Mutual Chip Authentication

Lucjan Hanzlik, Kamil Kluczniak, Łukasz Krzywiecki, Mirosław Kutyłowski

Wrocław University of Technology
Wrocław, Poland

ACS, TRUSTCOM 2013, Melbourne

Introduction

Personal identity cards - eID

- strong cryptographic authentication.
- wireless communication.

Advantages

- Protection against forgeries.
- Remote authentication.

E.g.: new German identity card (Personalausweis).

Extended Access Control (EAC)

Goal

Authenticated key exchange between a chip and a terminal.

Part 1: Terminal Authentication

- Authentication of an ephemeral key from the terminal.
- The ephemeral key is signed by the terminal.

Part 2: Chip authentication

- Derivation of a session key.
- Authentication of the chip by proving the knowledge of a DH secret key.

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$		$K := y_C^{x_{ep}}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$	$\xrightarrow{r_B}$	verify tag with K_C
$K_{session} := (K_A, K_B)$		$K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private,		x_T - signing key,
$y_C = g^{x_C}$ - public,		y_T - verification key,
$cert(y_C)$		$cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$		$K := y_C^{x_{ep}}$
$K_A := H(K, 1)$,		$K_A := H(K, 1)$,
$K_B := H(K, 2)$		$K_B := H(K, 2)$
$K_C := H(K, 3)$		$K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$	$\xrightarrow{r_B}$	verify tag with K_C
$K_{session} := (K_A, K_B)$		$K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$		$K := y_C^{x_{ep}}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$	$\xrightarrow{r_B}$	verify tag with K_C
$K_{session} := (K_A, K_B)$		$K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	
		choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
		$s := Sig_{x_T}(r_A \|\| y_{ep})$
	$\xrightarrow{r_A}$	
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$		$K := y_C^{x_{ep}}$
$K_A := H(K, 1)$, $K_B := H(K, 2)$		$K_A := H(K, 1)$, $K_B := H(K, 2)$
$K_C := H(K, 3)$		$K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$	$\xrightarrow{r_B}$	verify tag with K_C
$K_{session} := (K_A, K_B)$		$K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$ $\xrightarrow{r_A}$	$y_{ep} := g^{x_{ep}}$ $s := Sig_{x_T}(r_A \| \| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$		$K := y_C^{x_{ep}}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$ $K_{session} := (K_A, K_B)$	$\xrightarrow{r_B}$	verify tag with K_C $K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$		$K := y_C^{x_{ep}}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$ $K_{session} := (K_A, K_B)$	$\xrightarrow{r_B}$	verify tag with K_C $K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$		$K := y_C^{x_{ep}}$
$K_A := H(K, 1)$,		$K_A := H(K, 1)$,
$K_B := H(K, 2)$		$K_B := H(K, 2)$
$K_C := H(K, 3)$		$K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$ $K_{session} := (K_A, K_B)$	$\xrightarrow{r_B}$	verify tag with K_C $K_{session} := (K_A, K_B)$

EAC

Chip		Terminal
x_C - private, $y_C = g^{x_C}$ - public, $cert(y_C)$		x_T - signing key, y_T - verification key, $cert(y_T)$
	Terminal auth	
verify certificate	$\xleftarrow{cert(y_T)}$	choose x_{ep} at random
choose r_A	$\xleftarrow{y_{ep}}$	$y_{ep} := g^{x_{ep}}$
	$\xrightarrow{r_A}$	$s := Sig_{x_T}(r_A \|\| y_{ep})$
verify s with y_T	$\xleftarrow{s}$	
	Chip auth	
	$\xrightarrow{cert(y_C)}$	verify certificate
$K := y_{ep}^{x_C}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$		$K := y_C^{x_{ep}}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K_C := H(K, 3)$
$r_B := MAC_{K_C}(c_T)$	$\xrightarrow{r_B}$	verify tag with K_C
$K_{session} := (K_A, K_B)$		$K_{session} := (K_A, K_B)$

Privacy problems

Terminal

- strong evidence of terminal's presence
- the chip can send an x chosen by a third party and then returns a terminal's signature of x.
- the certificates are transmitted in clear, an observer gets information who it talking with the terminal

Goal

- make interaction between the chip and the terminal anonymous for an observer,
- preserve simplicity,
- provable key security and provable anonymity.

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random		chose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$		$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	check $cert(y_A)$ $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$ $K_{session} := H(K,5)$		$K_{session} := H(K,5)$

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random		chose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$		$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	check $cert(y_A)$ $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$ $K_{session} := H(K,5)$		$K_{session} := H(K,5)$

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random $h_A := H(a)$ $c_A := g^{h_A}$	$\xrightarrow{c_A}$	chose b at random $h_B := H(b)$ $c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$		$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	check $cert(y_A)$ $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$ $K_{session} := H(K,5)$		$K_{session} := H(K,5)$

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random $h_A := H(a)$ $c_A := g^{h_A}$	$\xrightarrow{c_A}$ $\xleftarrow{c_B}$	chose b at random $h_B := H(b)$ $c_B := g^{h_B}$
$K := c_B^{h_A}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K'_A := H(K, 3)$, $K'_B := H(K, 4)$ $r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	$K := c_B^{h_A}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K'_A := H(K, 3)$, $K'_B := H(K, 4)$ check $cert(y_A)$ $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$ $K_{session} := H(K, 5)$		$K_{session} := H(K, 5)$

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random		chose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$		$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	check $cert(y_A)$
		$r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$ $K_{session} := H(K,5)$		$K_{session} := H(K,5)$

AMA - Protocol Description

Alice		Bob
x_A - private, $y_A = g^{x_A}$, $cert(y_A)$		x_B - private, $y_B = g^{x_B}$, $cert(y_B)$
random a at random		chose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$		$K := c_B^{h_A}$ $K_A := H(K,1)$, $K_B := H(K,2)$ $K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$	$\xrightarrow{Enc_{K_A}(cert(y_A), r_A)}$	check $cert(y_A)$ $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert(y_B), r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert(y_B)$ $r_B \neq H(y_B, K'_B)$		
$K_{session} := H(K,5)$		$K_{session} := H(K,5)$

Privacy

Transcript indistiguishability

- A communication transcript is undistinguishable from random values.
- Certificates are hidden from an eavesdropper, he does not know the identity of the communicating parties.
- It is still true if an adversary gets a batch of communication transcripts.

Simultability

- Holding only the certificate (public key) of a user, we can generate the transcript with the same probability distribution.
- A communication transcript cannot be used as a proof, for third parties, that a particular user has participated in the communication.

Security

Long-term secret key leakage

If the long term secret keys of both parties leak, then a passive adversary still has negligible advantage to learn the secret key.

Ephemeral key leakage

If the ephemeral keys of both parties leak, then an active adversary still has negligible advantage to learn the secret key.

Efficiency and Implementation

Efficiency

	EAC	AMA
Exponentiations on chip	$1 + cert_{ver} + sign_{ver}$	$4 + cert_{ver}$
Exponentiations on terminal	$2 + sign_{gen} + cert_{ver}$	$4 + cert_{ver}$
Communication rounds	2	2

Implementation

- Prototype implementation on Standard Java Card (Gemalto MultiApp ID V2.1)
- Average execution time for 500 tests:
  - 1.261 seconds - secp192r1 elliptic curve
  - 1.602 seconds - secp256r1 elliptic curve

Conclusions

Anonymous Mutual Authentication (AMA)

- Symmetric.
- Secure in Real-or-Random model.
- Simultable.
- Identities of protocol participants are hidden from eavesdroppers.
- As efficient as EAC.

The End

Thanks for your attention.

Acknowledgment. We thank Gemalto company for the technical support.