Wrocław University of Technology

Mutual Restricted Identification

Lucjan Hanzlik, Kamil Kluczniak, Łukasz Krzywiecki, Mirosław Kutyłowski

EuroPKI 2013, September 12, 2013

German eID

EACv2 -Extended Access Control protocol with RI

eID: an identification document containing a chip that can run cryptographic protocols on behalf of the owner,

German eID

EACv2 -Extended Access Control protocol with RI

eID: an identification document containing a chip that can run cryptographic protocols on behalf of the owner,

Terminal: a computer system running a smart card reader talking with the eID.

German eID

EACv2 -Extended Access Control protocol with RI

Terminal Authentication: Terminal proves that it has the right to talk with the eID,

German eID

EACv2 -Extended Access Control protocol with RI

Terminal Authentication: Terminal proves that it has the right to talk with the eID,

Chip Authentication: eID proves that it is genuine – it proves to hold a secret key given by the document issuer,

German eID

EACv2 -Extended Access Control protocol with RI

Terminal Authentication: Terminal proves that it has the right to talk with the eID,

Chip Authentication: eID proves that it is genuine
– it proves to hold a secret key given by the document issuer,

Restricted Identification: eID identifies and authenticates itself against Terminal using its identity specific to the terminals domain.

German eID

Restricted Identification and privacy concept

Domain specific identity: terminals belong to disjoint domains (frequently: 1 domain - 1 Terminal),

German eID

Restricted Identification and privacy concept

Domain specific identity: terminals belong to disjoint domains (frequently: 1 domain - 1 Terminal),

Unlinkability: any activity of an eID in one domain cannot be linked (via cryptographic analysis) with activity within another domain,

German eID

Restricted Identification and privacy concept

Domain specific identity: terminals belong to disjoint domains (frequently: 1 domain - 1 Terminal),

Unlinkability: any activity of an eID in one domain cannot be linked (via cryptographic analysis) with activity within another domain,

Identity hiding: the domain identity is revealed after authentication,

German eID

Restricted Identification and privacy concept

Domain specific identity: terminals belong to disjoint domains (frequently: 1 domain - 1 Terminal),

Unlinkability: any activity of an eID in one domain cannot be linked (via cryptographic analysis) with activity within another domain,

Identity hiding: the domain identity is revealed after authentication,

One key concept: the eID should hold a single private key for all domains.

The Idea

Mutual Restricted Identification

What if two eID would like to communicate using Restricted Identification?

The Idea

The problems with EACv2

Asymmetric Contruction

One eID would have to perform the protocol from point of view of the terminal

The Idea

The problems with EACv2

Asymmetric Contruction

One eID would have to perform the protocol from point of view of the terminal

Proof of Communication

Due to the contruction of Terminal Authentication one eID would have an undeniable proof of communication

Related Work

AKE Protocols

- Group of protocols for establishing of an authenticated communication channel,

Related Work

AKE Protocols

- Group of protocols for establishing of an authenticated communication channel,
- The identity of the opposite party has to be exchanged before the protocol execution.

Our Contribution

The solution

MRI Protocol

- Efficient,

Our Contribution

The solution

MRI Protocol

- Efficient,
- Simultable,

Our Contribution

The solution

MRI Protocol

- Efficient,
- Simultable,
- Provable secure.

MRI Protocol

Parameters

eID A	eID B
$\mathrm{x_A}$ - private key $\mathrm{y_A} = \gamma^{\mathrm{x_A}}$ - public key $\mathrm{cert_A}$ - certificate for $\mathrm{y_A}$	$\mathrm{x_B}$ - private key $\mathrm{y_B} = \gamma^{\mathrm{x_B}}$ - public key $\mathrm{cert_B}$ - certificate for $\mathrm{y_B}$
OPTIONAL SETUP	
recompute γ $\mathrm{y_A} := \gamma^{\mathrm{x_A}}$ - derive own public key fetch $\mathrm{cert_A}$ check $\mathrm{y_A}$ with $\mathrm{cert_A}$	recompute γ $\mathrm{y_B} := \gamma^{\mathrm{x_B}}$ - derive own public key fetch $\mathrm{cert_B}$ check $\mathrm{y_B}$ with $\mathrm{cert_B}$

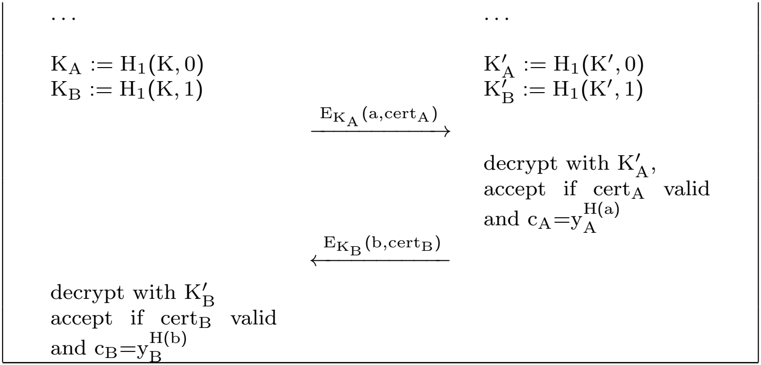
MRI Protocol

Part 1

<table>
<tr><th colspan="3">MAIN PROCEDURE</th></tr>
<tr><td>choose a at random</td><td></td><td>choose b at random</td></tr>
<tr><td>$h_A := H(a)$</td><td></td><td>$h_B := H(b)$</td></tr>
<tr><td>$c_A := y_A^{h_A}$</td><td></td><td>$c_B := y_B^{h_B}$</td></tr>
<tr><td></td><td>$\xrightarrow{c_A}$</td><td></td></tr>
<tr><td></td><td>$\xleftarrow{c_B}$</td><td></td></tr>
<tr><td>$K : {c_B}^{x_A h_A}$</td><td></td><td>$K' := {c_A}^{y_B h_B}$</td></tr>
<tr><td>$\ldots$</td><td></td><td>$\ldots$</td></tr>
</table>

MRI Protocol

Part 2



…

…

$K_A := H_1(K,0)$
$K_B := H_1(K,1)$

$K'_A := H_1(K',0)$
$K'_B := H_1(K',1)$

$\xrightarrow{E_{K_A}(a,cert_A)}$

decrypt with K'_A,
accept if $cert_A$ valid
and $c_A{=}y_A^{H(a)}$

$\xleftarrow{E_{K_B}(b,cert_B)}$

decrypt with K'_B
accept if $cert_B$ valid
and $c_B{=}y_B^{H(b)}$

MRI Protocol

Certificates for Domains

Three solutions

- store all certificates on cards or external memory,

MRI Protocol

Certificates for Domains

Three solutions

- store all certificates on cards or external memory,
- use self-blindable certificates,

MRI Protocol

Certificates for Domains

Three solutions

- store all certificates on cards or external memory,
- use self-blindable certificates,
- or use ...

MRI Protocol

Certificates for Domains

Schnorr like solution

- eID receives two private keys $x_1 = x + z \cdot x_2$ and x_2 (x, z secrets of CA),

MRI Protocol

Certificates for Domains

Schnorr like solution

- eID receives two private keys $x_1 = x + z \cdot x_2$ and x_2 (x, z secrets of CA),
- uses x_1 in MRI protocol,

MRI Protocol

Certificates for Domains

Schnorr like solution

- eID receives two private keys $x_1 = x + z \cdot x_2$ and x_2 (x, z secrets of CA),
- uses x_1 in MRI protocol,
- creates a proof of knowledge of x_2 such that $g^{x_1} = g^x \cdot (g^z)^{x_2}$ (g^x, g^z published by CA).

Conclusion

Mutual Restricted Identification RI can be performed by two eIDs within one domain,

Conclusion

Mutual Restricted Identification RI can be performed by two eIDs within one domain,

Efficiency The protocol is well suited for implementation on smart cards.

Conclusion

Thank You for your attention!
Questions?