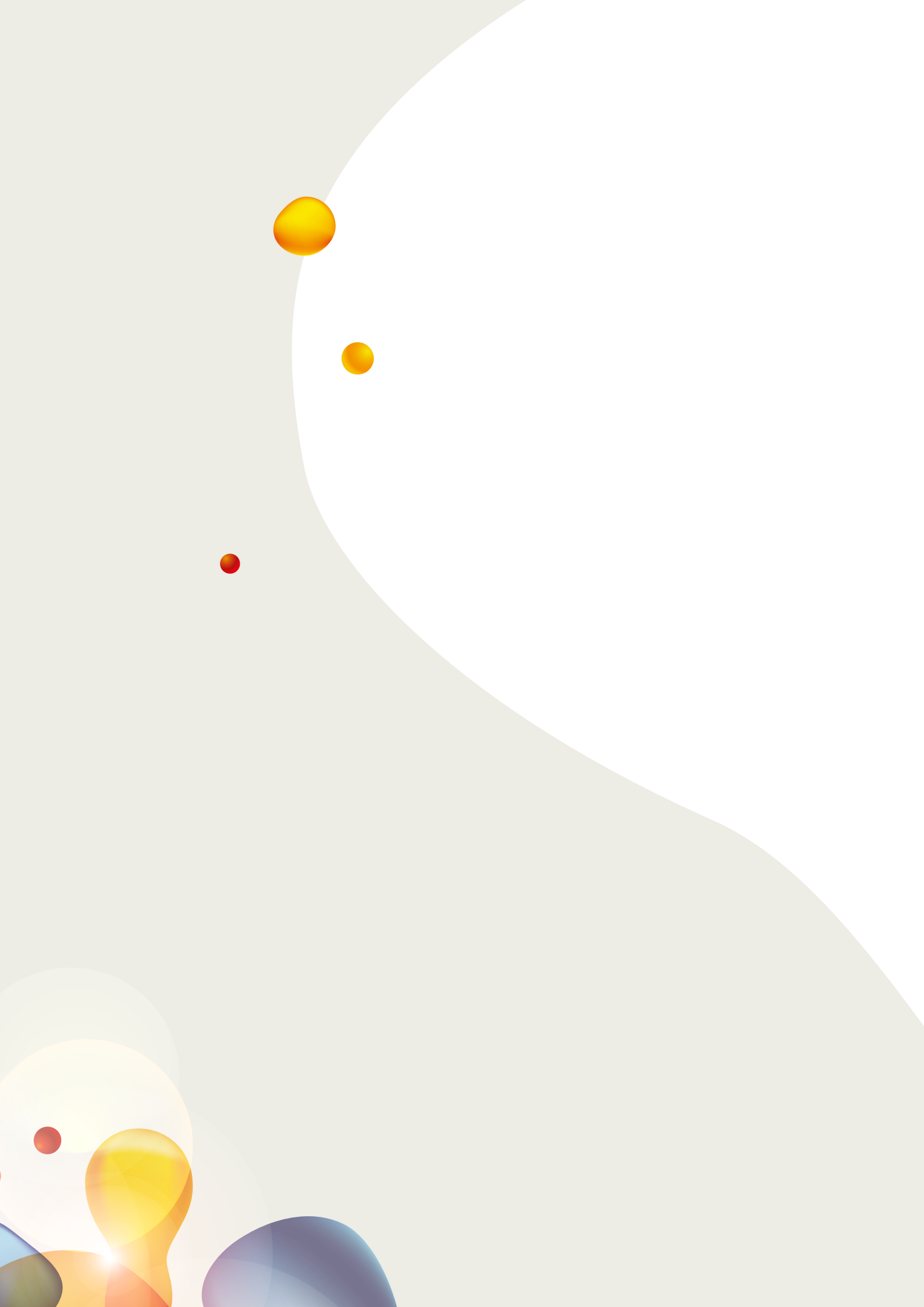
TRAVEL IDENTITY OF THE FUTURE

WHITE PAPER

ShoCard

SITA

Create success. Together



CONTENTS

INTRODUCTION

With the use of a mobile app and facial recognition, travelers need to be only identified once and can be quickly verified by non-affiliated airlines, airports or other agencies. Travelers' data is kept private with them on their phone and only shared with their permission. Their data can be authenticated by other airlines using blockchain technology securely and without compromising traveler privacy of information

SITA, *The world's leading specialist in air transport communications and information technology.*

In partnership with **ShoCard**, **Inc.**, *Identity Management on the blockchain.*

The purpose of this document is to describe the SITA Digital Traveler Identity App, which has been jointly developed by SITA and ShoCard, and the processes and technology it implements.

This demo application provides a starting point for engaging air transport industry stakeholders and drives the conversation on how a persistent, secure and interoperable Single Travel Token, based on biometrics (facial recognition), could be implemented. The demo application does not solve all the problems involved with biometric-based travel token, but it demonstrates the possibilities for using mobile and blockchain technologies in providing a unified identification experience for a traveler across multiple airports traveling on numerous airlines, across different countries. This demo uses the backend services from ShoCard, a company focused on identity management on the blockchain.

OVERVIEW

The future of air travel will depend on traveler convenience and the security of knowing who is passing through each point of travel process. Travel security should not be an inconvenience to a traveler across different airports and airlines. In fact, this technology will enhance the travel experience while improving security. Travelers will be able to easily go through checkpoint after checkpoint with digital identity verification, having the confidence that fellow travelers going through the same checkpoints are who they claim to be.

To enable this process, travelers will be granted a travel token embedded within their mobile app that also contains their identity. This information is certified by an agent or an automated kiosk during a registration process and the digitally signed validation hashes are written to the public blockchain.

A traveler can present the information from their mobile app to agents from different airlines or to airport security. The agent can then validate the authenticity of the traveler's identity and their travel token via the blockchain without accessing any proprietary databases or private data not required for each transaction.

EMERGENCE OF DIGITAL IDENTITY

Since the availability of the internet for the masses, digital identity has been key for allowing individuals to interact with service providers. In the early 1990s, this was largely managed through username and passwords. Today, with the prominence of mobile devices, individuals can increasingly use their digital credentials in both the digital and physical worlds. While there have been advances in improving digital identity, there remains a focus on strengthening the digital identification process of individuals across many industries. Digital identification is not only a trend in the air travel industry, but a strong emerging theme in the financial, health-care, enterprise and even emerging industries such as the Internet of Things (IoT).

Increasingly, financial institutions and FinTech (Financial Technology) companies are focusing on digital identity as banking moves from bricks-and-mortar to mobile and digital banking. With the absence of in-person verification of individuals, digital identification becomes more important in order to prevent fraud. Furthermore, new trends in FinTech are emerging that embrace shared identification of individuals across multiple financial entities. As digital identity evolves in different industrials, consumer expectations will equally increase in the manner by which they expect to consume services in other industries.

In parallel, new technologies are fast evolving, enabling new solutions that were simply not possible before. Perhaps one of the most disruptive technologies evolving today is the blockchain. The blockchain initially emerged as the underlying infrastructure that enables the Bitcoin virtual currency but is now being embraced by the broader tech industry as a game-changing technology.

When it comes to digital identification across disparate entities, the combination of the blockchain, mobile technologies and biometrics offers unique possibilities that simply didn't exist before. Many service providers can benefit from a federated identification system that does not require users to trust a third party with their private information. Individuals can then use their identification credentials for ease of access and improved service across air travel, hospitality, financial and banking interactions.

LIMITATION OF STATIC IDENTITY SOLUTIONS SUCH AS ePASSPORTS

Standardization and evolving technologies have improved identification for global travel.

Sometimes, simple changes go a long way. For example, the introduction of Machine Readable Zone (MRZ) on passports has enabled machines to quickly and easily scan and process passports. There are other new emerging technologies that will further ease the process and improve security.

For example, with ePassports, not only will passport information be available digitally, but individual biometrics can also be digitally embedded within a physical passport book.

However, these solutions, while improving existing identification methods, are limited since they are static in nature. An ePassport contains biometrics and passport information and cannot be extended with dynamic meta-data associated with the traveler. For example, there is no way to securely embed certifications for the identity of the individual such as a travel token, loyalty points, or other attributes that could be used by other global service providers to enhance a traveler's experience or to improve security. An ePassport will necessarily require a second form of documentation such as separate boarding pass or travel authorization.

THE SITA TRAVELER EXPERIENCE

The SITA-enabled Digital Traveler Identity App (Traveler App) demonstrates how using the technology described above can ease a traveler's journey through different airports and airlines using a single identity.

Once the traveler has booked their trip, they download the Traveler App, scan their passport and take a self-portrait (selfie). Later when checking-in at the airport – either at an automated kiosk or with an airline agent – the traveler then securely presents their information, via the Traveler App with a Quick Response (QR) code. At this point, the traveler may be asked to present their physical passport and other booking information for additional verification purposes. If at a kiosk, a new image is taken for facial comparison with the selfie or the agent can verify the selfie against the traveler in their presence. If the traveler's identity is confirmed, the Digital Traveler Identification is certified and a Single Travel Token is issued.

Once a traveler has their Single Travel Token, they can use the travel token to pass through any checkpoint equipped to process the Digital Traveler Identity App.

At a checkpoint, the user simply presents a new QR code issued at check-in to an agent, or uses a kiosk to scan that code and take another image of the traveler. The travel token is verified for authenticity and origination. The certified selfie of the user is then compared with the new image taken for facial recognition. If the information matches, the traveler can proceed.

The only information shared by the traveler is what he or she chooses to pass on to the agent via the Traveler App, and this only happens when the agent or station does the authentication and verification. No other entity can obtain the information without the traveler's permission.

The data used to verify a traveler is placed on the blockchain using one-way hashes that are digitally signed by the agent. This method ensures that the data and selfie images being verified were certified by an authorized agent using their private key. The data on the blockchain cannot be reverse engineered.

Any exchange of data between the traveler, an agent or an airline using this system is done through a secure envelope that is digitally signed and encrypted for only the intended recipient. This exchange mechanism follows FIDOs guidelines for secure exchanges between two parties.

All records placed on the blockchain serve the purpose of validation of data presented by the traveler. Each record written is always signed with the private key of the party writing the record, be it the traveler (via the Traveler App) or an airline agent. This creates an authenticated audit-trail of certifications that cannot be impersonated or hacked. Each certification or verification requires multiple factors of authentication (MFA) which makes it virtually impossible to cheat the system.

With this app, a user can use their Single Travel Token to walk through any compatible checkpoint easily, but without compromising security.

PRIVACY

Convenience of travel across multiple providers such as airlines, airports or government authorities usually means giving up control of personally identifiable information. This is usually the case because traveler data and identification information must be kept in a central database where agents and authorized users can access it. While access can be limited, privacy cannot be guaranteed. Central databases are subject to hacker attacks where large numbers of records can be compromised. These concerns, among others, limit the viability of central database solutions that involve sensitive personally identifiable information.

However, with the SITA Digital Traveler Identity approach, using a blockchain as the central point of validation, the traveler carries their personal data and travel information on a secured mobile device, and only shares select information with entities at the discretion of the traveler. Service providers do not need to communicate with other services or databases to validate the data.

However, all agents and security personnel, when presented with the traveler's information and credentials, can validate the authenticity of the data using the publically available blockchain. The data on the blockchain are, by design, only used for validation and do not contain the original data. Hence, hackers are not able to obtain personally identifiable information data from the blockchain.

A DETAILED LOOK UNDER THE HOOD

REGISTRATION DETAIL FLOW

App Installation and Setup

The first step of the registration process is for the traveler to install and setup the Traveler App. Once the Traveler App is downloaded, the traveler is automatically issued a ShoCardID and the app generates a set of private/public keys associated with the ID. Next, the traveler takes a picture of the passport using the Traveler App. The app uses the Machine Readable Zone (MRZ) fields of the passport to pre-populate the meta data that describes the passport. The user is also prompted to take a self-portrait (selfie). The selfie image along with the passport data is encrypted and stored locally. However the validation fields still need to be created and saved on the blockchain. (Fig.1)

Each field, such as the traveler's name, passport number, date of birth and the selfie image is first hashed using a one-way hash function on the data. Each hash is digitally signed using the traveler's private-key on the mobile device. These fields are combined and a seal record is generated. The seal record is then passed to the ShoCard API Server which records the seal on the blockchain.

The user is able to refer to this blockchain record using their unique ShoCardID, which is simply their unique address on the blockchain. This process can be done prior to arriving at the airport or immediately at the check-in counter. (Fig.2)

Traveler Registration with Airline Agent

At this stage, the traveler has downloaded the Traveler App and has a seal record on the blockchain of their personal information and selfie. The next step is the certification process: the traveler presents his or her identification to an airline agent. This process may be automated at a kiosk or done by a live agent. These validation steps, such as asking the traveler for their physical passport or driver's license, viewing their face and comparing it with the identification supplied, and reviewing flight information, are currently part of the existing standard verification processes. With the SITA Digital Traveler Identification process, once the validation is complete, the traveler provides their credentials by having the Traveler App create a QR Code that represents their identification along with their ShoCardID, including their selfie.

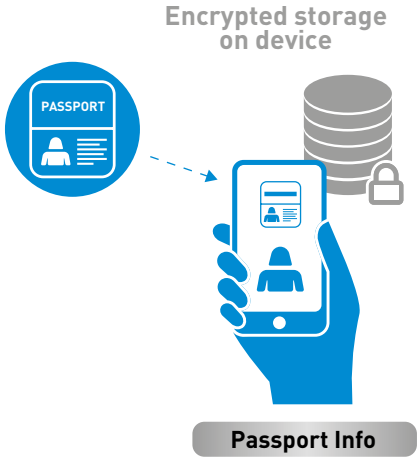


Fig.1

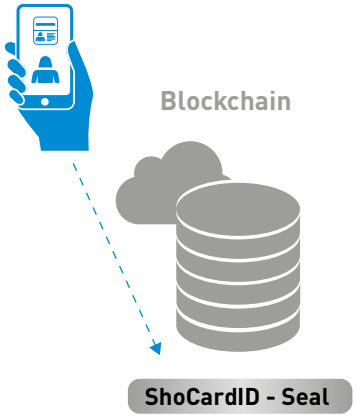


Fig.2

The agent uses the SITA Agent Mobile App (Agent App) to scan that QR Code – this provides a digital link to the traveler's information (for example the passport information and selfie image). This information is passed via a digital secured envelope to the agent. The agent verifies the credentials against the traveler's entry on the blockchain to confirm the traveler's ownership of the blockchain record that her ShoCardID points to. The information is also compared to the physical passport information and travel documents. The agent also verifies that the selfie is a picture of the traveler. If this process is automated through a kiosk, a new image of the traveler is taken and a facial recognition is performed to ensure that the images match.

If all information and photos match, the agent or kiosk makes a secure request through the Agent App to the airline server requesting a certification of the traveler and the generation of a new travel token. The airline server uses its private key to generate certification records for the traveler. The certifications identify the traveler's ShoCardID, the selfie image, and the travel token. These certifications are written to the blockchain. (Fig.3)

Once the certifications are complete, the Traveler App receives the travel token from the airline, which can be presented at a later point to other airlines or security personnel. (Fig.4)

At this point, the Traveler App creates an encrypted secure message that contains the following information:

1. A pointer to the traveler's ShoCardID and seal record on the blockchain
2. A copy of the selfie image (to be used for facial recognition)
3. The travel token
4. A pointer to the certification records

This message is first signed using the traveler's private key and then encrypted with a symmetric passcode that is maintained on the mobile device. The encrypted secure message is saved as an envelope on the ShoStore server for later retrieval. The Traveler App receives an EnvelopeID for future reference.

This completes the traveler registration process.

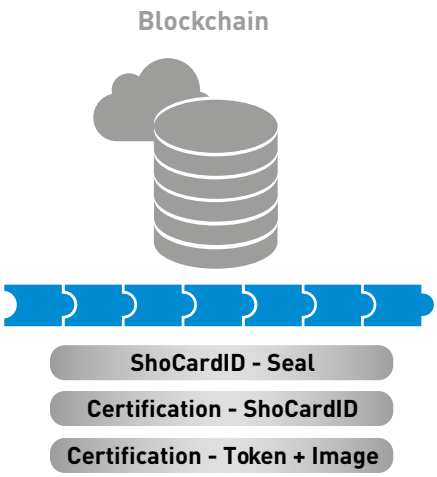


Fig.3

Fig.4

VERIFICATION DETAIL FLOW

Identity Confirmation Process

When a traveler arrives at a checkpoint where verification is required – be it entering a members-only lounge, boarding a plane or entering a gate – the traveler can be assisted by an agent or enter using a self-service kiosk. At this point, the traveler may or may not have network connectivity since they may have arrived in another country or region where access is not available.

To confirm their identity, travelers can use the Traveler App to generate a new QR code which contains the following information without having access to Wi-Fi or network connectivity.

1. The EnvelopeID received during registration. This points to the secure envelope stored on the ShoStore server.
2. The symmetric passcode created for that secure envelope.

The agent, using the Agent App, scans the QR Code to capture the above data. The Agent App uses the EnvelopeID to retrieve the traveler's secure envelope from the ShoStore server, but does not pass the symmetric passcode.

Once the envelope is received, the symmetric passcode is used to decrypt and retrieves the stored information. The traveler's seal and certification records are retrieved from the blockchain, and the following checks are performed:

1. Validation of the signature on the envelope data to ensure the traveler used the same private key to write the seal on the blockchain.
2. Verification of the passport information and the selfie image against the seal record on the blockchain.
3. Validation of the airline signature on the certification records and the seal and the selfie images.
4. Validation of the airline certified travel token.

If all of the above checks are validated, the Agent App next captures a new image of the traveler. The Agent App performs a facial recognition comparison using the previously recorded selfie image (from the ShoStore server) and the image taken of the traveler to biometrically validate that the individual presenting the travel token is the same person who was granted that token. If the facial comparison passes, the app will present a green signal indicating that the user has been verified and the traveler can proceed through the checkpoint.

CONCLUSIONS

This document describes the workflow, processes and underlying technology used in creating, certifying and verifying a persistent, secure and interoperable travel token based on mobile and blockchain technologies. The SITA Digital Traveler Identity App and SITA Agent App are intended to demonstrate one method of accomplishing this challenge. There remain additional areas for continued investigation and development, including:

1. FIDO Alliance Compliance, specifically ensuring that biometric information never leaves the traveler's device (in the SITA Digital Traveler Identity process, an encrypted copy of the traveler's image is stored on the ShoCard servers).
2. Integration with backend airline systems (DCS, Reservations) to link the travel token to the passenger booking/check-in records.
3. Integration with airport infrastructure, such as kiosks, bag-drops, security checkpoints, immigration gates and boarding gates.
4. Developing - in conjunction with the appropriate standards bodies (IATA, ACI, ICAO, etc.) - any required standards to implement a persistent and interoperable travel token.

There are many potential benefits of a Digital Traveler Identity System including:

Real time provisioning – The ability to certify and revoke certifications in real time. This is significant advantage to physical forms of identification which, once issued, cannot be modified. (ePassports, other forms of physical IDs)

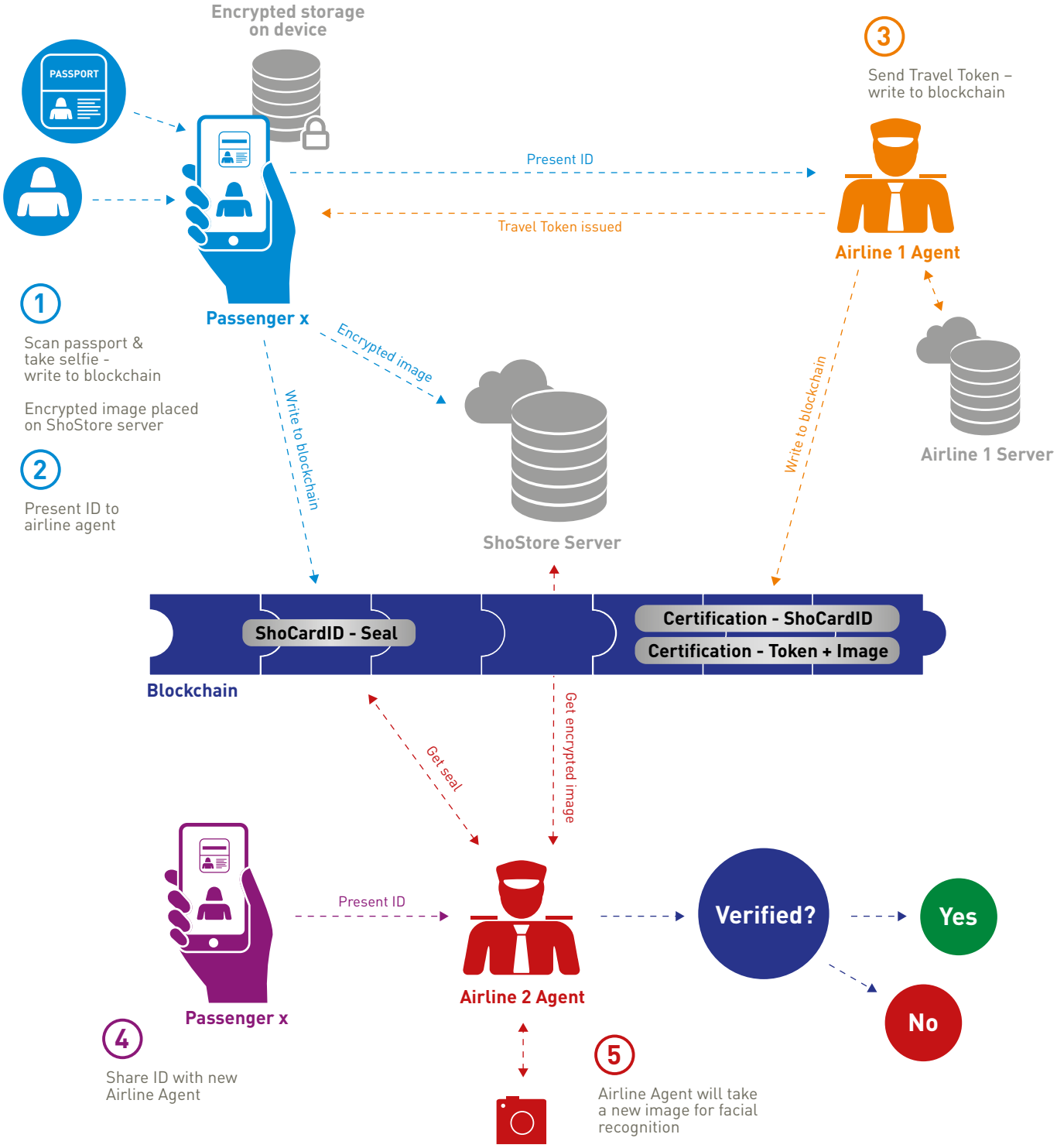
Extensibility of information passed and certified – Using additional data fields to pass qualified certified attributes to/from other entities including airline status, flight information, meal and seating preferences, etc.

A unified travel experience – Allowing travel to be encapsulated with preferences and service levels being shared from the airport, through baggage claim, to customized transportation, to tailored accommodation and hospitality. This would extend traveler-identification to industries outside of air transport without compromising user privacy yet enhancing the user experience.

While there are always additional features to add and challenges to solve, the SITA Digital Traveler Identity Demo Application illustrates how the combination of mobile technology, the blockchain and user biometrics may enhance the overall traveler experience while increasing security at the airport and beyond.

Creating a Web of Trust – With identity on the blockchain, it is possible to create a web of trust for individuals that are strengthened over time by interactions with different parties. This is possible because the user owns their data and the data is verifiable with user permission over the shared blockchain ledger. As a user travels with more airlines, their credentials can strengthen. As digital identity evolves beyond just air travel, other credentials, such as banking, employment and other certifications can further increase the web of trust over an individual. Hence, a user with a strong web of trust who chooses to share their information can be treated with greater preference and freedom in highly secure air-travel environments. With a web of trust established over time, a user is more than a simple boarding ticket or a travel token, but an identified person with a trusted history.

TRAVELER EXPERIENCE OVERVIEW



DEFINITION OF TERMS

The ShoCard Identity Management Services (IMS) is based on standard security techniques to ensure trust of data between parties, using public/private keys, encryption/decryption, sign/verify, data hashing and blockchain operations. This document will not provide detailed definitions for these concepts but instead describes each of them and what characteristic they provide in building a trusted system using ShoCard.

SECURITY TERMINOLOGY

Public/Private keys – a pair of values used to perform security operations. The intent is that the private key is kept secret (never shared). The intent of the public key is for it to be shared with a second party to perform security operations with the holder of the private key and only the holder of the private key.

Encryption/Decryption – Cryptographic operations that can be used to exchange data securely. When used with public/private keys, a user gives out their public key to a second party. The second party encrypts data using the public key and gives the encrypted data to the user. Anyone can see the encrypted data but only the holder of the private key can decrypt the data. The shared data remains private even if others are able to see the encrypted data. Only the private key holder can see the original clear text data.

Sign/Verify - Cryptographic operations that can be used to authenticate that particular data is from a particular user. To do this, a user signs the data with their private key and shares both the data and the signature. Anyone who has access to the public key can verify the data with the signature and determine that the data presented is identical to the data that was signed with a private key previously and no other key. The owner of that private key is then ultimately the signer of that data.

Sign/verify provides a means to be able to verify the source and integrity of data. Yet, the signatures are useless unless the clear text data is offered by the owner of that data in the first place. This provides for authentication of data by any third party, but only when the user explicitly chooses to share the data.

Hashing - Is a transformation of data usually into a shorter fixed-length value that represents the original data. Typically, the operation is one way, meaning that given some data, you can generate a hash value but there is no way to get back to the original value. Hashing is used in conjunction with signatures to minimize the cost of computation. In this case the original data is hashed then the hash is signed. Anyone who has the original data can recreate the hash (when the algorithm is publicized) and given the signature and the public key associated with that signature, can verify the value to ensure the data was signed by the owner of the private key. Hashing provides a small/fixed length value that represents the original data.

Symmetric and Asymmetric keys – Asymmetric keys are typically two keys required for encryption and verification processes such as a public and private key. An entity can encrypt a message with a public key and only the person with a private key can decrypt it. This operation is most common when the first entity knows exactly for whom the message is to be encrypted for.

With symmetric keys or symmetric passcodes, a message is encrypted with the same key that it is decrypted with. Symmetric keys provide the flexibility of encrypting a message that will be presented to someone who was not known at the time the encryption took place. It can also be shared with multiple entities. However, anyone with that symmetric passcode will be able to decrypt the message.

SHOCARD SPECIFIC TERMINOLOGY

The ShoCard identity solution uses these operations to ensure privacy and authenticity of data to provide two high-level identity services. ShoCard has defined its own terms for these operations. This section defines these terms, how they are built on standard security operations, and how they support its "Trusted User Identity" service.

Enveloping – When private data is shared between two endpoints it will be "enveloped", which means that it will be both encrypted and signed. An envelope uses a "To" and "From" set of keys, with which the data will be "hashed" and

signed by the "From" using his private key and encrypted with the "To" public key. What the envelope provides is a way to exchange data that can be proven where it came "From" and that only the "To" can read it.

If the identity of the "To" is not known when the envelope is created, the envelope can be encrypted with a symmetric key. When the envelope is then presented to a party, the "From" user needs to also provide the "To" user with the symmetric key.

Note: An envelope can be constructed using the same keys for both the "To" and the "From". One use for this kind of envelope is if one party wants to give some data to a second party that the second party will give back at a later time. While the second party holds the data, the first party cannot see the data or modify it.

Sealing – The ShoCard solution uses the term, "sealing" when it hashes a set of data, signs that data using its private key, and writes that hash and signed data to the blockchain. What this provides is a record of the data that can later be verified. If the data is modified, the hash will not match. The sealed record contains name/value fields, where the values are hashed and signed.

Certification – The ShoCard solution uses the term, "Certification," when a second party receives private data from a first party, then verifies the correctness of this data and writes a record indicating that it has verified the data. The certification record includes a reference to the seal of the first party data on the blockchain and the specific fields that have been verified and are being certified. Later the certifier can confirm that the user's data is the same as it was when it was certified by comparing the data with the seal.

It is also possible to write a certification record with additional data beyond the seal data for the given user. This could include appended data associated with the user such as a rating, a status, biometrics or a token.

Public key repository – The ShoCard solution provides a means for users to register their public key by their ShoCardID. This public key can be shared via the ShoCard service by those requiring it for a look up. A public key is generally considered to be "public" and not kept private, but the ShoCard service may impose limits when sharing that data.

Sharing – This term is used to indicate one party is going to "share" personal identification information with another party. Anytime personal identification information data is shared with a known party, it is always enveloped using the "To" and "From" keys to ensure privacy and authenticity. It may be necessary to "share" personal identification information where the public key of the receiving entity is not known. In this case the shared data is time-stamped and signed by the person providing the data. It may also be encrypted with only a symmetric key.

SITA

Create success. Together™

SITA AT A GLANCE

SITA transforms air travel through technology - for airlines, at airports and on aircraft.

- Our vision is to be the chosen technology partner of the industry, a position we will attain through flawless customer service and a unique portfolio of IT and communications solutions that covers the industry's every need 24/7.
- We are the innovators of the industry. Our experts and developers keep it fuelled with a constant stream of ground-breaking products and solutions. We are the ones who see the potential in the latest technology and put it to work.
- Our customers include airlines, airports, GDSs and governments. We work with about 400 air transport industry members and 2,800 customers in over 200 countries and territories.
- We are open, energetic and committed. We work in collaboration with our partners and customers to ensure we are always delivering the most effective, most efficient solutions.
- We own and operate the world's most extensive communications network. It's the vital asset that keeps the global air transport industry connected.
- We are 100% owned by the air transport industry – a unique status that enables us to understand and respond to its needs better than anyone.
- Our annual IT surveys for airlines, airports and passenger self-service are industry-renowned and the only ones of their kind.
- In 2014, we had consolidated revenues of US$1.7 billion.

For further information, please visit **www.sita.aero**

For further information, please contact SITA by telephone or e-mail:

Americas
+1 770 850 4500
info.amer@sita.aero

Asia Pacific
+65 6545 3711
info.apac@sita.aero

Europe
+41 22 747 6111
info.euro@sita.aero

Middle East, India & Africa
+961 1 637300
info.meia@sita.aero

Follow us on **www.sita.aero/socialhub**