BasGit: A Secure Digital ePassport Alternative

BasGit: Alternatif Güvenli Elektronik Pasaport Sistemi

Ceren Kocaoğullar, Kaan Yıldırım, Mert Atila Sakaoğulları, Alptekin Küpçü
College of Engineering, Koç University, İstanbul, Turkey 34450
{ckocaogullar15,kyildirim14,msakaogullari14,akupcu}@ku.edu.tr

***Abstract*—This paper discusses a new passport program that allows the passports to be printed on paper or carried in a smartphone application by the passport holders, without any interference or use of specialized equipment. The security and privacy implications, usability, and practicality of the proposed BasGit Passport Program are compared and contrasted with the already existing ePassport system that is widely used in the world. The paper then concludes with the overview of a proof-of-concept implementation and test results of it.**

***Index Terms*—e-Passport, border security, customs security, electronic visa.**

***Öz*—Bu makalede pasaportların evde kağıda yazdırılabilmesini veya mobil bir uygulamada tutulabilmesini sağlayan, kullanımı kolay ve maliyeti düşük alternatif bir güvenli elektronik pasaport sistemi öne sürüyoruz. Önerdiğimiz BasGit Pasaport Sistemi'nin güvenlik, gizlilik, kullanılabilirlik analizlerini yapıyor ve günümüzde yaygın olarak kullanılan ePasaport sistemi ile kıyaslıyoruz. Prototip kodlamamızın tartışması ve güvenlik testleri sonuçlarıyla makalemizi sonlandırıyoruz.**

***Anahtar Sözcükler*—e-Pasaport, sınır güvenliği, gümrük güvenliği, elektronik vize.**

I. Introduction

Passports are official travel documents that governments issue for their citizens to use for international travels. Passports contain information such as, but not limited to, the holder's name, photograph, date of birth, and signature. Started as a paper-based document, passports were rather recently enhanced with contactless Integrated Circuit (IC) chips and named electronic passport (or ePassport) for this reason. As of May 2017, 120 countries were using ePassports [1]. The standards for e-passports are set and managed by the International Civil Aviation Organization (ICAO) which is a specialized agency of the United Nations [2]. Prevention of counterfeiting and fraud is crucial for safeguarding national and international security. Several studies discussing the security and privacy issues of the ePassports exist [3]–[6].

The current ePassport system is constructed on the physical presence of a passport. Most counties register travel visas on the physical passport. The visa approval and issuing processes, which may take up to several weeks, withholds the holder from traveling abroad, as the original passport is kept by the visa issuing agency/country.

The security, privacy, and usability related issues indicate the necessity for a more reliable and convenient system for validating identity and crossing borders. Considering the ease of use and high-security requirements based on computers and mobile devices, this paper proposes a new passport system.

II. Literature Review

A recent research on mobilizing travel credentials by Bissessar et. al solely focuses on visas and electronic travel authorizations, and does not include mobilizing ePassports [7].

The most comprehensive effort on mobilizing ePassports has been done by the World Economic Forum. This initiative is a self-sovereign identity system that has no central authority. A distributed ledger technology with blockchain, pointers and hubs are used [8].

Also, an application named Mobile Passport is being offered as a free and paid service to United States passport owners and Canadian passport owners entering United States [9]. This mobile application aims to accelerate the customs operations and does not qualify as an ePassport. The travelers are required to present their ePassports as well as the mobile application upon inspection, whereas BasGit is a replacement to the current ePassport system.

III. Preliminaries

Digital signatures are algorithms that are used for validating integrity and authenticity of data [10]. They are based on asymmetric (public key) cryptography. The core idea of digital signature concept is, the signing party *A* distributes a public key for verification and keeps the matching private key secret. *A* digitally signs data using the private key, and this signature can be validated using the public key. This way, only *A* is able to sign data, and everyone who has access to the public key can assure that the data source is *A* and the data is unmodified.

In the paper, $info$ denotes the passport information, ssk denotes secret signing key and pvk denotes public verification key.

The passport signature function is:

$$\sigma = Sign_{ssk}(UUID, info) \tag{1}$$

The passport verification function is:

$$0/1 = Verify_{pvk}(UUID, info, \sigma) \tag{2}$$

If the verification function yields true and the obtained $UUID$ matches the passport holder's UUID, the passport is authentic. However, passport holder's legitimacy is a different concern. The current passport system requires either a visual validation by the control officer, or biometric verification. This topic will be further discussed in the following sections.

The managerial component of BasGit, the Administrative Web Interface (AWI) requires HTTPS connection for encryption, integrity checking, and server authentication. Whenever an internet connection to the AWI is mentioned, it is presumed that all parties have access to the genuine SSL (Secure Sockets Layer) certificate of the AWI, and can exchange and validate it through a legitimate PKI (Public Key Infrastructure).

IV. Objectives

Prevention of tampering and forgery in a passport system is crucial for national and international security. Weaknesses mainly arise from the validation mechanisms based on the contactless IC chip. The contactless IC chip and current access control mechanisms are prone to security and privacy compromises such as unauthorized communication with the chip, eavesdropping, skimming, and brute-force attacks [3]–[6].

One of the main objectives of the proposed BasGit system in this paper is to prohibit tampering and forgery by using the physical passport to only link individuals to the passport information stored in a secure central system. The proposed system does not claim safety against theft nor copying, however, an attacker retrieving an original or copied document does not cause any security risk. For each verification, the passport data is obtained from the central system and any biometric data mismatch can be quickly detected by the authorized staff. This also provides security against forgery, since the data carried by a physical passport is meaningful only if it has correspondence on the central system. For the same reason, the proposed system also does not require the same level of physical protection on the documents. Therefore, losing access to a physical passport should not constitute a major problem for the proposed system.

The proposed system aims to restrict the access to sensitive personal data only to authorized personnel. The existing ePassports contain identity information as plain text on the physical passport and includes biometric data in the embedded chip. This constitutes a threat to exploitation of sensitive personal data, including identity theft [5], [6]. Moreover, the current passports require the first page of the passport to be closed for security. Because the key for the initial authorization step for the IC chip, Basic Access Control, is calculated by reading information from the first page of the passport [6]. BasGit system aims to eliminate this privacy risk by not displaying or storing identity information on the passport and only giving access to this information to authorized readers. BasGit also aims to keep log of crucial information such as the identity of reader and time of access of each instance of passport reading. The ePassport system does not ensure recording this information in cases that the passport is inspected offline.

One major usability issue of ePassports is their financial cost, which can be as high as $333 or 125% of annual per capita national income [11]. Moreover, acquiring a passport usually has a high time cost because of the required bureaucratic processes. All these factors complicate the availability of ePassports for travelers. The proposed program in this paper aims to increase the availability of passports for the citizens.

In addition, in case of a stolen or lost ePassport, cancelling and reissuing may take up to several weeks. As a usability improvement, BasGit aims to reduce the duration of these actions down to seconds.

V. Specifications of The Proposed System

The main administrative element of the structure is a web-based system named Administrative Web Interface (AWI) (Fig.1c). It poses as the passport issuing, verifying, and maintaining authority.

The proposed system offers two different types of passport implementations: a printable, and a mobile application-based passport (Fig. 1a). Obtaining the former requires a printer and internet connection to access the AWI, while the latter requires a smartphone and also an internet connection to access the mentioned web interface.

The system proposes to employ a mobile application to be used by the control points (Fig. 1b).

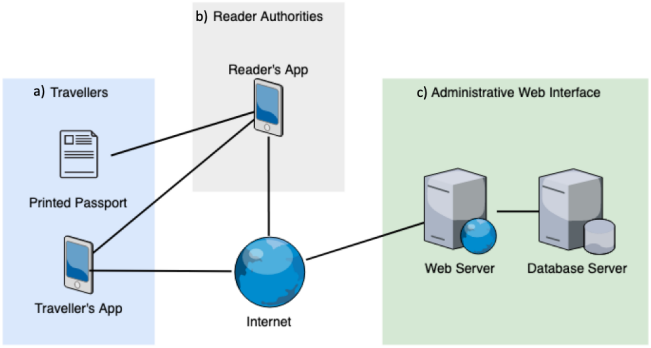

Figure 1. Architecture diagram showing the proposed system.

A. Administrative Web Interface (AWI)

Governing bodies of the participant nations must adopt the AWI in order to manage and supervise the proposed system. AWI is either a central or a distributed system that is capable of fulfilling the requirements of the program. In case of a distributed system, the participating nations have to determine the protocols for data exchange. The current ePassport system is a distributed system and utilizes ICAO Public Key Directory (PKD) to handle data exchange between states [12].

AWI has the features specified below:

- Contain the biographic information of the holder of a passport, including the full name of the holder, the birthplace and date, sex, nationality, and national ID number.
- Contain a digital biometric photograph of the holder that is compliant with the ICAO Machine-Readable Travel Documents Photo Guidelines [2].
- Contain information about the generated passport including at least the generation date, date of expiry, type of the passport, and the serial number.
- Keep log of each access to a passport by an authorized reader securely [13]–[21]. Log entries should include at least the access time and identity of the accessing personnel.
- Generate and contain a private/public key pair for digitally signing passport information, and share the public key with the readers.
- Authorize reader devices to prevent unintended devices from being used to read passports or act maliciously in the system.
- Support administrative operations such as passport revocation and travel restriction.
- Operate role based clearances that allow multiple types of authorities to use the system in parallel.

Separating all actions into roles as in Table I allows many government bodies to work together on the same system without causing security risks.

Table I
ROLES AND THEIR RIGHTS IN THE BASGIT AWI.

Security Authority	Reader Authority	Statistics Authority
Revoke Passport	Active Readers	Active Passports
Restrict Travel	Revoke Reader	Revoked Passports
Arrest Warrant	Reader Users	Expired Passports

1) Passport Issuing: The proposed system does not determine the means of registering citizens into the AWI. This can be handled similar to the web-based governmental systems in use [22]. However, the system requires each passport data stored in the central database to be digitally signed by the passport issuing authority. The issuing body can then decide whether a candidate is eligible for a passport using any information it has; this process is neither specified in this proposal nor by ICAO. Once the passport data is registered in the system, issuing a passport consists of the following steps:

1) A universally unique identifier is generated (UUID) for each passport. As the name suggests, UUID promises spatially and temporally unique identifiers of 128 bit length. UUID version 4 is generated randomly or pseudo-randomly, which is sufficient for backwards-compatibility and preventing predictability [23].
2) The system securely maps each UUID to the corresponding passport $info$.

B. Passport Acquiring

1) Paper Passports: The process of acquiring a paper passport consists of the following steps:

- **Step 1:** User logs into the web-based system and requests a paper-based passport.[1]
- **Step 2:** System finds the associated UUID, generates a QR code containing that user's UUID, and prepares a PDF file which only displays that QR code.
- **Step 3:** User downloads and prints the PDF file with the QR code of their UUID. This is now the passport of the user.

2) Mobile Passports: Acquiring a mobile passport consists of the following steps:

- **Step 1:** User logs into the system through the application[1] and requests a passport (Fig. 4a). When using the online login method, login credentials are stored in the secure containers provided by the operating system for sensitive data and cryptographic keys.
- **Step 2:** System finds the associated UUID and sends it to the application (Fig. 4d).
- **Step 3:** Application stores the UUID in the aforementioned operating system provided secure containers. The QR code containing the UUID is generated and displayed by application. This is now the passport of the user.

Once the passport is acquired, the user does not have to have an internet connection. This is because BasGit stores the login credentials and UUID securely to allow the user to login to the mobile application and present their passport even while offline. Therefore, in both paper and mobile passport versions, BasGit only requires the traveller to be online during passport acquiring, but not during their travels.

[1]A secure login can be achieved through two-factor authentication [24], [25]. A more convenient secure solution can be implementing a single password authentication protocol [26]–[29]

C. Passport Verification

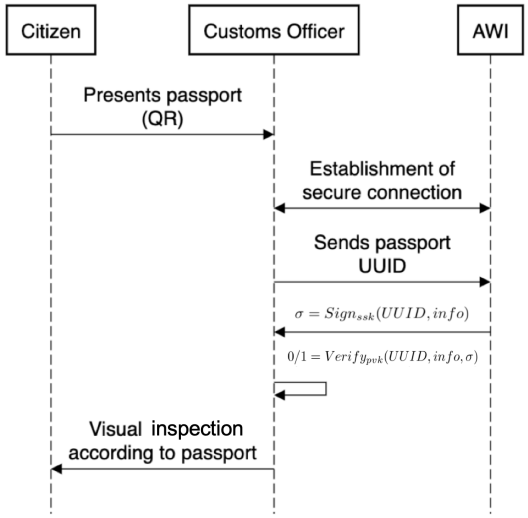

Figure 2. Sequence diagram showing the procedure of reading and verifying a passport.

In the BasGit system, the passports are verified using a smartphone application designed for the control officer. This mobile application must have internet connection to reach the central system to perform verification. Passport verification consists of these steps:

- **Step 1:** Officer logs into the system through the application[1] (Fig. 4e).
- **Step 2:** Reader application reads the QR and sends the UUID stored in the QR to AWI using a secure and authenticated connection.
- **Step 3:** AWI finds the associated passport information and sends it to the reader application along with the digital signature. Also, it logs the access time and reader's identity using a tamper-evident logging system [13]–[21].
- **Step 4:** Reader application verifies the digital signature and displays the passport information corresponding to the passport UUID (Fig. 4f).
- **Step 5:** Reader performs visual inspection to ensure that the passport holder is genuine.

As all the information related to the passport is retrieved when the passport is read by a reading authority. Step 4 can be altered to allow other ways of verification. For instance, it can be supported with biometric verification.

Mobile passports allow additional security measures for passport verification. A possible security measure against using the passport without holder's knowledge is adding support for two-factor authentication. The only drawback of this feature might be mobile network or internet connection constraints abroad. Providing secure wireless internet connection at the control points can be a solution to this.

D. Travel Visas

The visas granted to the ePassports are not stored within the contactless IC chip [30] as these chips cannot be written by multiple countries for security reasons. This separates the visa system from the passport system requiring multiple stages of verification, both for the passport and the visa [3].

The BasGit Passport Program enables a centralized online visa granting scheme using the aforementioned infrastructure.

Applying for a visa can be handled using online systems, which is already used in practice [31], [32]. BasGit does not propose any specific way of securely exchanging passport information between countries during the visa application process. Once the visa application is approved, the granting process occurs as follows:

- **Step 1:** A UUID is generated for each visa. The visa UUIDs are digitally signed by the visa granting country authority, using Equation 1 where $info$ is the visa information. This prevents attackers from scanning databases of different countries with one QR.
- **Step 2:** The system securely maps each UUID to the corresponding visa data and stores the UUID - visa information pair is stored in visa granting country's secure database.
- **Step 3:** The visa is digitally signed using Equation 1 and transmitted using any secure transmission method to the passport issuing country's system. It is securely mapped to the passport UUID of the individual.

Passport and visa UUIDs appear as separate QRs on the passport. Visa verification consists of only two steps:

- **Step 1:** Verifying the digital signature of the visa using Equation 2. As for the passport verification, an infrastructure similar to ICAO PKD can be used for data exchange for exchange of public key.
- **Step 2:** Verifying that the holder's passport has the visa UUID mapped to it.

Visa information obtained in the verification process can be used for confirming the visa type.

VI. Security Analysis and Comparison

A. An Overview of ePassport Security and Privacy Issues

The ePassport verification occurs when the customs officer reads the data stored in the contactless IC chip of a presented passport, after a series of steps for secure communication and authorized access [3]. The first step and the only mandatory step is Passive Authentication, which is basically using a PKI for checking if the chip is digitally signed by the issuing country [2]. Passive Authentication provides no protection against eavesdropping and skimming attacks [3].

The second step is the optional Basic Access Control (BAC). In essence, BAC aims to make sure that the first page of the e-passport that contains data is open as the reader tries to access the information in the IC chip. BAC system derives encryption and message authentication keys using the information stored in the Machine Readable Zone (MRZ) in order to establish secure communication for session key exchange. MRZ contains a maximum of 88 characters of information including name, surname, and date of birth of the owner, date of expiry, etc. [3], [33], [34]. Data stored in this area is usually easily guessable especially if the attacker knows the targeted passport holder. As a result, MRZ's entropy is not high enough to be immune to brute-force attacks [3], [33].

ICAO requires the IC chips used for ePassports to follow ISO 14443 standard [35]. Anticollision protocol of this standard requires the IC chips to emit a UID (Unique Identifier). This UID is fixed in some implementations and can be read by any reader device that complies with ISO 14443 protocol without any authorization. If the UID is fixed and unique to each chip, this protocol is prone to exposing the passport holder to be fraudulently tracked [5], [6], [33].

It is important to note that there are other optional security measures that ICAO proposes. One of these is Active Authentication, which intends to verify the authenticity of the contactless IC chip. Also, ICAO acknowledges that additional biometrics needs further protection and has proposed another optional security measure called Extended Access Control for this purpose. Even though Active Authentication aims to strengthen the security and privacy of the IC chips, it should be noted that if Active Authentication is used with RSA or Rabin-Williams signatures, the reader can acquire a value distinct to each chip. This way, the passport holder can be tracked without their knowledge [5].

B. Security Assessment of the BasGit Passport Program

The new passport design proposes to move all the personal information out of the passport itself and store it in central authorities. If a QR code for any passport is copied, at the inspection points this will be detected by the reader authorities who are performing visual inspection, biometric verification, or two-factor authentication in mobile passports. Also, the odds of an attacker generating a valid UUID at the time of inspection is negligible due to the random nature of the identifiers and their exponentially-large domain. In addition, the online verification obligation eliminates the risk of human error that may occur in border controls employing offline verification. Additionally, BasGit eliminates tracking attacks, since even though QR codes contain static UUIDs, they cannot be scanned unless they are visible to the reader.

The mobile application enables further security measures such as two-factor authentication and requiring login for preventing unauthorized access to the passport information. These measures are not necessities but opportunities.

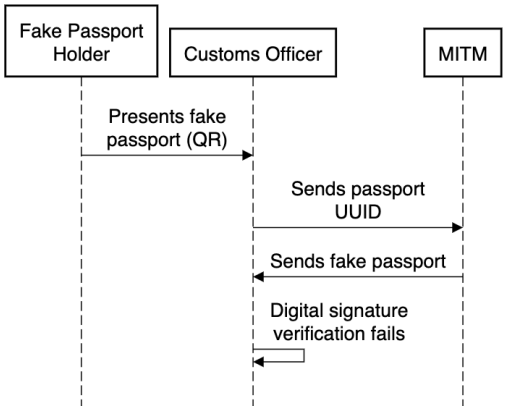

Figure 3. Sequence diagram showing an attack scenario where the attacker intercepts the connection between the reader and the central authority.

1) Man-in-the-middle Attacks: As the BasGit system is completely online, there is a considerable amount of network traffic between the readers and the central authorities. This traffic may be targeted by attackers (Fig. 3). Even though TLS connection makes it impractical, for this attack, we assume that the attacker can make the readers believe that they are connecting to the legitimate central authority. The attacker can achieve this by owning a fake certificate and performing DNS hijacking. If a malicious party intercepts the network traffic and replies to a reader with a fake passport, the reader will try to verify the digital signature of the sent passport.

Unless the malicious party can fake the digital signature of the central system, the verification will still fail. If the malicious party can indeed sign the fake passport, this means that the signing key of the central system is exposed, which is out of our scope.

2) Denial of Service (DoS) Attacks: The online systems of BasGit may be attacked with a denial of service attack to prevent the control points to reach the servers to authenticate the passport users, which will temporarily block travelers from crossing borders. A distributed system may be employed to prevent these types of attacks, which will increase the costs of implementing the program. However, this is necessary for the proper functioning as the availability of the system is crucial for international travel.

Observe that if the attacker can change the reader and put a different pvk and certificate into the reader application, then the attacker can have fake passports accepted or real passports denied. Unfortunately, such an attack cannot be prevented completely. But, we propose that a special passport QR entry can be hold at each border point, such that the officers can scan it before each shift starts to ensure that they are employing the correct certificate and signature verification key. For better security, this entry can be dynamically generated by the AWI.

3) Insider Attacks: The only foreseeable way to counterfeit a passport in the proposed system is an insider attack. People with high access levels may also alter the citizen records to create counterfeit passports with fake information to allow individuals to cross borders. However, insider attacks are nearly impossible to prevent as the access rights are given to ensure proper operation of the program. Logging activity done by the authorized personnel is the only way to prevent further damage by an insider attack as it is possible to find the attacker using the logs [13]–[21].

C. General Comparison of the Systems

ePassport and BasGit systems have advantages and disadvantages in terms of usability, security and privacy. BasGit is cheaper, easier to reissue and contains less information on the passport compared to ePassports. On the other hand, unlike BasGit ePassports allow some degree of offline verification and make producing fake passports difficult (Table II).

In addition to the broadly discussed security aspects of the two systems, a serious security risk for both is an attacker having reach to both ends of the validation structure. For BasGit, the attacker can validate a fake passport if they manage to change both pvk and ssk. Similarly, if the attacker can manipulate ICAO PKD as well as the private keys, they can achieve verifying counterfeit passports.

BasGit does not contain any personal information on the passport (the QR code), while ePassports expose private information such as the name, surname, date, and place of birth, details of travel history and in some cases profession and emergency contact information of the holder.

Table II

Comparison of BasGit vs. ePassport			
BasGit		ePassport	
Pros	Cons	Pros	Cons
Much cheaper for the citizens to use.	Only allows online verification.	Allows for some degree of offline verification.	Production cost of a passport is much higher.
Passport is easy to obtain once issued.	Easy to create a fake passport (but it will not verify).	Hard to create a fake passport.	Issuing requires long bureaucratic process.
No identifying information on the passport (privacy-preserving).			Identifying information visible on the passport (prone to identity theft).

VII. Implementation

To demonstrate the usability and security of the proposed system, we have implemented a proof of concept system. The implementation consists of three main components. First component is the new passport design that is paper-based and does not require the complicated production procedures the ePassports use. Second component is the AWI which issues the passports, manages the readers, and allows citizens to acquire passports online. The third and the last component is a relay between the citizens and the central authority, the mobile application, which allows the users to access their passports from their smart phones.

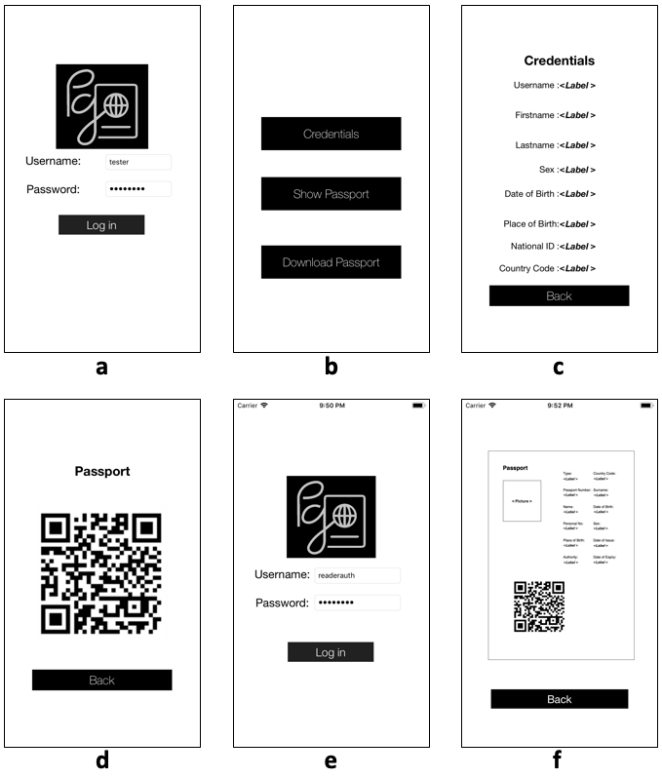

Figure 4. Figures a to d show screens for the traveller application. Figures e and f show screens for the reader application.

The proof-of concept system has been tested against vulnerabilities using open source tools [36], [37]. The main point of interest for the testing was the central authority as the other components of the system does not allow the attackers to alter user data permanently. Our implementation passed successfully from the tests against: Cross site scripting (XSS), Cross Site Request Forgery (CSRF), HTTP Strict Transport Security (HSTS), cookie vulnerabilities, SQL injections, Cross Origin Resource Sharing (CORS), session vulnerabilities, code injection and bypassing same origin policy.

VIII. Conclusions

The ePassports have some usability, security, and privacy problems. Many existing infrastructures, such as bank and government services requiring high levels of security, have been transformed into all-online systems to increase usability, security, and privacy. Therefore, it is realistic to anticipate that such an online passport system can be implemented as well.

Unlike the conventional ePassport systems, which require high levels of specialization in printing and material technology to print the physical travel documents, the proposed program offers passports to become printed at home or stored in smartphones. The proposed program lowers the cost and time for issuing, acquiring, canceling, and extending a passport. The BasGit program uses the physical passports to only link individuals with their information stored on a central system. This does not require the same level of physical protection on the documents as forging the document itself does not constitute a security risk as long as it will not be verified by the central system or the reader. Moreover, this system eliminates visa application processes withholding the holder from traveling.

Despite the requirement for a highly specialized central system, the governments already use such systems to verify national identities and check criminal records at checkpoints. It is possible to say that such systems can easily exist as similar ones do already [22]. The high, one-time cost of the central system will be compensated by the low operating cost. The eradicated cost of securing, developing, and printing passports will have a substantial financial effect.

To conclude, BasGit Passport Program may be developed with further research and field testing to become a more reliable and easier way of validating identity and crossing borders in the future. BasGit system currently does not offer a solution to the existing threat of insider attacks. An attacker can bribe or threaten passport issuing authority staff or an insider attacker can issue false passports [3]. What can be done to prevent this kind of attacks should be a part of future discussions. We plan to incorporate further cryptographic solutions as we learned via [38]. Also, considering the fact that passports are not only used as travel documents but also as identification documents, types of authorities with low-level access permissions can be employed, thanks to the role-based central system. The focused effort of ensuring security in only the digital medium compared to the currently divided attempts of trying to secure both the digital and the physical mediums will allow swifter and more stable progress in the field of international travel.

References

[1] Gemalto NV, "The electronic passport in 2018 and beyond," https://www.gemalto.com/govt/travel/electronic-passport-trends, [May. 26, 2019].

[2] ICAO, "Doc 9303, machine readable travel documents, part 3: Specifications common to all mrtds," 2015.

[3] G. S. Kc and P. A. Karger, "Ibm research report: Preventing security and privacy attacks on machine readable travel documents (mrtds)," 2005.

[4] V. Auletta, C. Blundo, A. De Caro, E. De Cristofaro, G. Persiano, and I. Visconti, "Increasing privacy threats in the cyberspace: The case of italian e-passports," in *FC*, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, and F. Sebé, Eds. Springer Berlin Heidelberg, 2010, pp. 94–104.

[5] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *SECURECOMM*, 2005, pp. 74–88.

[6] E. Kosta, M. Meints, M. Hansen, and M. Gasson, "An analysis of security and privacy issues relating to rfid enabled epassports," in *IFIPSEC*. Springer, 2007, pp. 467–472.

[7] W. E. F. S. I. on Shaping the Future of Mobility, "The known traveller: Unlocking the potential of digital identity for secure and seamless travel," 2018.

[8] F. A. C. A. David Bissessar, Maryam Hezaveh, "Mobile travel credentials," in *FPS*, 2018, pp. 46–58.

[9] A. M. Inc., "Mobile passport," https://mobilepassport.us/, [Sept. 3, 2019].

[10] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[11] D. McKenzie, "Paper walls are easier to tear down: passport costs and legal barriers to emigration." *World Development*, vol. 35, pp. 2026–2039, 2007.

[12] ICAO, "Security and facilitation: Public key directory," https://www.icao.int/Security/FAL/PKD/Pages, [May. 26, 2019].

[13] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM CCS*, 2009.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," *ACM TISSEC*, vol. 14, no. 1, p. 1–34, 2011.

[15] D. S. W. Scott A. Crosby, "Efficient data structures for tamper-evident logging," in *SSYM*, 2009, pp. 317–334.

[16] D. Cash, A. Küpçü, and D. Wichs, "Dynamic proofs of retrievability via oblivious ram," *Journal of Cryptology*, vol. 30, no. 1, pp. 22–57, 2017.

[17] M. Etemad and A. Küpçü, "Generic efficient dynamic proofs of retrievability," in *ACM CCSW*, 2016.

[18] ——, "Transparent, distributed, and replicated dynamic provable data possession," in *ACNS*, 2013.

[19] E. Esiner, A. Kachkeev, S. Braunfeld, A. Küpçü, and Ö. Özkasap, "Flexdpdp: Flexlist-based optimized dynamic provable data possession," *ACM Transactions on Storage*, vol. 12, no. 4, 2016.

[20] E. Esiner, A. Küpçü, and Ö. Özkasap, "Analysis and optimization on flexdpdp: A practical solution for dynamic provable data possession," in *ICC*, 2014.

[21] A. Küpçü, "Official arbitration with secure cloud storage application," *The Computer Journal*, vol. 58, no. 4, pp. 831–852, 2015.

[22] "e-devlet kapısı devletin kısayolu," www.turkiye.gov.tr, [July. 17, 2019].

[23] R. S. P. Leach, M. Mealling, *A Universally Unique IDentifier (UUID) URN Namespace*, https://www.rfc-editor.org/info/rfc4122, 2005.

[24] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *AICCSA*, 2009.

[25] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Otp-based two-factor authentication using mobile phones," in *ITNG*, 2011, pp. 327–331.

[26] T. Acar, M. Belenkiy, and A. Küpçü, "Single password authentication," *Computer Networks*, vol. 57, no. 13, pp. 2597–2614, 2013.

[27] D. İşler and A. Küpçü, "Threshold single password authentication," in *ESORICS DPM*, 2017.

[28] D. İşler, A. Küpçü, and A. Coşkun, "User perceptions of security and usability of mobile-based single password authentication and two-factor authentication," in *ESORICS DPM*, 2019.

[29] D. İşler and A. Küpçü, "Distributed single password protocol framework," Cryptology ePrint Archive, Report 2018/976, 2018.

[30] ICAO, "Doc 9303, machine readable travel documents part 7: Machine readable visas," 2015.

[31] "Republic of turkey electronic visa application system," https://www.evisa.gov.tr/en/, [May. 26, 2019].

[32] "Authorized portal for visa application to india," https://indianvisaonline.gov.in/, [May. 26, 2019].

[33] Z. Říha, "An overview of electronic passport security features," in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds. Springer Berlin Heidelberg, 2009, pp. 151–159.

[34] ICAO, "Doc 9303, machine readable travel documents, part 11: Security mechanisms for mrtds," 2015.

[35] ——, "Logical data structure (lds) for storage of biometrics and other data in the contactless integrated circuit (ic)," 2015.

[36] "arachni," https://www.arachni-scanner.com/, [July. 29, 2019].

[37] E. Torres, "Wmap using metasploit framework," https://www.metasploit.com/, [July. 29, 2019].

[38] A. Küpçü, "White paper on self study cryptography course," DOI: 10.13140/RG.2.2.13320.37124. [Online]. Available: https://sites.google.com/a/ku.edu.tr/self-crypto/