Anonymous Ticketing for NFC-enabled Mobile Phones

David Derler, Klaus Potzmader,
Johannes Winter, Kurt Dietrich

Institute for Applied Information Processing and Communications, Graz University of Technology

November 27, 2011

dderler@student.tugraz.at

IAIK TU Graz

Overview

- Introduction
  - Motivation
- Protocol
  - Proof-of-Concept
  - Moving to next-generation-smartphone plattforms
- Conclusion

IAIK TU Graz

Motivation

- Virtual Tickets on the mobile
  - convenient
  - always at hand
  - privacy-preserving
- Near Field Communication
  - Zero Configuration
  - ...more and more NFC-enabled (smart)phones
- Mobiles pre-equipped with secure chips

Source: mobilewhack.com

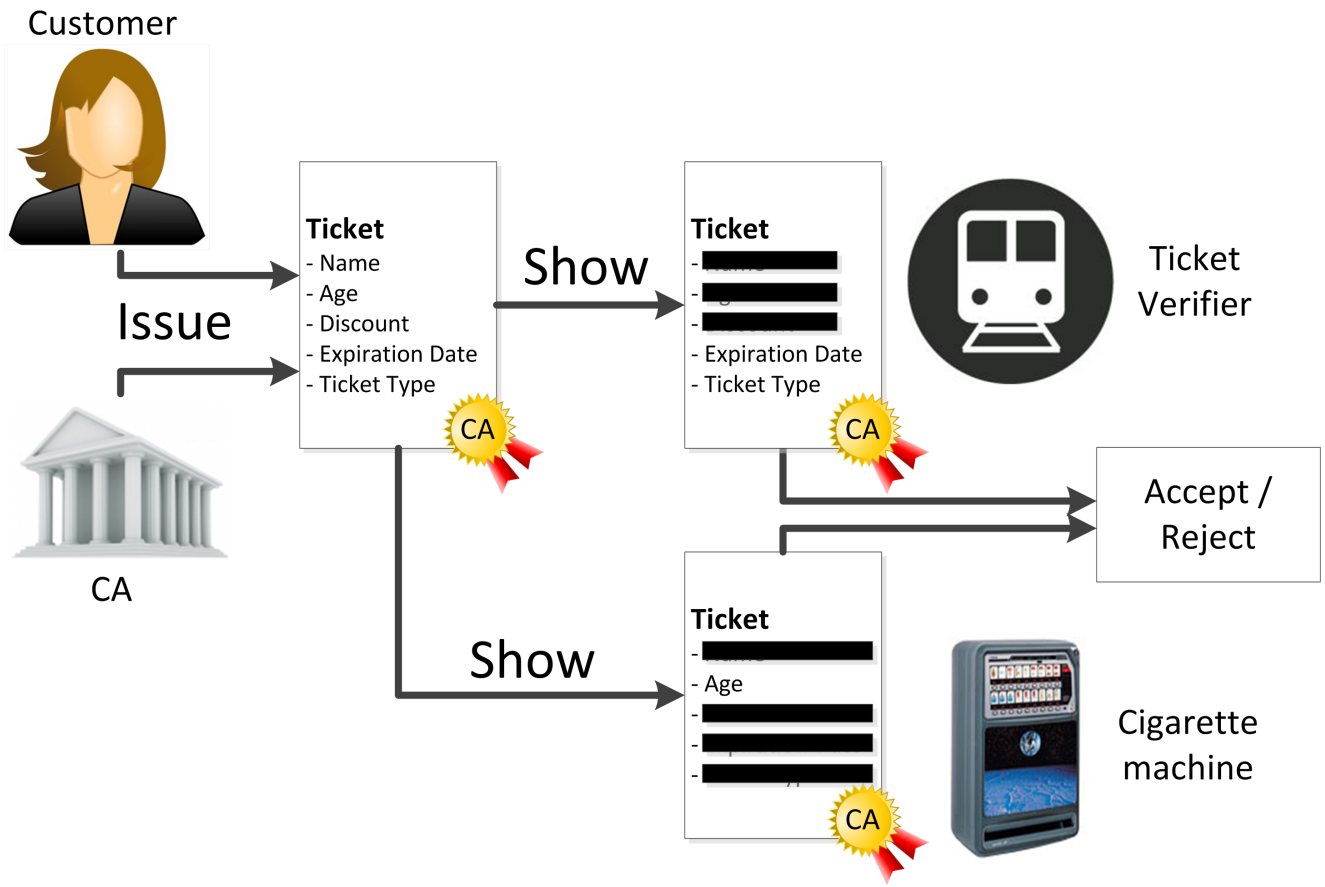
IAIK TU Graz

Mobile Ticketing

- A ticket denotes a set of properties (attributes) such as
  - Expiration date
  - Age
  - Name
  - ...
- Conventional verification is traceable
  - Operator sees name, age,...
  - ...but needs just expiration date
- long-term tickets allow detailed insight on daily route

IAIK TU Graz

Selective Disclosure Protocols - Zero Knowledge Proof



Sources: centrepad.org, clker.org, canstockphoto.com, tab.at, wellmanpropertylettings.co.uk

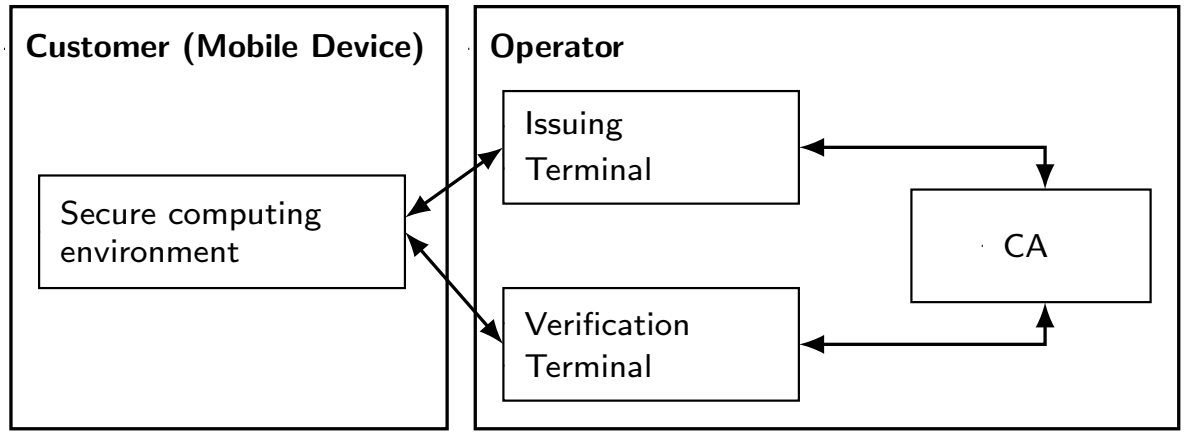
Protocol

- Proposed by Glenn et. al of Zero-Knowledge Systems [GGLS01]
  - Based on work of Brands [Bra00]
- Slight variations to suit our needs
  - Modular inversion $\rightarrow$ precomputation
- Ticket owners remain anonymous
- Unlinkability
  - Unlinkable between issue and show,
  - Although linkable between multiple show sessions

IAIK TU Graz

Protocol (2)

- Four parties
  - CA
  - Issuer
  - Customer
  - Verifier



- CA publishes DSA parameters and generators
- Issuer and customer jointly compute signature over attributes
- Verifier can ensure authenticity
  - without knowing who he's dealing with

IAIK TU Graz

Proof-of-Concept

- Nokia 6131
  - On-board G&D Sm@rtCafe Expert 3.1 Javacard
    - 72kB Memory
    - EEPROM (slow) and transient RAM (fast)
- SCM Microsystems SDI010 contactless reader
  - Addressable via `javax.smartcardio.*`

Source: Nokia, SCM Microsystems

IAIK TU Graz

Large Integer Arithmetic on Javacard

- Need for large Integer operations
- No `java.math.BigInteger` equivalent on Javacard
- **BigInt** - a collection of static methods for long integer arithmetics
  - Low memory consumption
  - Compatible to `BigInteger.toByteArray()` representation
    - And therefore to `new BigInteger(sign, byte[])`
    - Eases exchange of data a lot
  - all operations in place/with target array
- Limited computational power $\rightarrow$ performance?

IAIK TU Graz

Hardware aided (1)

- Utilization of crypto coprocessor
- Using RSA Cipher

$$\text{ciphertext} = \text{message}^{\text{public exponent}} \ \textit{mod} \ \text{public modulus}$$

- Why not use for modular Exponentiation?
- Limitations
  - $\text{message}^1 \rightarrow$ no aided modulo

IAIK TU Graz

Hardware aided (2)

- Modular Multiplication
  - Partial crypto coprocessor support by

$$a \cdot b \bmod n = \frac{(a+b)^2 - a^2 - b^2}{2} \bmod n$$

  - Division by two can be done by right shift
    - If numerator is odd add modulus ($odd + prime = even$)
  - Faster than software-only approach

IAIK TU Graz

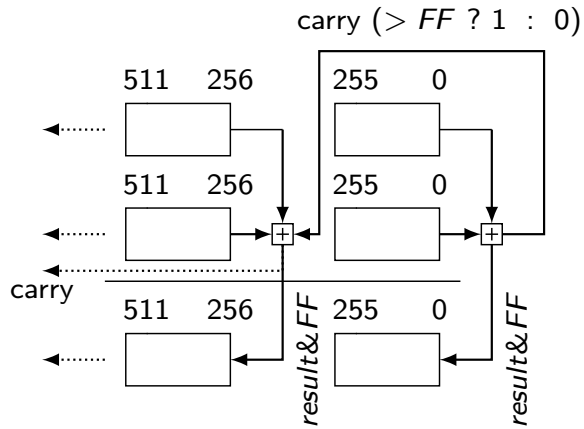
Hardware aided (3)

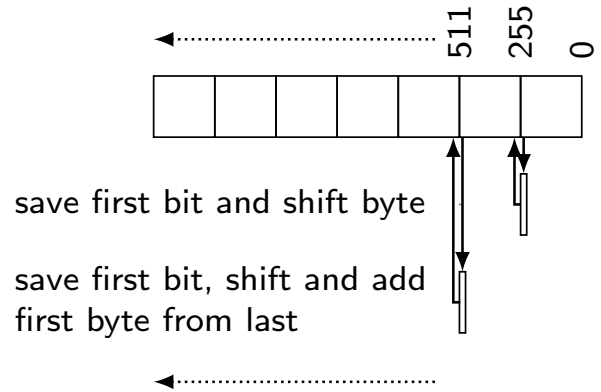
- Modular inversion
  - Euler-Fermat
    - $a^{\varphi(n)} \mod n \equiv 1 \mod n \rightarrow$
    - $a^{\varphi(n)-1} \mod n \equiv a^{-1} \mod n$
  - Just one Hardware aided exponentiation needed
  - Huge speedup compared to software-only approach
    - exponentiation is done in $< 1s$

IAIK TU Graz

In Software

- Add, Subtract
  - Bytewise operation with carry bit
- Shift
  - Bytewise shift with two temporary bytes
- Modulo





Results

- Timings

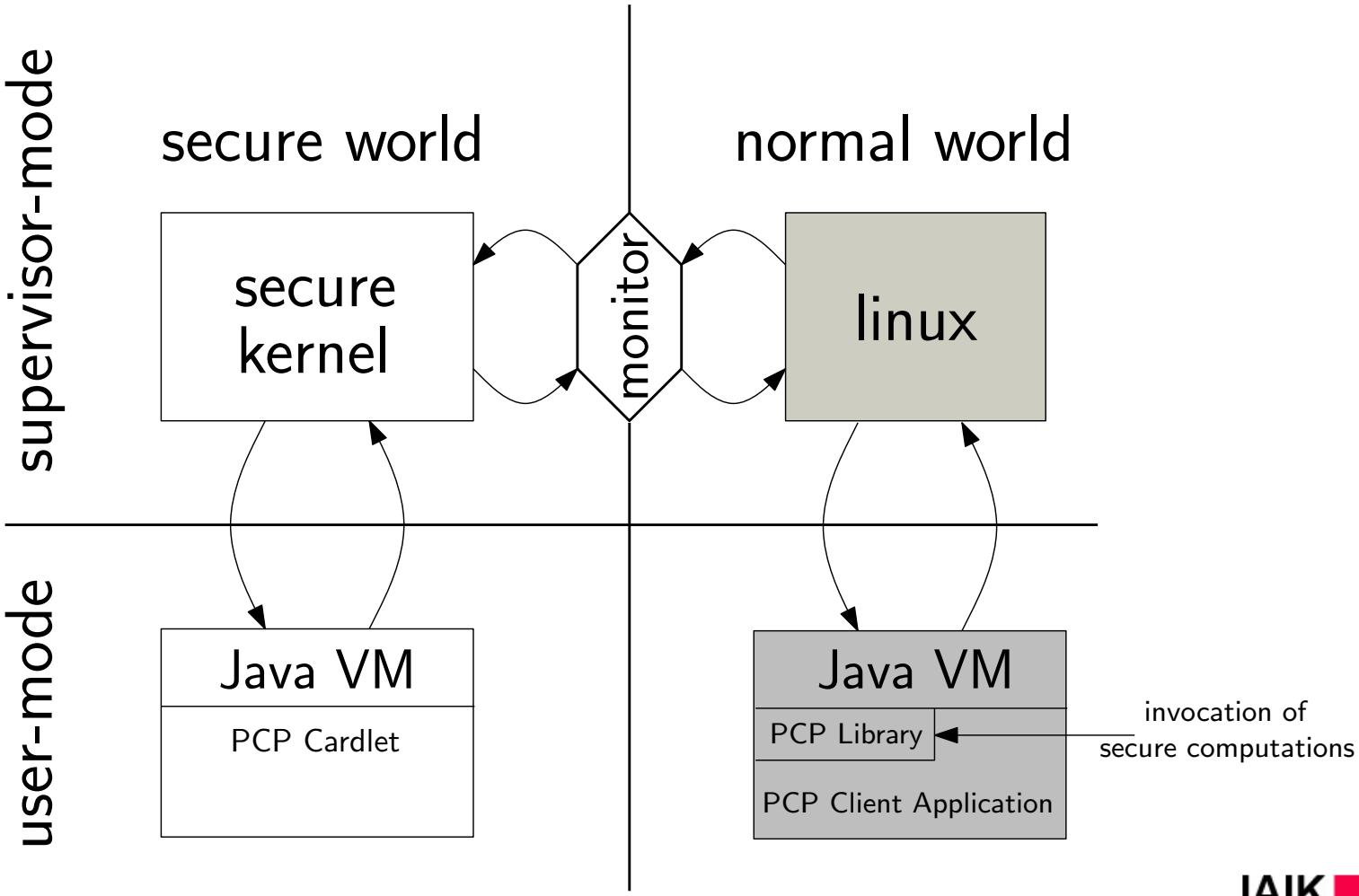
Key length [Bits]	*768*	*1024*	*1280*	...	*1984*
Precomputation[1]	1.2s	0.7s	1.1s	...	1.3s
Issue Session	5.5s	6.7s	8.6s	...	20.8s
Show Session	7.7s	9.5s	11.5s	...	16.7s

Table: Computation Times for different key-lengths

- Acceptable up to 1024Bit key-length
- 1984Bit and higher key-lengths exhaust the transient memory

[1] Runs as silent service in the background

Moving to next generation smart-phone platforms



Source: Paul Wiegele

Conclusion

- Javacard variant
  - Acceptable timings using precomputation
  - Computation times grow with increasing key length
  - Javacard 3.0 connected will provide further large integer support
- Trustzone variant
  - Timings on a real device would be interesting
- In general
  - NFC is of growing popularity
    - Huge field for further research

IAIK TU Graz

Thank you.

References

Stefan A. Brands.
Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.
MIT Press, Cambridge, MA, USA, 2000.

Ariel Glenn, Ian Goldberg, Frederic Legare, and Anton Stiglic.
A description of protocols for private credentials, 2001.

Laszlo Hars.
Modular inverse algorithms without multiplications for cryptographic applications.
EURASIP J. Embedded Syst., 2006:2–2, January 2006.

IAIK TU Graz