Lockstep White Paper No. 3

Lockstep Consulting Pty Ltd
Contact: swilson@lockstep.com.au

The "Security Printer" model for CA operations

A simple new conceptual model to describe the role of backend CAs

Stephen Wilson
Version 1.1, September 2005

Executive summary

Our historical view of the role of backend CAs has had them tied into the whole of the certificate management process. CAs tend to be joined in liability arrangements and contracts to potentially any wrongdoing or misadventure associated with certificates. CPs, CPSs and user agreements have been correspondingly difficult to construct. To date, the separation of roles of RA and CA has done little to quarantine the two functions from one another, nor to simplify liability arrangements. Accreditation remains complex and sensitive to the slightest changes at either the RA or CA. This exposure draft presents a new way of looking at backend CAs, likening them to conventional security printers, and outlines how a fresh metaphor might help simplify the accreditation of CAs.

Acknowledgements

Much of this paper was originally researched and developed by Lockstep Consulting under contract to the Department of Finance and Administration, represented by the Australian Government Information Management Office (AGIMO). Lockstep gratefully acknowledges the permission of AGIMO to reproduce this work. Note carefully that the "security printer" model is *not* Australian Government policy.

The business of security printing

For decades it has been well known that to combat fraud, special care must be taken in printing certain documents: blank cheques in particular, as well as business forms, prescription pads, gift vouchers and so on.[1] A whole industry

[1] The printing of banknotes is a special case and is not treated as part of the current discussion. "Security Printing" services for the purposes of this paper are regarded as businesses with the capacity to furnish a range of different printed products under commercial contract.

has been built around special printing technologies, including watermarks, holograms, reactive inks that detect photocopying, and micro-printing. Moreover, a whole business model has been built around *security printing bureau services*. In many sectors, standards have been written to cover the necessary security of premises and processes. And formal accreditation schemes govern compliance with these standards. For example, since January 1, 2005, written prescriptions for controlled substances in California must be on tamper resistant security prescription forms produced by a printer approved by the California State Board of Pharmacy.[2] The Australian Payments Clearing Association (APCA) is developing a Cheque Printers Accreditation Scheme (CPAS).[3] APCA's corresponding organisation in the UK, APACS, introduced its Cheque Printers Accreditation Scheme in 1995.

The governance of security printing

The scope of standards governing security printing is not unlike those for backend Certification Authorities. For example, APCA has outlined that its cheque printer accreditation will cover assurance of the following aspects:[4]

- *Equipment & Materials*
- *Premises Security*
  - *External security (prevention of unauthorised access)*
  - *Internal security (appropriate restrictions on access to different areas)*
- *Process Security*
  - *Process controls in place 'end to end' (eg from raw materials, through to end product)*
  - *Full audit trail in place for each print job*
  - *Destruction process for unused/damage stock*
  - *Protection of confidential information*
  - *Employee screening and confidentiality clauses*
- *Order Processing*
- *Quality Assurance*
- *Despatch & Delivery*
  - *Secure & auditable despatch system*
  - *Appropriate sign-off for delivery*
  - *Reliable and secure transport arrangements*
  - *Secure packaging*
  - *Appropriate labelling (not to identify as cheques)*
  - *Process for lost/stolen consignments*

[2] See www.pharmacy.ca.gov/consumers/security_printer_list.htm.

[3] See www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Cheque_CPAS.

[4] This list is adapted with minor editorial changes from "Cheque Printer Accreditation Scheme", a presentation to the Xplor 2002 Document Management Conference, by Michael Forey, Director, Project Management & Operations, APCA; see www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Xplor_May2002.pps/$File/Xplor_May2002.pps.

Accredited printers under the British CPAS variously emphasise their personnel screening, internal segregation of access-controlled security cages, and perimeter fences and monitoring systems. Clearly a similar degree of effort is involved physical, procedural and personnel security for security printing operations as for well run CAs such as those typified by accreditation under Identrus, WebTrust for CAs, Australia's Gatekeeper® scheme, or the UK's tScheme.

A worked example: stock exchange security barcodes

A practical worked example helps to further develop the comparison between backend CAs and security printers. The example is a system whereby a stock exchange secures statutory announcements made by listed companies and communicated by fax.

Each listed company is provided with a roll of self adhesive barcode labels; see Figure 1 below. The barcodes uniquely identify the company and are individually serial numbered. When a statutory announcement needs to be made in accordance with the stock exchange's Listing Rules, the announcement is printed, signed by a duly authorised company officer, and has one of the barcode labels affixed to it, before being faxed to the announcements processing centre. When received, optical character recognition (OCR) software scans the fax, extracts the announcement, and verifies the barcode, before re-formatting the contents of the announcement in a standardised manner to be broadcast across stockbrokers' systems.

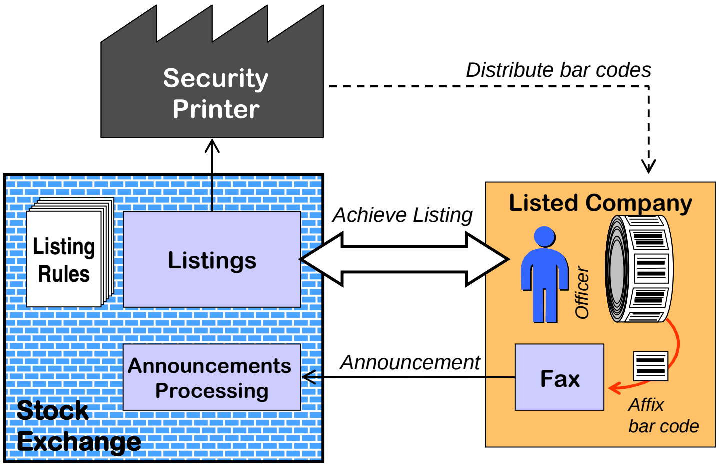

Figure 1: Authenticating faxed announcements by bardcode

Thus the barcode label represents an authentication token. Possession of a barcode label is taken as reasonable evidence that the holder is a listed company, operating under the stock exchange's rules. Clearly such labels are precious items. They need to be produced by a reputable security printer, with both the ordering and distribution processes being subject to strict controls.

Now, let us consider how the announcement processing system could be reengineered to use PKI and electronic messaging in place of fax machines. Figure 2 shows a nearly identical system, where the stock exchange's Listings unit operates an RA, and instead of ordering barcode labels from a security printer, it orders digital certificates from a backend CA. To make an official announcement, now the company officer would use the certificate to digitally sign the electronic message.

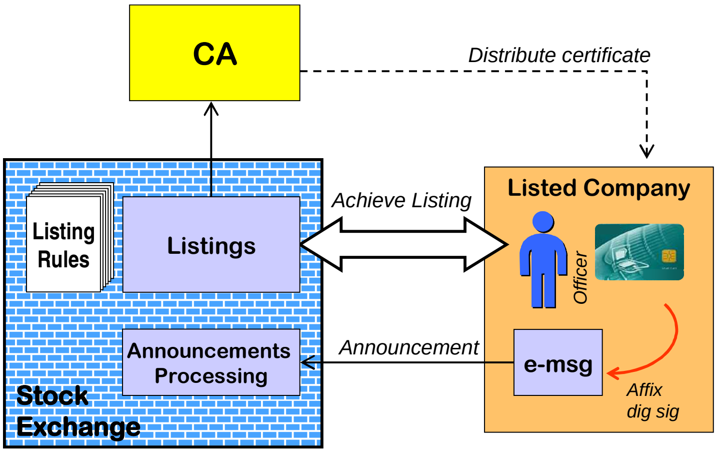

Figure 2: Authenticating electronic announcements by digital certificate

Security controls for the stock exchange announcement system

Regardless of whether the authentication is done using barcodes or digital certificates, the announcement system requires a common set of security controls:

1. The listing process must be robust and difficult to subvert.
2. It must be difficult to fraudulently order barcodes [or digital certificates].
3. Barcodes [or digital certificates] must be difficult to counterfeit.
4. The security printing [or backend CA] process must be difficult to subvert.
5. Barcodes [or digital certificates] must be distributed carefully.

If the conventions of orthodox PKI were to be applied to this operation, then a number of additional complexities would be imposed from outside on how the stock exchange runs its business. In Australia for instance, compliance with the federal Gatekeeper® accreditation program would require standardised identity proofing for all certificate recipients at a level equivalent to passport application, irrespective of how the existing listing rules operate. Accreditation would cover the stock exchange's registration processes and the backend CA's technical processes at the same time. Moreover, the company officer, as certificate subject, would have execute a user agreement with the CA. Changing backend CA would trigger major re-accreditation.

But comparing the digital certificate approach to the barcode system is suggestive of a more streamlined approach to PKI accreditation. Referring to the list of security controls above, we see that protecting against impersonation at the front-end is separable from protecting against counterfeiting at the backend. At the front-end, there is no logical difference between using barcodes or digital certificates, so we should expect the security of existing stock exchange registration processes to carry over to the PKI implementation unchanged. And at the backend, there is no need for the CA to be concerned with the details *nor even the integrity* of the registration process, so long as there are controls in place to mitigate against certificates being wrongfully ordered.

A proposition: translate the security printing business model into PKI

Why couldn't we treat backend CAs in much the same way as we treat security printing service providers? If CAs were set up as service bureaus, responsive to RAs[5] and minting public key certificates on instruction more or less automatically via standard PKCS protocols, then we should expect a set of simplifications to PKI management and governance, as follows:

— The CA need have no interest at all in the semantic contents of the certificates it mints on instruction from an RA. So long as there are safeguards in place to mitigate against false certificate requests being injected between the RA and the CA, the CA need not know anything at all about the RA's business process, nor the intended application of the certificates. The CA's business model and detailed processes could be entirely invariant over a wide range of different PKI applications.

— There is no need for a contract or other legal arrangement between end users of certificates and the backend CA (just as there is no need for end users of security forms like cheques and barcodes to have any relationship with the printer).

[5] As with all successful bounded PKI models, each RA would act on behalf of a community of interest, and register individual users for defined PKI-enabled applications, according to scheme or programme-specific business rules.

- The CA's liabilities are probably straightforward to analyse and codify. For example – and in stark contrast to orthodox RA/CA arrangements – it seems clear that a CA would not normally be joined in legal action resulting from an RA being negligent in registering an impostor. On the other hand, acts of omission or commission by a CA in minting poor quality certificates which led to harm on the part of message recipients, could be identified and prosecuted as such, and isolated from the RA.

- The meaning of the root key – which in orthodox PKI has led to so much confusion – can be likened to a unique watermark featured in all products from a given security printer. The chaining of a certificate back to the CA root would represent the simple fact that the certificate has come from an accredited facility. The root CA signature means only that it is extremely unlikely that a certificate has been forged, and does not impart any approval or endorsement by the CA of the contents of the certificate.

- It is likely to be much easier to novate backend CA service arrangements from one supplier to another.

Note that the security printing model would essentially preserve the physical, procedural, personnel and technology security controls of most current CA accreditation schemes, in order to protect against counterfeiting and subversion of the backend process. In particular, the benchmark of Common Criteria EAL4 rated CA and RA products would probably be retained, to help prevent fraudulent ordering of certificates.

Benefits to CA accreditation

If we were to co-opt the security printing model for the accreditation of CAs in general, the following benefits should obtain:

- Backend CA operations would become more independent of (and separable from) front-end RAs. The scope of accreditation for a backend CA could be made independent of the intended application of the certificates it mints on behalf of RAs. CAs would not need re-accreditation each time the semantics of a given digital certificate profile was changed. New certificate applications and community of interest RAs could be set up quickly, with no impact at all on backend accreditation.

- Backend CAs could simplify their business model, turning to a wholesale focus, and thus simplify the way they interact with and deliver services to front-end RAs.

— Certificate subjects would no longer be required to enter into contracts with backend CAs. Each subject's business relationship could be confined to just the RA, or even better, with the community of interest for which the RA simply acts as an agent.

— Certificate supply arrangements could be more readily novated from one backend CA to another, as RAs from time to time negotiate better deals for themselves. A change of backend certificate supplier need not have any impact at all on the accreditation of the front end, so long as the new supplier too has proper backend accreditation.

Further work

To realise the security printing model for backend CAs will require the following issues to be further researched and analysed:

— A new model CP/CPS may be needed for the general purpose minting of certificates by a backend CA independent of all details of the RA, including EOI and certificate profile. Certificate Practice Statements today tend to impose on the backend CA various details of front end operations, such as detailed of identity proofing, and circumstances for revocation. Under the security printing model, these matters would be of no concern to the CA, which would act more or less automatically on requests to create certificates, revoke them and so on.

— General principles may need to be worked out for the seamless novation of backend CA services without disruption to certificate Subjects, especially continuing support for directory and CRL/OCSP services.