



Clearing & Payment Services Case Study
BPO Conference 24,25,26 May 2004




Denis Malone, CEO, CAPS

Agenda

- 1) Experiences gained creating and running CAPS
- 2) Managing The Risks: Confidentiality and Security Issues
- 3) Evaluating Managed Security Service Providers

Milestones

- Q2 2001 - Feasibility Study was undertaken
- Q3 2001 - Decision to proceed was made and work to build the Utility started

- Q1 2002 - CAPS as a company emerged - based on equal shareholdings
 - ▶ **DBS** 
 - ▶ **OCBC** 
 - ▶ **UOB** 

- Q2 2002 - Integrated testing of CAPS together with Banks and CLS took place
- Q3 2002 - Technical & Operational Approvals with CLS were conducted
- Dec 2002 - CAPS and Banks went live with 7 first wave currencies

- Sep 2003 - CAPS and Banks went live with the Singapore Dollar and Scandinavian Currencies

CLS Processing

- Processing high value trades and payments on behalf of our customer banks
- Monitoring the status of these trades and payments throughout an extended business day
- Global visibility

Starting Point for Developing the Shared Service

4 questions were asked

- Is any one bank significantly worse off?
- Do the four banks benefit by working together?
- Will the financial industry benefit?
- Will Singapore benefit as a regional financial centre?

Yes

No

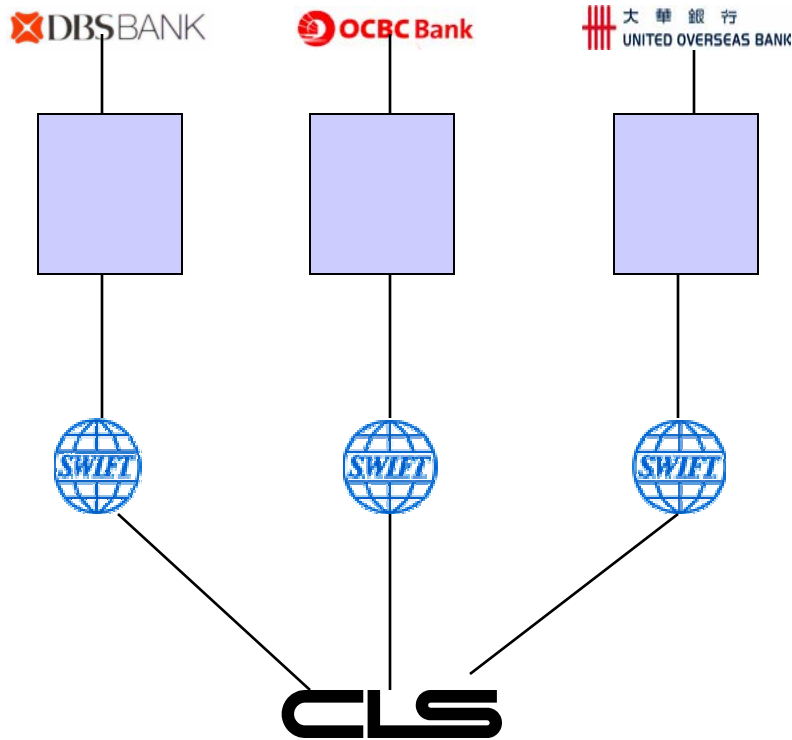


CLS Working Group recommends that the then four Banks, with the support from the MAS, move forward with the formation of a High Value Payments Utility that *initially* focuses on CLS.

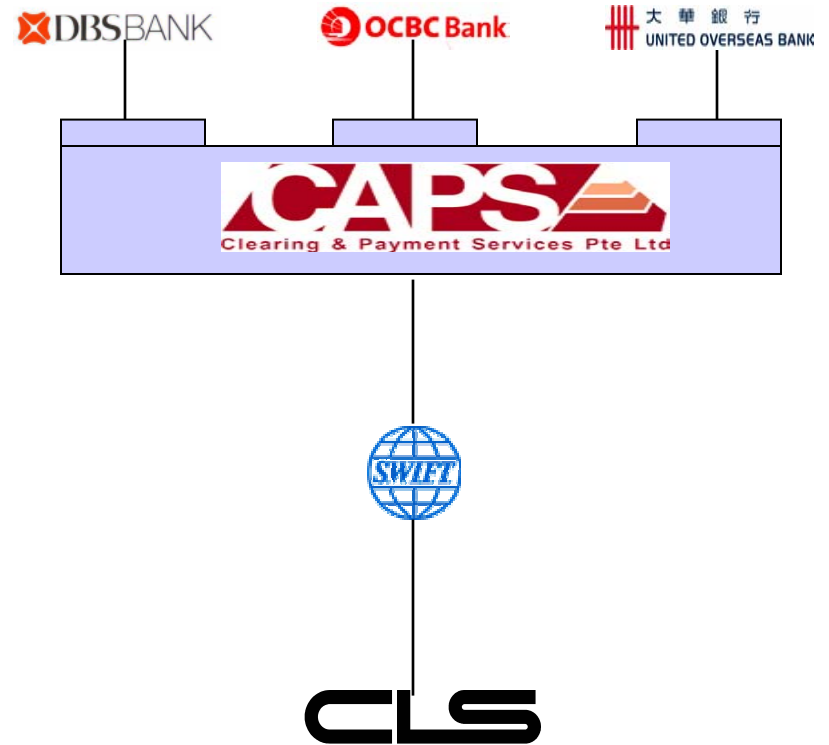
All partners committed to developing a shared services utility from the outset

Business Architecture of the Utility

Individually

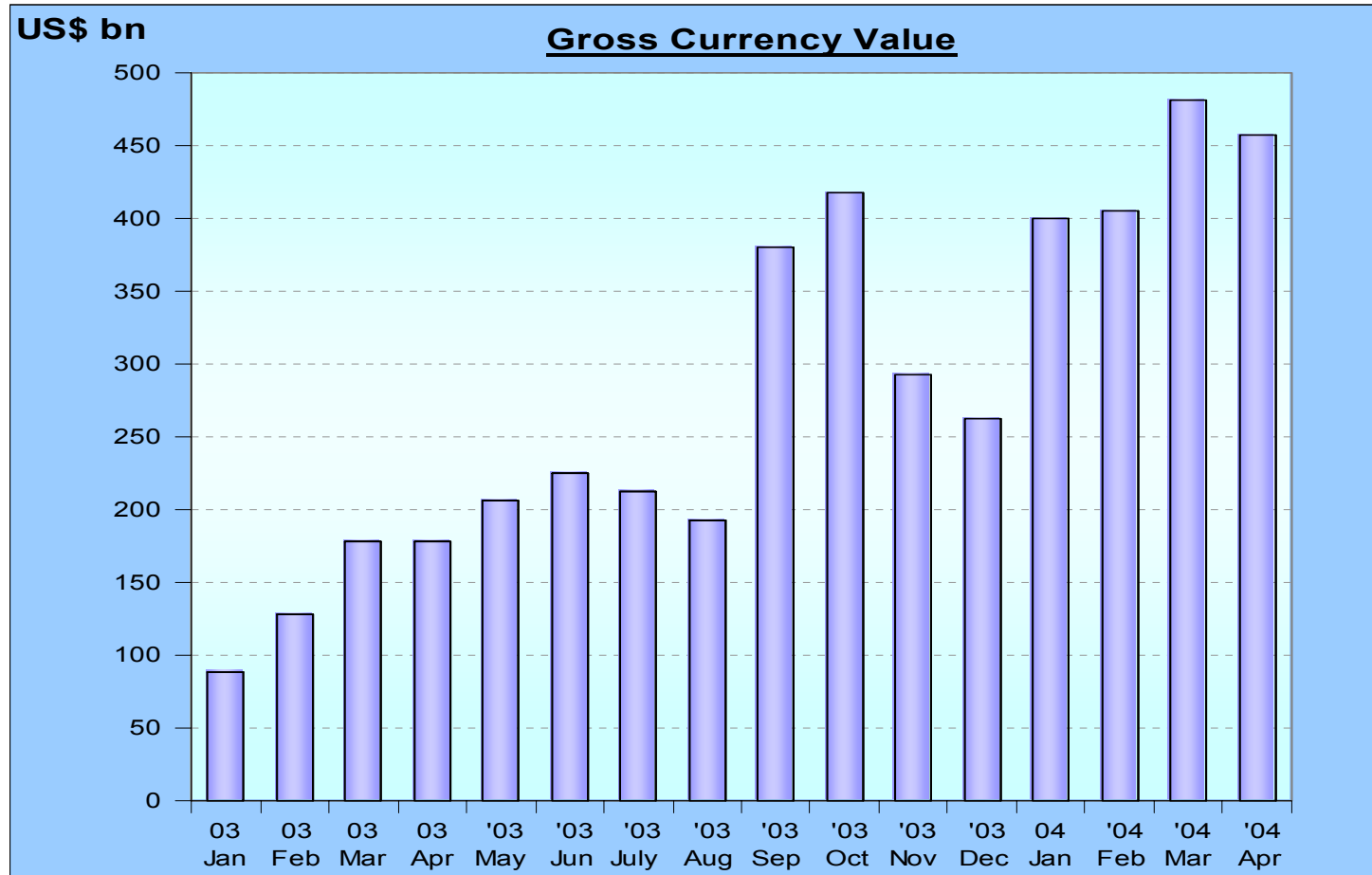


Utility Approach



Benefits accrued to banks from the rationalization of the business processes, technology, BCP, DRP and security infrastructures

Gross Currency Volumes to Date



Cumulative Gross Ccy Value
US\$ 4.556 trn

Cumulative Net Payment Value
US\$ 108.0 bn

Elements of Success in Building CAPS

- Co-operation between competitors (“collaborate to compete”)
 - Strong Leadership & Management
 - CAPS Build Committee to guide and control project
 - Quality professionals from Banks and Project Manager
 - Constant progress measurement and direction control
 - Transparency and openness
 - Culture of “No surprises”
 - Regular and clear communication amongst all participants
 - Highly skilled team
 - Members drawn from the banks and project manager providing a broad palette of skill sets with in depth industry experience
 - Stakeholder buy-in
 - Support from Monetary Authority of Singapore (MAS)
 - Top management support in each Bank

Utility Concept – The Underlying Principle

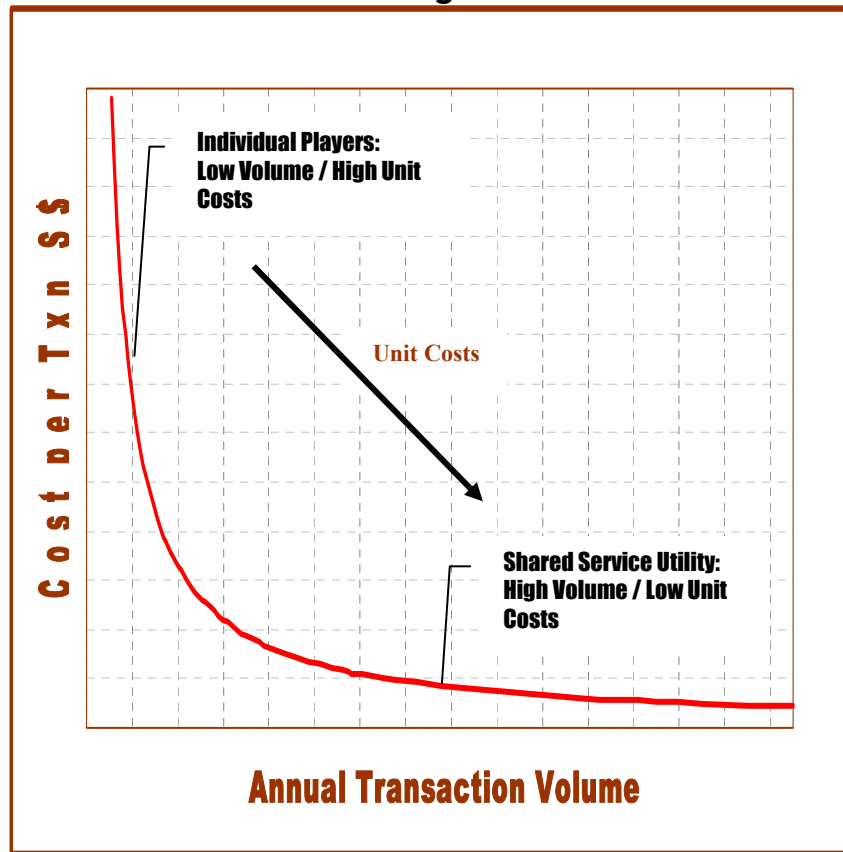
Objective is not to make excessive profits but to return the efficiencies of the utility to the customer in the form of lower unit costs

A small mark-up is made on each transaction

As the volume increases then the price per transaction to the customer should decrease

The actual pricing schedule is made available to CAPS customers

Economies of scale: driving costs lower



High volume/low cost model means that customers can operate at the end of the cost curve normally available to the large industry players.

Operating the Utility

- Expertise and Existing Infrastructure
 - An existing body of expertise and proven infrastructure that can be leveraged to significantly reduce the cost and risk elements impacting a CLS implementation project.
- Strong Governance:
 - A governance model ensuring best practice management.
 - Annual, independent reviews of the technology, operations and governance controls. Based in Singapore, a jurisdiction respected worldwide for stability and strong governance
- Independence and Confidentiality:
 - Utility not a subsidiary of a bank : No shareholder has a controlling stake
 - Utility is not a competitor to any of its customers: Not in the banking space
 - Customer data is kept separate at all times and robust systems and processes are in place to prevent release of data to any unauthorised third party. IT infrastructure has passed rigorous testing by professional security firms.
- Security and BCP:
 - Strong physical and IT security measures in place to protect customers. BCP systems in line with industry best practices to provide customers with highly resilient services.

Operating the Utility [contd.]

- Continuous Improvement Program
 - Program to implement improvements aimed at increased efficiency in service delivery and price.
 - Development and training programs to ensure staff are kept current in terms of skill-sets
- Customer Management
 - Regular formal meetings with each set of customer representatives
 - Regular user group meetings with all customers present
 - Twice yearly customer satisfaction survey
- Quality Program
 - Formal quality program in place to provide sound foundation for excellence in service delivery
 - Within this, substantial recording of metrics to facilitate service measurement
- Risk Management Framework
 - Implemented a formalised risk management process to identify, assess and put in place appropriate action plans to mitigate risks
 - Includes creation of a Governance & Risk Management Committee headed by an independent director
 - Annual independent review of internal controls by leading services firm
 - Report is made available to customers

Managing the Risks

- Ensure that the organisation itself and its services are resilient
- Initiative was led by a team from a leading services firm
- All staff were involved in the exercise, through workshops, interviews, reviews etc.
- The result was that a series of categories of Risks were identified
 - Governance
 - Business
 - Technology
 - Operational
 - Human Resource
 - Compliance
 - Confidentiality & Security
- Within each of these categories, a number of possible risks were identified, an assessment made of the significance of each of the risks and detailed action plans put in place to mitigate such risks

The Risks That Exist

- Ensure that the organisation itself and its services are resilient
- Initiative was led by a team from a leading services firm
- All staff were involved in the exercise, through workshops, interviews, reviews etc.
- The result was that a series of categories of Risks were identified
 - Governance
 - Business
 - Technology
 - Operational
 - Human Resource
 - Compliance
 - **Confidentiality & Security**
- Within each of these categories, a number of possible risks were identified, an assessment made of the significance of each of the risks and detailed action plans put in place to mitigate such risks

Confidentiality and Security Issues

Information needs to be protected to ensure:

- Integrity
 - The information delivered or available is as intended, and has not been modified without authority or, worse, intentionally corrupted.
- Confidentiality
 - The information is protected from unauthorised or accidental disclosure.
- Availability
 - The information is only made available to those who are authorised to access or view the data, be it users, support personnel or customers.

Confidentiality and Security Issues

If not protected, the implications can be severe:

- Commercial
 - Information can be used by competitors or rivals, with resultant loss of current or prospective business.
- Legal
 - The confidential nature of certain types of information is protected by law (eg. Banking Secrecy). Breaches of this could result in legal action (civil and criminal) being taken.
- Regulatory
 - Information made available contrary to guidelines issued by industry regulators can result in some form of sanction from these regulators.
- Reputation
 - Inadvertent or unauthorised disclosure or access can result in public embarrassment and negative perception of company's standing.

➔ Confidentiality & security should be core pillars of service provided by the outsourcer

➔ Not unusual in some banking outsourcing contracts to have clauses allowing banks to terminate if confidential information is leaked.

The Information Security Risk

The Risk

- Is there
- Will always be there
- And will probably get even worse

The Risk can be

- Intentional and malicious
- Accidental (eg. human error)

But the outcome can be just the same (eg. unauthorised disclosure of data)

The Risk is from

- Third parties
- Customers
- Suppliers
- Staff

Simply focusing on “Perimeter Protection” (ie. the firewall) only creates an illusion of Information Security (IS)

- Some estimates are that as many as 60% of all security breaches come from internal sources (*source “Moment of Truth” - TruSecure 2003*)
- The perimeter is disappearing given trends in mobile computing, tele-commuting, working from home etc.

Holistic Approach to Information Security in CAPS

A well rounded Information Security (IS) framework should have three main components:

1. Technology

- Separate databases to prevent co-mingling of customer data
- Dedicated and encrypted leased lines between CAPS and its customers
- Two-Factor authentication for accessing applications
- Standard security infrastructure products and tools such as multi-layer firewalls, intrusion detection systems (IDS), intelligent routers

2. Processes

- Sensible security policies and procedures that are easily made available to, and understood by, all staff
- Document control and ownership to ensure right documents go to the right customer
- Up to date monitoring of emerging threats and vulnerabilities, together with an effective malicious code/virus protection program

3. People

- Continuously educate people on the risks and how they can contribute to protecting the information assets
- Instill the message of personal accountability among the staff - if you do something funny then expect to face the consequences...

The IS framework is regularly reviewed as risk cannot be denied, it can only be mitigated, and as the risks change so too must the IS framework.



Security must be at the very least, as good as the customers' security models

Evaluating Managed Security Service Providers

What is a Managed Security Services Provider (MSSP)?

- Organisations that provide a range of security services such as firewall management, intrusion detection, vulnerability scanning and security monitoring, typically on a 24x7x365 basis.
- Also may find services which are not necessarily offered on an on-going basis such as penetration testing, overall security assessments, policy reviews etc.

Why Outsource Security Services?

- Competency Pool
 - Experienced, skilled and qualified security personnel are hard to find and retain. MSSPs can provide the full range of security services and free up organisations from the need to build up large internal teams of security specialists, especially for small and medium sized enterprises
- Costs
 - Economies of scale provide MSSPs with the ability to offer services at costs which may not be otherwise achievable by firms

Note: Organisations should consider maintaining or developing some in-house security capability. Someone needs to manage the MSSP and be aware of what the MSSP is doing.

Factors to Consider When Evaluating MSSPs

Evaluating MSSPs - at the MSSP side

- Expertise
 - Technical capabilities, market experience, skilled resources
- Financial Stability
 - Financially robust, sound funding, reliable business model, good governance structure
- People/Culture
 - Is this a firm you can do business with, and develop a productive partnership based relationship?
- Scalability
 - Ability to respond to surges in activity without customer service degradation
- Certification
 - Industry supported certifications at both the enterprise and employee level (eg. ISO 17799 / BS7799, CISSP)
- Cost
 - Service should be provided at a cost effective rate

The categories for evaluating an MSSP are quite similar to those used for evaluating any outsourcer. The difference is in the detail criteria within each of these categories.

Factors to Consider When Evaluating MSSPs

Evaluating MSSPs - at the customer side

- Scope
 - Clarity around the definition of what is being outsourced, and the service levels associated with the service
- Reviews
 - Process to review and measure the performance of the MSSP against the pre-agreed Service Level Agreement (SLA)
- Confidentiality
 - How is the customer data being protected, what are the controls in place within the MSSP, what happens to the data upon termination of contract?
- Termination / Early Exit
 - Clearly define the conditions under which a termination can be effected and the consequences of this
- Contingency
 - Ensure plan in place to cover the circumstance of service discontinuation (for whatever reason)

The categories for evaluating an MSSP are quite similar to those used for evaluating any outsourcer. The difference is in the detail criteria within each of these categories.

Thank You



For more information please log on to www.caps.com.sg