PASSPORTS AND VISAS VERSUS IDS

(Extended Abstract)

George I. Davida Yvo G. Desmedt

Dept. of EE & CS,
Univ. of Wisconsin - Milwaukee
P.O. Box 784,
Milwaukee, WI 53201, U.S.A.

ABSTRACT

Most of the proposed cryptographic based electronic IDs are not adequate when used in international identification protocols. In this paper we extend the concept of a cryptographic electronic ID to a system of electronic *passports* and *visas* that surpass existing paper versions.

I. INTRODUCTION

The need to identify oneself arises in many situations: cashing a check, using a credit card, checking into hotels, etc. Some employers require the employees to wear badges for identification and/or access privileges to certain areas of the place of employment.

Identifications schemes have become an increasingly important subject in cryptology. The use of cryptography in identification was first proposed by Diffie and Hellman [5] who suggested that identification corresponded to authenticating a message of the type "I am User X". Simmons suggested the use of the physical description of a person signed by a trusted center [8]. Recently Fiat and Shamir (and later Feige, Fiat and Shamir [6]) have proposed that identification corresponds with proving that one has knowledge of a secret without divulging the secret itself using zero-knowledge proofs [7]. These schemes have problems if the testing of the physical description of a person cannot be adequately done. Furthermore if the testing of physical description is adequately done, then the security of the Fiat–Shamir and Feige–Fiat–Shamir schemes need not depend on zero-knowledge proofs (see [3] and [4]).

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 183-188, 1988.

The very definition of what a *digital* identification is, needs to be studied. The most recent definition given in [2], which is an adaptation of the definition given in [7, p. 186] is:

> In a secure identification system at least one trusted center knows which unique individual corresponds with a certain public ID. Based on his ID A is able to convince B that he is A, but B can not convince others that he is A.

Proposed solutions to the problem of identification have to be studied more thoroughly and new methods need to be investigated. In [1] new methods are proposed in the context of classification of the fundamental techniques of identification namely:

1. Methods that rely on the "complete" physical description.
2. Methods that use the "complete" natural knowledge of the individual.
3. Methods that use *artificial* knowledge.

In the next section it will become clear that a normal ID can not be used for international purposes. An electronic version of passports and visas is necessary to have higher security than existing systems (see Section III.).

II. PASSPORTS AND VISAS

Fiat and Shamir considered a passport as an example of an ID [7, p. 186]. We will see that making secure passports requires more than what is necessary for having a simple (secure) ID-card.

In an international environment there will be many centers that issue IDs. The above definition works only if one trusts the center that issues an ID. It is however clear that many countries do not necessarily trust each other. So the *assumptions* on which the security of ID-cards is based are *inadequate* in an international environment. Electronic passports are a better solution. However passports are *much more* than just IDs. So extra requirements, beside those involving trust, are necessary.

Paper passports allow another country to stamp the passport at entry or upon leaving a country. These stamps are mostly date stamps and contain the name of the country which stamps, and other information such as the maximum allowed length of stay. The fact that this information is stamped inside a passport allows anyone who inspects a passport to read this information, particularly the center

that issued the passport. Sometimes access to a country is denied because of a lengthy stay in another non-friendly country. The center that issues the passport can also decide to issue a new passport such that a part of your record of visits is hidden from outsiders, while retaining this information at the center.

The above stamps should not be confused with visa stamps, which are another issue, because these stamps are delivered *before* one visits a foreign country. Visas serve to add to the passport *host* country controls. These controls may be multiple. Their purposes are to better control foreign visitors. Visas are also used to implement controls by differentiating between temporary work-visas, permanent-work-visas, tourist-visas, etc. Visas also allow the host country to keep information about a person, by numbering the visas and by transferring the visas from one's old passport to a new one. Finally the visas allow the host country to become an issuing center that does not have to rely on trusting the passport issuing country. Indeed the passport issuing country can carry out many deceptions. They can for example issue different persons the same passport and even use the same name. The visa issuing country can detect such a fraud if it keeps track of the visitors and their physical description. The visa issuing country can also use more advanced techniques to check the physical description of the persons than the passport issuing country does. It is clear that such a need for control exists, in particular when a citizen of a terrorist sponsoring country applies for a visa. There are many other needs for visas.

The security of the actual passports, stamps and visas is very low. They rely on the myth that tamperproof paper and/or plastic documents and ink-stamps would exist. False passports are well known and are used by criminals, terrorist and spies. So there is a need for a secure version of passports and visas which satisfy the same functionalities as actual passports and visas. Waiting too long to implement electronic passports would create the bizarre situation where cryptographic based ID-cards are issued for local use, but on an international level paper documents would still be acceptable. However many more deceptions are possible in international activities than in national ones, so better techniques are necessary.

The reader familiar with the modern cryptographic techniques for identification understands easily that the techniques of ID-cards themselves can not fulfill the needs of passports. We now discuss our solution in the next section.

III. ELECTRONIC PASSPORTS AND VISAS

From now on we assume that a secure simple identification system exists. We will use such identification system to come up with the passport, but it will be clear that more is necessary.

The main idea behind electronic passports is the use of a tamperproof device which uses an ID-card technology *which additionally contains an area (special memory) where data can be* appended *and read by everybody.* This special memory, which we call an Append and Read Only Memory (AROM), is mainly intended for stamping activities (see Section II. for a description of stamps). The stamp can contain information other than the date, such as a sequence number, and may include the entire history of visits by the passport holder. The stamp itself can be signed by the host country. It is the discretion of the *host* country to make entries and to determine which data it wishes to append in this area.

Appending data to the AROM can be controlled to prevent the abuse of the passport by other organizations which may want to write information that is not relevant to the proper use of a passport. This can be accomplished by encapsulating in the passport a list of public keys of organizations *authorized* to write into the electronic passport card. The passport card first *checks* to determine if the candidate writer is allowed to write. If so, the writer presents a signed message. The passport-card checks the signature before appending the data. If finally there is no room left over for new stamps, the carrier of the passport goes back to his country issuing center and asks for a new passport. The center can then read and record all this information, if it wishes, and deliver a new passport. The issuing country can compress the data and leave it in the original passport or issue a new one.

The tamperfreeness of the passport-card is necessary to guarantee the AROM properties. Because tamperfreeness is used, identification systems that are simple to implement can be used [4].

Let us now discuss how visas are included in the system. Because *tamperfreeness and trustworthiness* of the passport are a *function of the issuing country and its technology*, a visa being created as a *separate* ID device by the host country is better than (the current paper system of) placing visas in issuing countries passports. We therefore propose *physically separate* visa devices, which are issued by the host country. The visa is a special crypto ID-card, using the host country preferred identification system. The information written in such a visa can depend on all the *passport data* of relevance, on a sequence number, history of the carrier related to previous visits and other visas and even on the carrier physical description. The idea of including in the *visa-card information about the*

passport (*e.g.*, number, name, country) increases dramatically the security of the whole system. Indeed the *rental* problem of crypto ID cards, due to inadequacy of checking the physical description [3], can then be significantly reduced. Otherwise, use of passports independent of visas, can lead to the possibility of two users *simultaneously* presenting the "same" passport at different locations. Advantages of renting passports are discussed in [3]. Additional methods to dramatically reduce the risk that IDs can be rented are discussed in [1]. It is important to point out that the separation that we propose is physical and *not logical*. The idea of logical link between IDs can be generalized. Evidently all this information can be signed by the host country.

The *visa* proposed here is not to be *considered a stamp*, which is appended to the above AROM. If the host country wishes to leave a trace in the passport, then it can create the visa, give it a sequence number and append the following message to the AROM in the passport: "The carrier of this passport possesses a visa with: number, type, issuing date, location and issuing country". However such a trace is not necessary. In fact in some cases it is even recommended not to use such a trace. Indeed, because these passports are electronic and tamperfree the passport issuing country may be able to restrict its citizens from visiting certain countries. If, however, a citizen obtains a visa for such a country, the passport could destroy itself before the carrier reaches the host country. This, for example, would prevent the carrier from asking for political asylum. A visa issuing country that wants to cooperate with the carrier could choose to not leave a trace of the visa in the passport. This, however, still leaves the visa issuing country free to use passport information in the *visa* itself. Therefore the proposed scheme again contributes to improvement of functionality of passports and visas. Again, the tamperfreeness of the visa device is important in this scheme.

We finally remark that our system is compatible with actual passports and visas. Visa issuing centers can, independently from the passport issuing centers, decide to use electronic visas, while the passport can still be a paper document. To allow countries that do not have adequate technological means to use electronic systems, a paper version is attached to the electronic one.

IV. CONCLUSION

Recent crypto based ID schemes do not have the functionality necessary for international use. In this paper a new scheme for electronic passports and visas is presented that is as functional as current schemes but more secure.

REFERENCES

[1] G. Davida and Y. Desmedt. *"Complete" Identification Systems.* Tech. Report TR-CS-88-15, Dept. of EE & CS, Univ. of Wisconsin – Milwaukee, May 1988.

[2] Y. Desmedt. Major security problems with the "unforgeable" (Feige–)Fiat–Shamir proofs of identity and how to overcome them. In *Securicom 88, 6th worldwide congress on computer and communications security and protection*, pp. 147–159, SEDEP Paris France, March 15–17, 1988.

[3] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat–Shamir passport protocol. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto'87 (Lecture Notes in Computer Science 293)*, pp. 21–39, Springer–Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.

[4] Y. Desmedt and J.–J. Quisquater. Public key systems based on the difficulty of tampering (Is there a difference between DES and RSA?). In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 111–117, Springer–Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6), pp. 644–654, November 1976.

[6] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *Proceedings of the Nineteenth ACM Symp. Theory of Computing, STOC*, pp. 210 – 217, May 25–27, 1987.

[7] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 186–194, Springer–Verlag, 1987. Santa Barbara, California, U. S. A., August 11–15.

[8] G. J. Simmons. A system for verifying user identity and authorization at the point-of sale or access. *Cryptologia*, 8(1), pp. 1–21, January 1984.