Gerhard Claassen

4 May 2010

Crypto at the bottom of the pyramid

AFRICACRYPT Rump session

PRISM

TRUSTED TRANSACTIONS

Motivation

1. Not a marketing presentation
2. Neither Northern Africa vs Southern Africa
3. Focus on the unique requirements of Africa
4. Socio economical perspective
5. Application of cryptography

World Economic Pyramid

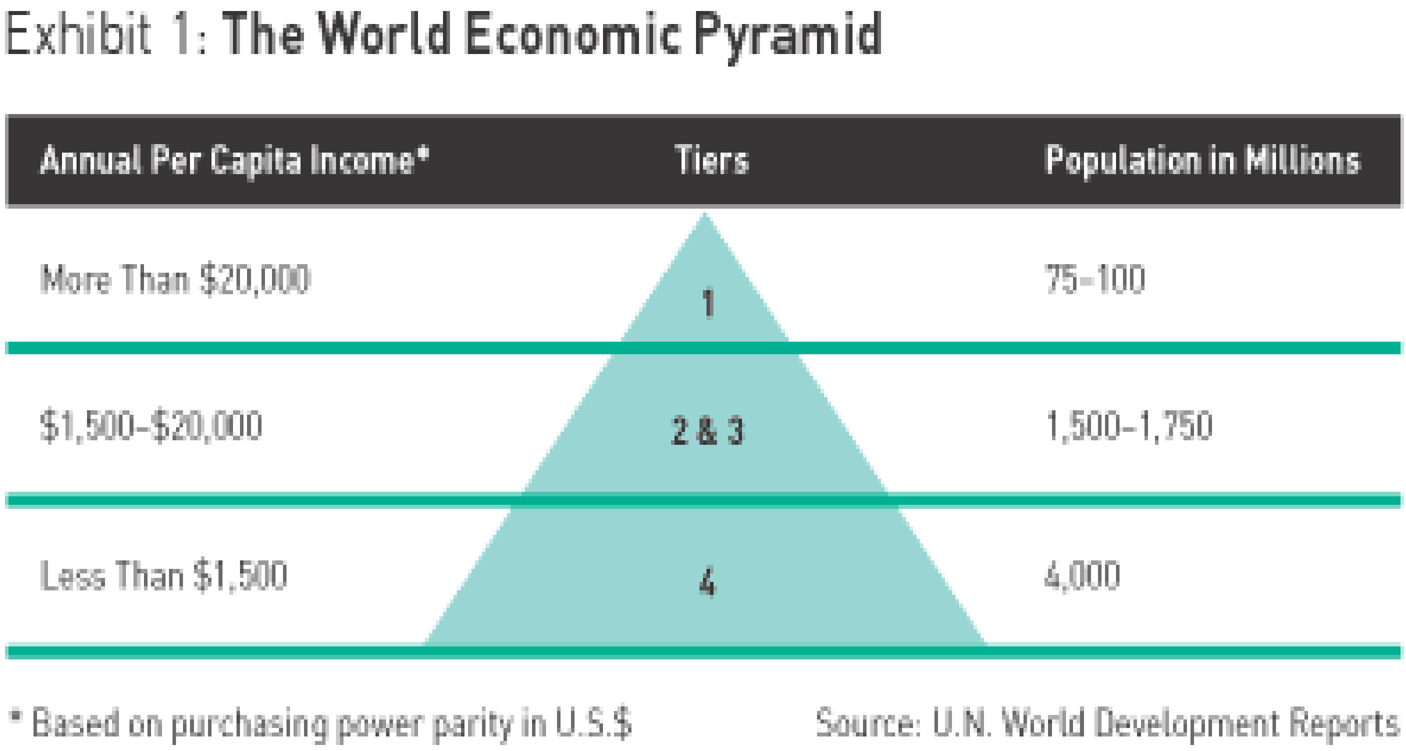


Exhibit 1: **The World Economic Pyramid**

Annual Per Capita Income*	Tiers	Population in Millions
More Than $20,000	1	75–100
$1,500–$20,000	2 & 3	1,500–1,750
Less Than $1,500	4	4,000

* Based on purchasing power parity in U.S.$

Source: U.N. World Development Reports

CK Prahalad, “Fortune at the bottom of the pyramid”.

CK Prahalad

1. This extreme inequity of wealth distribution reinforces the view that the poor cannot participate in the global market economy
2. Most Tier 4 people live in rural villages, or urban slums and shantytowns, and they usually do not hold legal title or deed to their assets
3. They have little or no formal education and are hard to reach via conventional distribution, credit, and communications
4. Fortunately, the Tier 4 market is wide open for technological innovation

What is needed is a better approach to help the poor, an approach that involves partnering with them to innovate and achieve sustainable win–win scenarios where the poor are actively engaged and, at the same time, the companies providing products and services to them are profitable.

Needs of the poor

1. The tier 4 poor also are unbanked
2. The do not have access to the financial system
3. They have a need to transact:
4. Receiving social grants and pensions
5. Paying for water and electricity
6. Buying food, etc

Social grants and pension payouts

13 million recipients in SA

4 million via one system

Registration: ID, fingerprint, smart card

Paypoints: ATM type terminals on pickup trucks in rural areas

Authentication: Fingerprint and card

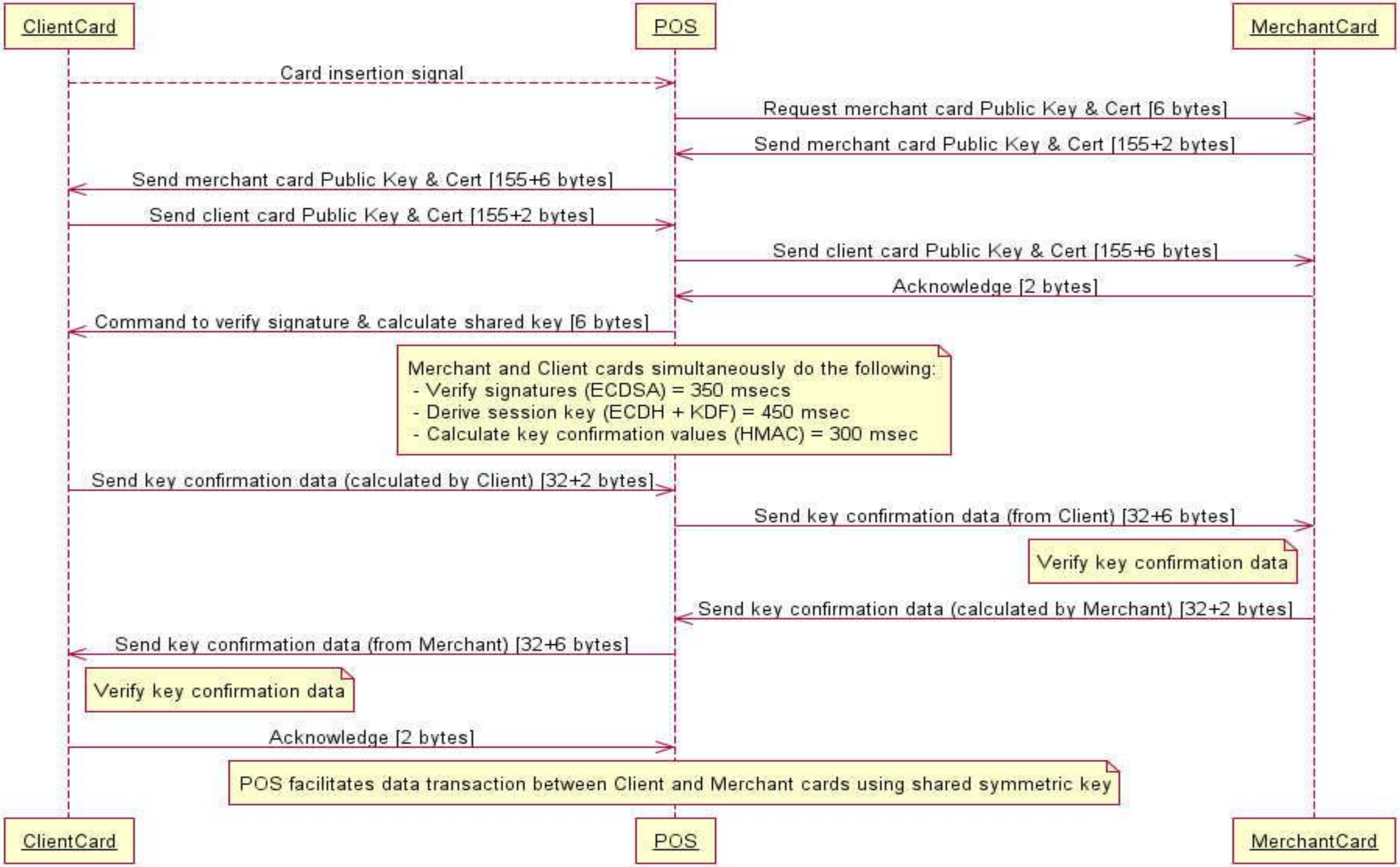
Payout: 10 digit token, cash or transfer to wallet on card

Wallet can be used to buy goods offline at participating stores

Authentication between client card and merchant card currently 3DES based

Moving towards Elliptic curve

High-level Key Negotiation Protocol



ClientCard

POS

MerchantCard

Card insertion signal

Request merchant card Public Key & Cert [6 bytes]

Send merchant card Public Key & Cert [155+2 bytes]

Send merchant card Public Key & Cert [155+6 bytes]

Send client card Public Key & Cert [155+2 bytes]

Send client card Public Key & Cert [155+6 bytes]

Acknowledge [2 bytes]

Command to verify signature & calculate shared key [6 bytes]

Merchant and Client cards simultaneously do the following:
- Verify signatures (ECDSA) = 350 msecs
- Derive session key (ECDH + KDF) = 450 msec
- Calculate key confirmation values (HMAC) = 300 msec

Send key confirmation data (calculated by Client) [32+2 bytes]

Send key confirmation data (from Client) [32+6 bytes]

Verify key confirmation data

Send key confirmation data (calculated by Merchant) [32+2 bytes]

Send key confirmation data (from Merchant) [32+6 bytes]

Verify key confirmation data

Acknowledge [2 bytes]

POS facilitates data transaction between Client and Merchant cards using shared symmetric key

ClientCard

POS

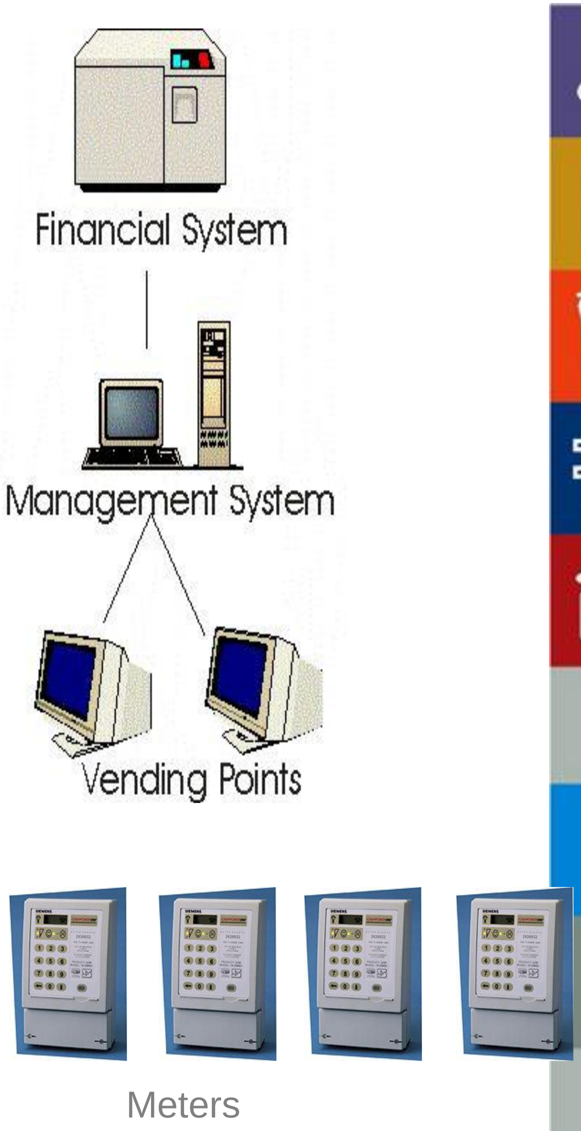
MerchantCard

Pre-paid electricity

- The **Standard Transfer Specification (STS)** has become recognised as the only globally accepted standard for prepayment systems, ensuring inter-operability between system components from different manufacturers of prepayment systems.
- STS systems continue to be deployed around the world since 1993, with systems now in use in some 28 countries, including 17 on and around the African continent.

Prepaid Electricity Major Components

- A prepaid electricity system involves the following components:
  - A **pre-payment meter** installed at the customer's residence. The meter accepts electricity tokens that transfer value to the meter. When the meter runs out of credit, it disconnects the electricity supply.
  - A **vending infrastructure** that provides the customer with access to points-of-sale from where electricity tokens may be purchased.
  - A **management system** to report on the vending infrastructure, perform financial reconciliations, configure system parameters such as tariffs and maintain the customer database.
  - The **management system can, as an option, interface to the supply authority's financial systems** to provide financial integration with other services that the supply authority may provide.



PIN Generation Processes

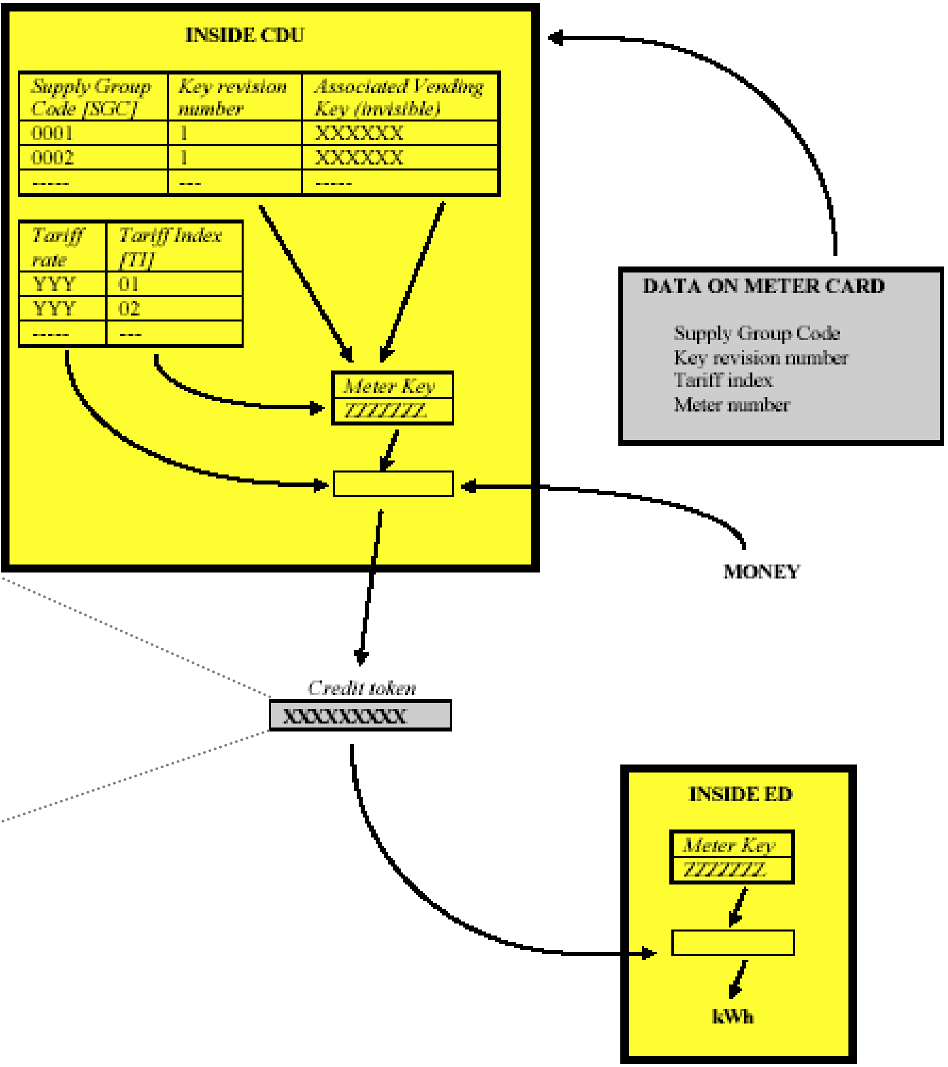
STS Numeric Token or PIN

Algorithm
STS

Serial	Supply Grp	Tariff	CDU ID
06319162043	300876	01	0001

Date	Type	Money	Energy (kWh)
230595	E	R100.00	100.0

1079 5376 9456
8605 0346



INSIDE CDU

Supply Group Code [SGC]	Key revision number	Associated Vending Key (invisible)
0001	1	XXXXXX
0002	1	XXXXXX
-----	---	-----

Tariff rate	Tariff Index [TI]
YYY	01
YYY	02
-----	---

DATA ON METER CARD

Supply Group Code
Key revision number
Tariff index
Meter number

Thank you
Any questions?

Disclaimer: The material in this document is presented strictly for information purposes. While every effort has been made to ensure its correctness, neither the correctness nor the suitability of the information for any purpose is warranted. Product specifications and features are subject to change without notice.