SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

Design of an RFID-embedded e-ID System for Privacy Protection

Sungbae Ji * Zeen Kim * Kwangjo Kim *

Abstract— An e-ID is considered to be an electrical form of official identification cards such as a national ID (NID) and an e-Passport to authenticate nationality or citizenship of an e-ID holder. Many countries are adopting e-ID systems in order to automate and facilitate the procedures of identification. Because an e-ID can be used for on-line identification with certificates, we can efficiently accommodate various kinds of services such as e-Government, e-Commerce, and online banking at reasonable cost. An ICAO-conforming e-Passport is a typical example of e-IDs used worldwide. It gets important as a universal e-ID in a globalized world. However, security and privacy issues of e-Passport have been raised because sensitive personal information including biometric data is stored in the e-Passport RFID chip and sent via insecure wireless channels. In this paper, we research security and privacy problems in RFID-embedded e-ID systems and discuss global trends in e-ID standards, especially in current e-Passport technologies. We also design an e-ID system to protect e-ID holders' privacy based on fine-grained access control and secure messaging with EAC Chip Authentication. Our proposed e-ID system can protect unnecessary information leakage because an e-ID replies the only data, which an e-ID reader requested, in an encrypted form. Also, an e-ID issuing authority authenticates the reader and verifies whether the reader requests data more than its access rights.

Keywords: RFID, e-ID, Privacy Protection

1 Introduction

An e-ID is considered to be an electrical form of official identification cards to authenticate nationality or citizenship of an e-ID holder. Many countries are adopting e-ID systems in order to automate and facilitate the procedures of identification. Japan and Singapore have already started to issue their national e-IDs from 2003, and China also has been issuing a national e-ID from 2004. Especially, China plans to issue an RFID-embedded national e-ID to more than a billion of population until 2010. Korea also have a plan to take a trial of e-ID for 10 thousand citizens.

An e-Passport is another type of e-IDs. Influenced by the International Civil Aviation Organization (ICAO) standard on machine-readable e-Passports for interoperability, 36 countries including 28 European countries, 7 Asian countries, and the United States (US) have adopted e-Passports as of June 2007. Additionally, about 15 countries are going to issue e-Passports until 2008. The Visa Waiver Program (VWP) initiated by the US [9] also accelerates this global trend because VWP nationals with e-Passports can travel to the US for tourism or business for stays of up to 90 days without obtaining a visa.

The reason why many countries are adopting e-ID systems recently is that e-IDs can be used not only for the benefit of simplified identification but also for the convenience of many applicable services. Because an e-ID can be efficiently used in on-line identification with certificates (*e.g.* e-Government, e-Commerce, and online banking services), we can build an efficient social overhead capital (SOC). Moreover, physically unforgeable or cryptographically secure features in the e-ID can prevent it from being abused by crimes. Especially, e-Passports can make it easy to deal with international crime or terror threat.

However, security and privacy issues of e-ID systems have been raised because sensitive personal information is stored in the e-ID and sent in wired or even wireless channels. e-Passports are leading e-ID technologies but several security and privacy problems of e-Passports have been pointed out by [2, 6, 5, 3, 4] even though ICAO-conforming e-Passports have introduced cryptographic protocols such as Passive Authentication (PA), Basic Access Control (BAC), Active Authentication (AA), and Extended Access Control (EAC).

Our Contributions. In this paper, we designed an RFID-embedded e-ID system for privacy protection. In our protocol, an e-ID sends the only data which an e-ID reader requests after encryption using a strong session key derived in EAC Chip Authentication. Also, an e-ID issuing authority authenticates the e-ID reader beforehand and check whether the reader requests personal data more than its access rights. Therefore, e-IDs can avoid unnecessary revealing of private information. Besides this fine-grained access control, our protocol solves problems in ICAO e-Passport protocols such as reader revocation and challenge semantics.

Organizations. The rest of this paper is organized as

* Information and Communications University, Munji-dong, Yuseong-gu, Daejeon, 305-732 Korea, {grail, zeenkim, kkj}@icu.ac.kr

follows: In Section 2, we briefly explain an e-Passport and security features in the ICAO e-Passport standard because an e-Passport is a widely used e-ID currently. We introduce PA, BAC, AA, and EAC protocols and their security problems. In Section 3, we define an e-ID system and present our protocol proposed for privacy-preserving e-ID systems. In Section 4, we analyze the security of our protocol and compare it with other protocols (*i.e.* PA, BAC, AA, and EAC). Finally, we summarize our paper with conclusion in Section 5.

2 Preliminaries

The ICAO standardizes Machine Readable Travel Documents (MRTDs) [1] such as passports and visas in Doc 9303. This de facto standard describes the specification of e-Passports which can store and transmit biometric information using contactless ISO/IEC 14443 RFID chip embedded in e-Passports. Biometric data stored in e-Passports are facial images, fingerprint, or iris data.

2.1 Communication Channels

e-Passports exchange data through an optical channel and a radio frequency (RF) channel as shown in Figure 1 [10]. The optical channel is a one-way channel from the optical memory on e-Passports to an optical reader. An optical reader reads data stored in the optical memory, *i.e.* Machine Readable Zone (MRZ) printed on e-Passports. Optical channels are relatively secure because data can be scanned only if e-Passport holders intend to open their passport to be directly scanned by a reliable optical scanner. On the other hand, RF channels are insecure two-way channels between an RFID chip and an RFID reader. Because an RFID chip and an RFID reader communicate each other over ISO 14443 air interface [12], RF channels should consider eavesdropping and skimming attacks. The backward channel of contactless RF communication has a communication range of 15 cm approximately and is relatively more secure than the forward channel. However, we can monitor the backward channel up to 10 m using antenna, amplifier, and PLL-Mixer Setup according to Carluccio *et al.*'s work [10]. Therefore, some countries protect e-Passports from unauthorized access using Faraday cages like shielding covers.

2.2 Logical Data Structure (LDS)

LDS is a logical structure for storing data into e-Passports and consists of 16 Data Groups (DGs). Two mandatory data, MRZ and facial image are stored in DG1 and DG2, respectively. Other biometric data (*e.g.* fingerprint or iris) or security information can be stored in DG3 to DG15. Security Object for the Document (SOD) contains all the hash values of each data group and the Document Signer's (DS's) signature over the hash values so that it can guarantee authenticity and integrity of LDS.

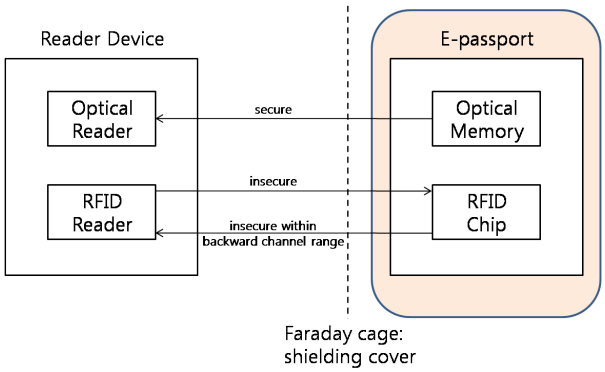

Figure 1: Communication Channels of e-Passports

2.3 Security Features in e-Passports

The ICAO e-Passport standard has three authentication or access control mechanisms: PA, BAC, and AA. However, the security and privacy problems of these protocols have been pointed out by [2, 6, 5, 3, 4]. In order to complement problems in ICAO standards, the European Union (EU) proposed and implemented EAC, but it still has some problems. In this subsection, we explain security features used in ICAO-conforming e-Passports and their problems.

2.3.1 Passive Authentication (PA)

PA is the only mandatory security mechanism in the ICAO standard. It verifies SOD to authenticate data stored in e-Passports. For a digital signature algorithm, RSA, DSA, or ECDSA are used. However, PA can be used only to provide data authenticity and integrity. e-Passports with cloned or swapped chip can bypass PA because it uses a static signature to authenticate e-Passports. Moreover, this static signature value is transferrable. Once an adversary obtains the SOD, it can be exploitable for replay attacks.

2.3.2 Basic Access Control (BAC)

BAC is optionally applied to e-Passports for confidentiality. BAC ensures that only authorized e-Passport reader can read e-Passport securely using a derived session key. BAC protocol can be applied only when an e-Passport holder intends to show their e-passport because a reader requires an optical scan of MRZ printed on the e-Passport. However, it is impossible to revoke the reader's access once the MRZ is read by the reader because anyone who knows the MRZ can successfully perform BAC protocol. Even if an adversary does not know MRZ, they can attack BAC. BAC keys (*i.e.* K_{ENC}, K_{MAC}) have small bits of entropy (*e.g.* 52 bits for U.S passport and 35 bits for Dutch passport) [2]. Carluccio *et al.* [5] proposed a hardware architecture (COPACOBANA) to perform cryptanalysis of BAC keys nearly in real-time. With COPACOBANA installed in airports and stations all over the world, an adversary can trace a specific person and also decrypt the personal information data. Liu *et al.* [11] present the first hardware implementation for cracking BAC

keys of the e-passport issuing schemes in Germany and the Netherlands based on COPACOBANA and demonstrate that this kind of attack on e-Passports is quite threatening in realistic scenarios.

2.3.3 Active Authentication (AA)

AA is an anti-cloning feature of e-Passport RF chip. In this protocol, an e-Passport signs an e-ID reader's challenge and responds with the signature, but it causes challenge semantics problem [3, 4]. The RF chip signs whatever the reader challenges. Therefore, the RF chip operates like a signature oracle in this protocol. If the reader's challenge contains the location information of the inspection system and current time, the signature can be an undeniable proof that violates e-Passport holder's privacy.

2.3.4 Extended Access Control (EAC)

EAC is a security feature adopted by the EU to restrict accessing sensitive data such as iris or fingerprint of e-Passports to authorized inspection systems only (*e.g.* border control) [7, 8]. EAC implements two authentication protocols, Chip Authentication and Terminal Authentication.

Chip Authentication - Chip Authentication is an implicit authentication protocol which verifies that the RF chip in an e-Passport is genuine. Because it solves challenge semantics problem of AA, it can replace AA. Chip Authentication also provides secure messaging between e-Passports and inspection systems using a strong session key generated by Diffie-Hellman key agreement.

Terminal Authentication - Terminal Authentication is a challenge-response protocol based on a public key infrastructure (PKI). In this protocol, an RF chip explicitly authenticates an inspection system. Inspection system with the valid certificate chain can be authenticated and access the sensitive data in e-Passports.

However, EAC can not provide fine-grained access control. It decides to allow the e-ID reader's access to only sensitive data such as iris or fingerprint. Another problem in EAC is that e-Passports can not keep current time thus it is impossible to revoke an inspection system certificate. When a compromised inspection system's certificate is not revoked, e-Passport may send their sensitive data to attackers.

3 Our Protocol

In this paper, we define an e-ID system as an RFID system for identifying people or checking their personal information. For examples, RFID-embedded e-ID systems are used for not only identifying who the e-ID card holder is but also confirming how old he or she is (*i.e.* no concern in identification but age). When an e-ID reader requests a specific personal data, the e-ID does not have to send data more than it requires. However, there is no access control for each item in current e-Passport features. For example, an e-ID reader requires an optical scan of the MRZ printed on an e-Passport in BAC, but the MRZ includes private information of the e-ID holder. Consequently, the e-ID reader can get all data included in the MRZ even if some of them may not be required. Moreover, all accesses to less-sensitive data (*e.g.* DG1, DG2, DG14, DG15, etc., and SOD) are granted to the e-ID reader after a successful BAC without considering the types of inspection systems [7]. EAC also grants the same access rights to e-ID readers for sensitive data (*e.g.* DG3 and DG4, and etc.). To solve this problem and provide fine-grained access control for privacy protection, we propose a privacy-preserving protocol for RFID-embedded e-ID systems. Our e-ID system consists of following three entities: e-ID, e-ID Reader, and e-ID issuing authority.

Table 1: Notations

Notation	Description
$\mathcal{C}$	An e-ID or an e-ID RF chip
$\mathcal{R}$	An e-ID reader
$\mathcal{I}$	An e-ID issuing authority or an issuer
$\mathcal{A}$	An adversary with RF devices
ID_A	Identity of an entity A
rnd_A	A random number generated by an entity A
SK	$\mathcal{I}$'s secret key
$\text{Sign}_{SK}(msg)$	Digital signature of msg with SK
$Enc_K(msg)$	Encryption of msg with K
m	All contents stored in $\mathcal{C}$
m_i	The i-th content stored in $\mathcal{C}$
n	The number of contents stored in $\mathcal{C}$
$seq\#$	A sequence number issued by $\mathcal{I}$
$hash(msg)$	Hashed value of msg

Entities of an e-ID System

- **e-ID:** An e-ID is an electrical form of official identification cards such as national ID (NID) and e-Passport to authenticate nationality or citizenship or to confirm a certain set personal data. An e-ID has an RF chip that communicates with an e-ID reader and stores personal information.
- **e-ID Reader:** An e-ID reader is an RFID reader to access data stored in the e-ID chip. e-ID readers belong to an official inspection system to identify e-ID holders (*e.g.* border control, police station, government service) or a commercial inspection system to retrieve and check partial data of e-ID holders (*e.g.* hotel check-in system, age restriction in the movie theaters).
- **e-ID Issuing Authority:** An e-ID issuing authority manages the whole e-ID system and issuance and revocation of e-IDs. Before issuing e-IDs, the e-ID applicant must take a formal procedure of verification and registration. The e-ID

issuing authority has a database (DB) for administration.

In our e-ID system, we assume the followings.

Assumptions

- The channel between an e-ID Reader (or an inspection system with e-ID readers) and the e-ID issuing authority is secure. We assume that the two parties authenticate each other mutually and establish a secure channel beforehand.
- The e-ID issuing authority operates with PKI but it is not necessarily a certificate authority (CA) or a root CA.
- Data items stored in e-ID chips and the e-ID issuing authority DB are subdivided as much as possible for fine-grained access control.
- e-IDs have security features for EAC Chip Authentication so as to be authenticated by an e-ID reader and derive a session key.
- To reduce communication overhead of this system, the e-ID issuing authority can have multiple replicas of its DB. When arranging replicas, the number of e-IDs that each replica can accommodate and the physical location of the replica should be considered. The e-ID issuing authority also can manage a distributed DB dispersed over multiple locations. Because the types and the locations of inspections systems decide the data items and the tuples accessed from DB, each fragment of the distributed DB can be designed as a horizontal fragment or a vertical fragment.
- If e-IDs are used globally, we require the PKI across the world based on the agreement between two countries. When a traveler goes abroad, the identification of the traveler can be done using a certificate chain between country verifying certificate authority (CVCA) and document verifying certificate authority (DVCA). During the admission into a country, the traveler's corresponding tuple can be cached into the e-ID system DB of the visited country.

Our protocol shown in Figure 2 performs the following steps. Notations used in our protocol are summarized in Table 1.

Protocol Steps

(0) In the initial state, $\mathcal{C}$ stores $seq\#$, m, and h where $m = (m_1, m_2, ..., m_n)$, $h = (h_1, h_2, ..., h_n)$, $h_i = hash(m_i)$, and $1 \leq i \leq n$. $\mathcal{I}$ also stores a tuple ($seq\#$, h) in its DB. $\mathcal{I}$ does not relate $seq\#$ to other identity information in other tables (*e.g.* social security number or resident registration number).

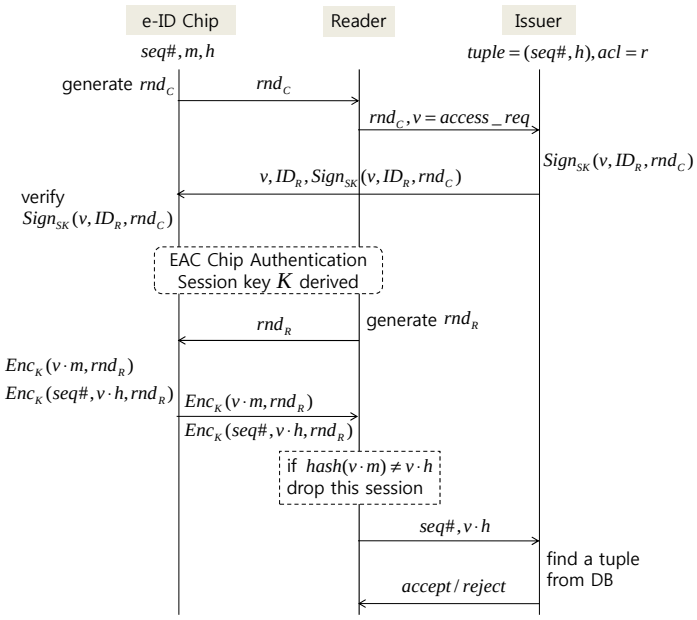

Figure 2: Our Protocol

(1) When $\mathcal{C}$ arrived within $\mathcal{R}$'s range, $\mathcal{C}$ responds to $\mathcal{R}$'s initial request with $rnd_{\mathcal{C}}$.

(2) $\mathcal{R}$ sends $access\_req$ to $\mathcal{I}$ where $access\_req = v = (v_1, v_2, ..., v_n)$, $v_i = 0$ or 1 and $1 \leq i \leq n$. $v_i = 1$ means that $\mathcal{R}$ requests m_i.

(3) $\mathcal{I}$ looks up the reader's access control list $acl = r$ and compare it with v where $r = (r_1, r_2, ..., r_n)$, $r_i = 0$ or 1, and $1 \leq i \leq n$. $r_i = 1$ means that $\mathcal{R}$ has an access right for m_i. If $v_i \leq r_i$ for each i, $\mathcal{I}$ signs v, ID_R, and $rnd_{\mathcal{C}}$ and sends the signed message $Sign_{SK}(v, ID_R, rnd_{\mathcal{C}})$ with v and ID_R to $\mathcal{C}$ via $\mathcal{R}$. Otherwise, drop this session. If $\mathcal{I}$'s certificate chain is not embedded in $\mathcal{C}$, $\mathcal{I}$ also sends its certificate chain to $\mathcal{C}$.

(4) In this step, $\mathcal{C}$ authenticates $\mathcal{R}$ by verifying $Sign_{SK}$ $(v, ID_R, rnd_{\mathcal{C}})$. If the signature is not valid, drop this session.

(5) $\mathcal{C}$ and $\mathcal{R}$ performs EAC Chip Authentication so that $\mathcal{R}$ can authenticate $\mathcal{C}$ and derive a session key K.

(6) After EAC Chip Authentication, $\mathcal{R}$ generates $rnd_{\mathcal{R}}$ and sends it to $\mathcal{C}$.

(7) $\mathcal{C}$ operates $Enc_K(v \cdot m, rnd_{\mathcal{R}})$ and $Enc_K(seq\#, v \cdot h, rnd_{\mathcal{R}})$ using K where $a \cdot b = (a_1 b_1, a_2 b_2, ... a_n b_n)$, $a = (a_1, a_2, ..., a_n)$, and $b = (b_1, b_2, ..., b_n)$.

(8) $\mathcal{C}$ sends $Enc_K(v \cdot m, rnd_{\mathcal{R}})$ and $Enc_K(seq\#, v \cdot h, rnd_{\mathcal{R}})$ to $\mathcal{R}$.

(9) $\mathcal{R}$ decrypts $v \cdot m$ and $v \cdot h$ from two received messages using K and then checks whether $hash(v \cdot m) = v \cdot h$ where $hash(a) = (hash(a_1), hash(a_2), ..., hash(a_n))$. If $hash(v \cdot m) \neq v \cdot h$, drop this session.

(10) $\mathcal{R}$ sends $seq\#$, $v \cdot h$ to $\mathcal{I}$.

(11) $\mathcal{I}$ finds a tuple $(seq\#, h)$ from its DB using $seq\#$. If $h_i = (v \cdot h)_i$ for each non-zero $(v \cdot h)_i$, $\mathcal{I}$ sends *accept* message to $\mathcal{R}$. Otherwise, sends *reject* message.

(12) If $\mathcal{R}$ receives an *accept* message, $v \cdot m$ is authentic.

4 Security Analysis

In this section, we present security analysis of our protocol. Our protocol is secure against eavesdropping, replay attacks, man-in-the-middle (MitM) attacks, tampering, cloning, and spoofing. It also provides forward security and privacy protection based on fine-grained access control (FGAC) and solves reader revocation and challenge semantics problems.

- **Eavesdropping:** Our protocol ensures data confidentiality against eavesdropping over RF channels. Using a session key K, the only requested data set $v \cdot m$ is encrypted and sent to $\mathcal{R}$.

- **Replay Attack:** $\mathcal{C}$ performs $Enc_K(v \cdot m, rnd_{\mathcal{R}})$ and $Enc_K(seq\#, v \cdot h, rnd_{\mathcal{R}})$ after receiving $rnd_{\mathcal{R}}$. Therefore, $\mathcal{R}$ can detect replayed messages if decrypted $rnd_{\mathcal{R}}$ in Step (9) is not equal to generated $rnd_{\mathcal{R}}$ in Step (6). Because $\mathcal{A}$ who does not know K cannot generate $Enc_K(v \cdot m, rnd_{\mathcal{R}})$ and $Enc_K(seq\#, v \cdot h, rnd_{\mathcal{R}})$, $\mathcal{A}$ cannot launch replay attacks.

- **Reader Revocation:** Our protocol does not require $\mathcal{R}$ revocation because the direct communication between $\mathcal{R}$ and $\mathcal{C}$ is not PKI-based. Whenever $\mathcal{C}$ needs to be accessed by $\mathcal{R}$, $\mathcal{C}$ sends a random challenge $rnd_{\mathcal{C}}$ and verifies $\mathcal{I}$'s response $Sign_{SK}(v, ID_R, rnd_{\mathcal{C}})$. In Step (4), $\mathcal{C}$ still has $\mathcal{I}$ revocation problem, but $\mathcal{I}$ is usually reliable and well-administered.

- **Man-in-the-Middle Attack:** Even though $\mathcal{A}$ actively drops, relays or inserts a message between $\mathcal{C}$ and $\mathcal{R}$ as if $\mathcal{A}$ were a legitimate chip or reader, $\mathcal{A}$ cannot generate a session key with $\mathcal{R}$ in EAC Chip Authentication phase because $\mathcal{A}$ with a fake Diffie-Hellman key pair is not able to be authenticated.

- **Tampering:** If $\mathcal{C}$ does not have a tamper-resistant mechanism, $\mathcal{A}$ can access $\mathcal{C}$ and change its contents. However, $\mathcal{I}$ can detect whether $\mathcal{C}$ has been tampered using h.

- **Cloning:** EAC Chip Authentication provides the anti-cloning feature in our protocol.

- **Spoofing:** $\mathcal{A}$ cannot pretend that $\mathcal{A}$ is a $\mathcal{C}$ because it is impossible to perform EAC Chip Authentication. Also, $\mathcal{C}$ cannot spoof either $seq\#$ or m because $\mathcal{I}$ can detect it.

Table 2: Comparison with other e-ID Protocols

Security Req.	Ours	PA	BAC	AA	EAC
Reader Revocation	O	-	X	-	X
Challenge Semantics	O	-	-	X	O
Replay Attack	O	X	O	O	O
Forward Security	O	-	X	-	O
Indistinguishability	X	X	X	X	X
FGAC	O	-	X	-	X
Tampering	O	O	-	-	-
Anti-Cloning	O	-	-	O	O
Spoofing	O	O	-	-	O
MitM Attack	O	X	O	X	O

O The protocol satisfies the security requirement or it is secure against the attack.
X The protocol does not satisfy the security requirement or it is insecure against the attack.
– The protocol is not designed for the security requirement, or the attack is not available.

- **Forward Security:** Every session, a fresh session key K is derived in EAC Chip Authentication. Even if $\mathcal{A}$ gets the current K somehow, $\mathcal{A}$ cannot decrypt the message from the previous or next sessions because anyone except $\mathcal{C}$ and $\mathcal{R}$ cannot derive a fresh session key K.

- **Privacy Violation:** m is not stored in $\mathcal{I}$'s DB and not delivered to $\mathcal{I}$. The only data requested by $\mathcal{R}$ is securely sent to $\mathcal{R}$ after encryption. Therefore, only authorized $\mathcal{R}$ can access $\mathcal{C}$ holder's private information at a minimum. Moreover, there is no challenge semantics problem in our protocol. Symmetric encryption of $rnd_{\mathcal{R}} = f(Date, Time, Location)$ in Step (7) cannot provide an undeniable proof of $\mathcal{C}$ holder's existence at a certain time and location.

However, $\mathcal{C}$ is not indistinguishable in our protocol. $\mathcal{R}$ and $\mathcal{I}$ can distinguish $\mathcal{C}$ with $seq\#$ from other e-IDs. Therefore, $\mathcal{I}$ and an inspection system which has many e-ID readers from place to place can trace $\mathcal{C}$. $seq\#$ is an inevitable element for $\mathcal{I}$ to check the authenticity of m. Using $seq\#$, $\mathcal{C}$ is traceable by $\mathcal{I}$, but $\mathcal{I}$ does not know who the $\mathcal{C}$ holder is because $seq\#$ is not related to any other ID information in $\mathcal{I}$'s DB. Also, $\mathcal{C}$ is indistinguishable to $\mathcal{A}$ (*e.g.* eavesdropper).

We summarize the security properties of our protocol compared with other e-ID protocols in Table 2. PA, BAC, AA, and EAC are the security features for more specific e-ID application (*i.e.* e-Passport), and three of them are designed in a two-party setting. Therefore, this simple comparison may be unfair, but there is no popular e-ID protocol other than these e-Passport protocols to the best of our knowledge. Because the e-Passport can be used as a domestic ID and also it gets important as a universal e-ID in a globalized world, we make a comparison between our protocol and e-Passport protocols.

When an e-Passport system uses EAC, it follows the advanced e-Passport inspection procedure [7]. Because the procedure performs PA, BAC, and AA as well as EAC according to its regular steps, the whole procedure can be insecure if one of the e-Passport protocols is insecure. On the other hand, our protocol is a standalone protocol. In our protocol, $\mathcal{R}$ does not rely on PKI in its communication with $\mathcal{C}$, it does not have to consider $\mathcal{R}$ revocation unlike BAC and EAC. Our protocols also solves challenge semantics problem in AA. EAC Chip Authentication adopted in our protocol provides the anti-cloning feature instead of AA, and $\mathcal{C}$ responds to $\mathcal{R}$'s random challenge with a symmetric encryption not a signature. Our protocol is secure against replay and MitM attacks and provides forward security using a fresh session key K derived in EAC Chip Authentication phase. The most significant improvement in our protocol is fine-grained access control. $\mathcal{I}$ can control $\mathcal{R}$'s access rights for each data item.

5 Conclusion

In this paper, we designed an privacy-preserving protocol for RFID-embedded e-ID systems and analyzed it. Our proposed e-ID system can protect e-ID holders from privacy violation based on fine-grained access control and secure messaging with EAC Chip Authentication. We also provide a comprehensive comparison with other authentication and access control protocols in ICAO-conforming e-Passport which will be a typical e-ID used worldwide. Our protocol solves several security and privacy problems in e-Passports such as reader revocation and challenge semantics. However, our protocol does not provide indistinguishability, and thus an e-ID issuing authority can trace an e-ID holder. This is an open problem whether an e-ID issuing authority can identify e-ID holders or verify their data without unique identifiers of their e-IDs.

Acknowledgement

This work presented in this paper was supported in part by IT R&D Program of Ministry of Information and Communication (MIC) / Institute for Information Technology Advancement (IITA) (2005-S-106-02, "Development of Sensor Tag and Sensor Node Technologies for RFID/USN").

References

[1] "Machine Readable Travel Documents," http://mrtd.icao.int/

[2] Ari Juels, David Molnar, and David Wagner, "Security and Privacy Issues in E-passports," *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005)*, pp. 74-88, 2005.

[3] Serge Vaudenay and Martin Vuagnoux, "About Machine-Readable Travel Documents," *Journal of Physics: Conference Series*, vol. 77, 012006 (9pp), 2007.

[4] Jean Monnerat, Serge Vaudenay, and Martin Vuagnoux, "About Machine-Readable Travel Documents: Privacy Enhancement using (Weakly) Non-Transferable Data Authentication," *RFID Security Workshop 2007*, 2007.

[5] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, Ahmad-Reza Sadeghi, "E-Passport: The Global Traceability or How to Feel Like an UPS Package," *The 7th International Workshop on Information Security Applications (WISA 2006)*, LNCS 4298, pp. 391-404, 2007.

[6] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur, "Crossing Borders: Security and Privacy Issues of the European e-Passport," *First Int'l Workshop on Security (IWSEC 2006)*, LNCS 4266, pp. 152-167, 2006.

[7] "Technical Guideline TR-03110: Advanced Security Mechanismsfor Machine ReadableTravel Documents. Extended Access Control (EAC) Version 1.1," http://www.bsi.bund.de/fachthem/epass/EACTR03110_v110.pdf, 2007.

[8] "Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD/17-WP/11)," http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP011.pdf, 2007.

[9] "Visa Waiver Program (VWP)," http://travel.state.gov/visa/temp/without/without_1990.html

[10] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch, "Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices," *Ambient Intelligence Developments Conference (AmI.d)*, 2006.

[11] Yifei Liu, Timo Kasper, Kerstin Lemke-Rust, and Christof Paar, "E-Passport: Cracking Basic Access Control Keys," *On the Move to Meaningful Internet Systems 2007 (OTM Conferences 2007)*, LNCS 4804, pp. 1531-1547, 2007.

[12] ISO/IEC 14443-2, Identification cards - Contactless integrated circuit(s) cards - Proximity cards (PICCS) - Part 2: Radio frequency power and signal interface, 2001.