Cryptographic Protocols for Modern Identification Documents

mgr inż. Lucjan Hanzlik

Streszczenie

W niniejszej rozprawie rozważane będą kryptograficzne algorytmy w kontekście nowoczesnych dokumentów tożsamości (eID). Dokumenty te, pomimo ograniczonej pamięci i mocy obliczeniowej, mogą wykonywać silne algorytmy kryptograficzne. W szczególności dotyczy to tworzenia podpisów cyfrowych, ustanawiania klucza sesyjnego, oraz silnego uwierzytelniania.

Wiele krajów rozpoczęło już realizację swoich projektów eID. Jednak zdecydowanie najciekawszy z nich, z naukowej i rynkowej perspektywy, to niemiecki projekt nPA (Neuer Personalausweis). Projekt ten wprowadził trzy aplikacje dla elektronicznego dokumentu tożsamości: ePassport, eID i eSign. W rozprawie tej skupimy się na dwóch pierwszych aplikacjach, gdyż trzecia jest standardowa.

Aplikacja ePassport jest zgodna ze standardem ICAO do odczytu elektronicznych dokumentów podróży (MRTD). Standard ten określa szereg algorytmów i protokołów wykonywanych w czasie kontroli granicznej. Jednak nie wszystkie algorytmy są wymagane, co oznacza, że biometryczny paszport może być zgodny z tym standardem implementując jedynie wymagane algorytmy. Niestety paszporty implementujące wyłączenie te algorytmy można sklonować. W celu ochrony przed klonowaniem, należy wdrożyć niektóre z opcjonalnych algorytmów (np. Active Authentication lub Extended Access Control). Minusem takiego rozwiązania jest jednak zwiększenie złożoności czasowej i wydłużenie odprawy granicznej.

W niniejszej rozprawie wprowadzamy rozszerzenie dla jednego z wymaganych przez ICAO algorytmów (tzw. Password Authenticated Connection Establishment (PACE)), które kosztem jednego mnożenia modulo (po stronie eID) dodatkowo uwierzytelnia eID i w ten sposób chroni przed klonowaniem dokumentów. Wyniki te zostały równocześnie otrzymane przez niemiecki Federalny Urząd ds. Bezpieczeństwa Informatycznego (BSI). Urząd ten opatentował to rozwiązanie i uzyskał włączenie go do standardu ICAO dla MRTD. Jednakże należy zaznaczyć, że dowody bezpieczeństwa zaprezentowane przez BSI oparte są o niestandardowe założenia wiedzy, a tym samym formalny dowód bezpieczeństwa ma ograniczoną wartość. W niniejszej rozprawie prezentujemy dowód bezpieczeństwa oparty o standardowy decyzyjny problem odwrotności Diffiego-

Hellmana (InvDDH).

Kolejnym wkładem niniejszej rozprawy jest inne rozszerzenie protokołu PACE kompatybilne z wszystkimi jego wersjami, w szczególności z PACE Integrated Mapping. Przypomnijmy, że standard ICAO definiuje dwie podstawowe wersje PACE: PACE-IM (Integrated Mapping) i PACE-GM (Generic Mapping). Opisane powyżej pierwsze rozszerzenie działa jedynie wraz z mniej efektywną wersją tj. PACE-GM.

W aplikacji eID rozważać będziemy stos protokołów realizowany przez nPA w zakresie uwierzytelnia online. Pomysł wdrożony w niemieckich dowodach osobistych polega na tym, że oparty jest o jeden klucz prywatny, który może być używany do różnych domen aktywności ale w taki sposób, że nie można skojarzyć ze sobą tożsamości tego samego użytkownika w różnych domenach. W rozprawie sformalizujemy ten pomysł i wprowadzimy bazowy mechanizm nazwany Uwierzytelnianiem Pseudonimowym (z ang. Pseudonymous Identification), w skrócie PI. Uchwyca on pożądane, w uwierzytelnianiu online, cechy. Wykonanie protokołu PI powinno umożliwić eID udowodnienie weryfikatorowi w domenie, iż:

- dokument eID jest autentyczny,
- użyto go do wygenerowania podanego pseudonimu,
- jest to jedyny pseudonim jaki eID mógł dla tej domeny wygenerować.

Dodatkowo wymagamy, aby pseudonimy w różnych dziedzinach aktywności nie można było ze sobą skojarzyć.

Pokażemy następnie, że rozwiązanie wprowadzone w nPA wymaga silnych założeń o bezpieczeństwie używanego sprzętu oraz dużego zaufania do organu wydającego eID. Dlatego proponujemy dwa rozwiązania, które posiadają tę samą funkcjonalność, ale nie wymagają one tak silnych założeń o sprzęcie. Co więcej, nasze rozwiązania są bezpieczne nawet, gdy wystawca dokumentów nie może być obdarzony zaufaniem. Pierwsze rozwiązanie jest podobne do rozwiązania z nPA pod tym względem, że efektem wykonania protokołu jest klucz sesyjny, co nie jest wymagane w naszej definicji PI. Ponadto rozwiązanie to wymaga dużej infrastruktury klucza publicznego (PKI), gdyż używa ona listy akceptowanych eID. Druga konstrukcja jest pozbawiona tej wady.

Rozwiązania przedstawione w rozprawie nie tylko wprowadzają nowe funkcjonalności, lecz również osiągają je w możliwie najprostszy sposób. Podejście to jest ważne z punktu widzenia przemysłu, gdzie preferowana jest prostota rozwiązania oraz użycie istniejących komponentów.

Abstract

In this dissertation we consider cryptographic algorithm in the context of modern electronic identification documents (eID). These eID documents, although with limited memory and computational power, can execute a number of strong cryptographic algorithms, including in particular creation of digital signatures, key agreement, and strong authentication.

Many countries have already launched their eID projects. However, by far the most interesting one, from the scientific and market perspective, is the German nPA project (neuer Personalausweis). The nPA introduced three applications: ePassport, eID and eSign. In this dissertation we focus on the first two components, as the third one is fairly standard one.

The ePassport application is compliant with the ICAO standard for Machine Readable Travel Documents (MRTD). This standard specifies several algorithms and protocols executed during border control document inspection. However, not all algorithms are mandatory, which means that to be compliant with this standard only the mandatory algorithm must be implemented. Unfortunately, ePassports implementing only mandatory algorithms can be cloned. In order to protect against cloning, one must implement some of the optional algorithms (i.e. Active Authentication or Extended Access Control). However, this increases the time of execution.

In this dissertation, we introduce an extension to one of the mandatory algorithms (called Password Authenticated Connection Establishment (PACE)), which at cost of one modular multiplication (on side of the eID) authenticates the eID and this way protects against clonining. Simultaneously, the same protocol has been designed by the German Federal Office for Information Security (BSI). BSI patented this extension and introduced it to the ICAO standard for Machine Readable Travel Documents (MRTD). However, their security argument is based on non-standard ad hoc knowledge assumptions and thereby has a limited value as a formal security proof. In this dissertation we reduce security of the extended scheme to a standard Diffie-Hellman-like decisional problem.

Our second contribution is an extension applicable to PACE Integrated Mapping protocol. Let us recall that the ICAO standard specifies two versions of PACE: PACE-IM (Integrated Mapping) and PACE-GM (Generic Mapping). The first extension discussed above works only for the less efficient PACE-GM.

In the eID application we consider the protocol stack implemented by the nPA for online anonymous authentication. The idea is to use only a single key to authenticate in different domain of activity but in such a way that we receive a new and unlikable identity in different domains. In this dissertation we formalize this idea and introduce a cryptographic primitive called Pseudonymous Identification (PI). This way we will capture the desired features, which the nPA protocol stack is supposed to have. Executing a PI protocol should allow the eID to prove to a verifier in a domain that:

- the eID is genuine,
- the eID was used to generate the domain specific pseudonym,

- this is the only pseudonym that can be computed by the eID for this domain.

Moreover, we require that pseudonyms in different domains cannot be linked.

We then show that the nPA solution requires strong assumptions concerning security of the used hardware and considerable amount of trust on the authorities issuing eIDs in order to be considered secure. Therefore, we propose two solutions that achieve the same features, but do not require strong assumptions about hardware security. Moreover, our solutions are secure even if the document issuer is not trustworthy. The first solution is similar to the one introduced for the nPA in the sense that at the end the verifier and the prover share a common session key, which is not required in our definition for PI. Moreover, it requires a large PKI structure, i.e., the solution uses lists of accepted eIDs. The later instantiation does not have this disadvantage.

The solutions presented in the dissertation not only introduce new functionalities, but also achieve them in a relatively simple way. This approach is important from the point of view of the industry, where design elegance and re-use of existing components significantly ease implementation.