Privacy-Preserving Management of Transactions' Receipts for Mobile Environments

Federica Paci, Ning Shang, Sam Kerr,
Kevin Steuer Jr., Jungha Woo, Elisa Bertino

Purdue University

April 15, 2009

Offline Shopping

Online Shopping

How Can Receipts Help?

Receipts Can Help

- Establish transaction-history-based trust
- Facilitate services such as discounts/promotions

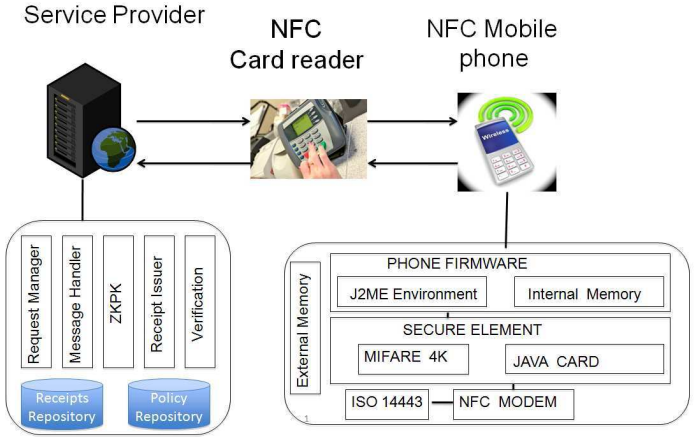
Challenge in e-Commerce: Receipt Management

- Customer needs to get e-receipts from offline stores
- Customer needs to show online transactions to offline stores
- Privacy & security

Solution: M-Commerce and Cryptography

- Customer-SP communications
  - Cell phones (NFC)
- Privacy-preserving management & proofs
  - Digital signatures
  - Zero-knowledge proof of knowledge (ZKPK)
  - Oblivious commitment-based envelope (OCBE)
  - Shamir's secret sharing scheme

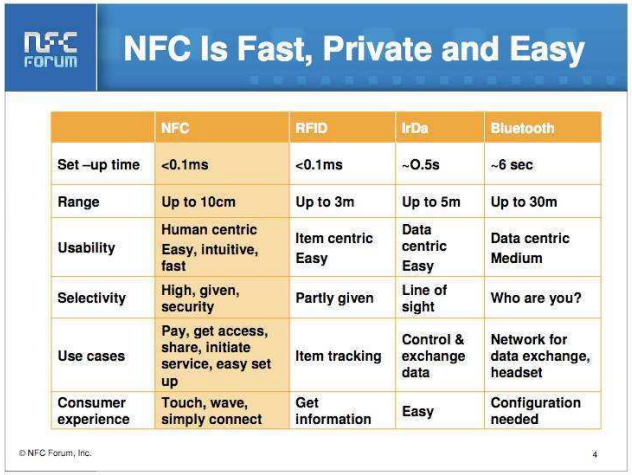
System Architecture



Near Field Communication (NFC) Technology

Courtesy `http://www.nfc-forum.org`

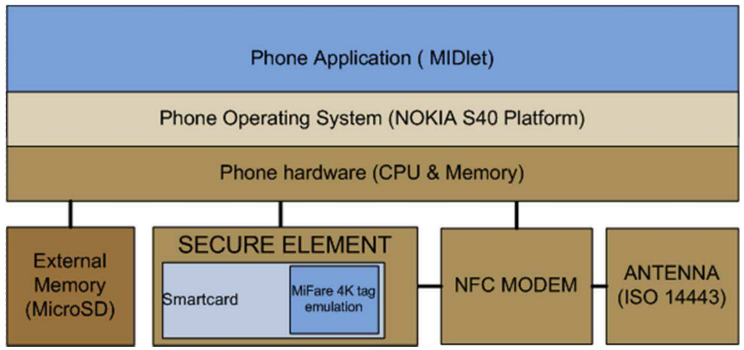
Near Field Communication (NFC) Technology



	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Courtesy `http://www.nfc-forum.org`

Nokia 6131 NFC Phone Architecture



Receipt Format

Public Param $= \langle G, p, g, h \rangle$
Pedersen commitment (COM): $c = g^{\text{attr-value}} h^r$

TRAN-ID	ATTR		COM		SIG
1234	BUYER	John Smith	BUYER	7645353 6366363	1124457 6590873 3647688
	SELLER	BookStore.com	SELLER	1312425 54546	
	CATEGORY	Books	CATEGORY	2224223 525	
	PRICE	30	PRICE	1341515	
	DATE	11-04-2008	DATE	1315657	

Integrity Verification: Digital Signatures

Service provider verifies digital signature according to "SELLER" attribute in receipt.

Options which allow signature aggregation

- Batch RSA signatures
  - Fast
  - Good if there is only one signer
- Boneh's aggregate signatures with bilinear maps (elliptic curve pairings)
  - Good for case of multiple signers
  - Slower than batch RSA

Ownership Proof: ZKPK

Service provider performs a ZKPK protocol with user (phone) on "BUYER" attribute in receipt.

ZKPK can

- convince SP that user knows the values name and r (authentication)
- prevent SP from learning the values name and r in clear text (privacy)

ZKPK (Schnorr's Scheme)

Public Param $= \langle G, p, g, h \rangle$

secret r
$c = g^{\text{name}} h^r$

(1). $c, d = g^y h^s$

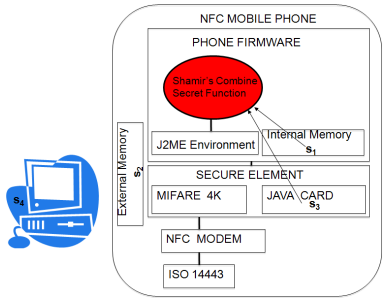
(2). challenge random $e \in \mathbb{F}_p$

(3). $u = y + e \cdot \text{name}, v = s + e \cdot r$

(4) accepts if $g^u h^v = dc^e$

Strong Protection of Secret Value: Shamir's Secret Sharing

(n, k)-threshold scheme
$n = 4$, $k = 2/3/4$ (security level L/M/H)



Secret value r can be reconstructed only if k shares are present

Verification of Conditions: OCBE Protocols

Service provider performs OCBE protocols with user (phone) to verify whether user satisfies conditions on attributes specified in policy

OCBE can

- convince SP that user's attribute values satisfy conditions given by comparison predicates (authentication)
- prevent SP from learning user's attribute values in clear text (privacy)

Verification of Conditions: Policy Language

Verification Policy Language: Example

Pol : Discount(OnItem = "Glamour", Amount= "\$15")
$\leftarrow$ SELLER = "bookstore.com", PRICE $>$ "\$80", DATE $<$ "11-04-2008."

The policy states that a user is qualified for a \$15 discount on an yearly subscription to Glamour magazine, if the user has spent more than \$80 at "bookstore.com" before the date "11-04-2008".

EQ-OCBE: Equality Predicates (Li & Li)

Public Param $= \langle G, p, g, h \rangle$

(1). $EQ_{x_0}, \mathcal{E}, H(\cdot)$

(2). c

(3). $y \xleftarrow{R} \mathbb{F}_q$, $\sigma = (cg^{-x_0})^y$

(4). $\eta = h^y, C = \mathcal{E}_{H(\sigma)}[\text{coupon}]$

secret r
$c = g^{\text{ctgry}} h^r$

(5). $\sigma' = \eta^r$, decrypts C with $H(\sigma)$ to get coupon

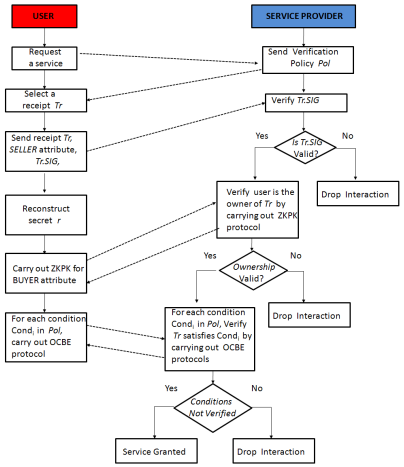
GE-OCBE: "$\geq$" Predicates (Li & Li)

GE-OCBE

- Similar to EQ-OCBE
  - bit-by-bit fashion
- More computationally costly than EQ-OCBE
  - parameter ℓ controls capacity and efficiency

Other OCBE protocols are similar.

Protocol Overview

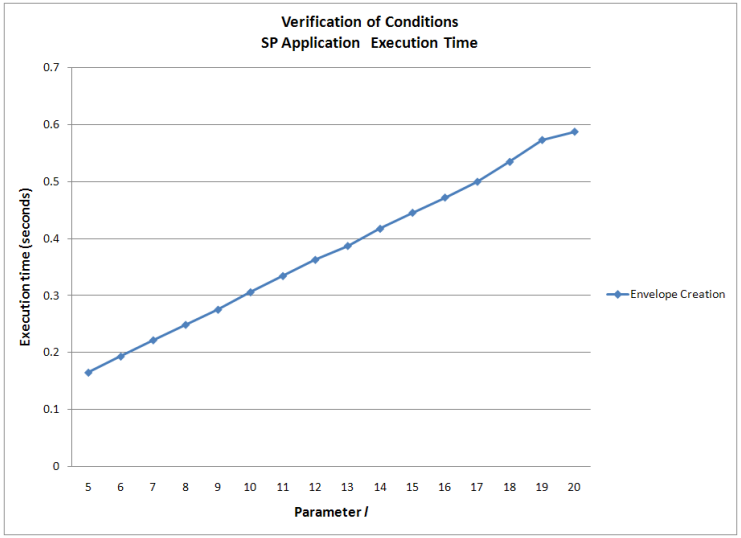


ZKPK Performance

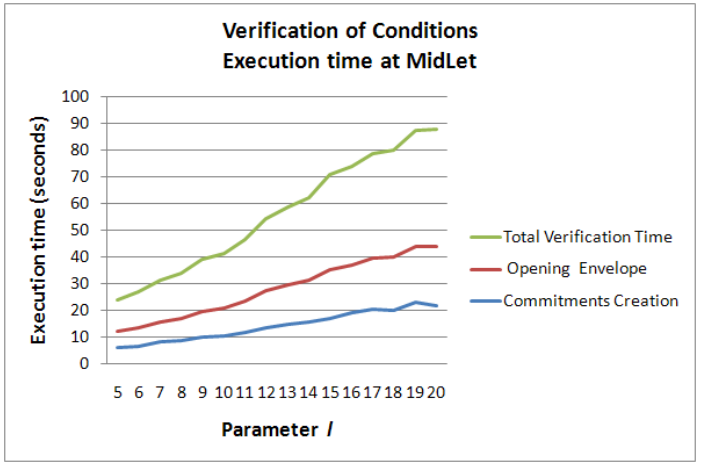
Time for receipt ownership verification via ZKPK

Customer MIDLet: 0.042 second
Service Provider Application: 0.0311 second

OCBE Performance on Service Provider



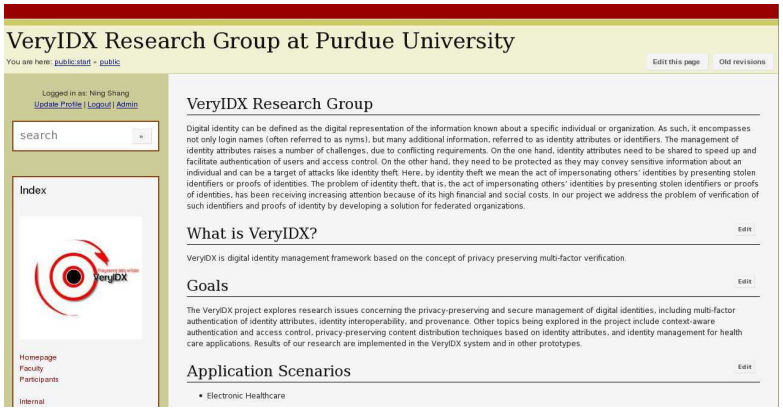
OCBE Performance on NFC Phone



Nokia 6131: ARM-9 228 MHz, JVM Interpreter (JBenchmark estimate)

VeryIDX Framework

The VeryIDX IdM Team at Purdue
`http://veryidx.cs.purdue.edu`



The End

Questions?