

KEYCORP

Trends and Challenges in the Payment Industry

John Smerek,
System Architect, Innovations Group

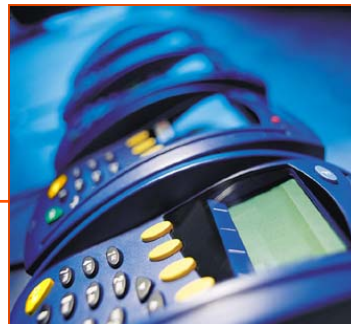
Trusted Transaction Solutions

51582909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
87890513218 0856464 5451582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
68247829090380 850 0025 132 087890513218 0856464 5451582909080 80 85002513208 780513218 65349 0 850025132 6783492



Agenda

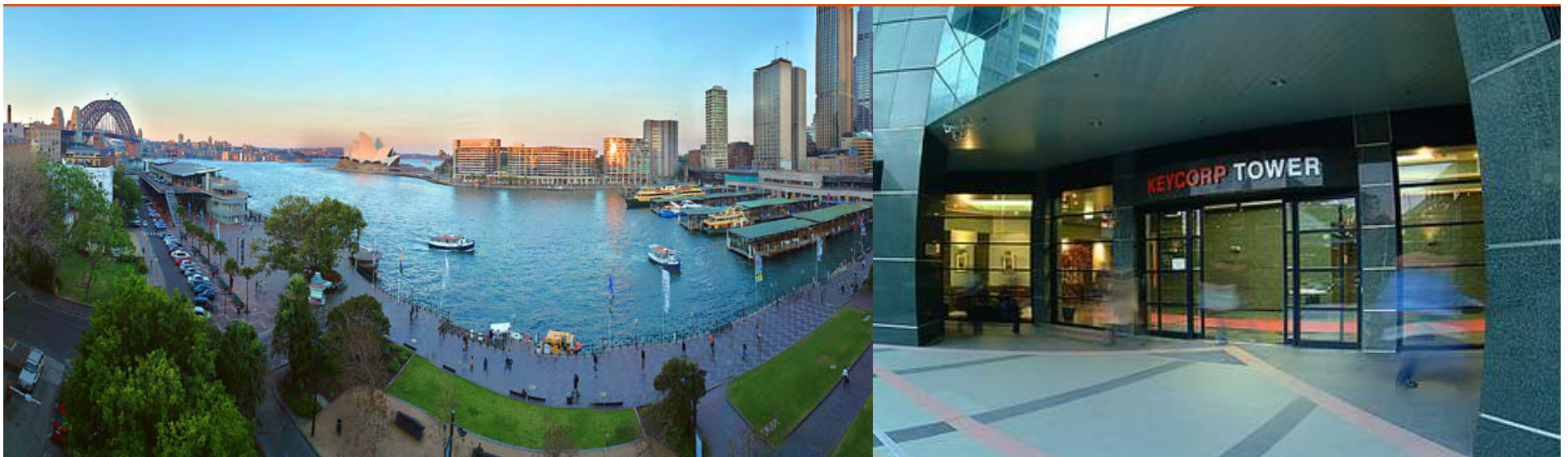
- Who we are
- Our mission
- Current Industry
- Trends and market forces
- Challenges
- Summary



Profile: Keycorp

*One of the most
successful and
profitable Top 300
ASX technology
companies*

- Established in 1984, listed on ASX 1987
- EFTPOS terminal supplier from 1992
- Smartcard technology supplier from 1993
- 184 staff
- Based in Sydney, Australia
- Secondary office in Toronto, Canada



Keycorp Overview

51562909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
 82890513218 0856464 545 1582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
 82890513218 0856464 545 1582909080 80 85002513208 780513218 65349 0 850025132 6783492

Smartcards



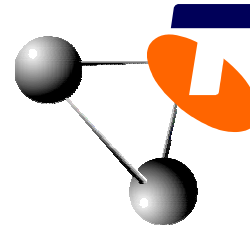
- MULTOS operating system
- Applications

Access Devices



- Payment terminals
- Applications
- Thales J.V.

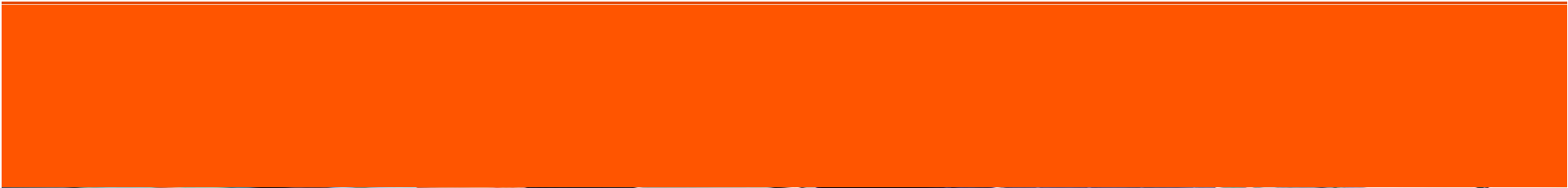
Transaction Networks



- Argent transaction network
- Leased line, dial, mobile
- Internet payment gateways

Fleet Mgt & Services

- Fleet rental
- Install & training
- Service & repair
- Staging & distribution
- Asset management
- Help desk



Our Mission



- To provide **trust** and services in electronic transaction solutions
- POS terminal management and maintenance
- Smartcard and terminal based solutions
- Secure network solutions
- Integration and management services



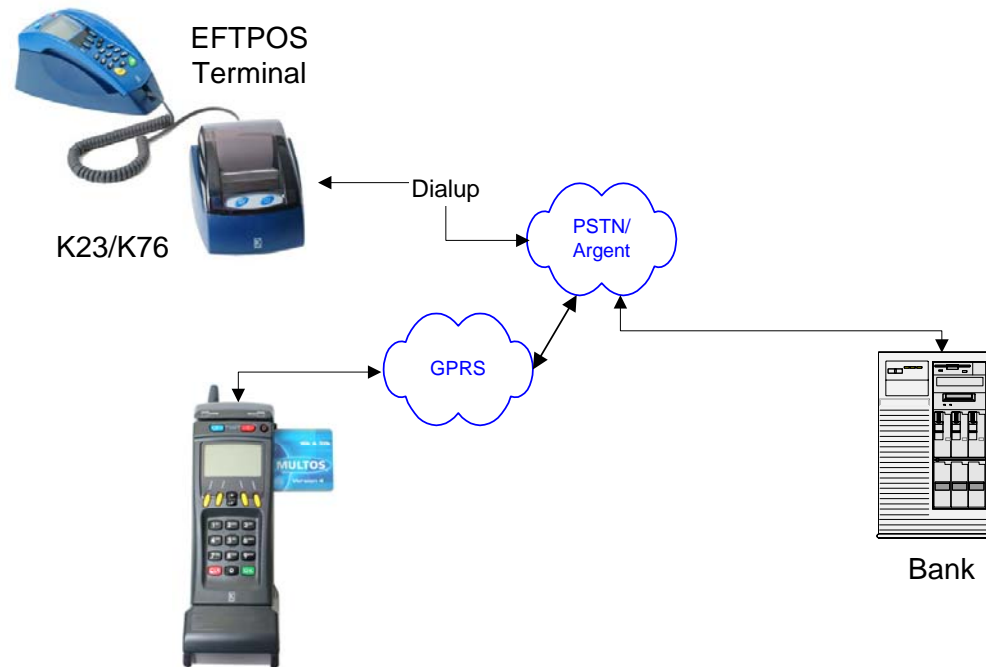
Trust



- **Trust** – the expectation that a device, system or process behaves in a particular manner for a particular purpose.
- **Transactions** – a transaction is defined as any transfer of information, secure or non-secure, and the protocols/policies associated with that information transfer.
- **Trusted transaction** - defined as the expectation that any part of the transaction has not been modified, tampered or spoofed.
- An enabling technology to achieve trust is the use of a trusted environment.
- **What is a Trusted environment?** Let us first take a look at the current transaction network.

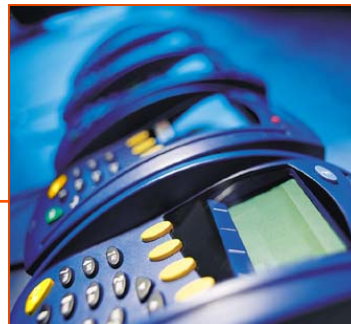
Current System

51562909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
87890513218 0856464 5451582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
68247829090380 850 0025 132 087890513218 0856464 5451582909080 80 85002513208 780513218 65349 0 850025132 6783492



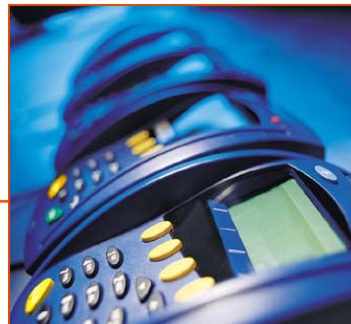
Driving Forces

- Broadband networks
- Evolving payment standards
- Increased security
- New input devices
- Price erosion in commodity devices
- Consumer trends



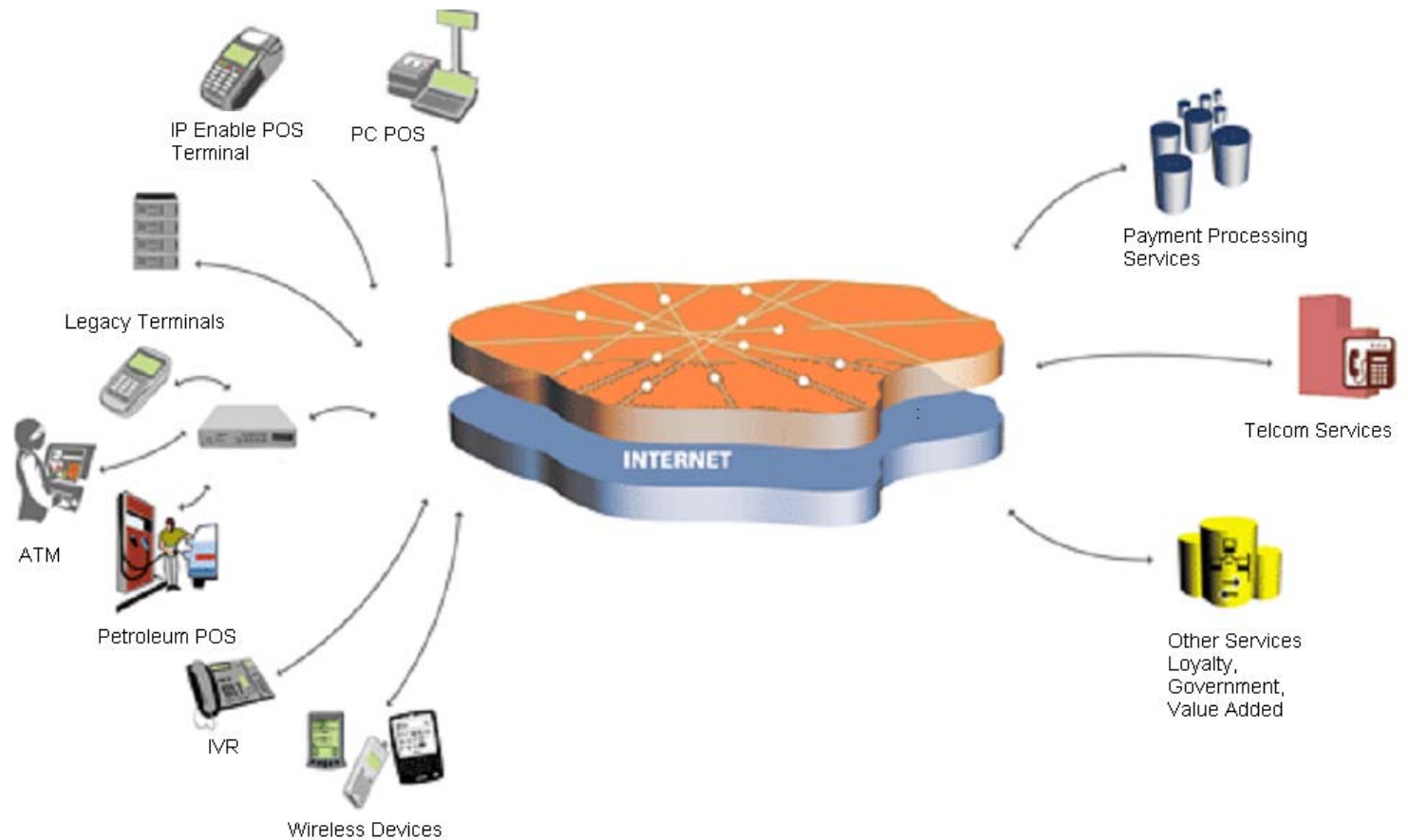
Requirements

- Fully secure
- High speed
- Available and reliable
- Fully managed services
- Simple, rapid service deployment
- Application/device independent connectivity
- Cost effective
- Global
- Rapid provisioning
- Legacy support



IP Enablement

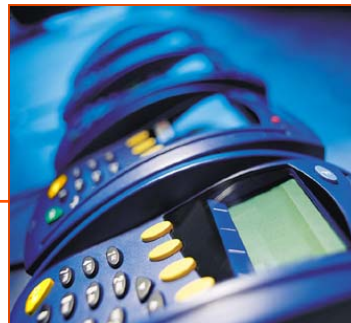
51562909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
87890513218 0856464 5451582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
89247829090380 850 0025 132 087890513218 0856464 5451582909080 80 85002513208 780513218 65349 0 850025132 6783492



Broadband Networks



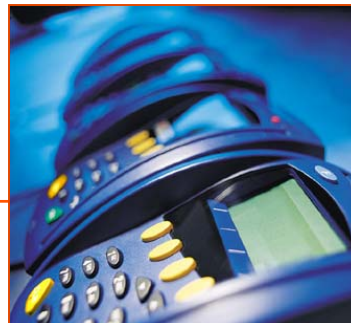
- Connectivity
- Always on-line, wired/wireless
- Continuous refinements/enhancements
- New standards and new connectivity
- Network monitoring
- Network services



Broadband Networks



- Hardware/software
- Broadband aware and capable
- Continuous change
- Off the shelf
- Value added services
- Platform Agnostic



Broadband Networks

51562909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
87890513218 0856464 545 1582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
88247829090380 850 0025 132 087890513218 0856464 5451582909080 80 85002513208 780513218 65349 0 850025132 6783492



- Security
- Open security standards
- Network security
 - SSL, IPSEC, Proprietary
- Platform Security
 - Trusted/Certified Applications
 - Firewall/Virus Protection
 - Trusted Platform (Let us examine what this is in detail)



Trusted Environment Properties



- All applications loaded to a Trusted Environment should be appropriately authorised.
- The deletion of any application from a Trusted Environment should be appropriately authorised.
- Applications should be able to be loaded to a Trusted Environment in an encrypted form and made available inside the trusted environment.
- No application in a Trusted Environment can interfere with the operation of any other loaded application or with the trusted environment.
- A Trusted Environment must be able to authenticate itself as a valid trusted system.
- A Trusted Environment must have appropriate limits on sensitive functions to disable the function if the trust system is attacked (trial and error, DNS, etc.).

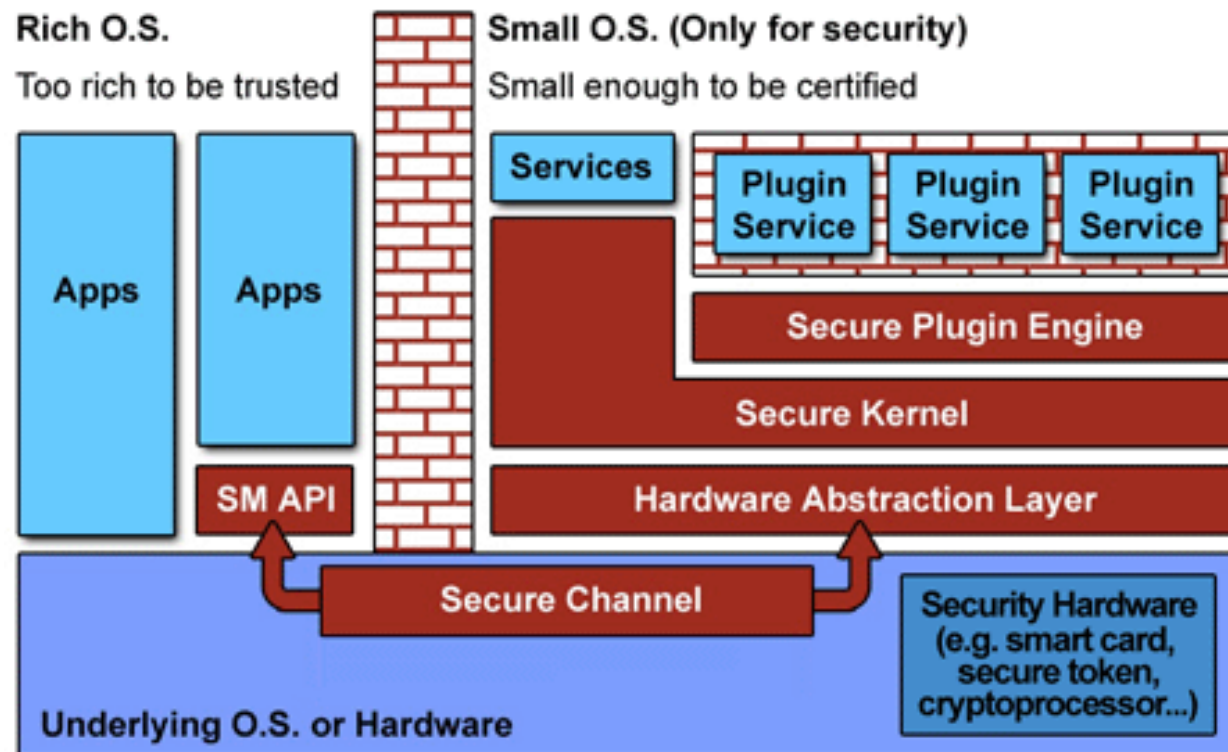
Properties – Continued



Where a trusted environment interfaces with a human operator,

- The trusted environment shall provide a path for secure information transferral to the operator by applications using appropriate sensory means. (E.G. Secure graphics).
- The trusted environment shall provide a path for secure information transferral from the operator to an application by appropriate means (e.G. Keyboard interface).
- An operator must be able to authenticate that the device is a trusted environment. Likewise a trusted environment must be able to authenticate a valid user.
- Trusted environments use open standards, systems and processes.

A Trusted Environment

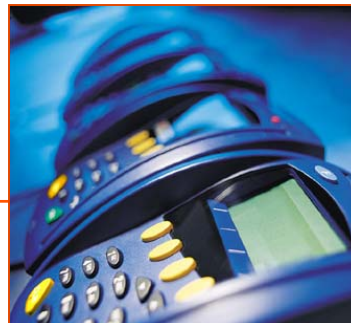


Payment Standards

51562909080 80 850 025 132 087890513218 0856464 5451582909080 80 850 025 132 5418 689122856980 5 132 5418 689122811
87890513218 0856464 5451582909080 80 850 025 132 08789051321825 132 0878905125 132 0878851420325 132 087890 54678
88247829090380 850 0025 132 087890513218 0856464 5451582909080 80 85002513208 780513218 65349 0 850025132 6783492



- Continuously Evolving
 - EMV, PCI, ...
- Objective is to minimize certification costs, and anticipate future security needs.
- Certify once, deploy everywhere.



Commodity Devices



- OTS devices, PDA, cell phone, PCs
- Decreasing cost, increase functionality
- Ubiquitous
- Direct use
- Sharing of communications infrastructure
- Connecting OTS products



New Input Devices



- Convenience to customer and merchant
 - Contactless swipe, smartcard
- Authentication
 - Migration away from signature and PIN
 - Biometric - fingerprint, retinal, vein



Migration Toward



- Open platforms using OTS components
- Increase in security standards
- Consolidation of standards
- Marginalization of hardware
- Integrating toward commodity devices
- End-to-end services/Pay per use
- Globalization
- Continuous change

