Brian Goldman, Marc Bonnet, Durgesh Das und Daniel Bachenheimer, die maßgeblich zu dieser Arbeit beigetragen haben.

Projektteam des Weltwirtschaftsforums

John Moavenzadeh, Leiter Mobility Industries und Systeminitiative, World Economic Forum LLC

Lauren Uppink Calderwood, Lead, Safe and Secure Mobilität, World Economic Forum LLC

Mary Loane, Wissensspezialistin, Mobilitätssystem Initiative, World Economic Forum LLC

Jorn van Wijnen, Projektmitarbeiter, Zukunft der Sicherheit in Reiseprojekt (sekundiert von Accenture Strategy)

Weitere Informationen zu diesem Bericht oder der Arbeit des Weltwirtschaftsforums zur Zukunft der Sicherheit in Anreise, Kontakt:

Lauren Uppink Calderwood

Führende, sichere und geschützte Mobilität Initiative „Zukunft des Mobilitätssystems“. Weltwirtschaftsforum LLC

Lauren.uppink@weforum.org

Tel.: +1 212 703 2325

Anhang A

Mobile Anwendungsdesigns für den Registrierungsprozessschritt (Frontend)

Der Reisende kommt an einer Registrierungsstation an und scannt den QR-Code.



Per QR-Code teilt der Reisende Passinformationen mit, die auf dem Bildschirm des Beamten angezeigt werden.



Der Einschreibungsbeamte scannt den Reisepass des Reisenden Scanner.

Passchip wird gelesen; Die Daten und das Foto werden an die gesendet Bildschirm.



Der Registrierungsbeamte scannt die biometrischen Daten des Reisenden (z. B. Gesicht).

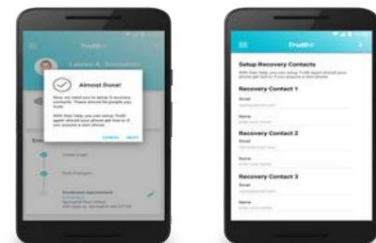
Der biometrische Abgleich vergleicht das gescannte Gesicht mit dem Foto vom Passchip.

Außerdem werden die Passdaten des Reisenden mit der registrierten Identität abgeglichen.

Ein Registrierungsbeamter scannt die Fingerabdrücke des Reisenden.



Der Reisende kann Wiederherstellungskontakte einrichten, die gebeten werden könnten, ihre Identität zu überprüfen, wenn der Reisende ein neues Telefon erhält (oder wenn sein Telefon gestohlen wird).



Der Reisende ist nun vollständig registriert und kann Dritten Zugriff auf seine Identität gewähren, was ein sichereres und nahtloseres Erlebnis ermöglicht.



Endnoten

1 UNWTO. UNWTO-Welttourismusbarometer – Fortschritt
Veröffentlichung Januar 2017. UNWTO. [Online] Januar 2017. [Zitiert: 18. Oktober 2017.] http://cf.cdn.unwto.org/sites/all/files/pdf/unwto_barom17_01_january_excerpt_.pdf. Es wird erwartet, dass sich der Flugverkehr insgesamt von 3,8 Milliarden Flugreisenden im Jahr 2016 auf 7,2 Milliarden Flugreisende im Jahr 2035 verdoppeln wird. IATA <http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx>

2 Gillen, David und Morrison, William. Luftsicherheit: Kosten, Preise, Finanzen und Leistung. sl Elsevier, 2015.

3 Im Allgemeinen wird die weltweite Reisebewegung von Personen nach lokal oder grenzüberschreitend (national oder international), Art (Land, Schiff und Luft) und Zweck (Geschäft oder Freizeit) aufgeschlüsselt. Dieser Bericht konzentriert sich auf internationale Flugreisen für alle Zwecke.

4 UNWTO. UNWTO World Tourism Barometer – Januar 2017. UNWTO. [Online] Januar 2017. [Zitiert: 18. Oktober 2017.]

5 Ebenda.

6 Ebenda.

7 WTTC. Global Economic Impact & Issues 2017. sl World Travel & Tourism Council, 2017.

8 Accenture. Bericht über globale Trends im Grenzmanagement. sl Accenture, 2016.

9 Gillen und Morrison. Luftfahrt Sicherheit.

10 Ebenda.

11 Accenture. Bericht über globale Trends im Grenzmanagement.

12 Gillen und Morrison. Luftfahrt Sicherheit.

13 Weltwirtschaftsforum, Incredible India 2.0, Oktober 2017.

14 TTG Asien. Flughafenkapazität begrenzt Wachstum der Ankünfte in Asien. TTGnordic.com. [Online] TTG, März 2016. <http://ttgnordic.com/Flughafenkapazitätsgrenzen-Asien-Ankunftswachstum/>

15 Es wird davon ausgegangen, dass sich die Reise des Reisenden von der Erfahrung des Grenzüberttritts auf dem Land- oder Seeweg unterscheidet.

16 Weltwirtschaftsforum. Initiative zur digitalen Transformation: Luftfahrt-, Reise- und Tourismusbranche. Genf: Weltwirtschaftsforum, 2017. REF 060117.

17. Weltwirtschaftsforum. Die vierte industrielle Revolution, was sie bedeutet und wie man darauf reagiert. sl Weltwirtschaftsforum, 2016.

18 Der für Flughäfen auf dem Spiel stehende Wert wird als begrenzt angesehen, da ein großer Teil der Sicherheitsmaßnahmen am Flughafen stattfindet, jedoch in der Verantwortung anderer Stellen wie Fluggesellschaften und Regierungen liegt.

19. Weltwirtschaftsforum. Initiative zur digitalen Transformation.

20 Weltwirtschaftsforum. Digitale Grenzen. sl Weltwirtschaftsforum, 2016.

21 Workshop zur Zukunft der Sicherheit im Reiseverkehr. Amsterdam: Accenture, 2017. Nachbesprechung der Arbeitsgruppensitzung am 9. Juni in San Francisco.

22 Weltwirtschaftsforum, Accenture Strategy. Die Zukunft der Sicherheit im Reisen gestalten: Auswahl technologischer Interventionen für Prototypen. Amsterdam: Accenture, August 2017. Entwurf eines Diskussionsdokuments für das Weltwirtschaftsforum.

23 DIF. Identitätsstiftung. [Online] Decentralized Identity Foundation , 2017. <http://identity.foundation/>

24 WCO/IATA/ICAO-Richtlinien zur erweiterten Passagierinformation (API), WCO/IATA/ICAO, 2013.

25 Weltwirtschaftsforum. Initiative zur digitalen Transformation.

26 UNWTO, WTTC. Die Auswirkungen der Visaerleichterung auf die Schaffung von Arbeitsplätzen in den G20-Volkswirtschaften. sl Welttourismusorganisation und World Travel & Tourism Council, 2012. Bericht erstellt für das 4. T20-Ministertreffen Mexiko, 15.–16. Mai 2012.

27 Weltwirtschaftsforum, Accenture Strategy. Gestaltung die Zukunft der Sicherheit im Reisen: Value Tree. Juli 2017. Entwurf eines Diskussionsdokuments für das Weltwirtschaftsforum.

28 Jagers, Chris. Digitale Identität und die Blockchain: Selbstsouveränität ist kein Selbstläufer; Es muss explizit in jede Blockchain-basierte soziale Infrastruktur integriert werden. medium.com. [Online] learningmachine.com, 16. Juli 2017. <https://medium.com/learning-machine-blog/digital-identity-and-the-blockchain -10de0e7d7734>

29 Lewis, Antony. Eine sanfte Einführung in die selbstsouveräne Identität. Bits auf Blöcken. [Online] 17. Mai 2017. [Zitiert: 18. Oktober 2017.] <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/>

30 Grassi, Paul, Garcia, Michael und Fenton, James. Richtlinien zur digitalen Identität. seiten.nist.gov. [Online] Juni 2017. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

31 Europäischer Datenschutzbeauftragter. Notwendigkeit und Verhältnismäßigkeit. Europäischer Datenschutzbeauftragter. [Online] 29. März 2017. [Zitiert: 1. November 2017.] https://edps.europa.eu/datenschutz/unsere-arbeit/subjekte/necessity-proportionality_de

32 Lundkvist, Christian et al. Uport: Eine Plattform für selbstsouveräne Identität. sl UPORT, 2017.

42 Der bekannte Reisende

- ³³ Tobin, Andrew und Reed, Drummond. Der unvermeidliche Aufstieg der Selbstsouveränität. sl The Sovrin Foundation, sovrin.org, 2016. und ID2020. Warum digitale Identität? ID2020.org. [Online] ID2020, 2017. <http://id2020.org/digital-identity-1>
- ³⁴ DIF. Identitätsstiftung. [Online] Decentralized Identity Foundation, 2017. <http://identity.foundation/>
- ³⁵ Weltwirtschaftsforum. Initiative zur digitalen Transformation.
- ³⁶ IBM. Schneller Vorlauf: Unternehmen, Ökosysteme und Volkswirtschaften mit Blockchains neu denken. sl IBM Institute for Business Value, 2016.
- ³⁷ Bitsonblöcke. Eine sanfte Einführung in die selbstsouveräne Identität. botsonblocks.net. [Online] Bits on Blocks, Mai 2017. <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-souverän-identity/>
- ³⁸ RIA. Datenaustauschschicht X-Road. ria.ee. [Online] Republik Estnische Informationssystembehörde, 2017. <https://www.ria.ee/de/x-road.html>
- ³⁹ Credits. Terminologie. Credits.readthedocs.io. [Online] 2017. http://credits.readthedocs.io/en/latest/blockchain_terms.html – Distributed-Ledger-Technologie
- ⁴⁰ Lewis, Antony. Was ist der Unterschied zwischen einem Distributed Ledger und einer Blockchain? Bits on Blocks [Online] 20. Februar 2017. [Zitiert: 29. November 2017] <https://bitsonblocks.net/20.02.2017/Was-ist-der-Unterschied-zwischen-einem-verteilten-Ledger-und-einer-Blockchain/>
- ⁴¹ IDC. Es war nur eine Frage der Zeit: Digitale Identität auf Blockchain. [Online] 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GIL12346USEN&>
- ⁴² Hase, Stephanie. HBR: Blockchain könnte uns helfen, die Kontrolle über unsere persönlichen Daten zurückzugewinnen. blog.accenture.com. [Online] Accenture, 5. Oktober 2017. https://blog.accenture.com/stephanie_hare/2017/10/05/hbr-blockchain-could-help-us-reclaim-control-of-our-personal-data/
- ⁴³ Buchner, Daniel et al. Dezentrale Identität/Hubs. Github. com. [Online] Github, 26. Juli 2017. <https://github.com/dezentralisierte-identität/hubs/blob/master/explainer.md>
- ⁴⁴ Lundkvist, Christian et al. Uport: Eine Plattform für selbstsouveräne Identität.
- ⁴⁵ Mattila, Juri. Das Blockchain-Phänomen – Das disruptive Potenzial verteilter Konsensarchitekturen. Berkeley Roundtable on the International Economy, University of California, Berkeley: ResearchGate, 2016., und Windley, Phil. Ist Sovrin dezentralisiert? Windley.com. [Online] 2017. http://www.windley.com/archives/2017/09/is_sovrin_decentralized.shtml
- ⁴⁶ Tobin, Andrew und Reed, Drummond. Der unvermeidliche Aufstieg der Selbstsouveränität. sl The Sovrin Foundation, sovrin.org, 2016.
- ⁴⁷ RIA. Public-Key-Infrastruktur-PKI. RIA.ee. [Online] Republik Estland, Informationssystembehörde, 18. April 2017. <https://www.ria.ee/en/public-key-infrastructure.html>
- ⁴⁸ O'Higgins, Conor. Digitale Identität Teil II – Identitätsnachweis. Criptoinsider.com. [Online] 2017. <https://cryptoinsider.21mil.com/digital-identity-part-ii-proof-personhood/>
- ⁴⁹ Reed, Drummond et al. DID-Datenmodell (Decentralized Identifier) und generische Syntax 1.0 Implementer's Draft 01. Github. com. [Online] November 2016. <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/did-implementer-draft-10.md>
- ⁵⁰ IDC. Es war nur eine Frage der Zeit: Digitale Identität auf Blockchain. [Online] 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GIL12346USEN&>
- ⁵¹ O'Higgins, Conor. Digitale Identität Teil II – Identitätsnachweis.
- ⁵² NIST. Gesichtserkennungsalgorithmen übertreffen Menschen. sl: NIST, 2016.
- ⁵³ Accenture. Bürgerunterstützung für die Verwendung biometrischer Daten Technologien zur Erleichterung des Reisens und zur Sicherung der Grenzen. sl: Accenture, 2014.
- ⁵⁴ NIST. Biometrie. 2017. <https://www.nist.gov/programs-projects/biometrie>
- ⁵⁵ Jagers, Chris. Digitale Identität und die Blockchain.
- ⁵⁶ Lundkvist, Christian et al. Uport: eine Plattform für selbstsouveräne Identität.
- ⁵⁷ DIF. Identitätsstiftung.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Das Weltwirtschaftsforum, das sich
der Verbesserung des
Zustands der Welt verschrieben
hat, ist die Internationale
Organisation für öffentlich-private Zusammenarbe

Das Forum bringt die führenden
politischen, wirtschaftlichen und anderen
Führungspersönlichkeiten der Gesellschaft
zusammen, um globale, regionale
und industrielle Agenden zu gestalten.

Weltwirtschaftsforum
91–93 Route de la Capite
CH-1223 Köln/Genf
Schweiz

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org