

# MobCom UG meeting

Idemix & DAA go mobile

Jorn Lapon  
Faysal Boukayoua  
Msec, KAHO

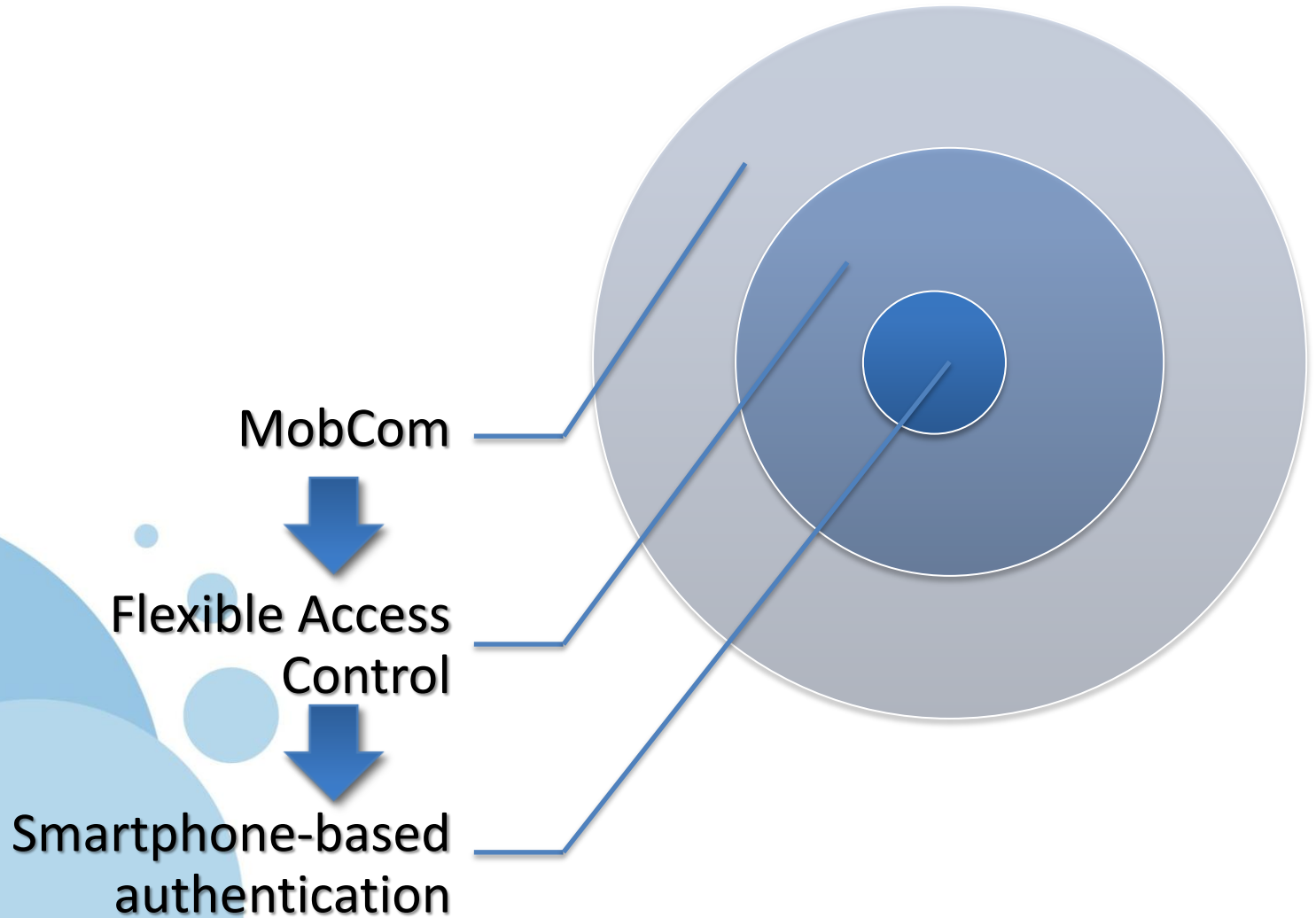
Stefaan Seys  
COSIC, KULeuven

# Overview

- Introduction
- Smartphone-based authentication
- Key technologies
- System components
- Functional description
- Research results
- Future work

# Introduction

## *Context*



# Introduction

*Why smartphone-based authentication?*



- Increasing capabilities
- Omnipresent
- Large backing from industry
- Allows for more flexible solutions

# Smartphone-based authentication

## *Intended use cases*

- Authenticate to:



- (Personalised) Web services



- Services within physical proximity

# Smartphone-based authentication

## *Demonstrator scenarios*

- Touristic trip
  - Validate bus ticket (DAA)
  - Validate bus ticket with location restrictions (Idemix)
  - Retrieve points of interest in a privacy-friendly manner (see *Context-aware services*)



# Smartphone-based authentication

*2 approaches, 2 apps...*



# Key technologies

## *QR codes*

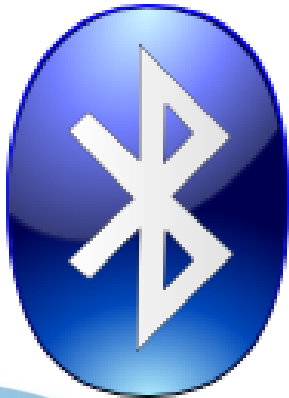


- What?
  - 2-dimensional barcodes
  - Up to 3kB of data
- Why?
  - Camera common in modern phones
  - Every workstation has a screen...



# Key technologies

## *Bluetooth*



- What?
  - Wireless communication protocol
  - Low-power: 2-10 mWatt
  - Transfer speed: ~ 2 Mbps
  - Range: ~ 10 m
- Why?
  - Common in modern phones
  - Cheap to add (USB dongles)
  - “auto-connect” when in range

# Key technologies

## *Tamperproof modules*



- Tamperproof
  - Strong cryptography
  - Secure credential storage
- ➔ Giesecke & Devrient Mobile Security Card SE 1.0

# Key technologies

## *Identity Mixer*

- Anonymous credential system
- Minimal attribute disclosure
- Provably accurate user info
- Credential usages unlinkable
- Deanononymisation upon abuse
- 2 modes implemented:
  - Entirely on smartphone
    - Faster
  - Master secret on secure  $\mu$ SD
    - Increased security: MS never leaves  $\mu$ SD



# Key technologies

## *Direct Anonymous Attestation (DAA)*

- Anonymous credential system
- Developed in the context of the Trusted Computing Group (TCG)
- Allows a user to convince a verifier that he uses a platform that has embedded a certified hardware module
- Privacy: Different proofs are not linkable
- Implementation: all security sensitive operations are carried out on the smartcard (e.g., it is impossible to obtain any information on the secret key)

# Key technologies

## *Idemix & DAA: comparison*

	X509 certificates	Direct Anonymous Attestation	Identity Mixer
Underlying technology	Public key cryptography	<ul style="list-style-type: none"> <li>• Camenisch- Lysyanskaya signature scheme</li> <li>• Zero-knowledge proof</li> </ul>	<ul style="list-style-type: none"> <li>• Camenisch- Lysyanskaya signature scheme</li> <li>• Zero-knowledge proof</li> </ul>
Anonymity levels	<ul style="list-style-type: none"> <li>• Identifiable</li> <li>• Pseudonymity per cred.</li> </ul>	<ul style="list-style-type: none"> <li>• Identifiability</li> <li>• Pseudonymity (per SP)</li> <li>• Anonymity (per Access)</li> </ul>	<ul style="list-style-type: none"> <li>• Identifiability</li> <li>• Pseudonymity (per SP)</li> <li>• Anonymity (per Access)</li> </ul>
Purpose	<ul style="list-style-type: none"> <li>• Binding between user attributes and public key</li> </ul>	<ul style="list-style-type: none"> <li>• Prove credential ownership</li> </ul>	<ul style="list-style-type: none"> <li>• Prove credential ownership</li> <li>• Prove attributes or properties thereof</li> </ul>
Privacy properties	<ul style="list-style-type: none"> <li>• Full attribute disclosure</li> <li>• Signatures linkable</li> </ul>	<ul style="list-style-type: none"> <li>• Proofs unlinkable</li> </ul>	<ul style="list-style-type: none"> <li>• Proofs unlinkable</li> <li>• Minimal attribute disclosure</li> </ul>
Performance on same platform	Faster	Comparable to Idemix without attribute proofs	Slower (slower when more attributes to prove)

# System components



**CREDENTIAL  
ISSUER**



**RELYING PARTY**



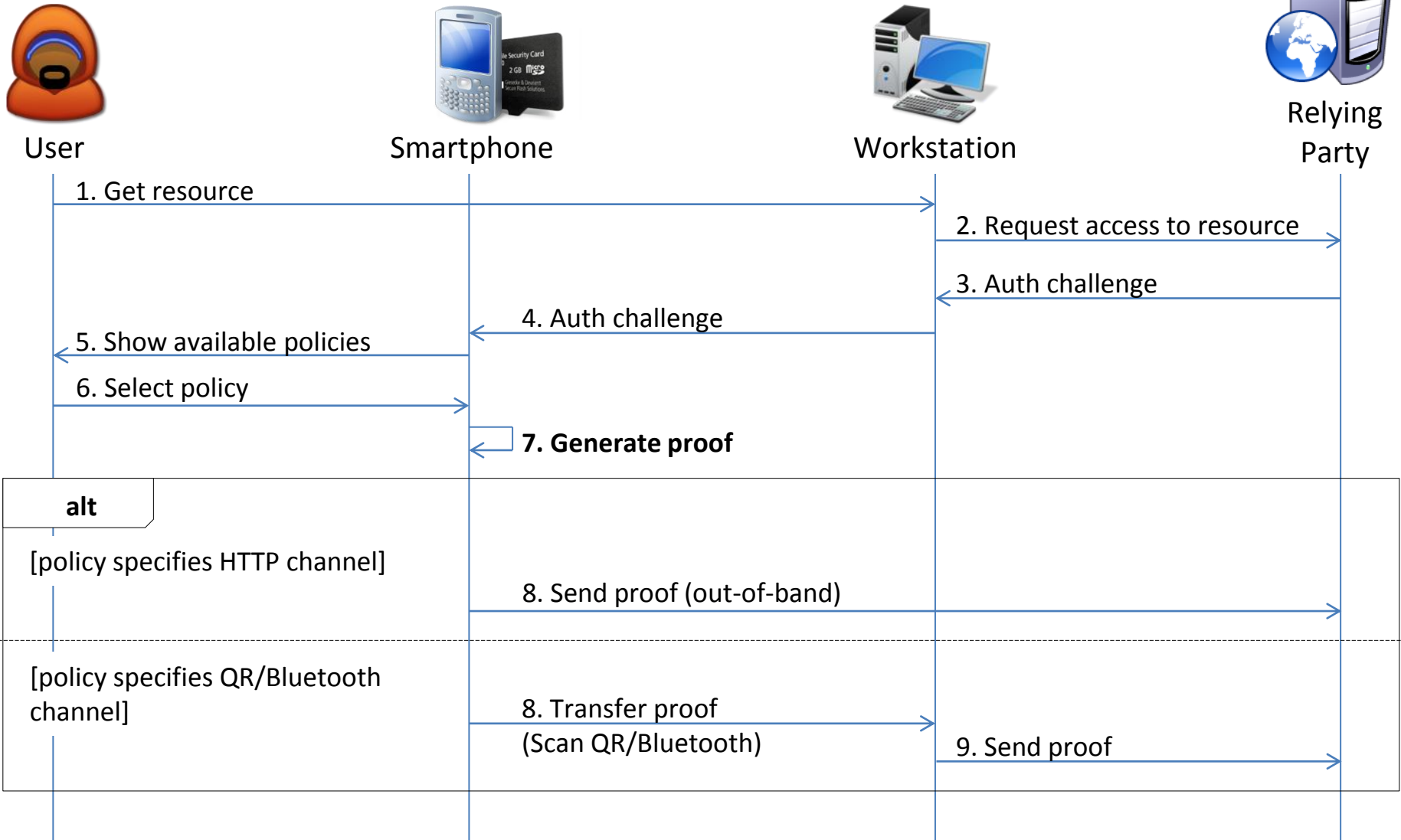
**Smartphone**



**Browser on  
workstation**

**USER**

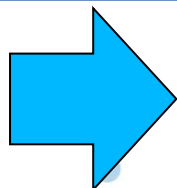
# Functional description



# Research results (1/2)

- Authentication:

Key size: 1024bits	Idemix	DAA
<i>Credential Ownership</i>	0.3s + 1.2s ( $\mu$ SD)	7.5s
<i>Enumeration (region)</i>	+ 0.15s	X
<i>Reveal attribute</i>	- 0.024s	X



- Examples:

- Enumeration:*

“Bus Credential” - region OVL, VBR  
Proof Credential is valid in OVL

- Reveal Attribute:*

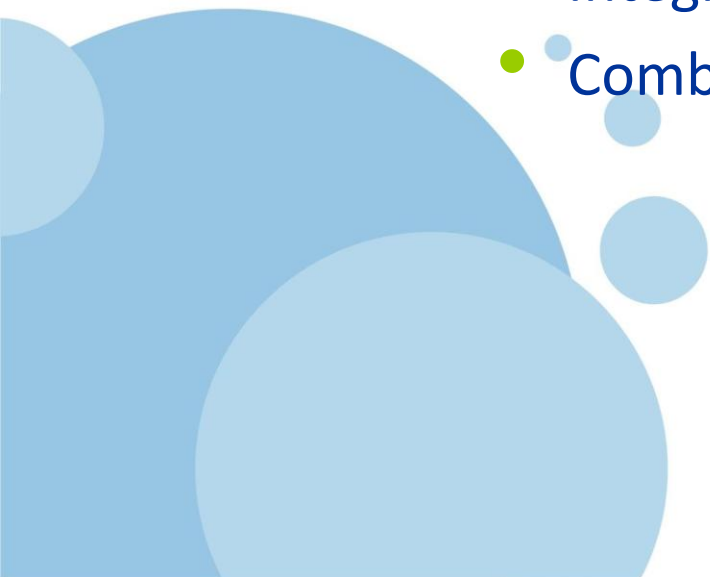
negative time: easier proof



## Research results (2/2)

- Revocation:
  - Lost/stolen credential  $\Rightarrow$  **revoke**
  - But:* Anonymity reveals no serial to use of verifying the revocation state !
- Research on Several Revocation Strategies  
Overhead per party/Performance/Usability
  - e.g. Verifier Local Revocation Belgium:
    - 375.000 revocations/year
    - Verify: 18 minutes (Java/PC)

## Future work

- NFC communication (in progress)
  - Greater part of Idemix on trustworthy hardware
  - Integration in access control systems
  - Interoperability with standards
  - Verifiable Encryption + Deanononymisation
  - Integration in ADAPID framework
  - Combine with biometrics on the phone
- 
- A decorative graphic in the bottom-left corner consisting of several overlapping light blue circles of various sizes.

# Questions

