Incorporating Digital Signing & Encryption in Transactions in the Payment System of Sri Lanka

Presentation by
Sunimal Weerasooriya, CEO
LankaClear (Pvt) Ltd.

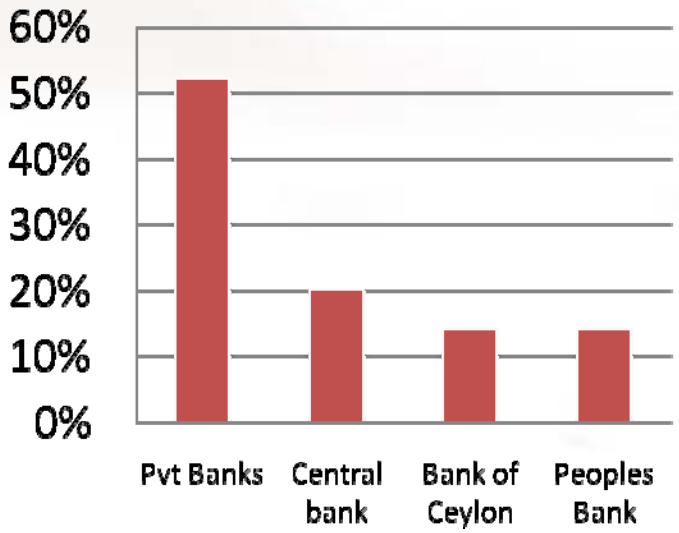
Introduction to LankaClear

LankaClear
TRANSACT THE FUTURE

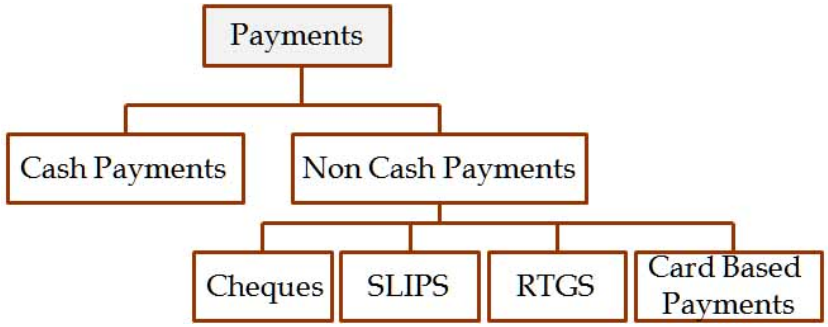
- Originated as Sri Lanka Automated Clearing House (SLACH) under Central Bank of Sri Lanka (CBSL) – 1987
- Divested as a limited liability company owned by all Commercial Banks and the Central Bank of Sri Lanka (CBSL) – 2002

Introduction to LankaClear…

Share Holders



Payment Structure of SL



Product Range of LankaClear

CITS

SLIPS

LANKA SIGN

Establishment of LankaSign CSP

- Cyber security, information piracy, data theft, etc, are words we hear often these days in a world going High Tech at an ever increasing speed.
- Eliminating information piracy, data theft, etc. and ensuring security of information transmitted online is even more necessary as e-payments are fast becoming the norm than the exception.

Establishment of LankaSign CSP

Recognizing the need, The Central Bank of Sri Lanka (CBSL) invited LankaClear (Pvt) Ltd. (LCPL) to be the Financial Sector's Certification Service Provider and LCPL launched LANKASIGN on 22nd May 2009, as per the provisions of the Electronic Transactions Act No. 19 of 2006.

Root Signing Key - Protection

- LANKASIGN-CSP Root signing key pair is ensured with the use of SafeNet Protect Server Gold HSM which is certified to FIPS-140 -2 Level 3. The LANKASIGN-CSP Root signing key pairs are 2048-bit and were generated within the Protect Server Gold HSM.
- The LANKASIGN-CSP takes necessary precautions to prevent compromise or unauthorized usage of the key.

Root Signing Key - Recovery

- LANKASIGN-CSP Root CA signing keys are encrypted and stored within a secure environment.

- The decryption key is maintained on a physical media and stored in a physically secured offline environment which requires two or more authorized officials of the LANKASIGN-CSP to again access. When any LANKASIGN-CSP Root signing key expires, it will be archived for at least 10 years.

# of Digital Certificates

erver Certificates

gnature Certificates

y Encryption Certificates

mail Certificates

rtificates are available for use in both private networks and public domain.