Turkish Journal of Electrical Engineering and Computer Sciences

Volume 33 | Number 5 Article 8

9-25-2025

BasGit: a secure digital ePassport alternative

CEREN KOCAOĞULLAR

KAAN YILDIRIM

MERT ATİLA SAKAOĞULLARI

ALPTEKİN KÜPÇÜ

Follow this and additional works at: https://journals.tubitak.gov.tr/elektrik

Recommended Citation
KOCAOĞULLAR, C, YILDIRIM, K, SAKAOĞULLARI, M. A, & KÜPÇÜ, A (2025). BasGit: a secure digital ePassport alternative. *Turkish Journal of Electrical Engineering and Computer Sciences 33* (5): 631-646. https://doi.org/10.55730/1300-0632.4148

This work is licensed under a Creative Commons Attribution 4.0 International License.
This Research Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Electrical Engineering and Computer Sciences by an authorized editor of TÜBİTAK Academic Journals. For more information, please contact academic.publications@tubitak.gov.tr

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2025) 33: 631 – 646
© TÜBİTAK
doi:10.55730/1300-0632.4148

BasGit: a secure digital ePassport alternative

Ceren KOCAOĞULLAR[1], **Kaan YILDIRIM**[2], **Mert Atila SAKAOĞULLARI**[3], **Alptekin KÜPÇÜ**[2,*]

[1]Department of Computer Science and Technology, University of Cambridge, Cambridge, UK
[2]Department of Computer Engineering, Koç University, İstanbul, Turkiye
[3]Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, USA

Received: 04.03.2025 • **Accepted/Published Online:** 20.07.2025 • **Final Version:** 25.09.2025

Abstract: We present a solution to the challenge of securely issuing both paper-based and mobile phone-based passports without requiring specialized production techniques. Our solution offers improved security, privacy, and usability compared to the ePassport mechanism currently used worldwide. We also describe how our solution can be extended to support offline verification and present the test results of our proof-of-concept implementation.

Key words: ePassport, electronic travel documents, border security, customs security, electronic visa

1. Introduction

Passports contain various information, including, but not limited to, the holders full name, a biometric photo, place and date of birth, and signature. Traditionally, passports have been paper-based documents, but in recent years, contactless integrated circuit (IC) chips have been added, creating electronic passports (ePassports). As of May 2025, 178 countries use ePassports[1]. The International Civil Aviation Organization (ICAO), an agency of the United Nations [1], defines ePassport standards.

The ePassport solution relies on the physical existence of a passport. This includes the biographic elements, as well as international visas printed on the passport itself. The visa issuance and approval process can take several weeks or even months, during which the passport holder cannot travel internationally because the visa-issuing authority retains the physical passport for processing. There are very few recent exceptions, such as the UK, which allows applicants to keep their passport during the decision process for an additional fee.[2]) For example, visa waiting times[3] can range from 7 days to nearly 3 years.

Issues related to the security, privacy, and usability of ePassports [2–9] highlight the need for a new system that allows identity validation and border crossing in a more reliable and convenient manner. Considering the widespread use of mobile devices and computers, their security and usability capabilities, and users' willingness to adopt online identity management systems [10], this paper proposes a new passport system (BasGit) based on ubiquitous devices.

*Correspondence: akupcu@ku.edu.tr
[1]https://www.inverid.com/blog/countries-epassports
[2]https://visa.vfsglobal.com/tur/en/gbr/premium-services
[3]https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/global-visa-wait-times.html

This work is licensed under a Creative Commons Attribution 4.0 International License.

2. State of the art

ICAOs New Technologies Working Group has a specialized Digital Travel Credentials (DTC) subgroup that proposes several solutions, including a hybrid method combining both a physical and a virtual token. The UK government currently verifies passport holder identities through online channels as part of the EU Settlement Scheme. This scheme is not an international travel system but a program that allows EU citizens to remain in the UK after Brexit. The UK, along with Australia, also uses eVisa systems designed to carry out visa application processes primarily online [11].

The trusted or registered traveler concept has been explored by various organizations. However, these schemes lack internationally recognized standards. A comprehensive initiative in this field has been undertaken by the World Economic Forum, known as the Known Traveler Digital Identity concept. This international travel initiative proposes a self-sovereign identity system without a central authority, instead using distributed ledger technology with blockchain [12]. Currently, the trusted traveler concept is implemented bilaterally by the United States and Canada through a mobile application known as Mobile Passport.[4] This scheme requires the inspector to verify both the original ePassports and the mobile application. In contrast, our solution, BasGit, proposes a complete replacement of the existing ePassport system.

Recent work on virtualizing travel credentials addresses the handling of visas and electronic travel authorizations [13]. Alternative approaches that integrate ePassports with blockchains have also been proposed [14–16]. For a more detailed discussion, see [17] and [18].

Numerous studies have demonstrated the vulnerabilities of ePassports [3, 6–9] to eavesdropping and skimming [2], unthrottled guessing and tracking [2, 4, 5, 19, 19], version rollbacks [20], and biometric attacks [21].

3. Specifications of the BasGit passport system

BasGit has three main components: (i) travelers with a paper-based printable and/or a mobile application-based passport (Figure 1a), (ii) reader devices for verification at the control points (Figure 1b), and (iii) an administrative component that is called the administrative web interface (Figure1c). AWI is the leading authority for issuance, verification, and maintenance of passport data.

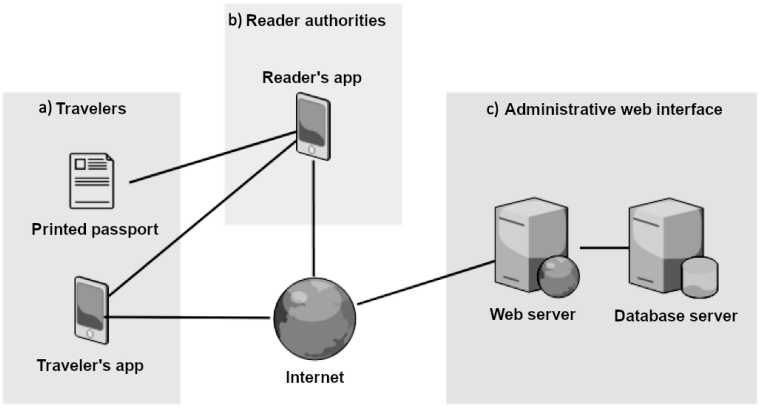


Figure 1. Architectural overview of BasGit, including travelers, customs authorities, and administration.

[4]https://mobilepassport.us/

Administrative web interface (AWI): The governmental agencies of the participating countries must adopt AWI to join the BasGit system. In practice, AWI can be implemented as either a centralized or distributed system. It is assumed that the participating countries have agreed upon the data exchange protocols. The current ePassport system uses the ICAO public key directory (PKD) in a distributed manner to facilitate data exchange between states.[5] The features of AWI are as follows:

- Contains the biographic information of the owner of the passport, such as full name, birth place and date, nationality, sex, and national ID number.
- Contains the passport holder's biometric digital photograph, which complies with the ICAO Machine-Readable Travel Documents Photo Guidelines [1].
- Can contain additional identifying biometric data such as fingerprints.
- Contains information about the passport, including the type of the passport, the issuance date, expiry date, and serial number.
- Keeps access logs in a tamper-evident manner [23–31], possibly via a blockchain-based mechanism [32–35].
- Generates and securely keeps (e.g., via hardware security modules) a digital signature private/public key-pair. Shares with the readers the public key using the appropriate PKI mechanism.
- Authorizes reader devices, preventing unauthorized devices from accessing passport information or engaging in fraudulent activities.
- Supports administrative operations such as travel restrictions and passport revocations.
- Operates role-based access control and allows simultaneous usage by multiple authority types, enabling a multitude of government bodies to work together without causing security risks (Table 1).

Any biometric data must be protected in accordance with international standards, such as ISO/IEC 24745:2022, and secured using cryptographic mechanisms [22]. The EU GDPR and AI Act specify the regulatory requirements for the collection, storage, use, safeguarding, and cross-border transfer of biometric data.

Table 1. Authority roles in AWI.

Security authority	Reader authority	Monitoring authority
Revoke passport	Activate reader	View active passports
Restrict travel	Revoke reader	View revoked passports
Issue arrest warrant	Read passport	View expired passports

Issuing a passport: BasGit does not impose any restrictions on how citizens are registered in the AWI. In practice, many web-based governmental systems[6] [7] manage this process. The governmental body responsible for issuing passports determines whether a candidate is eligible for international travel, as it would under normal procedures; this process is not specified in this proposal nor by ICAO. What is critical for BasGit is that the AWI database records the data of each travel document along with its corresponding digital signature. Assuming that passport data is readily available, issuance proceeds as follows:

1. For each passport, a 128-bit universally unique identifier (UUID) is generated randomly or securely pseudorandomly, which enables backward compatibility while preventing predictability [36].
2. Each UUID is securely mapped to the corresponding passport information in the database.

Acquiring a paper passport: To acquire a paper passport in BasGit, the following steps are performed:

1. The user signs into the web-based system to request a paper-based passport[8].

[5]https://www.icao.int/Security/FAL/PKD
[6]https://www.turkiye.gov.tr
[7]https://e-estonia.com
[8]Two-factor authentication can be employed for this purpose [37]. State-of-the-art single password authentication protocols may

2. The associated UUID is retrieved, a QR code containing the UUID is generated, and a PDF file displaying this QR code is created.
3. The user downloads and prints this PDF file, which is the BasGit paper-based passport of the user.

Acquiring a mobile passport: A mobile application-based passport is acquired via the following steps:

1. The user logs into the system through the mobile application and requests a passport (Figures 2A–2C). The user's login credentials can be stored in the operating system's secure containers, which are designed to store sensitive data and cryptographic keys.
2. The associated UUID is retrieved (Figure 2D).
3. The mobile application stores the UUID in the secure containers provided by the operating system. The application generates a QR code from this UUID, which can be displayed at control points for verification. This QR code serves as the BasGit mobile passport for the user.

The user is not required to have Internet access after acquiring the passport. The BasGit mobile application securely stores the access token and UUID, enabling the user to present the QR code of their passport safely even while traveling internationally without Internet connectivity. Authentication is performed offline using the securely stored credentials. Therefore, in both versions of BasGit (paper and mobile), the traveler only needs to be online during the acquisition process and not while traveling internationally.

Verifying a passport: In its standard operation, the passport reader must be online and connect to the AWI via a secure, server-authenticated channel (e.g., TLS) to perform verification (offline verification is discussed later in Section 6). Passport verification proceeds as follows (Figure 3):

1. The officer signs into the system through the reader application (Figure 2E).
2. The officer uses the reader application to scan the QR code, whether in paper or mobile form. The UUID contained in the QR code is then sent to the AWI.
3. AWI verifies that the reader is authorized, retrieves the associated passport information using the UUID, signs it, and sends the passport $info$ to the reader device along with the generated digital signature. AWI also maintains a tamper-evident log of access times and reader identities.
4. The reader verifies the digital signature and then displays the passport information on the screen (Figure 2F).
5. The officer visually inspects the information and verifies the biometric photograph and/or other biometric identifiers, such as fingerprints, to ensure that the person presenting the passport at the border is the legitimate owner, as is currently practiced.

For mobile application-based passports, BasGit can provide additional security measures during verification. For example, two-factor authentication can be employed to ensure that the passport cannot be used without the owners knowledge. Once the QR code of a citizen's passport is read by a reader authority, the passport request will trigger a verification code to be sent through an SMS or an automated call [43]. Such features may not be available while traveling internationally due to mobile network or Internet connection constraints. Using time-based one-time password (TOTP) can constitute a solution.

Integrating visas: The existing ePassport system does not store any information about issued travel visas in the IC chip [1]. The main reason is that these chips can only be written to by the passport-issuing country; therefore, other countries do not have write access to record their visas in the chip. This results in complex processes and requires multiple complicated stages for verifying the passport and the visa [2].

be preferred [38–42]

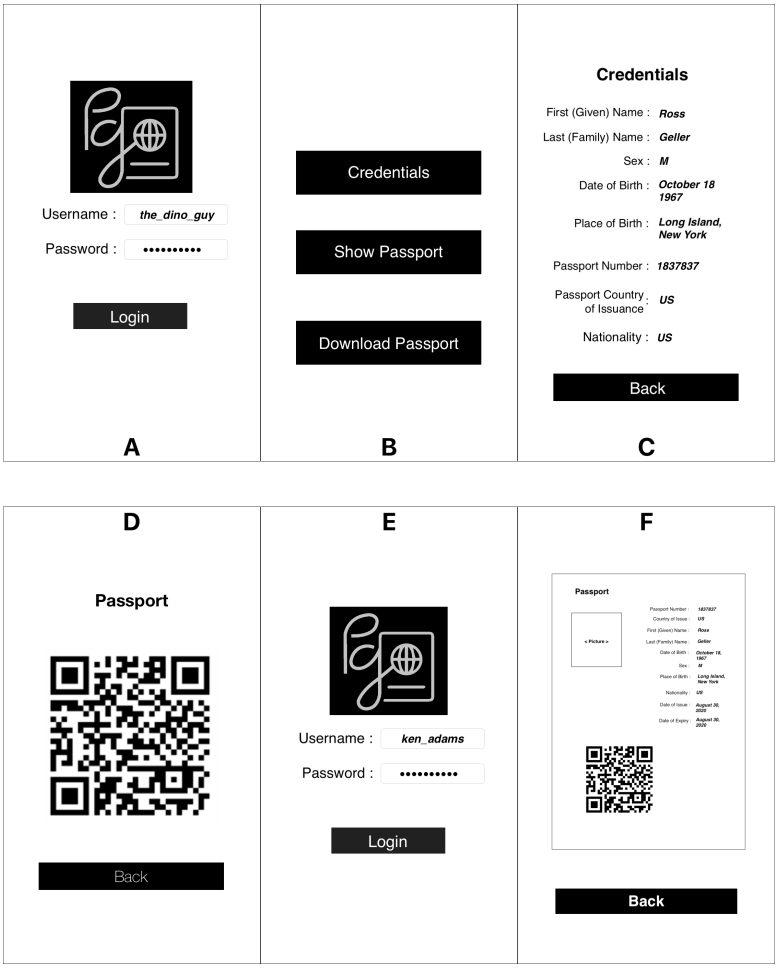


Figure 2. Traveler application screens for login, options, passport data, and UUID QR code (A–D), and the customs officer's reader application screens for login and verification (E,F).

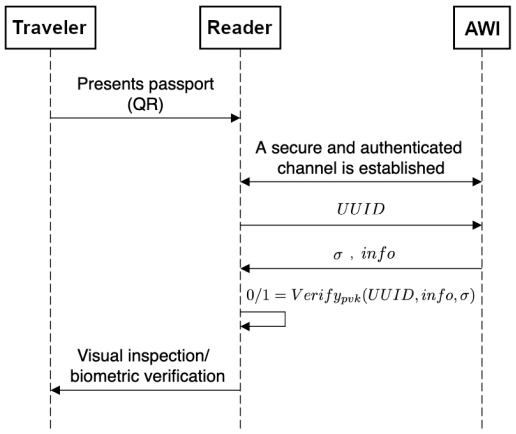


Figure 3. Verifying a passport. In order: the traveler presents the QR code, the reader verifies the passport via AWI, the officer performs visual or biometric inspection.

Online governmental systems already in use, such as those in Türkiye[9] and India[10], can also be used to manage visa processing. BasGit does not impose restrictions on how countries securely exchange passport and visa information. Once a visa is approved, it is granted through the following steps:

1. A UUID is created and attached to each visa.
2. The UUID is then mapped to the corresponding visa data, and the UUID together with the visa information are securely stored in the database of the visa-granting country.
3. The visa-granting country digitally signs the visa information. The signed visa is transmitted to the passport-issuing country's system using a secure communication medium. In the database of the passport-issuing country, the visa UUID and the passport UUID are mapped. Alternatively, the visa-issuing country can keep the mapping between the visa UUID and the passport UUID without holding any other information regarding the passport.

For each visa, a QR code representing its UUID is generated and added to the passport. If it is a paper-based BasGit passport, visa QR codes are also printed. For mobile passports, the mobile application separately displays visa QR codes. For verification, the following is done:

1. The digital signature on the visa is verified with the visa issuing country's public verification key. As with passport verification, an infrastructure similar to ICAO PKD can be used for public key exchange.
2. The mapping between the passport UUID and the visa UUID is performed. This can be done via the passport-issuing country's AWI or the visa-issuing country's AWI, depending on the visa issuance process.

Unlike passport verification, visa verification does not demand extra visual inspection and/or biometric verification. Once the passport is verified (together with visual inspection and/or biometric verification), verifying the digital signature of the passport and ensuring that the visa UUID is mapped to the passport UUID is sufficient.

4. Threat model

We provide a detailed discussion of the threat model, including potential attacks on passport systems and the countermeasures implemented in the BasGit solution. In the following section, we present a comparative analysis of the proposed BasGit program.

4.1. The traveler

1. ***Privacy***

   Threat: Exposing sensitive personal information on the passport to adversaries.

   Attack: Physical observation.

   Countermeasure: Avoid storing any personal information on the paper or mobile passport itself; instead, store sensitive information exclusively within the capacities of central authorities.

2. ***Cloning***

   Threat: Reproducing valid passports by duplicating QR codes.

   Attack: Copying the QR code of a valid passport.

   Countermeasure: Performing biometric verification and/or visual inspection at the inspection points, and/or employing multifactor authentication mechanisms in mobile passports.

3. ***Man-in-the-middle***

   Threat: Presenting a valid passport without the knowledge of its holder.

   Attack: Relaying valid passport UUIDs.

   Countermeasure: Same as for cloning.

[9] https://www.evisa.gov.tr/
[10] https://indianvisaonline.gov.in/

4. ***Unthrottled guessing***

Threat: Replicating existing passports.

Attack: Guessing UUIDs to find one that is linked to an actual passport.

Countermeasure: Chance of generating a valid UUID is negligible since they are randomly generated and their domain is exponentially large in the security parameter.

5. ***Unauthorized tracking***

Threat: Fraudulently tracking a passport holder.

Attack: Using the information on the passport to track an individual.

Countermeasure: Even though the passports in BasGit are made up of QR codes that represent static UUIDs, line-of-sight is necessary to read them. Paper BasGit passports can be folded and kept in pockets or wallets, and the mobile BasGit application may remain closed until inspection.

6. ***Denial-of-service***

Threat: Making the passport unrecognisable for the reader.

Attack: Physically damaging the passport.

Countermeasure: BasGit does not propose a countermeasure to this type of attack; however, its passport's high level of availability reduces this attack's capacity for damage since the user can quickly and cheaply reproduce a valid paper/mobile passport. Forming a direct solution can be explored in future works.

7. ***Malware***

Threat: Malware on the user's mobile device.

Attack: Cloning user credentials.

Countermeasure: Employing operating-system provided secure containers, multifactor authentication, and having paper-based alternative. Further measures remain as open problems.

4.2. The Reader

1. ***Man-in-the-middle (MITM)***

Threat: Relaying, eavesdropping, and possibly altering the network traffic.

Attack: Intercepting the network communication between the reader and AWI to alter or clandestinely monitor information.

Countermeasure: TLS connection to the AWI and digital signature verification.

2. ***Denial of service***

Threat: Temporarily blocking travelers from crossing borders.

Attack: Over-flooding the AWI with requests.

Countermeasure: The general mechanism of resisting denial of service attacks is employing a distributed solution. This increases the costs associated with the deployment of the program; yet it is crucial for availability.

3. ***Stealing***

Threat: Fraudulently verifying passports.

Attack: Acquiring a reader device without permission.

Countermeasure: To revoke a reader device, the AWI session associated with it can be marked expired. IP restriction for the reader devices can also be employed.

4. ***Insider Attacks***

Threat: Getting counterfeit passports accepted or genuine passports denied.

Attack: Tampering with the reader and putting a different public signature verification key and certificate into the reader application.

Countermeasure: We acknowledge that such an attack cannot, in general, be entirely prevented. However, countermeasures can still be implemented to reduce its effectiveness. For example, a special-purpose QR code could be publicly displayed at each border control location. Control officers would scan this QR code before starting their shifts to ensure that the valid certificate and public signature verification key are in use. For enhanced security, this QR code could be generated dynamically. While this may not completely prevent the attack, it would significantly limit its extent.

4.3. The AWI

1. ***Insider attacks***

   Threat: Allowing individuals to cross borders with fake travel documents or steal travel document data.

   Attack: Authorized personnel altering the database to create counterfeit travel documents with phony information or stealing the travel document data of citizens.

   Countermeasure: In many schemes, insider attacks are nearly impossible to prevent because they are carried out by already authorized personnel. Tamper-evident logging is the only measure that can discourage and limit the damage caused by an insider attack.

2. ***Signature key stealing***

   Threat: Forging passports that will be validated by the system.

   Attack: A malignant insider stealing the signature key and using it to sign counterfeit passports.

   Countermeasure: A threshold signature [44, 45] scheme can be employed to divide the responsibility of signing passports between multiple parties. Additionally, hardware security modules can be employed.

3. ***Unauthorized database access***

   Threat: Stealing travel document data.

   Attack: An attacker gaining unauthorized access to the database.

   Countermeasure: Since the travel document data are stored unsigned, the attacker cannot use the stolen data to forge travel documents.

5. Comparison of ePassports and BasGit

BasGit passports are easier and cheaper to issue and reissue, and pose less of a privacy risk since they contain no useful information in clear text. Unlike BasGit, ePassports are difficult to clone and forge. A serious security concern for both passport systems is the possibility of a malicious party gaining access to both sides of the infrastructure. For BasGit, this would mean having access to both the AWI and the reader, allowing the attacker to validate a fraudulent passport by altering the public digital signature verification key used by the reader and/or the private digital signature signing key used by the AWI. Similarly, if the ICAO PKD and/or the associated private keys are manipulated by the attacker, counterfeit ePassports could be accepted as valid.

The comparison criteria in this section are based on [46]. We added 10 new criteria and adapted 8 of the existing ones to suit the objectives of this research. The legend for the comparison criteria used in Tables 2–3 is provided below. It can be seen that BasGit significantly improves many aspects of ePassports.

○ = *Does not offer the solution* ◐ = *Partially offers the solution* ● = *Offers the solution*

Deployability comparison criteria

- *Accessible*[11]: Physical disabilities do not prevent a user from using their passport.
- *Scalable*: Significantly increasing the number of users has conceivable financial and time costs.

[11] Adapted from [46].

- *Negligible-cost-per-user*[11]: Producing a passport has negligible cost-per-user, including the cost of establishing the infrastructure and generating the passport.
- *Mature*[11]: The scheme has large-scale deployment beyond research purposes.

Table 2. Deployability comparison of BasGit and ePassport.

	BasGit	ePassport	Explanation
Accessible	●	●	Neither of the two imposes any problem for physically disabled users.
Scalable	●	○	BasGit only requires scaling the infrastructure, while ePassport requires scaling the production mechanisms of the physical passports as well.
Negligible-cost-per-user	●	○	BasGit is either virtual and free of material costs or printed on regular paper, while ePassports comprise special materials and an IC chip.
Mature	○	●	ePassports compliant to ICAO standards have been in use since 2003.

Security comparison criteria

- *Resilient-to-forgery*: An attacker cannot forge a passport to deceive border inspection systems.
- *Resilient-to-cloning*: It is not feasible to create an identical copy of an existing passport that can also pass as a legitimate travel document.
- *Resilient-to-data-tampering*: An attacker only having access to a travel document cannot make changes to the travel document data.
- *Revocation-detection-by-authorities*: Border inspection can identify a revoked passport.
- *Resilient-to-physical-observation*[11]: An attacker cannot steal personal information or obtain any knowledge that can be used for unauthorized access to travel document data by physically observing a passport.
- *Resilient-to-clandestine-tracking*: An attacker cannot secretly track the movements of a user.
- *Resilient-to-unthrottled-guessing*[11]: A probabilistic polynomial time adversary cannot figure out the secret information that can be used to access a user's travel document data.
- *Resilient-to-theft*[11]: If an attacker steals the travel document of a user, they cannot use it to deceive border inspection systems or perform identity theft.

Usability comparison criteria

- *Nothing-to-carry*[11]: The user does not need to carry any item solely for the purpose of a travel document.
- *Easy-to-learn*[11]: It is easy to learn and remember how to acquire, use, revoke, and recover a passport.
- *Easy-acquirement*: The user can easily acquire a passport without going through complicated procedures and spending a lot of time.
- *Easy-revocation-by-user*: Revoking a passport does not cost a user a significant amount of time and does not require arduous paperwork.
- *Easy-recovery*[11]: The user can effortlessly recover a passport in case of loss, theft, or physical damage.
- *Low-financial-cost-to-user*: Acquiring a passport has almost no financial cost to the user.

6. Offline verification

Even though BasGit is primarily an online system, it can be adapted for offline work on mobile devices with small modifications. These modifications can be utilized to increase the system's robustness by enabling the system to operate even in case of network failures at border control points. The online verification principle of BasGit is structured upon the exchange of UUIDs that represent travel documents registered in the online

Table 3. Security comparison of BasGit and ePassport.

	BasGit	ePassport	Explanation
Resilient-to-forgery	●	○	Because ePassports store extensive information on both the paper document and the embedded chip, the system is vulnerable to forgery. In BasGit, the only information stored on the passport is UUID, which does not allow the attacker to change any passport information.
Resilient-to-cloning	●	◐	Although ePassports include security measures to prevent cloning, some attacks can still partially clone ePassports and modify their contents to bypass certain protections, particularly because backward-compatibility and some security practices are only recommendednot mandatoryby the ICAO [20]. Since the BasGit passport is represented as a QR code, it is also susceptible to cloning. However, a cloned BasGit passport cannot be used as a legitimate travel document by another user.
Resilient-to-data-tampering	●	○	BasGit stores only a UUID on the passport itself, which cannot be used to manipulate data in any meaningful way. In contrast, ePassports contain personal and identifying information on the chip. Although some fields are digitally signed, not all are protected, which allows an attacker to remove certain fields from the passport to bypass additional security measures.
Revocation-detection-by-authorities	◐	◐	Revoked passports may be overlooked by authorities when offline authentication is employed.
Resilient-to-physical-observation	●	○	ePassports pose a security risk whenever the first page of the passport is observable, leaking the key for basic access control [5].
Resilient-to-clandestine-tracking	●	◐	ePassports are susceptible to tracking.
Resilient-to-unthrottled-guessing	●	◐	BAC mechanism in ePassports employ the information stored in MRZ with low entropy, being susceptible to brute-force attacks [2, 19].
Resilient-to-theft	●	◐	In case of theft, ePassports carry the risk of identity theft and tampering, whereas BasGit has the advantage of easy revocation and reissuance, without leaking any personal information.

Table 4. Usability comparison of BasGit and ePassport.

	BasGit	ePassport	Explanation
Nothing-to-carry	●	○	BasGit mobile does not require the user to carry anything extra.
Easy-to-Learn	◐	●	Acquiring BasGit may be difficult for the first-time users.
Easy-acquirement	●	○	BasGit's both paper and mobile versions bypass many bureaucratic processes and are significantly easier to acquire.
Easy-revocation-by-user	●	○	BasGit users can effortlessly revoke their passports in a short amount of time using the mobile or the AWI interface of the system.
Easy-recovery	●	○	Even though both systems are susceptible to being physically damaged or stolen, BasGit is easier to recover by printing or downloading.
Low-financial-cost-to-user	●	○	ePassports can cost as much as $333 or 125% of annual per capita national income [47].

system. For the introduction of an offline version, the primary requirement is to store and transmit travel document data over an offline medium. The ePassport standards published by ICAO define the minimum chip size as 32 KB [1]. Therefore, this paper presumes that the ePassport data is around 32 KB.

In this paper, we examined several communication media based on their availability, novelty, and usability, and presented a comparison in Table 5. The comparison considers transmission rate, feasibility of establishing a secure channel, and ease of setup.

Table 5. Comparison of offline verification data transfer media.

	Bluetooth	**NFC**	**Wi-Fi**	**Audio**	**QR codes**
Transmission rate	>0.9 Mbit/s	424 Kbit/s	<9608 Mbit/s	<1.2 Kbit/s	<24 Kbit/QR
Easy setup	×	✓	×	✓	✓
Secure channel	✓	✓	✓	×	×
Notes	Fast (< 1 s) but requires pairing	Fast (< 1 s)	Fast (< 1 s) but requires setup	Slow (> 4 min)	Inefficient (11 QR or 4 HiQ -High capacity color QR- code scans)

The offline verification process occurs in several steps (displayed in Figure 4). When a user logs into the AWI and requests a passport, the signed travel document data and the travelers UUID are sent to the device. The travelers mobile application then encrypts and stores the signed travel document data. The encryption key is kept in secure containers provided by the operating system, potentially utilizing secure on-chip technologies. Once the data is available on the users device, verification can be performed by communicating with a reader device using one of the listed communication media.

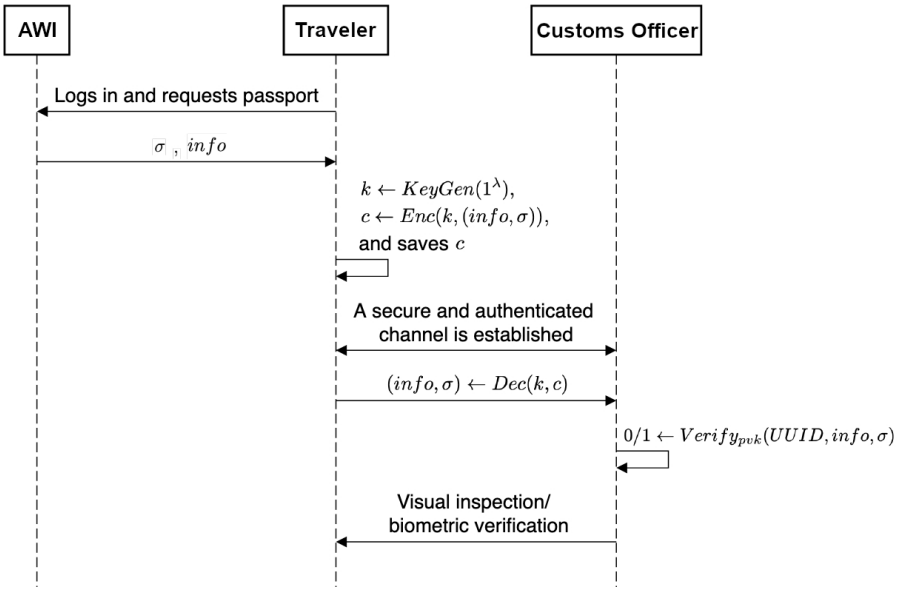


Figure 4. Offline verification in the mobile version. First, the traveler device obtains passport information from the AWI. Second, a secure and authenticated channel is established between the traveler's mobile device and the customs officer's reader device. Third, the passport information is verified by the reader. Lastly, the customs officer performs visual or biometric inspection.

Comparing the asymmetrical media (audio and QR) to the symmetrical media (Bluetooth, NFC, Wi-Fi), it can be seen from Table 5 that the former provide more accessible setup procedures due to their simplistic data transfer processes. However, considering the transmission rates provided by both of the options, it is clear that the transmission time creates considerable overhead to the travel document verification process. These media also lack some of the essential security features like secure and reader-authenticated channels, and as a result, the asymmetrical data transfer media are not recommended for use. Within the symmetrical data transfer media, all of the options have sufficient transmission rates to create acceptable overhead during the travel document

verification process and support the establishment of a secure and reader-authenticated channel. Compared to Bluetooth and Wi-Fi, the NFC method has an easier setup and is the preferred data transfer medium. One drawback of NFC compared to its competitors within the symmetrical data transfer media is its comparatively limited availability on older devices. Bluetooth media are also recommended due to their high availability these days, even on smart watches.

Offline verification is suggested as an extension to the proposed scheme. This is done to show that BasGit can support offline verification through different media. Online verification is superior in terms of security and usability; hence, it must be preferred whenever possible.

7. Implementation

We implemented a proof-of-concept to demonstrate the usability and security aspects. The screenshots can be seen in Figure 2. The first component is a paper-based passport design that removes the need for complex materials and procedures the ePassports require for their production. The main AWI component that issues the passports and manages the readers is also implemented. As the third component, we also implemented a mobile application allowing access to passports using smartphones. As a testing environment, two iOS devices—iPhone 7 and iPhone Xs—were chosen, and the applications were coded in Swift 4.2.4. Two open-source, MIT-licensed libraries were used: Alamofire[12] for HTTPs network communication, and CommonCrypto[13] for SHA256 hashing. The salted and hashed password, salt, and downloaded passport data are all stored at the operating system level, requiring both successful application login and iOS Keychain login for access. Our implementation reinforces password protection by requiring login each time after the app is off-screen.

We tested our proof-of-concept implementation against potential vulnerabilities using open source tools: Arachni[14] v1.5.1 and WMAP using Metasploit[15] framework v5.0.21. While our goal was not to develop a production-grade implementation, we primarily aimed to test the AWI component. Our implementation successfully passed tests for HTTP Strict Transport Security (HSTS), SQL injection, Cross-Origin Resource Sharing (CORS), code injection, Cross-Site Scripting (XSS), session vulnerabilities, cookie vulnerabilities, same-origin policy bypass attempts, and Cross-Site Request Forgery (CSRF).

8. Conclusions and limitations

The existing widely deployed passport system, ePassport system, has usability, security, and privacy concerns. Moreover, it requires specialized material and printing technology. In contrast, the BasGit passport program allows passports to be printed at home on paper or stored on widely adopted smartphones, thereby significantly reducing the costs of acquiring, issuing, extending, canceling, and reissuing a passport. BasGit passports do not require physical protection, and the visa application timelines no longer limit the international travels of the travelers.

Even though BasGit requires a new online system to be deployed, governmental national identity management systems already exist in many countries[6] [7]. Existing information systems' security policy implementations and best practices can be translated to satisfy the proposed system in numerous ways [48]. This one-time setup cost of deploying the BasGit framework would undoubtedly be reimbursed by its much lower operational costs in the long run. The reduced cost of creating and securing the passports themselves, as well as maintaining the

[12]https://github.com/Alamofire/Alamofire
[13]https://github.com/soffes/CommonCrypto
[14]https://www.arachni-scanner.com/
[15]https://www.metasploit.com/

infrastructure, will have a notably positive financial impact for both the deploying nations and their citizens. We note that ePassports also incurred large initial deployment costs, which slowed their adoption. However, many adopting countries observed benefits such as a 40% reduction in forged documents and a 30% decrease in waiting times at airports.[16] Considering that Türkiye provides the most expensive passports and that one in every 10 countries have passport costs exceeding 10% of annual per capita income [47], deploying BasGit would definitely benefit both governments and citizens economically in the long run.

In the case of ePassports, bribery, coercion of authorized staff, or insider attacks pose problems related to the issuance of fake passports [2]. BasGit likewise does not prevent insider attacks. Strategies to prevent such attacks against BasGit should be included in future discussions. Furthermore, passports are often used as identification documents, in addition to their primary function as international travel documents. Furthermore, offline verification procedures, different communication media, security of user devices, and procedures and security of the visa process should be analyzed in detail as part of future work.

Considering the strengths and weaknesses of the proposed BasGit Passport Program, conducting a pilot trial among a small group of countries with a limited number of participants may be valuable. Key future research directions for BasGit include its deployment as a fully distributed system, evaluation of throughput and scalability, examination of privacy-related regulatory aspects (e.g., GDPR compliance), and assessment of user experience and usability, all of which are beyond the scope and page limits of the current manuscript.

[16] https://newswire.net/pr/the-global-rollout-of-electronic-passports-a-new-era-in-travel-identity-and-security.html

Acknowledgments

We acknowledge the support of The Scientific and Technological Research Council of Türkiye (TÜBİTAK) through projects 119E088 and 123E462. We also thank Murat Güç from Koç University.

References

[1] ICAO. Doc 9303, Machine Readable Travel Documents. Montréal, Quebec, Canada: International Civil Aviation Organization, 2015.

[2] Kc GS, Karger PA. Preventing security and privacy attacks on machine readable travel documents (mrtds). Cryptology ePrint Archive, Paper 2005/404, 2005.

[3] Auletta V, Blundo C, De Caro A, De Cristofaro E, Persiano G et al. Increasing privacy threats in the cyberspace: The case of Italian e-passports. In: International Conference on Financial Cryptography and Data Security (FC); Canary Islands, Spain; 2010. pp. 94-104.

[4] Juels A, Molnar D, Wagner D. Security and privacy issues in e-passports. In: International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM); Athens, Greece; 2005. pp. 74-88.

[5] Kosta E, Meints M, Hansen M, Gasson M. An analysis of security and privacy issues relating to rfid enabled epassports. In: International Conference on Mobile Data Management (MDM); Mannheim, Germany; 2007. pp. 273-277.

[6] Filimonov I, Horne R, Mauw S, Smith Z. Breaking unlinkability of the icao 9303 standard for e-passports using bisimilarity. In: European Symposium on Research in Computer Security (ESORICS); Luxembourg; 2019. pp. 577594.

[7] Bădită AG. Security of Romanian electronic passports: The protection of personal data in the digital age. In: International Conference on Cybersecurity and Cybercrime (CYBERCON); Bucharest, Romania; 2024. pp. 102-108.

[8] Rwegasira DB, Yustina LA, Mazana MY. Assessment of the effect of users satisfaction with the e-passport system on service delivery in the Tanzania immigration service department. African Journal of Empirical Research 2024; 5 (3): 1301-1312.

[9] Radutoiu AT, Bassit A, Veldhuis R, Busch C. A study on the next generation of digital travel credentials. In: International Conference of the Biometrics Special Interest Group (BIOSIG); Darmstadt, Germany; 2024. pp. 1-6.

[10] RoSSnagel H, Zibuschka J, Hinz O, Muntermann J. Users' willingness to pay for web identity management systems. European Journal of Information Systems 2014; 23: pp. 36-50. https://doi.org/10.1057/ejis.2013.33

[11] Smith T, Bonner R. Seamless and secure travel: The future of international passenger travel and border control. Surrey, UK: International Border Management and Technologies Association, 2019.

[12] Bissessar D, Hezaveh M, Alshammari F, Adams C. Mobile travel credentials. In: International Symposium on Foundations and Practice of Security (FPS); Montreal, Quebec, Canada; 2018. pp. 46-58.

[13] System Initiative on Shaping the Future of Mobility. The known traveller: Unlocking the potential of digital identity for secure and seamless travel. Geneva, Switzerland: World Economic Forum, 2018.

[14] Jahan N, Reno S. Utilizing hyperledger-based private blockchain to secure e-passport management. In: Data Intelligence and Cognitive Informatics (ICDICI); Tirunelveli, India; 2023. pp. 579593.

[15] Jahan N, Reno S, Ahmed M. Securing e-passport management using private-permissioned blockchain and ipfs. In: International Conference on Electrical, Computer and Communication Engineering (ECCE); Chittagong, Bangladesh; 2023. pp. 1-7.

[16] Başer MY, Büyükbeşe T, Kizildag M. What if we could travel without passport? first sight to blockchain-based identity management in tourism. Asia Pacific Journal of Tourism Research 2023; 28 (4): 341-363. https://doi.org/10.1080/10941665.2023.2229922

[17] Azman M, Sharma K. Smart boarding system with e-passports for secure and independent interoperability. SN Computer Science 2022; 3: 52. https://doi.org/10.1007/s42979-021-00938-5

[18] Avoine G, Quisquater JJ. Passport security. In: Jajodia S., Samarati P, Yung M. (editors). Encyclopedia of Cryptography, Security and Privacy. Switzerland: Springer, 2025, pp. 17761779. https://doi.org/10.1007/978-3-030-71522-9_129

[19] Říha Z. An overview of electronic passport security features. In: The Future of Identity in the Information Society. Berlin, Germany; 2008. pp. 151-159.

[20] Calderoni L, Maio D. Cloning and tampering threats in e-passports. Expert Systems with Applications 2014; 41(11): 5066-5070. https://doi.org/10.1016/j.eswa.2014.02.044

[21] Blundo C, Persiano G, Sadeghi AR, Visconti I. Resettable and non-transferable chip authentication for e-passports. In: Conference on RFID Security (RFID); Las Vegas, NV, USA; 2008.

[22] Choudhury ZH, Munir Ahamed Rabbani M. Biometric passport security by applying encrypted biometric data embedded in the QR code. In: Data Engineering and Communication Technology; Singapore; 2020. pp. 41-52.

[23] Erway C, Küpçü A, Papamanthou C, Tamassia R. Dynamic provable data possession. ACM Transactions on Information and System Security 2015; 17 (4): 1-29. https://doi.org/10.1145/2699909

[24] Ateniese G, Burns R, Curtmola R, Herring J, Khan O et al. Remote data checking using provable data possession. ACM Transactions on Information and System Security 2011; 14 (1): 1-34. https://doi.org/10.1145/1952982.1952994

[25] Scott DSW, Crosby A. Efficient data structures for tamper-evident logging. In: USENIX Security Symposium; Berkeley, CA, USA; 2009. pp. 317-334.

[26] Cash D, Küpçü A, Wichs D. Dynamic proofs of retrievability via oblivious RAM. Journal of Cryptology 2017; 30: 22-57. https://doi.org/10.1007/s00145-015-9216-2

[27] Etemad M, Küpçü A. Generic efficient dynamic proofs of retrievability. In: ACM Cloud Computing Security Workshop (CCSW); Vienna, Austria; 2016. pp. 85-96.

[28] Etemad M, Küpçü A. Transparent, distributed, and replicated dynamic provable data possession. In: International Conference on Applied Cryptography and Network Security (ACNS); Banff, AB, Canada; 2013. pp. 1-18.

[29] Esiner E, Kachkeev A, Braunfeld A, Küpçü A, Özkasap Ö. FlexDPDP: Flexlist-based optimized dynamic provable data possession. ACM Transactions on Storage 2016; 12 (4): 1-44. https://doi.org/10.1145/2943783

[30] Esiner E, Küpçü A, Özkasap Ö. Analysis and optimization on flexdpdp: A practical solution for dynamic provable data possession. In: International Conference on Intelligent Cloud Computing (ICC); Muscat, Oman; 2014. pp. 65-83.

[31] Küpçü A. Official arbitration with secure cloud storage application. The Computer Journal 2015; 58(4): 831-852. https://doi.org/10.1093/comjnl/bxt138

[32] Putz B, Menges F, Pernul G. A secure and auditable logging infrastructure based on a permissioned blockchain. Computers & Security 2019; 87: 101602. https://doi.org/10.1016/j.cose.2019.101602

[33] Hassanzadeh-Nazarabadi Y, Küpçü A, Özkasap Ö. LightChain: Scalable DHT-based blockchain. IEEE Transactions on Parallel and Distributed Systems 2021; 32 (10): 2582-2593. https://doi.org/10.1109/TPDS.2021.3071176

[34] Dousti MS, Küpçü A. Moderated redactable blockchains: A definitional framework with an efficient construct. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology (CBT); Guildford, UK; 2020. pp. 355-373.

[35] Dousti MS, Küpçü A. Tri-op redactable blockchains with block modification, removal, and insertion Turkish Journal of Electrical Engineering and Computer Sciences 2022; 30 (2): pp.376-391. https://doi.org/10.3906/elk-2105-221

[36] Leach P, Mealling M, Salz R. A universally unique identifier (uuid) urn namespace. RFC-4122, 2005.

[37] Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones. In: IEEE/ACS International Conference on Computer Systems and Applications (AICCSA); Rabat, Morocco; 2009. pp. 641-644.

[38] Acar T, Belenkiy M, Küpçü A. Single password authentication. Springer Computer Networks 2013; 57 (13): 2597-2614. https://doi.org/10.1016/j.comnet.2013.05.007

[39] ler D, Küpçü A. Threshold single password authentication. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology (DPM); Oslo, Norway; 2017. pp. 143-162.

[40] ler D, Küpçü A, Cokun A. User perceptions of security and usability of mobile-based single password authentication and two-factor authentication. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology (DPM); Luxembourg; 2019. pp. 99-117.

[41] ler D, Küpçü A. Distributed single password protocol framework. Cryptology ePrint Archive, Paper 2018/976. 2018.

[42] Bicakci K, Atalay NB, Yuceel M, van Oorschot PC. Exploration and field study of a browser-based password manager using icon-based passwords. In: International Conference on Financial Cryptography and Data Security (FC); St. Lucia; 2011. pp. 104118.

[43] Qian H, Surapaneni CS, Dispensa S, Medhi D. Service management architecture and system capacity design for phonefactora two-factor authentication service. In: IFIP/IEEE International Symposium on Integrated Network Management (IM); New York, NY, USA; 2009. pp. 73-80.

[44] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In: Advances in Cryptology (CRYPTO); Santa Barbara, CA, USA; 1991. pp. 457-469.

[45] De Soete M, Quisquater JJ, Vedder K. A signature with shared verification scheme. In: Advances in Cryptology (CRYPTO); Santa Barbara, CA, USA; 1989. pp. 253-262.

[46] Bonneau J, Herley C, Van Oorschot PC, Stajano F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: IEEE Symposium on Security and Privacy (SP); San Francisco, CA, USA; 2012. pp. 553-567.

[47] McKenzie D. Paper walls are easier to tear down: passport costs and legal barriers to emigration. World Development 2007; 35 (11): 2026-2039. https://doi.org/10.1016/j.worlddev.2006.11.009

[48] Niemimaa E, Niemimaa M. Information systems security policy implementation in practice: from best practices to situated practices. European Journal of Information Systems 2017; 26: 1-20. https://doi.org/10.1057/s41303-016-0025-y