Lockstep White Paper No. 2

Lockstep Consulting Pty Ltd
ABN 59 593 754 482
Contact: swilson@lockstep.com.au

Relationship Certificates

A modified form of "identity" certificate for conveying credentials

Stephen Wilson
V 1.3 August 2005

Introduction

This paper outlines a new type of "identity" digital certificate, intended for use only within a defined community of interest. By restricting certificate usage to an established context, under existing business rules and liability arrangements, all problems of cross-recognition and minimum levels of identity proofing disappear. The total cost of ownership is reduced, and many auxiliary complexities also disappear, especially in software design. Registration is streamlined, and certificate uptake can be expected to be radically improved.

Acknowledgements

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.

Objectives

The fundamental objective of PKI should be to help automate online transactions between parties, equivalent to traditional paper-based transactions. The hallmark of a good PKI application is that the *signature* of one or both parties is required. Practical experience tells us that PKI works best in 'closed' user groups [1].

Traditional PKI focuses on proof of identity. Everyone knows that traditional PKI suffers from many problems, including high legal complexity, expensive and/or inconvenient registration processes, and low take up rates. PKI has therefore come to be seen as risky by many e-business projects. Many organisations which would otherwise like to use PKI have dropped it from their plans, for fear it will jeopardise their e-business rollouts. Yet with the benefit of hindsight, we can see that most of the problems with traditional PKI derive directly from the attempt to provide general purpose proof of identity.

The objective of the new Relationship Certificate is to streamline the registration of certain types of users of certain types of applications. Registration should be quicker and smoother in a number of ways, including not having to present in person to register, and not having to visit and create a new relationship with any third party bureau.

What would a "Relationship Certificate" stand for?

Traditional digital certificates stand for the personal identity of their holders, and are intended to be used in a wide range of non-descript applications (most Certificate Policies are deliberately vague on intended application, in order not to limit applicability). An "identity certificate" is issued after an RA performs identity proofing on the Subject, and therefore represents an affirmation by the RA that the Subject has met certain conditions. A Relationship Certificate would simply involve a different type of affirmation, namely that the Subject has a particular type of relationship with the RA. The Relationship Certificate would expressly instantiate the Subject's rights or entitlements to participate in certain transactions sanctioned by the relationship. A Relationship Certificate would lose its meaning outside the context of the relationship.[1]

Examples of formal relationships

In Australian e-government applications, we commonly find that certain Agencies and their customers have formal relationships which confer special credentials on users, meaningful in a restricted context. In most if not all cases, such Agencies are authoritative over their respective domains. Such Agencies will only deal with Customers who already have a formal relationship with them; no other relationship or credential will have standing with the Agency. Likewise, many professional qualifications are directly conferred by the fact of membership of certain chartered bodies, in accounting, medicine, engineering the law and so on.

Examples of relationships which constitute formal credentials include:

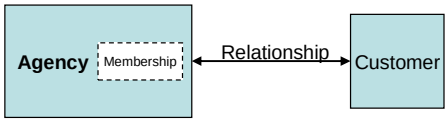
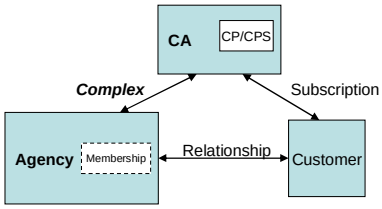
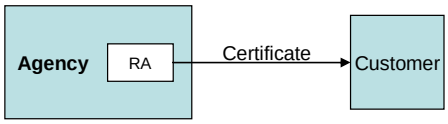
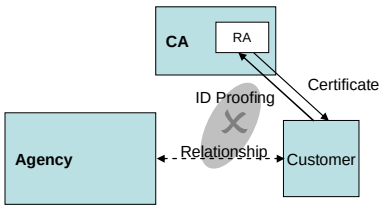
Agency[2]	**Customers credentialed**
Australian Securities and Investments Commission	Company Directors
Health Insurance Commission*	Medicare service providers
Australian Customs Service*	Customs Brokers
State traffic authorities	Licensed transport operators
State legal admissions boards	Lawyers, Conveyancers
NSW Department of Fair Trading*	Real estate agents
IP Australia	Patent Attorneys

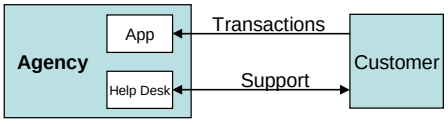
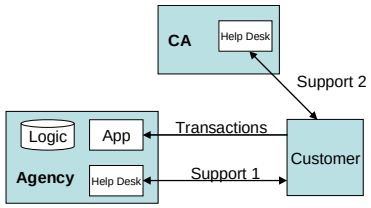
[1] In the real world, all credentials have context, and the appropriate credential depends on the transaction at hand. For example, if a doctor were pulled over by a traffic cop and is asked to present her drivers licence, she should get nowhere trying to present her medical qualifications.

[2] Agencies marked with an asterisk have already tried PKI, with mixed success.

Comparing Relationship and Identity Certificates

The following table compares Relationship and traditional, third party-issued Identity Certificates, with regard to how they express trust relationships, how the PKI elements are implemented, and how they support transactions.

	Relationship Certificates	Third Party Identity Certificates
Trust	 An Agency has an established relationship with its Customer. There might be a formal membership function which manages and maintains the relationship. In some cases, the relationship is formalised to the extent that it becomes a *licence*.	 The Customer is required to obtain their Identity Certificate from a third party CA. A new legal relationship is entered into, shaped by the CP and CPS, not the prior relationship with the Agency. Legal analyses usually hold that the Agency and CA have no relationship but that is an oversimplification. In reality, Agencies negotiate long and hard with one or more CAs, advocating on behalf of their Customers.
PKI	 The Agency operates its own RA and issues a certificate directly to the Customer. An outsourced CA (not shown here) simply 'mints' a certificate according to an agreed customised X.509 profile with a Policy OID which uniquely indicates the relationship.	 The Customer submits to identity proofing, which has nothing at all to do with the Agency's existing knowledge of the customer. That is, id proofing is blind to any existing relationship. Usually in-person presentation is required at the third party RA, before the Customer can transact online with the Agency, even if it already knows her.

	Relationship Certificates	Third Party Identity Certificates
Transactions		
	A Relationship Certificate presented to a matched application can be processed straight-through, with no additional business logic (save for the revocation check).	Transacting on the basis of a Third Party Identity Certificate requires additional business logic in the Agency Application to determine the Customer's rights and entitlements. Two Help Desks are required, one for the application and one for the certificates.

Automatic Registration

Relationship Certificates can be issued to Known Customers with little or no additional evidence of identity (EOI) needing to be presented.[3] If a recognised credentialing authority has established relationships with its members, according to formal rules, and desires to transact with those members online under the same terms and conditions as it does on paper, then it should be free to push out Relationship Certificates, performing automatic registration with information already held on its member database.

For new members of the authority's community of interest, where the relationship has only just been established, a Relationship Certificate could be generated essentially as a side effect of the process of bringing the new member onboard.

The multiple certificate trade-off

The reduced registration overhead and simplified operation of Relationship Certificates represent a trade-off against reduced applicability. That is, Relationship Certificates should be restricted to certain families of applications; subjects would be expected to have multiple certificates if they participate in different families of PKI transaction. However, with radically improved registration and ease of use, there is no reason to believe that users will find multiple certificates any harder to use than they do multiple *applications*.[4] If the cost of issuing Relationship Certificates is in fact greatly reduced,

[3] Note that the *activation* of an automatically registered Relationship Certificate might call for the Customer to answer some identification challenge, in order to control the risk of the Certificate falling into the wrong hands.

[4] For example, a typical doctor will run medical software with which they might transact with the Department of Health and other providers, and separate accounting software to send tax returns

then we will find that the total cost of managing a number of them is lower than the cost of managing a single, general purpose, high grade identity certificate.

Historically, a great deal of effort has gone into finding ways of re-using existing certificates, just to avoid having to issue extra ones. But perhaps the perceived value of existing certificates is as high as it is purely because they are artificially so difficult to obtain! If certificates were easier to get (and easier to use) we should be less concerned about needing more than one of them.

Disadvantages of separating Identity and credentials

It has become something of an orthodoxy in e-security for "authentication" and "authorisation" to be treated separately. In PKI, a widespread and corresponding view is that in order to assert special credentials, one should carry a general purpose identity certificate and supplement it with extra information (classically, an *Attribute Certificate*) specific to the credential concerned. When a digital signature is required to be produced, in this vein it tends to be thought that the general purpose identity certificate should be used. When that digital signature is intended to capture the person's credentials, then the supplementary credential information must somehow be incorporated with the signature or the signed data. This approach brings several practical disadvantages, making it even more complex than traditional PKI, and therefore it is even less likely to succeed where PKI has failed. The problems include:

- Significant user complexity, because this approach requires professionally credentialed people to go to the trouble and cost of obtaining a special identity certificate to supplement their online credential (in contrast to their bricks-and-mortar experience which is generally that their credential alone supports most if not all their workaday transactions).
- More complex software design for both signing and verifying, to include the necessary credential data from the supplementary source.
- A lack of agreed standards to date that would govern exactly how credential data should be incorporated into the digital signature process (as opposed to 'straight' digital signatures which are well standardised).
- Where the supplementary information comes from an Attribute Certificate, the Relying Party software must parse not one but two separate certificate chains back to their respective roots, in order to validate the identity as well as the credential.

---

and statutory reports to other government agencies. It is unlikely that any doctor would find it difficult or confusing to use the two applications in their respective contexts (and moreover, well designed PKI-enabled software will invoke the appropriate certificate seamlessly). There is no call for all B2G services to be converged onto one super application, and so there is no compelling need for multiple communities of interest to use the one certificate.

- Where the supplementary information comes from a database, then Relying Party software may have to be permanently online in order to retrieve credential information; furthermore, re-validation of a signed transaction at some future time will require long term archiving of credential databases.
- It becomes necessary for the general purpose identity certificate, including the identity proofing procedure, to be designed to be sufficiently robust to support all anticipated applications, now and in the future.
- There is great legal complexity in working out how to apportion liability in the event that a fraudulent identity certificate is involved with a credential-related wrongdoing or misadventure.
- It complicates the business processes of professional bodies which today do not have to consider the quality and veracity of any separate identity certificate, nor form new relationships with the issuers of such certificates.

Finally therefore, all the advantage of a "known customer" issuance model is effectively lost when the credential cannot be used without also having the general purpose identity certificate.

Thinking differently about "identity"

The supposed advantage of separating "authentication" and "authorisation" has to do with architectural purity. While purity is important for ensuring robust, future-proof software designs, in this case, it is premised on a particular restrictive view of "identity"; *viz* that each of us has a unique immutable biological identity and a constellation of changeable roles. There is truth to this perspective of course, but an equally valid view is that we each have a set of changeable *context-dependent virtual identities*, separate from our biological self.[5]

This is not merely a semantic or philosophical point. A simple example demonstrates that we actually conduct ourselves as if we have multiple virtual identities, especially in business, and that we seamlessly switch between them. Furthermore, when we exercise a context-dependent identity, we beneficially mask our biological one. Consider Alice, the company secretary of Acme Inc. Acme's bank is Bank-Won. Alice is a signatory to the Acme corporate bank account and has custody of a Bank-Won key card for the purpose. Alice might also hold a personal account with Bank-Won. When she banks on behalf of Acme, she exercises a different identity compared with when she banks on her

[5] Dr Stephen Kent, joint chairperson of the authoritative IETF PKIX standards committee, and author of the US government report *Authentication Through the Lens of Privacy* [2], recently offered similar observations about identity: "For many big CAs, there is an assumption that a single certificate is all a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience. For personal privacy and security, multiple independent certificates per user are preferable." [3].

own behalf, even if she is in the same branch or at the same ATM. For obvious reasons, nobody would ever wish to merge these two identities into one.

The proposed Relationship Certificate readily supports these sorts of virtual identities, by recognising that most such identities derive from trusted relationships between credentialing authorities and their members.

The Relationship Certificate profile

Relationship Certificates would have information in their X.509 profile to specify the relationship, allowing straight-through processing by any Relying Party software application configured to recognise the validity of the relationship. The best way to codify the meaning of a Relationship Certificate is in the Policy OID. In some cases, where an issuing authority runs a real or virtual CA, it may be possible for the Certificate Issuer name to convey further meaning.

Ideally, technical controls should be implemented as well to make it difficult to misuse a Relationship Certificate outside its intended context. One way to implement technical restrictions on misuse would be to include a Critical extension in the profile. Recall that the X.509 standard requires any software processing a certificate which has an extension marked as Critical to reject that certificate unless it expressly recognises the extension. Since special purpose software (as opposed to general purpose web and e-mail clients) is usually used in PKI-enabled transaction systems, within communities of interest, programming in awareness of Critical extensions is easy. And by the same token, it is safe to assume that if a given software program does not recognise the Critical extension, then it is proper behaviour to reject the certificate, on the grounds that such certificates are not supposed to be used outside special purpose applications. Critical extensions proved unpopular in the past because they were thought to harm interoperability. But if a special purpose Relationship Certificate is only intended to work with certain applications, then "interoperability" is moot.

Benefits of Relationship Certificates

As is apparent from the comparison table above, Relationship Certificates will bring major simplifications over third party identity certificates in several areas:

- Reduced overhead to register for certificates; Known Customers are able to receive certificates from credentialing authorities with whom they have a relationship, without having to present in person at an unfamiliar RA.
- Certificate holders probably require no legal relationship with the backend CA; any necessary elements of the traditional Subscriber Agreement can be subsumed into the credentialing authority's formal contractual relationship with its members.

— Reduced support overheads and complexities by having one Help Desk for all business, application and certificate-related matters.

Users will no longer be required to pay up-front for a certificate from a third party CA in order to use PKI-enabled applications.[6] Furthermore, the cost (to the community of interest) of each certificate should fall towards "wholesale" levels, because the cost of identity proofing associated with traditional identity certificates will be eliminated.

The total cost of PKI enabling online services traditionally involves a range of investigations and negotiations which result directly from how accredited CAs do *their* business. With Relationship Certificates, communities of interest will enjoy additional efficiencies as follows:

— No need to spend time investigating the CP and CPS of candidate CAs and evaluating how CAs' processes fit with the community's business needs.

— No need to spend time advocating and negotiating with CAs on behalf of a community's Customers.[7]

— With improved take-up of certificates, organisations will enjoy more rapid rollout of their PKI-enabled services, and reduced cost of coping with non-compliant Customers who are slow to register or renew.

References

[1]. *Position Statement on PKI of the Australian Security Industry*, Stephen Wilson, Australian IT Security Forum (AITSF) V3.0, November 2003 http://www.aitsf.aeema.asn.au/ArticleDocuments/175/pki.

[2]. *Who Goes There? Authentication Through the Lens of Privacy* Stephen Kent and Lynette Millett, editors, Committee on Authentication Technologies and Their Privacy Implications, US National Research Council of the National Academies, National Academies Press, 2003.

[3]. *Global PKI: Status, Trends and the Future* Dr. Stephen Kent, co-chair IETF PKIX Working Group, Taipei International PKI Conference, September 2005 http://www.pki.org.tw/pkiforum2005/d_file/01_Stephen%20Kent.pdf.

[6] Many users have found it objectionable that they might have to be out of pocket to a third party CA in order to be able to transact online with an Agency they have long dealt with off-line.

[7] In the Australian Federal Government sector, Agencies commonly also negotiate with the Gatekeeper® accreditation programme to allow PKI processes to be tailored to the Agency's business needs. These negotiations too would be saved with Relationship Certificates, since Project Gatekeeper® would no longer impose its external Evidence of Identity rules on Agencies which have established arrangements with their own Known Customers.