March/April 2000 Issue No. 23

PAYMENTS MONITOR

ISSN 1321-7755

*PAYMENTS MONITOR is published by APCA each quarter.
Its purpose is to keep members and interested parties
abreast of developments in payments clearing.*

INTERNET BASED PAYMENT APPLICATIONS – TRUST AND DIGITAL CERTIFICATES

> “The internet, by broadening markets, will lessen the degree of business-to-business intimacy between trading partners. In this environment it will be particularly important to retain trust in payment systems.”

The Internet & Payments

The Internet will broaden markets, but it will work effectively only if it is underpinned by appropriate payment arrangements.

Payment arrangements can be classified as closed or open. Closed arrangements are those where the payer and payee deal with the same provider of payment services.

Open arrangements are those where different providers of payment services are involved. In this case, common procedural and technical standards are needed to hold the arrangement together. These are often provided by umbrella organisations. This is what APCA does in Australia. Open systems are more powerful than closed systems and largely dominate the payments business.

Trust is very important in open payment systems. It is particularly important in an internet environment in circumstances where certainty and non-repudiation are essential counterparts of trade.

Trust

Banks and other deposit takers – credit unions and building societies - have the inside running in generating this trust. They have the account relationships, provide undoubted value, and have the ability to extend, and the skills to manage, credit.

The real issues are the mechanism banks will use to underpin trust, and the extent to which they will be involved either alone, or in alliances, in the commercial transactions that lead up to payment.

Digital Certificates

Digital certificates will provide an important part of the mechanism for underpinning trust. The current alternatives, of a shared secret password between customer and bank and the one-sided authentication/customer repudiation model applying to the use of credit card payments, are both limiting.

Banks are well placed to control and manage the issuance of certificates. As noted, they already have the account relationships and can therefore fairly easily identify their customers and guarantee their credit position.

But banks cannot operate individually in this area and be effective. Certificates will work effectively only if common standards of the kind that glue banks together in open payment systems are also applied to the issuance and validation of certificates. Banks, therefore, will need to cooperate through organisations like APCA. At the same time, there may well be boundaries to cooperation, particularly on an international scale.

Published By:
Australian Payments Clearing Association Limited
A.C.N. 055 136 519

Level 24
25 Bligh Street
SYDNEY NSW 2000

Tele: (02) 9221-8944
Fax: (02) 9221-8057
Web: http://www.apca.com.au

INTERNET BASED PAYMENT APPLICATIONS (CONT'D)

Interoperability

Common standards or interoperability between members of the same public key infrastructure (PKI) is axiomatic. Digital certificates issued by one bank should be recognisable by another within the same PKI and be capable of being validated.

However, interoperability becomes an issue when it is between different PKIs or between members of different PKIs.

PKI architectures can be split into four levels – while keeping in mind that they are by no means independent of each other.

First, is the specification of the certificate itself. **Second**, the policies and practices governing the issuance and revocation of certificates and the technical and security standards to be applied in doing that. **Third**, are the tailored rules and processes which may be put in place to allow the recipients of a certificate (and their banks) to validate its authenticity and its applicability, force and limitations. **Fourth**, are the particular payment applications for which certificates can be used.

At APCA we are building a public key infrastructure for our members, which currently addresses the first two of these levels. We are building it to best practice standards. But, it's important to note that it is at the validation and application levels - the third and fourth levels - where interoperability will have practical impact in facilitating payments.

How far should the need for interoperability be taken?

There would appear to be advantage in having as common standards as is feasible in respect of the first two levels of PKI architectures, as described. A number of international forums are contributing to this objective. It has found expression, for example, in the X509 certificate (through the International Telecommunications Union (ITU)); in cooperation between technology providers (through the PKI Forum); and in the development of a documentary policy and practices framework (through the Internet Engineering Task Force (IETF)). This might well lay the basis for selective cross-certification between PKIs and piecemeal convergence at the validation and application levels between individual banks.

However, it neither seems practical or necessary, and it would certainly slow things down enormously, to aim for PKIs with assured interoperability at validation and application levels, as part of some grand plan. This is particularly the case if certificates become important in most countries to support localised domestic internet payment arrangements.

Overlapping PKIs seems a more promising model. A business might have two certificates. For example, one issued by its bank under the auspices of a PKI with international coverage; one under the auspices of a domestic PKI.

This is an extract from a speech to be delivered by APCA's CEO, Peter Smith, to the Payment Systems International Conference 2000 in Bruges, Belgium, 10 – 12 May 2000.

APCA EXTRANET

> "APCA's extranet is a technology driven communications channel that is used for the electronic distribution of APCA documentation. Essentially, it is an on-line electronic information service, with the technical capability to provide users with 'real time' access to content."

APCA's extranet service was implemented in June 1999. At the time of implementation, the objective was to provide designated representatives of member organisations with an alternative means of access to APCA documentation.

Up until June 1999, members had only one option for accessing APCA documentation – in printed format. Since then, members have been provided with the additional option of electronic access to documents. By making electronic copies of documents available on the extranet, members are now able to utilise existing electronic files to enhance the internal distribution processes of APCA documentation within their organisations.

User IT requirements

In order to login to the extranet service, users require access to the internet. A browser is also required (eg. Microsoft Explorer, Netscape Navigator), preferably version 4 or later for best viewing results.

Electronic copies of documents on the extranet are currently available in Microsoft Word format. Scanned copies of attachments are available in PDF (portable document format).

Access

Access to the extranet is administered by authorised user login ONLY. Access to the extranet may be granted to individuals who qualify as one (or more) of the following:

- A Director of APCA;
- A representative of a Share Member organisation (ie. a person advised to APCA as the share representative for that member in Ordinary, A, B, C, or D class);
- A representative of a Participating Member organisation (ie. a person advised to APCA as the contact for that Member in CS1, CS2, CS3, or CS4);
- A member of an APCA committee (MC1, MC2, SPC3, MC4);
- A member of an Advisory Council (subject to any limitations under clearing system regulations);
- A person who has accreditation within APCA. 'Accreditation' means that the person is known within APCA to work with or provide assistance to a Director, Management Committee Member, Advisory Council Member, or to a representative of a Share Member or Participating Member organisation.

Access application procedure

In order to gain access to the extranet service, users are required to lodge an application with APCA. Electronic application forms are submitted via APCA's public web site.

Once an application has been approved, all relevant login information is sent to successful applicants via email.

User access profiles

In general, individuals are granted access to databases that correspond with their level of direct involvement with APCA. Access is stratified by committee type and clearing stream.

Outlook

It has been proposed that APCA's extranet service be deployed as the primary communications channel for the distribution of committee and operational documentation, thereby replacing the current method of paper copy distribution.

YEAR 2000

"APCA's Y2K Industry Program ends on a successful note."

Year 2000 Leap year Date Transition

APCA's Y2K Communication and Co-ordination Centre (C&C Centre) operated during the 'leap year' date period 29 February to 1 March 2000, inclusive. APCA's members (banks, building societies and credit unions) were required to report any payment system operational difficulties, should they occur, to the C&C Centre.

The APCA C&C Centre received no reports from members advising of any Y2K difficulties affecting the normal operation of their payments systems, which fall under APCA in respect of clearing arrangements [cheques, direct entry credits and debits, ATM/EFTPOS, and high value].

APCA's Year 2000 Industry Program Completion

APCA and its members carried out considerable work to avoid Y2K disruptions to payment systems over the two critical periods, the transition from 1999 to the year 2000 and the 'leap year' date.

Clearly the work has been successful and APCA's year 2000 industry program has been completed.

"APCA's focus in relation to the Year 2000 problem is to co-ordinate industry testing and industry preservation and contingency planning to deal with that problem from a payments system-wide perspective. Responsibility for achieving the aims stated above for each of these initiatives cannot rest solely with APCA, as its work is not a substitute for, and is meant to complement, the due diligence/ remediation work and contingency planning each institution must separately undertake to identify and address the particular Year 2000 problems that are likely to effect that institution."

"This statement is a Year 2000 disclosure statement authorised by the Australian Payments Clearing Association Limited for the purposes of the Year 2000 Information Disclosure Act 1999. A person may be protected by that Act from liability for this statement in certain circumstances."

CONTINUOUS LINKED SETTLEMENT

"APCA is currently working with member institutions to facilitate the entry of CLS Bank International into our High Value Clearing System. It is expected that this will occur in the latter half of 2001."

CLS Services is an organisation that was established by major financial institutions to provide member organisations with a service in respect of the settlement of foreign exchange (FX) transactions.

When it becomes fully operational the process is to be operated by a new bank called CLS Bank International ("CLS Bank"), which will act as a settlement intermediary between the two counterparties to an FX trade or between their correspondents.

Each settlement member will be required to maintain a single multi-currency account with CLS Bank, which under normal circumstances, will have a zero balance at the beginning of each settlement day.

Each Settlement Members will pay in funds in accordance with the pay-in schedules generated by CLS Bank and the Settlement Member's account will be credited and debited as a result of both funding transfers and settlement transfers.