ePassport Protocol on the Spi Calculus

Safa Saoudi[1], Souheib Yousfi[2], and Riadh Robbana[3]

LIP2, Tunisian Polytechnic School, Tunisia[1],
LIP2, INSAT, Tunisia[2],
LIP2, INSAT, Tunisia[3]

Abstract. Electronic passport promises the possibility of a secure, simple and quick travel formalities. Many countries have started delivering electronic documents to their citizens. This is a proof of the importance of ePassport protocols which aim to improve the document security and the traveller authentication. Three generations of security solutions in ePassports were specified. We model via this work a new protocol of ePassport to provide better authentication and to protect sensitive data. Elliptic curve cryptography and secret sharing scheme present the main topics referred to in the proposed protocol. This coupling strengthens the eMRTD security, data storage and the authentication of both ePassport and its bearer. The Spi calculus is an adequate formalism to model cryptographic aspect of such electronic protocol and allows us to verify its properties.

Keywords: ePassport, Border Security, Authentication,Secrecy, Elliptic Curve Cryptography, Secret Sharing, Spi Calculus

1 Introduction

Developing technologies and security standards has encourage governments to pursue the issuance of more sophisticated Machine Readable Travel Documents (MRTDs) to their citizens. The electronic MRTDs, also called ePassports or biometric passports differ from the ordinary travel booklets, they contain biometric traits and embedded Radio Frequency chip to store information about the document owner. A successful implementation of biometric and radio frequency identification (RFID) technologies [11] aims to enhance the security level. Malaysia is the first nation to issue electronic passports to its citizens. The first major step towards the global implementation of electronic passports was taken by the United States in 2006. US mandates the adoption of electronic passports by the 27 nations in its Visa Waiver Program (VWP) to increase the security of borders [22]. Border control authorities should benefit from secure ePassports. In fact, this electronic document provides automated verification of identity, faster immigration inspection and greater border protection and security. The most important processes, that aim to provide border security, are the authentication of the ePassport chip and the identification of its bearer. Since the data stored in the ePassport is digital, it is easily altered or used by attackers. First generation specifications of electronic documents is based on standards set by the International Civil Aviation Organization (ICAO). However, many security threats are detected in the first generation. Therefore, a new specification, based on a set of protocols, is proposed to cover certain flaws of the first generation [6]. But, some concerns still needed to be addressed in this second generation [12]. To improve ePassport security, several protocols are proposed in order to move to a third generation [22].

1.1 Related Work

Because of the sensitive data that can be stored in ePassport and the importance of this document, several studies are conducted in order to enhance security and privacy issues of ePassport. The International Civil Aviation Organization (ICAO) is the first responsible organization for cross border policies and air travelling standards. It sets a standard specification for ePassports. It defines a security mechanism based on several protocols with the use of RFID (Radio Frequency Identification) and biometric technologies [7]. However, after the adaptation of this standard, Juels et al. describe in their analysis of United States ePassport [11] the privacy and security issues. They highlight important vulnerabilities about authentication: the use of unauthenticated access to read chip information may increase the risk of attacks and the cryptographic system based on Basic Access Control (BAC) suffer from the low entropy of key generation mechanism. They try to provide solutions for some ICAO specifications weaknesses. To strengthen ePassport security, the European Union has released a new specification called Extended Access Control (EAC) [12]. The primary goal of EAC is to provide more comprehensive authentication protocols between terminals (Inspection System and chip) and to promote the implementation of secondary biometrics for additional security. Its specification denies access to biometric data before being authenticated as a legitimate reader to prevent unauthorized access. Pasupathinathan et al.'s analysis in [24] shows that the EU proposal does not provide sufficient security because it still considers the BAC protocol for access control and uses, in an extensive way, a Public Key Infrastructure (PKI). This puts the security mechanism in doubt. Then, they introduced a new protocol, called on-line secure ePassport protocol (OSEP). OSEP provides an active monitoring system regarding the inspection system (IS), that attempts to detect criminal behaviour. It includes a mutual authentication protocol between ePassports and IS. However, OSEP depends on online and it risks the connection failure. Researches are still in progress until today. The last official document of the ICAO published in 2015 mentions the newest protocols and standards used on electronic travel documents [8]. It considers a new access control protocol: Password Authentication Connection Establishment as replacement of BAC. The PACE is specified by the German Federal Office for Information Security (BSI) to establish a secure communication between ePassport and reader [3]. Many recent surveys: [22], [26] and [2] determine that current specifications and protocols are still insecure and allow attackers to eavesdrop, identify and track electronic passports. In this paper, we propose a new alternative in order to cover more existing flaws and to ensure better security level. We sketch the idea of building a shared secret between more than two entities in order to protect sensitive data. The importance of formal verification cryptographic protocols during the development process cannot be unheeded. Thus, we use Pi calculus to formalize the description of our authentication protocol.

1.2 Paper Organization

We first describe the related structure of an electronic passport and existing protocols. Then, we introduce our scheme providing authentication in ePassport. The proposed solution employs distributed authority mechanism. We exploit the Elliptic Curve Cryptography features. This approach aims to enhance security properties and struggles against data leakage. This paper is organized as follows: the next section describes the ePassport structure and the used technologies. In section 3, we describe the existing schemes and mention some of their vulnerabilities. In section 4, we introduce a detailed description of our contribution. Section 5 contains a formal verification of the ePassport protocol and an automated verification using Proverif reasoning tool. Finally, we conclude this work. The aim of this contribution is to avoid falsification, identity theft and to prevent authentication flaws by protecting the stored data in the ePassport and to ensure that the bearer is genuine.

2 Epassport Structure

This section sheds the light on the technical structure of the existing ePassport. Two main specifications distinguish an electronic Machine Readable Travel Document (eMRTD) from a classic one: the Radio Frequency Identification (RFID) technology and the Integrated Circuit Card (ICC) adapted to communicate with RFID tags or readers.

2.1 RFID

Radio Frequency Identification is a term for a family of technologies that transmit data via a wireless network based on Radio frequency radiations. The advantage of RFID is the absence of direct contact or line-of-sight scanning [14]. An RFID system consists of three components: an antenna, a reader and a tag (a small embedded chip). The antenna uses radio frequency waves to transmit a signal that activates the reader. When activated, the tag transmits data back to the antenna. This data is used to notify a programmable logic controller that an action should occur. The action could be as simple as raising an access gate or as complicated as interfacing with a database to carry out a monetary transaction [11]. Integration of RFID technology for ePassport began in 2004. The ICAO specification for ePassports relies on the International Organization for Standardization (ISO) 14443 standard, which specifies a radio frequency of

13.56MHz. This frequency have short transmission ranges. It's between 10 centimetres and 1 meter [1]. This short range of interrogation zone allow powering the tag of ePassport chip in order to communicate with the reader.

2.2 Integrated Circuit Card

To ensure a global interoperability, the ICAO issues a standardized data structure called Logical Data Structure (LDS) for the storage of data elements. The LDS initially consists of 16 data groups. The specifications state that all the 16 data groups are write protected and can be written only at the time of issue of the ePassport. A hash of data groups 1-16 are stored in a (SO_D) , each of these hashes should be signed by the issuing state. So, an Integrated Circuit Card (ICC) of ePassport is composed of a LDS and SO_D . ICAO specifies that only DG1 and DG2 are mandatory and the rest of DGs depends on the issuing country schemes and implementation. The Figure 1 from ICAO official document [9] presents the data embedded in the contactless chip conforming to the ICAO guidelines.

2.3 ISO/IEC Biometrics

Biometrics are considered as sensitive data. They are used as supplemental verification item to enhance security. To protect biometrics while storage and transfer, ISO/IEC 24745 provides a standard under various requirements. The architecture according to ISO/IEC is valid for all biometric modalities. When enrolment of a biometric modality takes place, a feature extraction from the captured sample results a Pseudonymous Identifier (PI) and Auxiliary Data (AD). During a verification, a new feature extraction from fresh biometric sample results a new pseudonymous identifier (PI^*) which equals PI if and only if the same person provided the biometric sample [5].

3 Security Issues of ePassport

3.1 Cryptographic Protocols

In order to provide full protection of electronic passport, a set off security features is implemented. Cryptographic protocols are specified to prevent skimming of data from the Integrated Chip (IC), prevent eavesdropping on legitimate communication between IC and reader. Thus, ICAO [8] defines a batch of protocols to achieve the following goals

- Gain a secure access to IC,
- Data authentication,
- Chip authentication,
- Additional access mechanism to biometrics,
- Reading data securely.

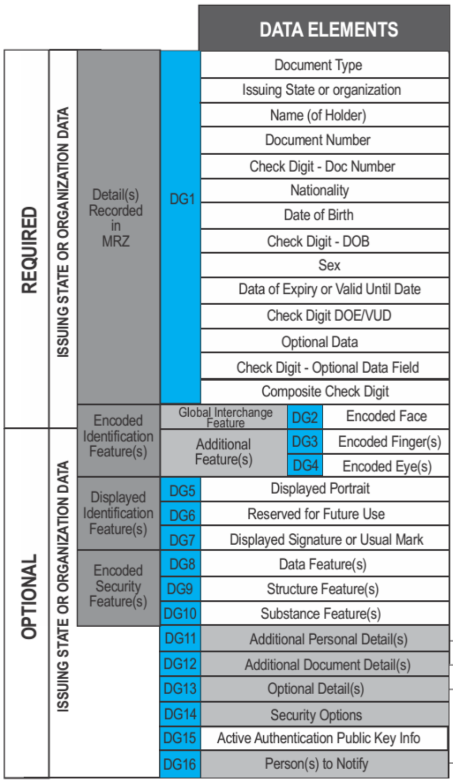

Fig. 1: Logical Data Structure.

In literature, two protocols are dedicated to provide access control: Basic Access Control (BAC) [8] and Password Authentication Connection Establishment (PACE) [18].

BAC: Is a session key establishment mechanism based on symmetric cryptography. Keys are derived from Machine Readable Zone (MRZ) of the ePassport, Document Number(DN), Date Of Birth (DOB) and Date Of Expiry (DOE) followed respectively by their checksums are the extracted data and concatenated under $SHA\breve{}1$ to result a key K_{seed}. The 16 more significant bytes of K_{seed} are concatenated to 00000001. The result is hashed under $SHA\breve{}1$ to compute the key encryption K_{ENC}. The same process is performed to compute K_{MAC} by concatenation of K_{seed} to 00000002.

$$K_{seed} = SHA\_1(DN|DOB|DOE)$$

$$K_{ENC} = SHA\_1(K_{seed}|00000001)$$

$$K_{MAC} = SHA\_1(K_{seed}|00000002)$$

Then, a set of messages is exchanged between IC and reader to verify keys and to establish a session and secure messaging mechanism.
PACE: Is a supplemental access control launched in 2014. It is a countermeasure to weaknesses of BAC. PACE is a Diffie-Hellman [4] key agreement protocol that provides secure communication and password-based authentication of the IC and the inspection system (IS). IC and IS share the same password Π and the same key $K_{\Pi} = SHA\_1(\Pi|3)$. PACE establishes secure messaging based on weak (short) passwords.
Passive Authentication PA: To ensure data authentication, the Document of Security Objects SO_D contains hashes of existing data groups and is signed by the issuing country. Inspection systems contain Document Signer public keys of each State or have read related certificates. It is a passive authentication mechanism that read hashes and verify signature of SO_D to validate data authenticity and integrity. PA is the only mandatory protocol [8].
Active Authentication AA: Implementing this protocol makes the chip authenticate itself to the reader. AA public key is stored in the data group DG15 and its corresponding private key in stored in a secure memory of the integrated chip. AA aims to verify is not cloned.
EAC: To protect supplemental sensitive information, an Extended Access Control (EAC) mechanism takes place. EAC is a set of Extended Access Keys used instead of BAC [3]. EAC still not standardized by the ICAO. Each issuing country define its own security measures. For European Union, the BSI defines two protocols: Chip and Terminal authentication (CA and TA).
CA: Keys are computed using Diffie-Hellman key agreement protocol. CA provides implicit authentication of both IC itself and the stored data by performing secure messaging after establishment of session keys.
TA: A successful execution of terminal authentication is a proof to the chip that interrogating reader is not an intruder. This protocol requires a specific certification architecture. Regarding to the BSI, each country issuing EAC ePassport needs a trusted point: Country Verifying Certificate Authority (CVCA) issues Document Verifier DV certificates. CVCA public key must be stored in ePassport chip and DV issues certificates for Inspection Systems. More details are set in [3].

3.2 Vulnerabilities

Many vulnerabilities have been identified in the literature. Attacks can be classified according to their objectives [2].

- Obtaining data contained in ePassport's chip,
- Recognition of a set of passports,
- Recognition of individual passport,
- Obtaining a proof of presence.

Attackers can easily identify and track an ePassport. The main flaw is the absence of a standard normalization. It is a lack of interoperability. According to

ICAO specification, only two GDs are required and the rest is optional. Security measures depends on issuing country. This diversity is a beneficial factor for attackers to identify batch of ePassport depending on error messages, response time and other aspects related to manufacturing and country policies. The security of the BAC protocol is based on a low entropy of two access keys derived from data items on the MRZ of ePassport. Keys are easily guessable because their entropy is, at maximum 46 bits. In some cases, when the MRZ generation pattern is known, the entropy is lower. This allows identifying an ePassport, tracking and obtaining its data applying brute-force attacks. PACE provides better entropy compared to BAC but still depends on passwords derived from MRZ. PA and EAC require sophisticated cetification structure and roots verifications. ePassports suffer from lack of international standards and implementations.

4 Proposed Scheme

Our proposal is based on the Elliptic Curve Cryptography and its advantages specially for ICC.

4.1 Elliptic Curve Cryptography

Elliptic curves have been studied in mathematics for 150 years. Their use within cryptography was first proposed in 1985, by Koblitz [13] and Miller [19]. Elliptic Curve Cryptography (ECC) is based on properties of a particular type of equation created from the mathematical group derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result [25]. Kobliz and Miller believe that the Discrete Logarithm Problem (DLP) is harder to solve for elliptic curve than for a finite field. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is described as follows: P is a point on the curve, if $Q = xP$, where x is a digit, try to find x. It is hard for an attacker to retrieve x. ECC offers a same or stronger level of security using much smaller keys. It is an attractive option for electronic documents such as ePassports that contain smart cards which have less memory because of the decreased key size and computational complexity. For example, to use Rivest Shamir Adleman (RSA) [16] or Diffie-Hellman (DH) [4] cryptographic protocol for a 128-bit symmetric key security level, RSA and DH should use 3072-bit parameters and equivalent key size for elliptic curves is only 256 bits [21]. So, ECC provides smaller key sizes resulting in faster computations with lower power consumption and memory. The most standard form used in ECC is the Weierstrass-form defined as bellow :

Let F_q be a finite field, $q = p^m$ where p is a prime number and m is integer ($m >>> 1$), E is an elliptic curve defined over F_q for $a, b \in F_q$ such that $4a^3 + 27b^2 \neq 0$

$$E : y^2 = x^3 + ax + b \tag{1}$$

for $a, b \in F_q$ such that $4a^3 + 27b^2 \neq 0$.
Montgomery [20] introduced the non-standard form of elliptic curves

$$E^M : by^2 = x^3 + ax^2 + x, \ (a, b) \in F_q \tag{2}$$

The Montgomery form of elliptic curves is faster than the Weierstrass form elliptic curves by about 10 percent [23].

Although ECC is not a dominant implementation for cryptography, it promises a high security with harder discrete logarithm problems. It will be used in practice progressively to instantiate cryptographic protocols. In this paper, we consider elliptic curves over a finite field F_q. We describe in the following the proposed scheme.

4.2 The Protocol in Detail

The protocol begins in a setup phase. In this stage, a set of authorities in cooperation generate the key materials and publish the corresponding public parameters. Then, the registration phase takes place. In order to authenticate himself, an ePassport bearer needs to prove his identity using his fingerprint template.

Our system consists four entities:

- **The user** is the person who requests to have an ePassport noted **US**;
- **The reception authority** that delivers ePassport at the citizen request noted **RA**;
- **The document verifier** is the entity who confirms the ePassport creation (It can be the interior ministry), noted **DV**;
- **The inspection system** verifies the eMRTD and its bearer while crossing border, noted **IS**.

Personalization phase

First, the user is enrolled during the personalization phase. His biometric enrolment is realized according to the ISO/IEC 24745 and resulting (PI/AD) [10]. Secondly, the RA sends this information to DV in order to check if this applicant has the right to own an eMRTD (not criminal, don't have another travel document...). When receiving the validation from the DV, the RA of issuing country personalizes the ePassport and adds the appropriate data on the LDS of the ePassport 1 then delivers the electronic document to the applicant with a unique ID and a date of expiration. At this stage, the ePassport is ready to be used.

Security features

As prerequisite, we consider the equation 2 of the Montgomery form [20] over a finite field $\mathbb{F}_q$, P a generator of E^M, $P \in E^M$ and a hash function

$$H_1 : \{0, 1\}^* \rightarrow E^M$$

While personalization of ePassport, the applicant, the reception authority and the document verifier are authorities of the system. **Secret Sharing** scheme consists of creating a secret between more than two participants. To guarantee the approach success, it is mandatory that one of the authorities must be honest. In ePassport case, the issuing country is considered the most honest entity (represented via the DV). Each authority participate to the scheme by generating a part of the secret. The entire performs as a distributed key generator. Otherwise, each entity knows a master key fragment. Computation can be performed only when the three authorities collaborate. To establish a secure authentication process, the applicant offers the first fragment of the secret. It's extracted from his biometric template noted S_1: Since secret is derived from the user identity (his fingerprint template), it presents a strong mapping between an ePassport and its owner. The process of biometric enrolment is standardized and protected according to the ISO/IEC 24745 [10]. The RA provides the second part S_2 and the secret is completed by the DV fragment S_3. So, S_A is the shared secret needed. The key S_A is the sum of the fragments $S_i \in \mathbf{Z_q}$ of each authority.

$$S_A = S_1 + S_2 + S_3 \tag{3}$$

In order to build the secret, parties engage in an interactive protocol to map secret with the elliptic curve. The mapping of the 3 segments of the secret is described as follow:

$$S_1 = H_1(PI) \tag{4}$$

$$S_2 = H_1(X_a) \tag{5}$$

$$S_3 = H_1(X_{dv}) \tag{6}$$

while PI is generated from the biometric enrolment (Personal Identifier), X_a and X_{dv} are random numbers chosen respectively by the reception authority and the document verifier. Then, an ePassport Identifier (ID), Expiration Date (ED) and the built secret S_AP are written on the LDS (Figure 1): Data is stored in the related DGs and S_AP is hashed in the Document Security Object (SO_D). The DV is the most honest authority as mentioned above. It supplies a segment of the secret to the IS to avoid connexion establishment risks. In fact, it sends an entity $X = S_2P + S_3P$ and the inspection system saves it in its local database. Then, the electronic document is delivered to its owner. Now, the ePassport is ready to be used.

Operational use

To verify the traveller's identity and if the ePassport is original, the Inspection System (IS) needs to collect data and verify the secret. As prerequisite, this approach is run under the assumption that a Password Authentication Connection Establishment (PACE) is executed in order to establish a secure communication between IS and the ePassport chip. Reading the MRZ allows inspection system to load the corresponding certificates and parameters of electronic document and its issuing country. Consequently, IS queries its local data base to get the secret fragment given by the DV after the registration phase ($X = S_2P + S_3P$).

A connection is established between the chip and the IS in order to read the stored secret S_AP. The ePassport bearer needs to regenerate his segment of the shared secret. Thus, a biometric probe is measured and (PI*, AD) are extracted, the secret (S'_1P) is generated and sent to the IS when P is a generator of the elliptic curve.

As mentioned above, the DV sends beforehand the partially generated secret $X = S_2P+S_3P$. IS retrieves the secret $S'_AP = S'_1P+X$ after receiving S'_1P and compares it to S_AP stored in the chip of correspondent ePassport. The proposal aims to optimize the use of resources by using only one elliptic curve and to avoid storage of all the user entire related data in the DV database. The short keys length is an interest for the RFID technology which uses less memory. From a secure point of view, our contribution provides an authentication protocol based on the uniqueness of fingerprint template, ECC and secret sharing advantages. On the proposed scheme, there is no need to verify independently the chip and its holder.

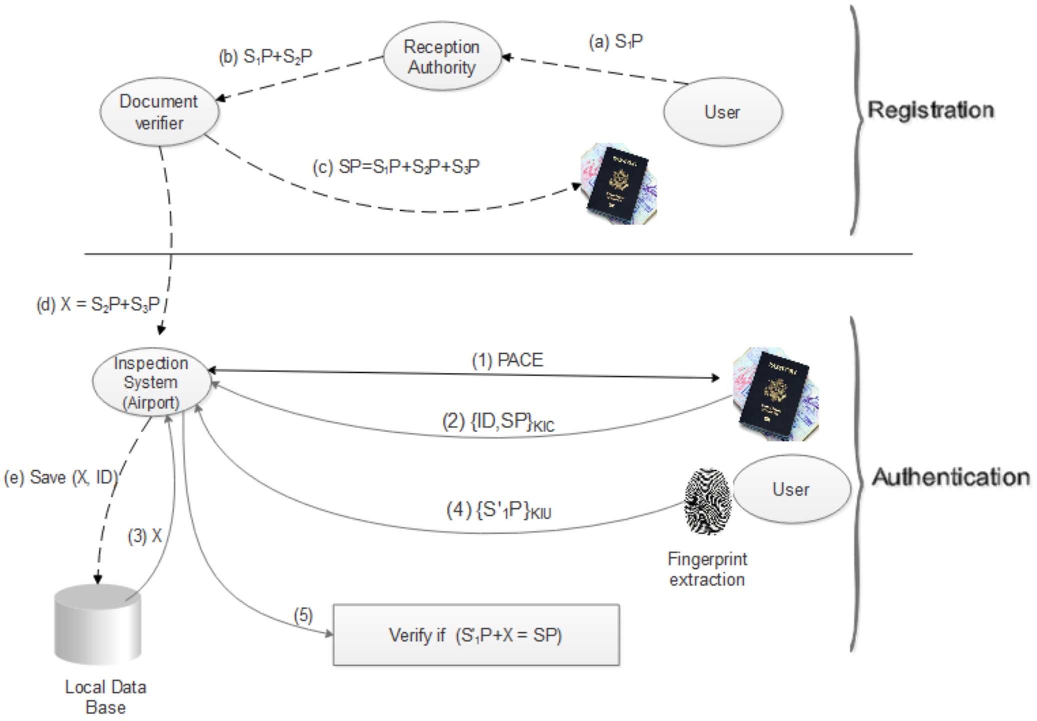

Fig. 2: Scheme of exchanged messages

The next session describes an analysis and a formal verification of the protocol authentication process with the Spi calculus.

5 Formal Verification of Proposed Scheme

The need for applying formal methods has been recognized and widely used. It helps specifying and reasoning about security properties. The Spi calculus [15], which is a variant of the Pi calculus extended with shared-key cryptographic primitives seems to be well-suited for modelling our security protocol. We define the Spi calculus language and an initial model of our ePassport process using this formal grammar.

5.1 The Spi Calculus

The Spi calculus is a language for describing systems of processes that communicate on named channels. It is a mathematical model that describes concurrent processes and their interactions. It has been used to study a variety of security protocols, such as those for private authentication.

Grammar

To describe protocols with the Spi calculus, one needs to define a set of names, a set of variables which will be used in order to define terms. Processes are considered to describe behaviour and terms are representing data (messages, keys, channels). We start with a sort of variables (such as x and y) and a sort of names (such as n). The set of terms is defined by the grammar:

$U, V ::=$	terms
c, n, s, K	names
(M, N)	pair
x, y	variables
0	zero
$suc(M)$	successor
$\{M_1, .., M_k\}_N$	shared-key encryption

The set of processes is defined by the grammar The nill process 0 does nothing, $P \mid Q$ is the parallel composition of P and Q, the replication $!P$ behaves as an infinite number of copies of P running in parallel. The process $\nu n.P$ makes a new name n then behaves as P. We often use ν as a generator of unguessable seeds. In some cases, those values may serve as nonces or as keys. In others, they may serve as seeds, and various transformations may be applied for deriving keys from seeds. The match $[M\ is\ N]P$ construct if $M = N$ then P else the process is

$P, Q ::=$	plain processes
0	nil process
$P \mid Q$	parallel composition
$!P$	replication
$(\nu n).P$	name restriction
$[M\ is\ N]P$	match
$u(x).P$	message input
$\bar{u}\langle N\rangle.P$	message output
$case\ L\ of\ \{x\}_N\ in\ P$	sharedkey decryption

stuck. The input process $u(x).P$ is ready to input from channel u, then to run P with the actual message replaced for the formal parameter x, while the output process $\bar{u}\langle N\rangle.P$ is ready to output message N on channel u, then to run P. In both of these, we may omit P when it is 0. Processes are intended to represent the components of a protocol, but they may also represent attackers, users, or other entities that interact with the protocol. As an abbreviation, we may write: let $x = U$ in P. It can be defined as $(\nu c)(\bar{c}\langle U\rangle|c(x).P)$, where c is a name that does not occur in U or in P. Shared-key decryption process runs when a shared key N is only known by the sharing principals. It attempts to decrypt a term L with the key N.

5.2 Protocol modelling

The Spi calculus representations of protocols often model secure channels as primitive, without showing their possible cryptographic implementations. As preliminaries, we assume that c is a secure channel on which all principals may communicate. Therefore, we do not restrict the scope of c with the ν operator. In our formulation, it is possible for a principal to receive a message intended for other principal, and for the processing to get stuck. Master keys are related to trusted authorities witch are : Inspection system, document verifier and reception authority. On the verification phase, only IS master key is needed K_I. We model the messages in the protocol rather directly. We describe each principal of the ePassport protocol via a process: C for the chip, I for the inspection system and U for the User. The variable msg is used as and $msg =$ "Get_id" and the id refers to the ePassport identifier which is known by the inspection system after reading the MRZ. K_{IC} is a shared keys between Inspection System and Chip. K_{IU} is a shared keys between Inspection System and User.
The process F represents the behaviour of Inspection System while comparing collected data. We assemble the pieces so as to represent a system with the process P.

$$
\begin{array}{ll}
C(id, SP, msg) & \triangleq\ c(x).case\ x\ of\ \{msg\}_{K_{IC}}\ in \\
 & [x_1\ is\ msg] \\
 & \\
 & \nu(SP).(\bar{c}\langle\{id, SP\}_{K_{IC}}\rangle). \\
I(id, msg) & \triangleq\ \bar{c}\langle\{msg\}_{K_{IC}}\rangle in \\
 & c(y).case\ y\ of\ \{x_1, x_2\}_{K_{IC}} in \\
 & [x_1\ is\ id] \\
 & c(z).case\ z\ of\ \{z_2\}_{K_{IU}} in \\
 & F(z_2, x_2). \\
 & \\
U(S'_1P) & \triangleq\ \nu(S'_1P)\ \bar{c}\langle\{S'_1P\}_{K_{IU}}\rangle. \\
 & \\
F(x, y) & \triangleq\ [x\ is\ y].0 \\
 & \\
P & \triangleq\ \nu(K_{IC}, K_{IU})(\ !C \mid !I \mid !U \mid !F\ )
\end{array}
$$

Discussion

Discrete logarithm problem Let A be the process of an active intruder. As mentioned above, if a process receives a message from an intended principal, the processing gets stuck. We suppose that the intruder breaks a key and tries to behave as one of the principals.

$$
\begin{array}{ll}
A & \triangleq\ \bar{c}\langle\{msg\}_{K_{IC}}\rangle in \\
 & c(x).case\ x\ of\ \{y\}_{K_{IC}}.
\end{array}
$$

This scenario is the hardest that an intruder can get. Even if a shared key is guessed or broken, the secret S_AP is not broken because it still protected by the DLP (Discrete logarithm problem) and is applicable to all communicated messages via the ePassport protocol. This way, we guarantee the authentication property.

Observational Equivalences In the analysis of protocol security, we usually verify that two given processes cannot be distinguished by any attacker. The processes are observationally equivalent. In Spi calculus, static equivalence is written $\approx_s$ it relates processes that cannot be distinguished by any term of comparison [15]. Firstly, the attacker cannot distinguish two messages sent to the same principal from two different instances (two ePassports proceeding the authentication) : For example

$$\nu(M_1).\bar{c}\langle\{id1, M_1\}_{K_{IC}}\rangle \approx_s \nu(M_2).\bar{c}\langle\{id2, M_2\}_{K_{IC}}\rangle$$

M_1 and M_2 are not distinguished by A. An attacker who observes the communicated messages cannot distinguish the two substitutions and the secret S_AP still protected. The proposed protocol may detect many threats and cover ePassport security flaws: Cloned document, unauthorized ePassport, unauthorized ePassport holder can be detected if the comparison of shared secrets results a failure.

6 Conclusion

This paper presents the ePassport specifications and reveals the evolution of cryptographic protocols used to improve MRTDs security features. It points out weaknesses of previous generations specified by ICAO, EU and BSI. In a second part, the paper illustrates a new scheme of ePassport authentication. The protocol is based on Elliptic Curve Cryptography, uniqueness of biometric features and the secret sharing between entities. The proposed scheme is modelled and verified (manual reasoning) using the Spi calculus. An automated analyse of the property of secrecy succeeds using Proverif verification tool. Nevertheless, countries follow different and dissimilar policies. Security weaknesses are based on inconsistent implementations and measurements. This work aim to reduce vulnerabilities and help to build a more robust solution for the future.

References

1. Smart Border Alliance. Rfid feasibility study final report. 2004.
2. G. Avoine, A. Beaujeant, J. Hernandez-Castro, L. Demay, and P. Teuwen. A survey of security and privacy issues in epassport protocols. volume 48, pages 1–37, 2016.
3. BSI. Advanced security mechanisms for machine readable travel documents and eidas tokens. In *Part 1: eMRTDs with BAC/PACEv2 and EACv1*. German Federal Office for Information Security, 2015.
4. Diffie and Hellman. New directions in cryptography. In *IEEE Transactions on Information Theory 22*, pages 644–654, 1976.
5. C.Mueller G.Duffy B.Deufel and T.Kevenaar. Biometric passwords for next generation authentication protocols for machine-readable travel documents. In *In DuD:Datenschutz und Datensicherheit*, 2013.
6. Feng Hao, Ross Anderson, and John Daugman. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.
7. ICAO. Machine readable travel documents. In *Part 1: Machine Readable Passport, Specifications for electronically enabled Passports with Biometric Identification Capabilities*, Canada, 2006. INTERNATIONAL CIVIL AVIATION ORGANIZATION.
8. ICAO. Machine readable travel documents. In *Part 11: Security Mechanisms for eMRTDs*, Canada, 2015. INTERNATIONAL CIVIL AVIATION ORGANIZATION.
9. ICAO. Machine readable travel documents. In *Part 10:Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*, Canada, 2015. INTERNATIONAL CIVIL AVIATION ORGANIZATION.
10. JTC1, SC27, and IS. Iso/iec 24745, biometric information protection. 2011.
11. A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in epassports. pages 74–88, 2005.
12. Justice and Home Affairs. Eu standard specifications for security features and biometrics in passports and travel documents. In *Technical report*, pages 48–63, 2006.
13. N. Koblitz. Elliptic curve cryptosystems. volume 48, pages 203–209, 1987.

14. B. LIANG. Security and performance analysis for rfid protocols. In *ProQuest LLC*, 2011.
15. M.Abadi and A.D.Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148(1):1081–1088, 1999.
16. Marjono and M. Phil. The rivest, shamir, adleman (rsa) public key cryptosystem and cyclic codes. In *INTEGRAL*, volume 7 no. 1, 2002.
17. M.Fischlin, J.Bender, and D.Kugler. Security analysis of the pace keyagreement protocol. In *In Information Security Conference ISC*, 2009.
18. M.Fischlin, J.Bender, O.Dagdelen, and D.Kugler. The pace|aa protocol for machine readable travel documents and its security. In *In Financial Cryptography and Data Security - 16th International Conference*, 2013.
19. V. Miller. Use of elliptic curves in cryptography. In *Lecture Notes in Computer Science,CRYPTO'85*, volume 218, pages 203–209, 1985.
20. L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. volume 48, pages 243–264, 1987.
21. Security Agency National. The case for elliptic curve cryptography. 2009.
22. R. Nithyanand. A survey on the evolution of cryptographic protocols in epassports. In *IACR Cryptology ePrint Archive*, pages 1–15, 2009.
23. K. Okeya, H. Kurumatani, and K. Sakurai. Elliptic curves with the montgomery-form and their cryptographic applications. volume 1751, page 238–257, 2000.
24. V. Pasupathinathan, J. Pieprzyk, and H. Wang. An on-line secure e-passport protocol. volume 4991, pages 14–28, 2008.
25. W. Qingxian. The application of elliptic curves cryptography in embedded systems. In *ICESS Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05)*, pages 527–530, 2005.
26. A. Sinha. A survey of system security in contactless electronic passports. volume 4, pages 154–164, 2010.