

Leveraging external accreditation to achieve PKI cross-recognition

Stephen Wilson, Director Policy & Strategy
PricewaterhouseCoopers beTRUSTed

July 2001

Abstract

This paper proposes a light touch, standards based framework for leveraging the accreditation of Certification Authorities under external Public Key Infrastructures, to allow such external CAs to be used within local communities of interest.

The proposed framework is a response to the current situation where certificate users (both Relying Parties and would-be Subscribers) are increasingly faced with the option of using existing CAs, which typically operate outside the users' immediate community of interest. All things being equal, users wish to avoid the cost and lead time of establishing local CA solutions from scratch, and they therefore require reliable information about the appropriateness of available external PKIs. The framework places the responsibility for that information in the hands of the local community of interest, and allows it to make maximum use of existing accreditation of CAs under external PKI schemes. The proposal preserves the autonomy of local community to set its own business rules and minimum standards.

Background and context

Multiple PKI schemes have been established to date, many involving formal accreditation of Certification Authorities (CAs). The trend is towards schemes dedicated to particular vertical market segments, especially finance, government and healthcare. We can expect many more PKI schemes to follow, in new verticals, and in other countries and communities of interest.

Now, with transactions crossing between jurisdictions or communities of interest, users are faced with the question of how to decide whether or not to accept a transaction signed using an "external" certificate. This is the fundamental issue in electronic authentication. The APEC E-Security Task Group defines authentication as *the means by which the recipient of a transaction or message can make an assessment as to whether to accept or reject that transaction.*¹

Users in a community of interest require information and guidance from their community leaders about the fitness for purpose of whichever external certificates can be expected to be received with incoming transactions. With a range of CAs issuing certificates for different uses, it is essential that a Relying Party can tell if an incoming certificate is acceptable for the transaction concerned; ideally

¹ See APEC E-Security Task Group home page www.apii.or.kr/apec/atwg/preatg.html.

their software application should be able to decide on-line and automatically whether to accept or reject a given certificate.

If a CA has been accredited under an external PKI scheme, then the issue boils down to whether or not that accreditation is acceptable to the local community of interest for the intended use of the certificates. This is perhaps the simplest statement of the problem of “cross-recognition” of PKIs.

It should be in most parties’ interests to promote the cross-recognition of external PKIs. Cross-recognising external PKIs and thereby approving the use of their CAs’ certificates within a local community of interest brings the following benefits:

- local users have greater connectivity with external parties
- local users have a wider choice of certificates for authenticating transactions
- external parties’ costs are lowered by avoiding additional local accreditations
- local community costs are lowered by avoiding the construction and maintenance of new accreditation schemes.

Cross-recognition principles

Cross-recognition is a state where a defined community of users is able to rely upon certificates issued under an external PKI for use in certain applications. The certificate Subscribers may be outside the community, seeking to transact with members of the community (Figure 1), or else they may in fact be inside the community but for various reasons prefer to use the services of a CA accredited under an externally operated PKI (Figure 2).²

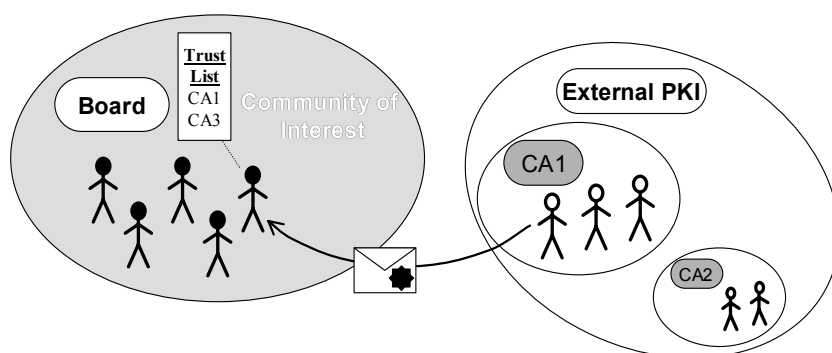


Figure 1: External CA under an external PKI

² This approximates the situation with the “Angus” agreement between the four major Australian banks and the Australian Commonwealth Government. Local users will get their certificates from banks operating under the international Identrus scheme rules, and according to the agreement expect to have their certificates accepted for transacting with Australian government (i.e. non-banking) entities. See www.govonline.gov.au/projects/publickey/abn-dsc-angus.htm.

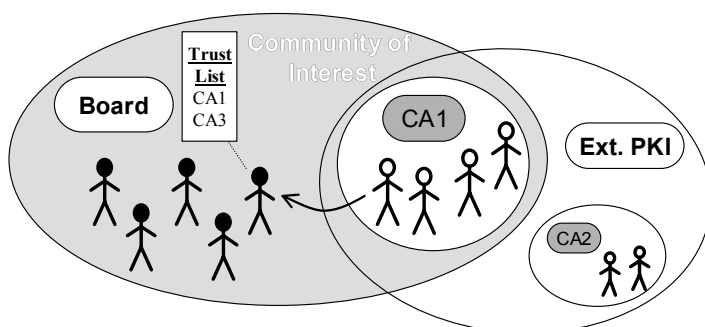


Figure 2: Local CA under an external PKI

The APEC E-Security Task Group defines *cross-recognition* as

*An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa.*³

Note that two-way cross-recognition is not in fact intrinsic to the process, despite the “vice-versa” clause of the APEC definition. For the sake of generality and technology neutrality, we should not assume that Relying Parties in the local community even have their own CA (that is, you should be able to process someone else’s certificate without necessarily belonging to a CA yourself). To achieve the aim of leveraging existing external accreditations for CAs, we shall concentrate on one-way cross-recognition, where local users are able to rely upon certificates issued under other PKI schemes.

The terms “PKI scheme” and “accreditation programme” are used broadly in this paper. Both are taken to mean any formal system that confers approval upon a CA. Examples of such programmes include Identrus, WebTrust for CAs, Project Gatekeeper, and potentially tScheme (the UK voluntary accreditation programme being set up in accordance with the European Directive on electronic signatures).

Trust Lists

It is obviously important that the state of cross-recognition be visible to Relying Party applications online, so that the decision to accept or reject individual transactions may be automated. One way to make cross-recognition visible is the so-called *Trust List* model, currently being examined by the APEC E-Security Task Group. A Trust List is a data structure created and issued by an appropriate authority, containing the root public keys of all CAs that are recognised at the time. The List is integrated with the Relying Party application software; ideally it should be digitally signed by the authority that issued it.

³ See *Achieving PKI Interoperability* at www.apectelwg.org/apecdata/telwg/eaTG/eatf06.html.

The Trust List concept is an extension of the Root CA store that features in most web browsers. The browser's Root CA store suffers from having no formal management process for constructing and maintaining the list, and from not being tamper resistant. A Trust List on the other hand would be formally managed, with transparent auditable procedures for adding (and removing) CAs, and would be tamper resistant, by being digitally signed.

This form of Trust List however is not yet supported by native browser software, but it can be contrived by overlaying manual administration procedures. Such procedures would cover firstly configuring and updating the Root CA store in the browser of each user in the community, and secondly periodically checking the expected hash values (or "fingerprints") of the CA public keys in the store.

A further enhancement to the Trust List model would be for the lists to contain the accepted Policy identifiers as well as the accepted CAs' root public keys. This would allow finer grain definition of the classes of certificates from each CA that are approved for use in the local community of interest.

Scoping cross-recognition and accreditation

Note carefully that cross-recognition should operate between the local community management and external PKI schemes, rather than individual external CAs. Cross-recognition should be founded on approval of the management processes of the external PKI, so that any CA's demonstrated compliance with those processes means that certificates issued by that CA can be accepted locally more or less automatically.

Now, as discussed above, an external CA might issue certificates to external users who then present them to local Relying Parties (Figure 1). Or an external CA might issue certificates to *local* users for use within the local community (Figure 2). For local users to merely rely upon externally issued certificates to authenticate incoming transactions, it should only be necessary for the community of interest to cross-recognise the external PKI. If however local users wish to obtain their own certificates from an external CA, then further conditions may have to be applied, over and above the cross-recognition of the CA's PKI scheme. In particular, the local community may wish to lay down its own business rules in the interests of its members. For example, the community may require that an external CA have a local office and a local support infrastructure, and/or that it demonstrates commercial stability and long-term commitment to the PKI business.

Therefore, cross-recognising an external scheme and accrediting where applicable an individual CA from within that scheme should be separate, sequential steps. Accreditation for local use of all CAs in an external scheme should not flow automatically from cross-recognition of that scheme.

Fitness for purpose

Digital certificates are increasingly becoming application specific. PKI schemes in vertical industry sectors are refining the business rules for registering users and for managing CAs, in line with the conventions and existing standards of those sectors.

For example, in Identrus, registration rules are fine-tuned by member banks in accordance with their local financial “know your customer” regulations. And the Australian Government’s ABN-DSC standard permits businesses already enrolled in the programme to nominate additional employees to receive certificates representing the business, without those employees needing to register face-to-face with the CA.

Such refinement of a PKI’s business rules means that the certificates issued under the PKI are specific to applications in that business. CAs will generally seek to restrict the use of their certificates to certain classes of defined applications. And Relying Parties should only accept transactions that are authenticated with certificates acceptable to their community of interest.

Fitness for purpose is therefore a central and critical concept in cross-recognition. The local community can be expected to lay down rules for accepting external CAs for specific types of application conducted by the community. To do this, the community has to understand the fundamentals of their applications and characterise precisely what it is about users that matters in allowing them to sign transactions in those applications.

Now, this understanding of their own applications should of course come naturally and preferentially to the communities of interest. For instance, healthcare organisations have the best understanding of what medical credentials are required for particular transactions in their community. Moreover, they are in the best position to adjudicate the suitability of external medical credentials and of external authorities conferring those credentials. Indeed, most national healthcare authorities have already established formal protocols for approving foreign professionals, and these protocols should be at the heart of any cross-recognition of healthcare PKI.

An intrinsic part of the proposed cross-recognition framework therefore is the careful characterisation and delineation of the applications of interest, and the scoping of applicable external PKIs accordingly.

Responsibilities of the local Management Board

Cross-recognition requires a policy and management function to act on behalf of the local community of users. A local Management Board will have the following responsibilities:

- Understand, characterise and define the types of PKI-enabled application in use by the local community.

- Control the Trust List for all users in the community, updating and distributing the List as required.
- Map available external PKI schemes onto the local application types of interest, specifying which types of external accreditation are deemed relevant for which applications.
- Define a set of minimal CA control objectives to apply to all cross-recognised CAs.
- If desired to accredit external CAs to issue certificates locally, define local business rules that may be mandated over and above any external accreditation. These rules would mirror local legal and regulatory requirements, as applicable.
- Formally cross-recognise external PKI schemes, through a review protocol based on the minimal CA control objectives.
- For individual candidate CAs seeking local accreditation, review their external accreditation status (and potentially also their individual audit reports, and assess their compliance with the community's local business rules.

A number of other management responsibilities will also apply to the Board, in connection with the maintenance of each CA's accreditation, and dispute resolution.

The framework in detail

There are three separate elements of the proposed framework:

- 1 **Cross-recognition of external PKI schemes**, representing the community's decision that certain schemes are expected to produce certificates fit for purpose for prescribed types of application
- 2 **Execution of each external PKI scheme**, involving external auditors and management bodies, working under scheme rules that are fully transparent to the local community of interest
- 3 **Formal conferring of local accreditation** of external CAs, subject to additional local business conditions, to issue certificates locally.

These elements are considered in more detail below.

Cross-recognition of external PKI schemes

Cross-recognition begins with a minimal set of CA control objectives acceptable to the community of interest. These would be defined and maintained by the Management Board. An illustrative, high level set of CA controls is provided in an Appendix to this paper.

We can expect that any acceptable external PKI will have set down its own scheme rules, incorporating relevant PKI standards, and either directly or indirectly specifying its own set of minimal CA control objectives. Most if not all current PKI schemes include a set of mandated controls and standards.

Moreover, PKI schemes include formal mechanisms for ensuring that the controls are properly implemented by each CA. These mechanisms include auditors working to defined standards, plus the means for selecting acceptable auditors. Typically a PKI scheme looks to existing audit standards (such as SAS 70, WebTrust for CAs and ISO 17799) and professional bodies (such as ISACA, and national auditor associations) for providing an available pool of competent auditors.

To achieve cross-recognition requires the Management Board to review the external PKI scheme's rules, and to determine if the following two conditions hold true:

- 1 the external PKI's minimal control objectives correspond to those of the local community, and
- 2 fit and proper mechanisms are applied to enforce the external scheme's controls, including the type of auditors used and the process for selecting those auditors.

Execution of each external PKI scheme

Any external PKI scheme will in general be executed as follows (see Figure 3):

- 1 The external PKI sets its own Scheme Rules, incorporating relevant PKI standards, and appoints one or more Auditors.
- 2 An appointed Auditor audits the CA, with reference to the Scheme Rules, and writes a Report.
- 3 The External Scheme considers the Report, and if satisfied that all necessary conditions are met, accredits the CA.

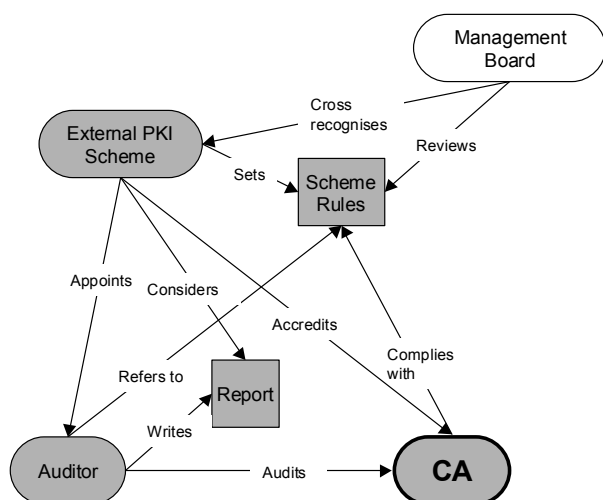


Figure 3: General execution of external PKI

Formal conferring of accreditation

The final stage of formal accreditation of a candidate CA by the local Management Board would consist of the following steps (see Figure 4):

- The Board considers the accreditation status of the candidate CA under a cross-recognised external PKI. At its discretion, the Board could also refer to the original auditor reports of the CA, should the Board feel that this would add to its understanding of the CA's status.
- If the CA is to be accredited to issue certificates locally, then the Board assesses the CA's compliance with the Board's prescribed local business rules.
- Once satisfied by all material at its disposal, the Board confers accreditation upon the CA and adds the CA to the Trust List.

If at any stage the Board was to find itself not satisfied by its findings, it would reserve the right to variously seek clarification from the CA, seek corrective action with re-audit, or to reject a CA's application for local accreditation.

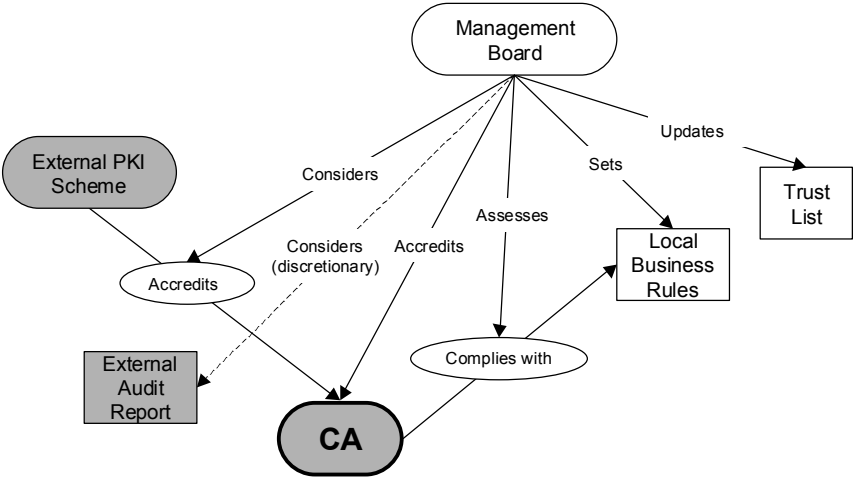


Figure 4: Conferring local accreditation

Accreditation would be expected to be qualified in most if not all cases, with the Management Board specifying which types of application the accreditation applies to. Ideally, the Trust List should be able to specify the Policy Object Identifiers (OIDs) for which the accreditation applies.

Appendix: Illustrative minimal CA control objectives

This appendix provides an illustrative set of minimal control objectives for a Certification Authority. A list similar to this would be developed by the local community of interest's Management Board to form the basis of its cross-recognition of external PKIs.

Typical CA cryptographic management control objectives	
CA Key Generation	– CA keys are generated in accordance with industry standards.
CA Key Storage, Backup and Recovery	– CA private keys remain confidential and maintain their integrity.
CA Public Key Distribution	– integrity and authenticity of the CA public key is maintained during distribution.
CA Key Usage	– CA keys are used only for their intended functions in their intended locations.
CA Key Destruction	– CA private keys are completely destroyed at the end of the key pair life cycle.
CA Key Archive	– archived CA keys remain confidential and are never put back into production.
CA Cryptographic Hardware Life Cycle Management	– CA cryptographic hardware is not tampered with during shipment and storage; – access to CA cryptographic hardware requires dual access control – CA cryptographic hardware is functioning correctly.
Typical subscriber key & certificate lifecycle control objectives	
Subscriber Registration	– subscribers are properly identified in accordance with the CP/CPS; – subscriber certificate requests are accurate, authorised, and complete.
Certificate Renewal	– certificate renewal requests are accurate, authorised, and complete.
Certificate Issuance	– new, renewed and re-keyed certificates are generated and issued in accordance with the CP/CPS.
Certificate Distribution	– upon issuance, complete and accurate certificates are available to subscribers and relying parties.
Certificate Revocation	– certificates are revoked based on authorised and validated certificate revocation requests.
Certificate Revocation List Processing	– complete and accurate Certificate Revocation Lists are generated and issued on a timely basis, in accordance with the CP/CPS.
Smartcard Life Cycle Management	– smartcard preparation is securely controlled by or on behalf of the CA; – smartcard usage is enabled by the CA prior to smartcard issuance; – smartcards are securely stored and distributed by or on behalf of the CA.
Typical environmental control objectives	
CPS/CP Management	– CP/CPS revision management controls are documented and effective.
Security Management	– management direction and support for information security is provided; – information security is properly managed within the organisation; – the security of facilities, systems, and information assets accessed by third parties is maintained.
Asset Classification and Management	– the security of information is maintained when responsibility for particular CA functions is delegated to another entity.
Personnel Security	– personnel in Trusted Roles receive appropriate training; – all security personnel have clear and accurate understanding of their roles and responsibilities; – personnel exit procedures ensure the integrity and confidentiality of all information assets.
Physical and Environmental Security	– physical access to CA facilities is limited to properly authorised individuals; – facilities are protected from environmental hazards; – potential loss, damage, or compromise of assets are minimised.
Operations Management	– compromise or theft of information and information processing facilities are prevented; – the correct and secure operation of CA information processing is ensured; – the risk of CA systems failure is minimised; – the integrity of CA systems and information is protected against malicious code; – damage from security incidents and malfunctions is minimised through the use of incident reporting and response procedures; – media are secured to protect from damage, theft, and unauthorised access.
System Access Management	– CA system access is limited to properly authorised individuals.

Typical CA cryptographic management control objectives	
Systems Development and Maintenance	<ul style="list-style-type: none"> – CA systems development and maintenance activities are properly authorised to maintain CA system integrity.
Business Continuity Management	<ul style="list-style-type: none"> – the CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster; – CA maintains controls to provide reasonable assurance of continuity of operations in the event of the compromise of the CA private key; – potential disruptions to subscribers and relying parties will be minimised in the event of cessation of CA services.
Monitoring and Compliance	<ul style="list-style-type: none"> – the CA complies with legal requirements; – compliance with the CA's security policies and procedures is ensured; – the effectiveness of the system audit process is maximised; – interference to and from the system audit process is minimised; – unauthorised CA system usage is detected.
Event Journaling	<ul style="list-style-type: none"> – significant CA environmental, key management, and certificate management events are accurately and completely logged; – the integrity of current event journals is maintained; – the integrity of archived event journals is maintained; – event journals are completely and confidentially archived; – event journals are reviewed periodically by authorised personnel.