Which Root Certification Authority can you trust?

Australia can show you the way.

By

Simon R Grant LLB LLM, Senior Legal Officer, Crown Law Queensland & Mediator

and

Steve Mathew, FIMC CMC, Director ArticSoft Limited

With the advent of commerce on the Internet, trading partners or parties in the business community (both vendor and purchaser) have had to come to grips with many intricate new predicaments. A significant part in this Internet process is gaining the trust of each party that the Internet transaction is not one where they are exposed to any greater risk than if dealing in person.

In the electronic world all you know is who the vendor is telling you they are, whether or not it is true. One method of proving information such as “who” I am dealing with is through a Public Key Infrastructure, or PKI. But (mathematics aside) any PKI is only as strong as its Root Certification Authority – the RCA.

Whilst the customer service officer at the computer in a multi-national will never physically make the decision, at some point someone will have to decide how on-line transactions are going to be verified as being trusted. With the vast number of PKI systems possibly available, it may be that you wish to trust a government run system only. But is this necessary? Are you limiting your options on places/people to deal with?

But the only way you will know is to look at each of the systems and assess what level of trust you need for a particular transaction.

Public Key Infrastructure Frameworks

The basic concept behind PKI systems is that, through proper application of the system, you can trust certain information provided to me through the system. This information may be a name, an address, an amount of money, or any piece of information you consider important. The way the PKI system does this is through the use of two “keys”, being unique results of a mathematical algorithm that are applied to the electronic information.

What the keys allow you to prove is not necessarily the truth of the information that is encrypted. They are proving whatever has been proven to a certification authority. For example, it may be that the keys are held by a certain person, or it may be that the holder of the keys, though nameless, has the authority to spend on a company account. Certification authorities (CAs) certify information by applying their own keys to the persons keys – that is, the owners ‘public’ key is signed by the CA.

Therefore, there is now a third party in the relationship– the Certification Authority (CA). But, how do you know that the certification authority is real? For example, through Microsoft you can set up your own public/private keys. Can you be sure the owner hasn’t just signed the information themselves?

The RCA is the point at which trust commences in a PKI system. The RCA is the certification authority which certifies the existence and quality of other certification authorities in the particular PKI that you wish to use. The way you identify the body that is the RCA depends on the structure.

Hierarchical Structures

Figure 1 below is a general hierarchical structure, as described by Ford and Baum in *Secure Electronic Transactions*. In this example, each entity with an upper-case identifier is a certification authority, whilst the entities with lower-case identifiers are end-users of the PKI system. The arrow directions indicate which entity provides a certificate. In this system, as the certificates across the PKI flow both ways, an end-user can choose which certification authority or authorities it considers to be the root certifier/s, that is, the authorities it considers the most trusted.

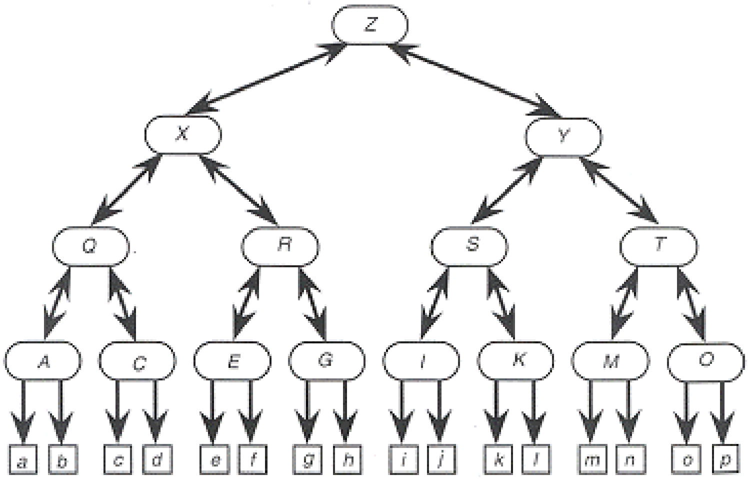

Figure 1 – The General Hierarchical Structure

A variation of this hierarchy is demonstrated by Ford and Baum in Figure 2, with the inclusion of additional links.

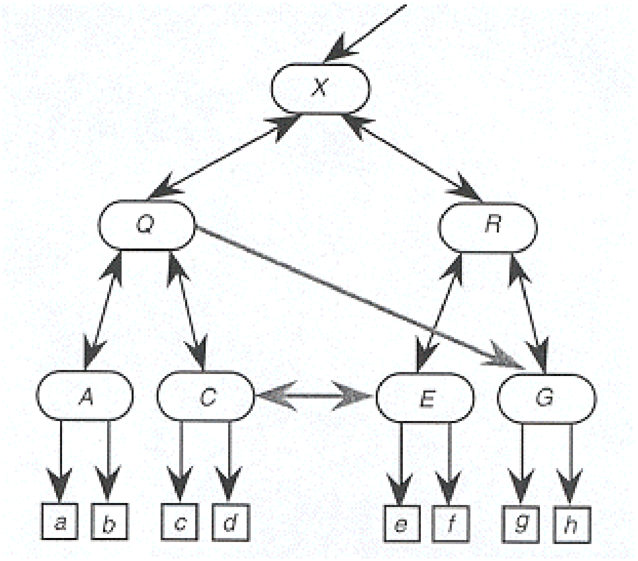

Figure 2 – The General Hierarchical Structure With Additional Links

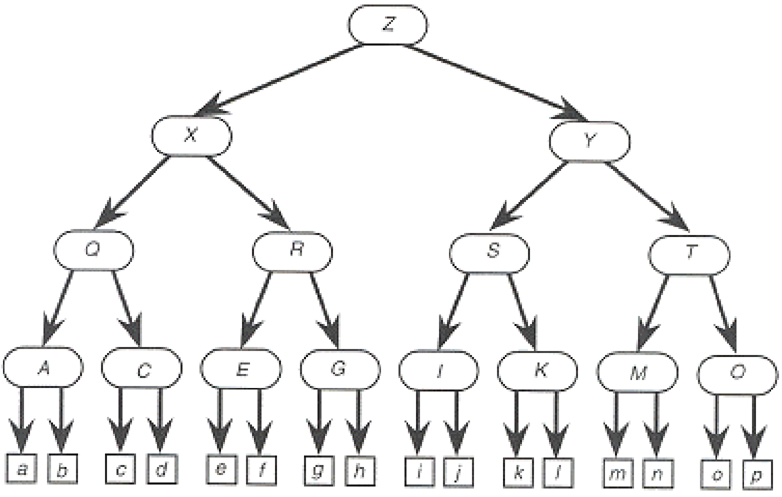

Figure 3 – The Top-Down Hierarchical Structure

This structure was developed by the United States Department of Defense. The advantage of this type of structure is that control can be kept of all information with only one certification pathway for each entity. The trust accorded to each level of certification authority follows the structure, decreasing as you go down the hierarchy.

But which type of PKI is the one for you? And why would you choose it? Whilst the rigid pathways of Figure 3 suit the natural chain-of-command found in the military and government departments, such a system may only readily apply to in-house transactions, and not general commerce.

Finance and SET

The business and Internet communities are not waiting for some over-arching system to be put into place by governments or agencies such as the UN. They are seizing opportunities as they arise, putting in place systems that they trust and selecting their own RCA – a PRIVATE RCA – if they select one at all. An example of this is the Secure Electronic Transaction (SET) PKI developed by Visa and MasterCard. Figure 4 represents the basic SET PKI as identified by Ford & Baum. A new version of the SET protocol has recently been introduced, sometimes referred to as 3DSET. It expects to provide the customer with a provable digital receipt for a transaction, establishing the formality of the contract between the customer and the merchant, something that was lacking in the original implementation.

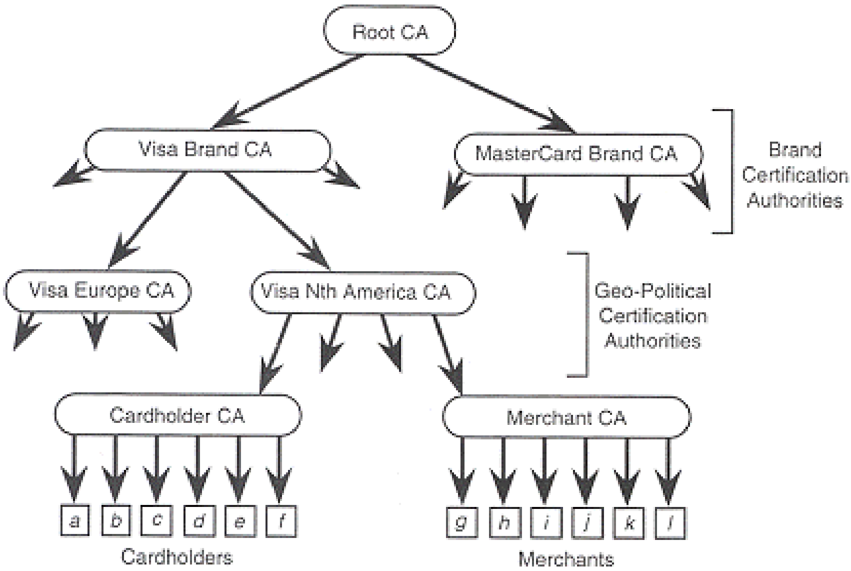

Figure 4 – The SET Hierarchical Structure

Under this system, Visa and MasterCard developed the RCA “SET Co.”. They agreed on the format of the hierarchy, being a top-down hierarchy similar to that developed by the US Dept of Defence. Also, they agreed that they would trust the other to design their half of the system as they saw fit for their individual business.

What this system demonstrates is that it is possible for companies to develop an entirely PRIVATE RCA without any government or regulator involvement. But that may not work for all areas of commerce. What if you don’t want to start your own RCA? How do you identify an already existing RCA that you can trust? Sure you can check various websites, but once again, you are only reading what they want you to. This is where governments can assist.

A government has two options – it can designate a certification authority to be the government certification authority, that is the PUBLIC RCA. Otherwise it can assist in developing trust in various RCA’s by stating they are the designated PRIVATE RCA’s that are approved by government for business. In either case, such a designation would be, of course, a powerful marketing tool for any certification authority.

Web of Trust

Another example of self-development is the Web of Trust developed through the PGP PKI – PGP being the acronym for Pretty Good Privacy. In this system, each and every user can certify any other user’s public key as being correct by signing it. It is up to each individual user to check the veracity of the public key prior to certifying it.

Users must decide for themselves whether or not to trust the key they are being offered. This involves considering whether you trust –

(a) that you have a correct copy of the certifying user’s public key; and also

(b) that the certifying user has properly certified this user.

If you do not have sufficient ‘trust’, then you can decide either not to place commercial reliance on the new user’s key, or only trust it in certain circumstances (but you have to manage this control yourself). In this way, chains of trust are developed, without any specific body being an RCA.

Such a system is useful in non-structured dealings, such as e-mail communities that wish to protect privacy. But for commerce to develop, the risk of liability needs to be allocated through structured systems, involving strict standards of behavior. Recognizing this requirement, various PKI systems have been developed or encouraged by governments around the world.

Legal Frameworks

The UNCITRAL Model Law on Electronic Signatures

In September 2000, the United Nations Work Group on Electronic Commerce approved its Model Law on Electronic Signatures, along with the draft guide for enactment of that law. No specific mention of RCA’s is made within the Model Law. In the draft guide, the Working Committee acknowledged that entities such as RCA’s could exist, but states that the question of whether certification entities should be public or private was considered to be a matter of too great contention for determination.

However, what the Model Law does discuss is the need for some form of system to be put in place to assess the certification services provided, and also the need to identify the liability of certification authorities. This, of course, readily lends itself to the concept of the RCA.

The United States Experience

Many of the legislative provisions dealing with E-commerce within the different jurisdictions of the United States were enacted prior to the UNCITRAL Model Law. At the Federal level, the *Electronic Signatures in Global and National Commerce Act* was enacted on 24 January 2000. It deals specifically with the recognition of electronic signatures in any transaction involving interstate or international commerce only, and in no way addresses PKI systems. This has been left to the individual States. The legislative schemes adopted by States that have implemented PKI legislation vary from the comprehensive to the minimalist.

The comprehensive approach is to pass legislation that controls the entire PKI structure, apportioning liability, nominating the involvement of specified third parties, as well as giving legal effect to electronic signatures *within* the system. An example of this approach is the *Utah Digital Signature Act*.

Now codified as Title 46 Chapter 3 of the Utah Code, the Act when passed in 1995 contained 5 distinct parts. The second part of the legislation deals with the controls for the registration and licensing of certification authorities by an entity known as “the Division”. Under the legislation, this entity could be a certification authority itself. In fact, the commentary to the Act reveals it was envisaged it would be one. The Division was to have a limited role as a certification authority, certifying the keys of other certification authorities only. Therefore, it can be said that the Division is a PUBLIC RCA. The third part of the legislation outlines the duties of certification authorities and users.

The advantage of the comprehensive approach is that all users can immediately identify the apportionment of liability within the system, their rights and duties, and the PKI structure itself. However, the Utah Act can be criticized for placing unreasonable liability upon signature users, whilst failing to address specifically the duties upon signature users.

In contrast is the “minimalist approach” adopted by California. This approach merely gives effect to electronic signatures, and does not designate anything further. The signature must merely be unique, able to be proven as unaltered, and the signature user must also be able to prove control of that signature. Perhaps most significantly, these requirements are limited to communications with public entities only.

This approach certainly allows great freedom for development of PKI systems as well as the expansion of laws to include transactions not involving public entities. However, such legislation on its own fails to provide any assistance in building the sense of trust in PKI systems required by private enterprise. Also, it is left to the common law of contract to identify the apportionment of liability. An example of the possible adverse outcome is demonstrated by the disclaimers developed by a number of the private certification authorities that attempt to absolve them of all liability or restrict it to the bare minimum.

European Experience

In **Germany**, the *Federal Law to Regulate the Conditions for Information and Communications Services (Multimedia Law)* places duties expressly upon certification authorities with respect to information security. By doing this, all certification authorities are required to maintain a high level of technological development to ensure that the security it provides is at all times relevant. Where the legislation falls down is that it does not prescribe a standard by which the users or the authority can assess its liability.

In **Spain**, the enactment of the LORTAD has provided also provided a PKI system. Users can register their confidential files with the Data Protection Agency, outlining the security involved to protect the information. The agency can inspect the adequacy of this security and take action if it considers it is inadequate. The Agency is almost a PUBLIC RCA as it can certify the security applied to the information. However, no liability is attributed to the Agency for security breaches. Under the legislation, liability rests with the individual responsible for the files. Therefore, whilst you know where the liability lies, can you trust that you know who you are dealing with?

The **UK** has passed an Act that allows for self-regulation of CAs within a government approved scheme, the T-scheme. Both regulated and non-regulated CAs may be used in the UK, but their activities may be subject to other legislation such as the RIP Act (rightful interception) which gives the government powers to order the disclosure of confidential messages.

Finally, the **European Union** has passed the 'digital signature directive' introducing the qualified European signature and certificate that are currently being standardized by the European bodies of CEN and ETSI. The result of the Directive has been to cause member states to introduce national legislation to provide at least the requirements set by the Directive. Whilst members have, in the main, done this, the results are not entirely consistent, and this has potentially opened up the possibility of locating CA (and Registration Authorities – RAs) authorities where legislation is more convenient to the provider. The Directive allows for both regulated and non-regulated authorities to offer qualified European certificates.

The Current Australian Framework

The Gatekeeper

The Commonwealth government of Australia has reacted to the increase in e-commerce on a number of different levels, indicating an understanding of the many conflicting requirements of doing business on the Internet.

Firstly, the Commonwealth has recognized the legality of electronic signatures and electronic record keeping in the *Electronic Transactions Act 1999 (Cth)*. By providing force of law to the ability to complete transactions electronically, the Commonwealth commences building trust in PKI systems.

Secondly, the Commonwealth has involved itself in the systems as a user. This is the GATEKEEPER Strategy. An authority was established to develop an accreditation process for private certification authorities to use to gain accreditation as certification authorities accepted by the Commonwealth Government. The Commonwealth will only deal with PKI's involving those certification authorities. The process is based upon standards developed by Standards Australia, based in part upon work done internationally, in particular the International Telecommunications Union and the International Organization for Standardization standards designated X509.

As a result of this strategy, without the use of any legislative RCA, the government is assisting in development of the PKI system of Australia. *As an informed user*, the Commonwealth can ensure that the systems it deals with are secure. The companies who can prove this to the government can then trade off that fact, promoting growth of its own PKI system.

Commercial responses

Law and regulation have addressed the RCA, CA and RA facilitation of PKI. The laws have been framed in a variety of ways, some of them being technology neutral whilst others consider a firm regulatory framework binding PKI users to a specific technology implementation model.

So far we have considered how Australia and other nations have approached giving legal effect to the digital signature and creating assurance in the technical validity of those signatures for commerce and the public. However, two other areas remain to consider. Liability and commercial viability.

Liability remains a difficult question in the PKI model expected by much legislation. A CA or an RA may be expected to be liable for the adequacy of the work done to verify the actual identity of the person issued with a digital certificate, but it is not clear what value the recipient of the digital signature can put upon that. Some regulations include the concept of liability for the CA or the RA in the commercial value of transactions

From a practical perspective, the CA cannot 'know' what liabilities are being incurred through the use of the certificate because there is no mechanism through which the 'relying party' can check this with the CA and the CA acknowledge the specific liability. All a 'relying party' can do is see, anonymously, if the issued certificate is still valid (and that at the instant of the transaction, whereas revocation may have already happened but not yet published!) This creates practical problems for the CA because it is difficult to insure unknown amounts of risk. This problem threatens the PKI concept of placing liability with the CA, and calls into question the value of 'third party' opinions as axioms of trust, and therefore of the ability to trade with people you do not know. (As a matter of technical fact it is impossible to have an encrypted communication with someone you do not know because you must have their public privacy key first.)

Commercial viability is a different problem. The prospectus of the CA software providers claims that the certificate is a thing of great value and must command a high price. The public user already has 'identity tokens' called credit cards, and knows that they are free because the provider wants them to do business. There is therefore a mismatch of expectations which is exacerbated when the user cannot find any business applications to use with his PKI certificate (a lack of utility).

Specific law may address some of these issues through measures such as strict liability, but it is difficult to believe that such an approach will be successful on a global basis, particularly where existing law tends to become entrenched before global agreements are reached.

Conclusion

In essence, the Australian legislation and GATEKEEPER Strategy is a well-rounded response to some of the problems of e-commerce. When compared to the systems in place internationally, it can be seen that Australia is taking perhaps a more internally coordinated approach than other nations. Whilst it may be easy to say that this is what is required across the globe, of course the reality is not as easy. Australia, in following the minimalist legislative approach, may lead the way in the administrative approach through the Strategy. But there are obviously at least three other systems, evidenced in Utah, Germany and Spain, that may also in the end prove of benefit. Legislation, whether using a 'light touch' or more direct regulation, cannot reverse the commercial fundamentals, and it remains to be seen if the current approach to implementing PKI will succeed or if the pressure of commerce will produce new approaches.

Accordingly, at this time, counsel advising on whether any particular form of identification process can be trusted need to take into account the importance of the transaction as against the cost of certifying identity. Regard should also be had to the location of any proffered certifying authority so as an assessment of the apportionment of liability can be made. And finally, in matters where repeated transactions are to be entered into, selection of a preferred RCA will prove essential.

This article has previously been published in:

Trust Me: Public Key Infrastructure (part 1)" (2002) 11 E-Law Practice 48

Trust Me: Public Key Infrastructure (part 2)" (2002) 12 E-Law Practice 48

and

World Information Technology Contacts Handbook 2002 under the title "Australia Shows the Way on PKI Certification" by Euromoney PLC