PACE with Mutual Authentication – towards an upgraded eID in Europe

Mirosław Kutyłowski, Patryk Kozieł, Przemysław Kubiak

Wrocław University of Science and Technology, Wrocław, Poland

ESORICS 2021

Electronic personal ID document

personal identity document with an electronic layer:

data carrier: **secure container for** (authenticated) **personal data** of the eID holder

token: a cryptographic token that authenticates itself as **issued by an authorized institution** and **unclonable**

eID communication

master-slave model: **eID is a slave**, it must respond to any reader,

wireless: communication over a **public wireless channel**

Threats

Eavesdropping

an adversary learns authenticated personal data transmitted over a radio channel, and can misuse it

⇒ **establish a secure session before transmitting data**

Tracing

an adversarial reader opens a session with the eID and learns personal data

⇒ **explicit owner's consent for a connection must be necessary in the technical sense**

Cloning, Impersonation

prevent an adversary to impersonate an eID or a reader

⇒ **secure devices with private keys, authenticate with these keys**

. . . and many other

Consent and PAKE

PAKE - Password Authenticated Key Exchange

- a reader and an eID hold the same password,
- a secure session key derived iff the same password used by both parties

Password – options

CAN - number printed on the eID, to be scanned optically (not by radio!)

user input – entered by the eID holder on a PIN board

Password authentication on identity documents

ICAO –international authority issuing standards for travel documents

- step by step increasing security level of *biometric passports*
- PAKE is one component

EU Regulation 2019/1157 on personal identity documents

Regulation 2019/1157 on personal identity documents:

- compulsory implementation of ICAO standards for documents issued since August 2021
- other (optional) functionalities **must not interfere** with ICAO protocols

GOAL

- **technical interoperability** of electronic identity cards in the EU,
- compliance with **privacy-by-design** principle (GDPR)

PACE

origin PAKE algorithm developed by BSI (German information security authority) and extended by French authority (PACE IM)

ICAO versions PACE GM (General Mapping) and PACE IM (Integrated Mapping) adopted by ICAO

extension PACE CAM = PAKE + strong authentication of the eID – adopted by ICAO as well

PACE GM in short

Phase 1 -password encrypted random nonce

- $K_\pi := \mathrm{Hash}(\pi \| 0)$, where π is the password
- s chosen at random by the eID
- $z = \mathrm{Enc}(K_\pi, s)$ sent to the reader

- z does not betray the password, offline analysis of z is useless for an adversary!
- the parties hold the same s if they use the same π

PACE GM in short

Phase 1 -password encrypted random nonce

- $K_\pi := \mathrm{Hash}(\pi \| 0)$, where π is the password
- s chosen at random by the eID
- $z = \mathrm{Enc}(K_\pi, s)$ sent to the reader

Phase 2 - deriving password related random generator

- DH key exchange resulting in a shared key h
- $\hat{g} := h \cdot g^s$ (g is a fixed group generator)

- different password lead almost always to different $\hat{g}$

PACE GM in short

Phase 1 -password encrypted random nonce

- $K_\pi := \mathrm{Hash}(\pi \| 0)$, where π is the password
- s chosen at random by the eID
- $z = \mathrm{Enc}(K_\pi, s)$ sent to the reader

Phase 2 - deriving password related random generator

- DH key exchange resulting in a shared key h
- $\hat{g} := h \cdot g^s$ (g is a fixed group generator)

Phase 3 - master session key

- DH key exchange for generator $\hat{g}$ resulting in a shared key K
- encryption and MAC session keys derived from K

Phase 4 - verification

tags depending on K exchanged to prove possession of key K

PACE CAM

designed independently as

- *Simplified PACE|AA Protocol* L. Hanzlik, K. Kluczniak, Ł. Krzywiecki, M. Kutyłowski, ISPEC 2013
- *The PACE|CA Protocol for Machine Readable Travel Documents*, J. Bender, M. Fischlin, D. Kügler, INTRUST 2013

adopted by ICAO to its standard

Problem solved by PACE CAM

- PACE does not guarantee that a reader connects to a genuine eID,
- a remedy would be to present data signed by the eID issuer
- but this would be risky! – the reader could forwarding them to third parties together with the signature!

PACE CAM idea

authenticating eID with public key $X = g^x$

- during the first DH key exchange the eID sends $X_A = g^{x_A}$ for x_A chosen at random
  - note: eID must know x_A in order to compute DH key
- final step after PACE: eID has to show $w := x_A/x$
- the reader checks that $X_A = X^w$
  - rationale: eID has to know both w and x_A so it knows x as well

Design features - how to extend a protocol

- **backwards compatibility**: connection should be established even if the reader/eID runs the plain PACE
- **minimal changes**: just fine tune the original protocol,
  new steps come at the end
- **reuse** the code and expensive cryptographic operations
- guarantee that the **security arguments** for the plain version are **still valid**

PACE Mutual Authentication

authenticate the reader before sending personal data

- personal data protection must be *by-design* according to GDPR
  - eID should not reveal personal data of its owner blindly to any reader

- the user's password is not guarding the data well enough – many readers know it (and can trade them)

PACE MA - idea

reuse X_A and X_B for static DH authentication

- reader authentication (reader's public key $Y = g^y$):

  reader computes $K_B := (X_A)^y$

  eID computes $K_B := Y^{x_A}$

  later the reader proves that it knows K_B

- eID authentication (eID's public key $X = g^x$):

  eID computes $K_A := (X_B)^x$

  reader computes $K_A := X^{x_B}$

  later the eID proves that it knows K_A

PACE MA - strategies to prove knowledge of K_A and K_B

Option 1 - exchanging new tags after PACE

- fully compatible with PACE
- 1 extra message per each side for authentication

Option 2 - redefining slightly the tags used by PACE

- compatible with PACE (downgrade dance)
- no extra message compared to PACE, 1 less than for PACE CAM (where one side authentication only)

Properties of PACE MA

1. extremely simple
2. backwards compatible
3. minimal changes with regard to PACE
4. no new operations ⇒ reusing code – code size is critical for the smart card chip!
5. security properties of PACE inherited:
   - fragility (⇒ active adversaries no more powerful than passive ones)
   - resistance to offline attacks
   - . . .
6. we have not applied for a patent, after publishing this presentation it becomes *state-of-the-art* and is secured against patenting threat

Final Recommendation

Personal ID cards in Europe should implement not only PAKE but also mutual authentication.

It is doable with a small effort.

Thank you for your attention