DigiTally

Khaled Baqer, Johann Bezuidenhoudt and Ross Anderson

Cambridge
The mobile money revolution
Mobile money achievements

• Brought banking services to hundreds of millions who didn’t have them
• Built mechanism for direct payments and remittances; store of value; personal safety; transaction history; access to credit
• Provided direct channel for government payments and services
Remaining challenges: can we...

- Extend payments to areas with no mobile service (mountains, deserts, islands)?
- Make service work even when network service intermittent (congestion, power cuts)?
- Cut network charges (do we really need three SMSs per payment, even regular customers)?
- Provide a usable system for feature phones (without camera, Bluetooth, NFC, etc.)?
Goal: operate in offline or constrained environments

- Existing offline purses: UEPS, Geldkarte, etc
- These systems can be implemented in SIM toolkits (phone applets)
- Problem 1: money operators (usually MNOs) limit access to SIMs
- Problem 2: existing systems are designed for complex messages between devices
- Problem 3: simple phones lack features
Enabling tech: overlay SIMs

- Tamper-resistant SIM to compute authorization codes, as in EMV
- Sticks on top of the regular SIM
- Bypasses the mobile network operator
- Independent secure device
DigiTally

• DigiTally is a purse system we’ve built for offline mobile payments (prototype ready)
• Grant by Bill & Melinda Gates Foundation (GCE)
• It will be free open source software
• It can also be implemented in a SIM toolkit or as a smartphone app, or in overlay SIMs for simple phones (as our prototype is)
• It works by copying short authentication codes from one phone to another ...
Initial step: Alice increases her purse balance by exchanging cash for DigiTally credit (e.g. via an agent, similar to the role of agents in current mobile payment networks)

Contact information is entered manually or selected from a previously saved contact entry

Now, Alice wants to pay Bob Ksh 450

Both devices will authenticate transactions using PINs
DigiTally payment (2)

• Bob then enters “450” on his phone
• It shows an eight-digit authorization request

Give Alice Code 1: 3651 7623

• Alice enters “450” and the code above on her phone
• Agreement: Alice’s phone shows “OK”
DigiTally payment (3)

- Alice’s phone displays an eight-digit authorization response, which she shows or reads out to Bob

  Give Bob Code 2: 9302 4515

- If code 1 was correct (agreement), then code 2 authorises increasing Bob’s balance by Ksh 450 (Alice’s balance already decremented)
Both devices show the transaction log

If the transaction is interrupted (on either device), it can be resumed at any time
Security case

• Implementation in tamper-resistant overlay SIMs, which will be EMV compliant by 2016
• Cryptography can use AES or 3DES to generate authentication codes
• Payment protocol formally verified and sent to a crypto conference for peer review
• White paper detailing the technical details available online (project page)
DigiTally benefits

• Serve customers in villages with no network
• Serve customers when the network is congested or down
• Cut network costs for repeated transactions between the same customer and merchant
• Works on feature phones and smartphones
Next steps

- Test prototype system using overlay SIM Java Card toolkit (from Taisys)
- Will do small-scale trial end of June 2016
- Incorporate lessons learned into larger-scale field trial
- Make first DigiTally reference implementation available Q1 2017
- Free open-source software for all to use!