PKI Interoperability Models (February 2005)

Chris Connolly, Peter van Dijk, Francis Vierboom and Stephen Wilson, Galexia

Email: consult@galexia.com **Web:** www.galexia.com **Ph:** +612 9660 1111 **Fax:** +612 9660 7611
Post: Suite 95 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

Contents

Document Control

Version

1.0

Date

3 February 2005

Source

The latest version of this article is available from http://www.galexia.com/public/research/articles/research_articles-art32.html

Copyright

1. Introduction

PKI is still considered the problem teenager of e-commerce. Its applications have been limited to small closed groups, defying the often unreasonable hype suggesting promising that PKI will revolutionise all forms of electronic transactions. But with patience, the demand will grow for more and more PKI systems to interoperate. The full potential of electronic signatures may only be realised if the large organisations that issue digital certificates, Certification Authorities (CAs), are interoperable.

PKI interoperability models are now the subject of discussion, research and pilot testing in international and regional forums. This article explains and assesses the leading PKI interoperability models that have emerged and the early attempts being made around the world to use them.

2. Defining PKI interoperability

In the classical PKI scenario, someone receives a document signed with a digital certificate. The recipient must trust the creator of that certificate (the Certification Authority (CA)) to be able to confirm the identity of the sender. This is simple if the sender and recipient are using the same CA. The need for interoperability arises where the document has been signed with a certificate from a CA that the recipient does not know.

The obvious approach is to centralise as much trust as possible and avoid this problem entirely. This is reflected in the root CA and hierarchy PKI models discussed below. However, those models require tight central control and unanimous support. More flexible solutions are also considered in this article – such as cross-certification meshes, cross-recognition, bridge CAs and certificate trust lists.

PKI interoperability is often described as a “multi-layered” issue, with both technical and management aspects. For PKI sub-systems and applications to work together, all software interfaces must conform to technical standards and complex, up-to-date information about the fitness for purpose, quality and status of digital certificates is required.

A good way to explain PKI interoperability requirements is to examine PKI interoperability from the relying party’s perspective.

The APEC eSecurity Task Group defines authentication as:

The means by which the recipient [Relying Party] of a transaction or message can make an assessment as to whether to accept or reject that transaction.[1]

In the case of digital certificates, from the perspective of the relying party, there are several pieces of information required for them to be able to authenticate an incoming certificate:

[1] Asia Pacific Economic Cooperation, Telecommunications Working Group, Business Facilitation Steering Group, Public Key Authentication Task Group Preliminary Report, September 1997 <http://www.apectelwg.org/apecdata/telwg/eaTG/eaTG-1.html>.

Requirement	Test	Solution
Fit for purpose.	The receiver must be able to tell if the Certificate is fit for purpose That is, was the certificate issued under circumstances that allow it to support the transaction? And did the issuer intend for the certificate to be used in this way?	In general, this information must be considered at the time the receiver's application is designed. Where the PKI is either closed or limited to a certain community, only particular CAs and certificate types are involved, allowing designers to "hard wire" their software to expect certificates bearing certain identifiers.[2] In open PKIs, the software must be designed with appropriate business logic in order to process certificates and extract the necessary authority information, either from the certificates directly, or from other sources such as directories.
Certificate validity	The receiver must be able to tell if the Certificate Subject is currently valid	Typically the certificate will be checked against a Certificate Revocation List (CRL) or validated using an Online Certificate Status Protocol (OCSP) inquiry. This will ensure the certificate is currently valid, before accepting the incoming message.
Certification Authority (CA) validity	The receiver must be able to tell if the Certificate Issuer (usually a CA) is valid.	Certificate path validation will usually trace all certificates in the chain back to a recognised Trust Anchor, checking the issuer's own certificate along the way

To meet all three of these requirements, and to achieve PKI interoperability two interoperability processes are required:

1. A political or contractual process for establishing recognition
This is used to establish that a given CA meets certain technical and management interoperability requirements. This is typically achieved through the cross-certification or cross-recognition processes discussed below.

2. A technical mechanism for conveying recognition
This is used to convey sufficient information about the standing of a CA, as established by the first process, in a machine readable form, so that receivers of digital certificates can automatically decide whether or not to accept them. There are at least four options for conveying recognition of a CA: hierarchical CA certificates, cross-certificates, certificate trust lists and a bridge CA. All of these options are discussed below.

[2] These identifiers can take the form of Policy Object Identifiers (OIDs), which identify the Certificate Policy under which the certificate has been issued, or Issuer Distinguished Names.

3. Current PKI Interoperability Activity

There are numerous PKI interoperability discussions taking place in international and regional forums. This activity is being driven by government and business requirements to develop mechanisms to ensure disparate PKIs can work together:

> Businesses are deploying Public Key Infrastructures (PKIs) to support internal business processes, implement virtual private networks, and secure corporate assets. In addition, most businesses have industrial partnerships with other businesses for economic reasons. If these industrial alliances wish to exploit their internal security capabilities for business to-business (B2B) electronic commerce applications, connection of their corporate PKIs will be required. However, corporate PKIs may implement different architectures, security policies, and cryptographic suites. A flexible mechanism is needed to link these corporate PKIs and translate these corporate relationships into the electronic world.[3]

Unfortunately, there is no single agreed set of the available PKI interoperability models, but some clear trends can be discerned from current discussions and activity.

3.1. Europe

The European Commission is making some of the most recent moves to promote PKI interoperability. The IDABC (Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens) Programme[4] is working on a Bridge/Gateway CA project[5], beginning with a feasibility study commissioned in 2001 and published in July 2002[6], with a progress note on *Trust List Usage Recommendations*[7] in September 2003.

The feasibility study canvassed five general PKI interoperability models:

- Validation Authority (VA);
- Hierarchy;
- Mesh (cross-certification);
- Web/Internet Trust (white lists); and
- Bridge.

[3] William T. Polk and Nelson E, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, Hastings National Institute of Standards and Technology, September 2001
<http://csrc.nist.gov/pki/documents/B2B-article.pdf>.

[4] <http://europa.eu.int/idabc/>

[5] <http://europa.eu.int/idabc/en/document/2318>

[6] European Commission – Enterprise DG: IDA, *A bridge CA for Europe's Public Administrations: Feasibility Study*, July 2002
<http://europa.eu.int/idabc/servlets/Doc?id=17267>.

[7] European Commission: IDA, *Trust List Usage Recommendations for a Bridge/Gateway CA Pilot for Public Administrations*, September 2003
<http://europa.eu.int/idabc/servlets/Doc?id=17261>.

However, it settled on its own model, dubbed the Modified BCA (Bridge Certification Authority) PKI, which combines the flexible management structure of the bridge model with the technical simplicity of trust lists and the option to use cross-certificates. This is discussed further below.

Additionally, in the second half of 2003, the EU's Interdisciplinary Centre for Law & Information Technology issued a detailed report on *The Legal and Market Aspects of Electronic Signatures*.[8] It outlined EU Member States' activities in implementing the 1999/93/EC Directive, which required that electronic signatures be recognised as the legal equivalent of handwritten signatures.

3.2. OASIS PKI Forum

The Organization for the Advancement of Structured Information Standards[9] (OASIS) is a body that authors standards for a wide range of e-commerce applications, including PKI. The PKI Forum, originally set up by a group of private vendors, was taken over by OASIS in 1999, and has done important work in the development of PKI over the past five years.

OASIS recognises seven models for PKI Interoperability:

- Cross-certification ;
- Cross-recognition;
- Bridge CA;
- Certificate Trust Lists;
- Accreditation Certificate;
- Strict hierarchy; and
- Delegated path discovery and validation.

However, they note that "some of these options are not necessarily mutually exclusive, and a single solution may not be appropriate for all conceivable environments".[10]

[8] European Commission – DG Information Society, *The Legal and Market Aspects of Electronic Signatures*, 30 September 2003 <http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf>.

[9] <http://www.oasis-open.org>

[10] Oasis PKI, *CA-CA Interoperability Whitepaper*, March 2001 <http://www.pkiforum.org/pdfs/ca-ca_interop.pdf>.

The OASIS Public Key Infrastructure Technical Committee has begun implementation of its PKI Action Plan[11], which attempts to address the primary obstacles to PKI deployment and usage. One small part of the action plan is to improve interoperability through further testing. OASIS plans to:

> Provide conformance test suites, interoperability tests, and testing events for the three most popular applications (Document Signing, Secure Email, and Electronic Commerce) to improve interoperability. Certificate management protocols and smart card compatibility are also a concern… The PKI TC will work with organisations that have demonstrated involvement in or conduct of PKI interoperability testing or conformance testing to identify and encourage existing or new efforts in this area.[12]

3.3. The Asia PKI Forum

The ASIA PKI Forum[13] is an international organisation composed of representatives from PKI forums in Korea, China, Japan, Taiwan, Singapore, Hong Kong, Macau and Hong Kong. Its goal is to promote co-operation and interoperability among PKIs across the Asia/Oceania region.

In 2004 the Asia PKI Forum Interoperability Working Group released the *Asia PKI Interoperability Guidelines*[14], a document created to promote the development of a mutually agreed regional PKI framework. The Guidelines have been described by the Working Group as a referential roadmap for those parties interested in achieving PKI interoperability.

These Guidelines describe five PKI models and list the technical standards needed for interoperable PKI schemes. The five models are:

- Cross-certification;
- Cross-recognition;
- Bridge CA;
- Certificate Trust Lists; and
- Accreditation.

In addition to the PKI Trust Models, the Guidelines also list technical standards for the infrastructure, and the manner in which they should be adopted.[15]

[11] Oasis PKI Technical Committee, *PKI Action Plan*, 22 February 2004 <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf>.

[12] See footnote 11.

[13] <http://www.asia-pkiforum.org/>.

[14] Interoperability Working Group, *Asia PKI Interoperability Guideline (Version 1.0)*, Asia PKI Forum, March 2004 <http://asia-pkiforum.org/Asia_PKI_Interoperability_Guidelinev1.0.pdf>.

[15] Version 2.0 of the Guidelines is expected shortly.

In 2001 Japan, Korea and Singapore formed their own Interoperability Working Group (the JKS-IWG) within the Asia PKI Forum, and conducted an interoperability pilot project. The results of the project are available online[16]. The project successfully demonstrated complete interoperability in cross-border transactions between the three CAs from each country. It is notable that the project simultaneously used cross-certification in Korea and Japan and cross-recognition in Singapore. (Cross-certification and cross-recognition are discussed below.)

3.4. APEC

The Asia-Pacific Economic Cooperation[17] (APEC) is a regional forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific. The APEC Telecommunications and Information Technologies Working Group (APEC TEL) is the main APEC forum that examines e-security (including authentication). The eSecurity Task Group (ESTG) is a sub-group of APEC TEL. The ESTG has developed *Draft Guidelines for Schemes to issue certificates capable of being used in cross border jurisdiction ecommerce* (the ESTG PKI Guidelines[18]).

The Guidelines begin with a set of *Guiding Principles for PKI-based Approaches to Electronic Authentication*. Relevant sections include.

— The development of frameworks that set out parameters for the establishment and operation of certification authorities (CAs) can facilitate cross-jurisdictional acceptance of the services they provide.

— Such frameworks should allow for the acceptance of services originating in other jurisdictions.

— The establishment of legislative and legal frameworks that give legal effect to documents and signatures in electronic form produced by both domestic and foreign CAs will facilitate legal predictability on a cross-jurisdictional basis.

— Such frameworks should not unduly require the use of particular technologies. In addition, they should allow for changing market standards, developments in existing technology and the introduction of new technology.

— Requirements for the institutional standing of CA service providers (including capital and financing requirements for the establishment and operation of CAs) can generate public trust and confidence and facilitate cross-jurisdictional recognition of certificates issued by those CAs.

— Assessment schemes that utilise recognised standards and best practice to ensure technical interoperability between participants can facilitate cross-jurisdictional recognition of certificates.

— The implementation of widely accepted technical standards and management in PKI assessment schemes can allow for CAs to be assessed.

[16] See Japan, Korea and Singapore PKI Forum, *Achieving PKI Interoperability: Results of the JKS-IWG Interoperability Project*, 30 April 2002 <http://www.japanpkiforum.jp/shiryou/IPA/final.pdf>.

[17] <http://www.apectelwg.org>.

[18] APEC eSecurity Task Group, *Draft Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction E-Commerce*, March 2004 <http://www.apectel29.gov.hk/download/estg_20.doc>.

— Policies and procedures for cross-jurisdictional recognition of PKI assessment schemes can facilitate legal predictability and certainty in respect of certificates issued under those schemes.

Although the basic APEC interoperability model is cross-recognition (discussed in detail below), the Guidelines include detailed interoperability requirements for the accreditation and oversight of CAs which could be useful for other interoperability processes such as cross-certification, a bridge CA or a certificate trust list.

4. Current PKI Interoperability Models

The exact number and definition of PKI Interoperability models varies depending on the discussion forum (see above), but most of the models can be adequately contained within the following five models.

4.1. Root CA/Hierarchy Model

The root CA/hierarchy model describes a set of models based on a Root CA and/or a strict hierarchy of certificates.

The simplest approach to a PKI framework is to have a single (root) CA. It holds all certificates; all end-users refer to and trust it for all transactions.

The model can include Registration Authorities (RAs) which process the initial identification of users and issue key pairs. This adds some flexibility in the system by allowing for smaller groups to have their own local and customised services.

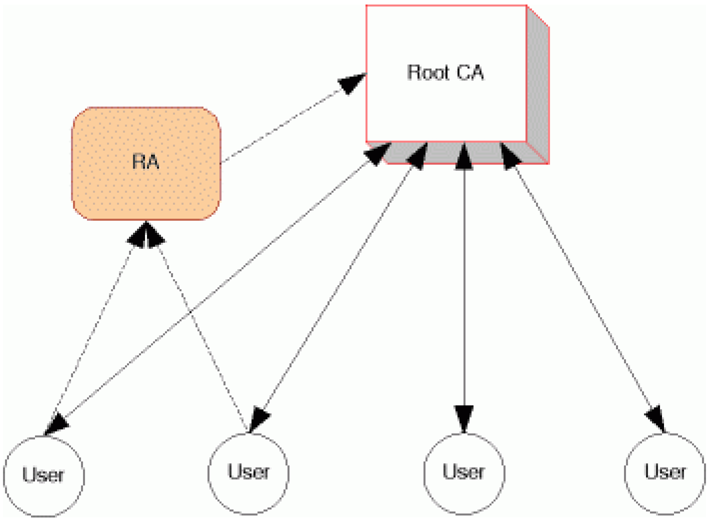

Figure 1. Root CA Model

This architecture simply avoids the various problems of interoperability and provides a single, convenient point of access. However, it suffers from a number of limitations, especially as the number of users increases:

— The technical and administrative workload of the CA would be enormous for large (country-wide) PKI schemes;

— Different groups of users will have different needs which a single CA cannot address all at once – for example, sensitive applications like health will require advanced and complex procedures, while tax applications will place far more value on speed and efficiency;

— It may be difficult to get all users to accept a single provider; and

— The single CA provides an obvious target for hackers and a security breach affects the entire system.

The root CA model is the basic unit of all PKIs, but it does not provide a useful approach to interoperability. A logical variation is the **strict hierarchy** model.

In a strict hierarchy, there is a trusted root CA which issues a certificate to subordinate CAs. Those CAs may, depending on the relevant policy, certify other CAs.

Each CA is trusted because the higher CA that certifies it is trusted. Only the root CA must be trusted on its own.

The hierarchical structure means there is a short and definite path to trace a certificate back to a trusted source, avoiding the more difficult processes of validating a certificate in a flat structure such as a cross-certification mesh (discussed below).

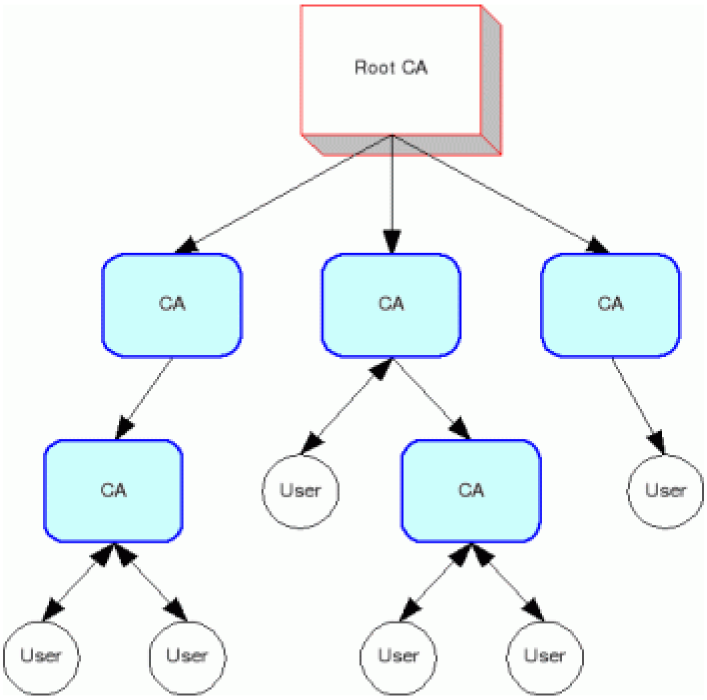

Figure 2. Hierarchy Model

This model adds an extra layer of flexibility to the simple root CA model and allows for competition and specialisation between CAs. However, in practice it suffers from many of the same limitations.

— Participants must be persuaded to subject themselves to the root operator;

— The root CA remains a critical security point; and

— The technical policies imposed by the root may restrict innovation and competition.

The root CA/hierarchical model has advantages in some situations:

— It avoids interoperability problems; and

— It provides a useful structure for organised and centralised groups such as governments, the military, large multinational companies or even well organised industry groups by enforcing practices and policies on CAs

Root CA/Hierarchy working example: Identrus

Identrus[19] is a private New York corporation set up by some of the world's largest banks to operate a PKI under a root CA for banking operations. It certifies banks as CAs so that they can issue certificates to customers for online transactions. It keeps its CA policies and requirements private, but markets itself as setting an exceptionally high standard in PKI security. A small group of participating banks operate CAs under it.

Despite being well-resourced and having a recognisably useful product – interoperable digital certificates for banking clients – Identrus is yet to firmly establish itself after five years. Identrus' slow start demonstrates the inherent weakness of the root CA model; it is highly prescriptive and requires a large initial investment. Nevertheless it is the obvious and perhaps the only marketable model for such a high-value application.

Identrus is a careful and competitive project, and has designed several other digital certificate products. It may yet become a significant player with the emergence of larger PKI markets, providing high quality certification services.

Root CA/Hierarchy working example: RegTP

The German national telecom provider, RegTP, is one of several CAs set up as a national root by European governments. However it is cited by a European report[20] as an example of a poorly executed root CA because of its failure to closely observe PKI standards, undermining the interoperability advantages of the root CA model. This failure was blamed on the approach of combining the root CA and supervision/accreditation functions into the same organisation, which left RegTP with no external supervision or auditing.

Root CA/Hierarchy working example: Johnson & Johnson

Johnson & Johnson, a multi-national healthcare company, has set up a PKI that uses over 100,000 certificates, issued to its employees and business partners. It enables a variety of applications in the company's sensitive operations – such as clinical research, marketing, and financial/legal departments – and at the same time complies with the security standard required by US health data laws and pharmaceutical regulations. This is a widely cited success in the PKI sphere, and has prompted recent activity towards establishing a broader PKI for pharmaceutical corporations.

4.2. Cross-Certification (Mesh) Model

Cross-certification is a different approach to interoperability. Instead of a hierarchy, CAs deal with each other as peers and choose whether or not to trust each other.

[19] <http://www.identrus.com>

[20] Refer to footnote 8, page 125.

If they do, the CAs issue cross-certificates to each other. A user can then trace a certificate from an unknown CA back to a local trusted CA. This may be implemented by allowing users to contact their trusted CA's repository of certificates or by including a chain of signatures on the certificate itself.

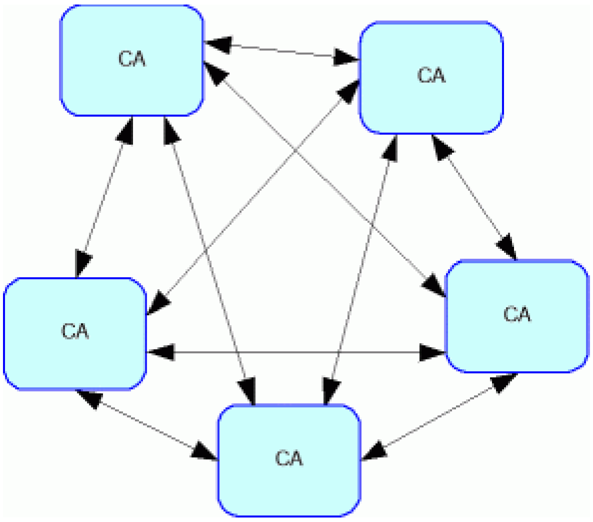

Figure 3. Cross-Certification - Full Mesh Model

However, achieving interoperability through a mesh of certifications is technically and logistically challenging. It is not easy for a single pair of CAs to co-ordinate their policies and technical systems, and as the mesh grows, the number of cross-certifications grows even faster. If every pair of CAs cross-certifies (to create a fully meshed network), the number of cross-certifications required is almost n^2 (if n is the number of CAs). However, if some CAs do not directly link to each other, the network of trust becomes wider and more risky. A chain of CAs must be trusted for each verification. In this 'partial mesh' it may become necessary for users to have a way of limiting the chain of certificates that can be used to verify a signature.

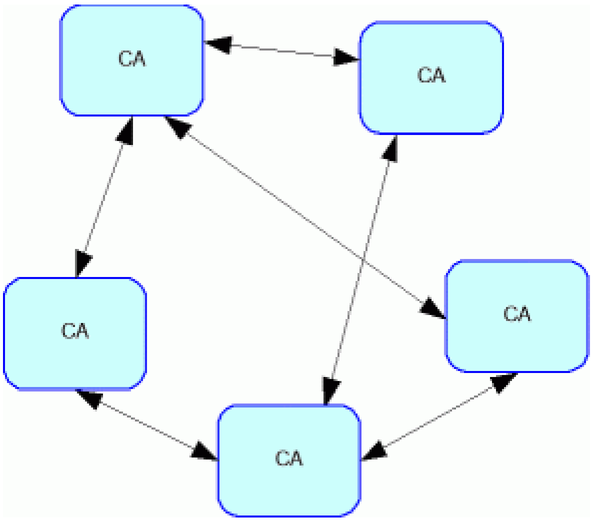

Figure 4. Cross-Certification - Partial Mesh Model

The sprawling nature of cross-certification where CAs are not familiar to each other means it is not an ideal approach to establishing a broad, multi-national PKI. Instead, cross certification is most suited where two or three related CAs are required to interoperate with each other.

For example, two government departments with their own CAs might find it simple to cross certify each other for a particular tax application because their policies and technical specifications were already closely aligned. Such networks might grow organically across other government departments, but any such process would be slow, careful, and built on already-strong relationships.

4.3. Bridge CA Model

The bridge CA model is based around a central (bridging) CA which cross-certifies with each CA. It functions as a communication channel between each of the CAs.

This combines aspects of both the root model and the cross-certification model. It provides much of the administrative simplicity of the root model, because it only requires one pair of cross-certifications for each CA, rather than n^2 certifications in a completely meshed system.

It also provides some of the flexibility of the mesh model because it is not conceived as imposing strict technical requirements on complying CAs. Nevertheless the bridge must set certain minimum standards for CAs to participate. For example, in the USA, the Federal Bridge CA specifies several different levels of assurance that a CA can be certified at. The bridge itself is focused on the task of providing interoperability.

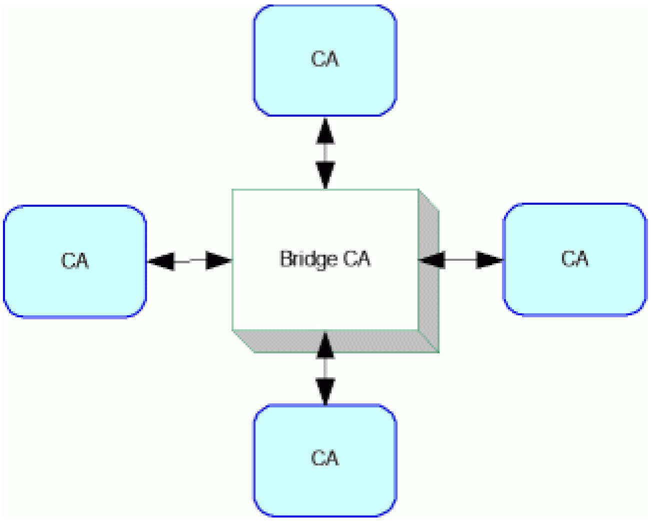

Figure 5. Bridge CA Model

The bridge is an attractive model because it helps to centralise the management of interoperability problems in the one authority that can develop and promote the best solutions.

The bridge model allows for PKIs built using different models to be joined together in a single, interoperable network.

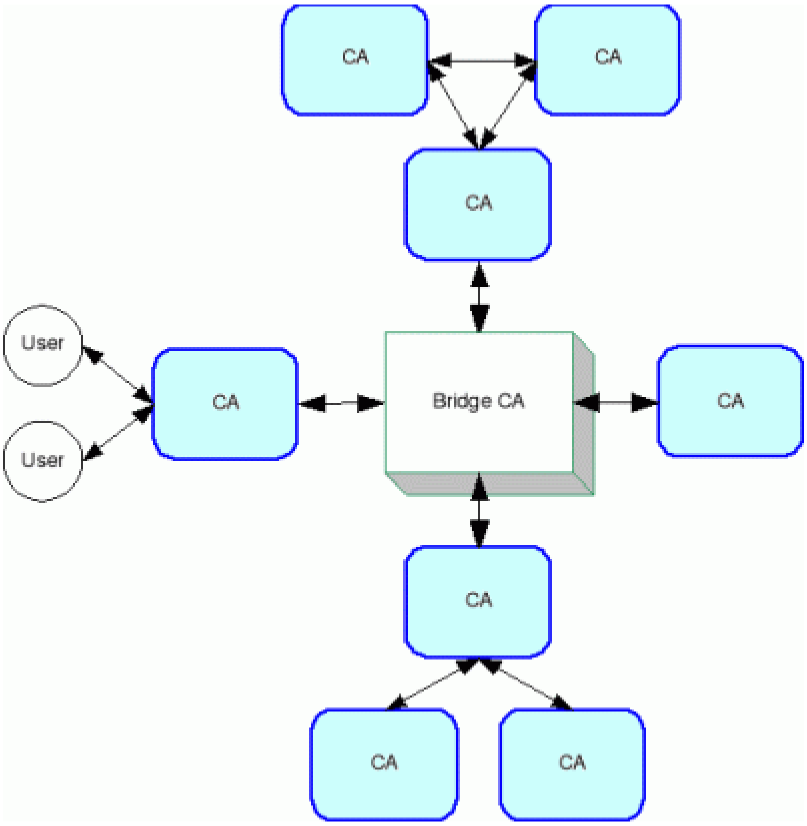

Figure 6. Expanded Bridge CA Model

This model also allows for bridge-to-bridge mutual cross-certification[21].

[21] Federal Bridge Certification Authority, *US Government PKI Cross-Certification Criteria and Methodology*, October 2004 <http://www.cio.gov/fbca/documents/crosscert_method_criteria.pdf>.

Bridge CA working example: US Federal Bridge CA

The bridge CA model has been pioneered in the US government's Federal Bridge Certification Authority (FBCA) project[22].

In 2000, the Federal Chief Information Officer's Council approved the FBCA Certificate Policy. This policy defines the FBCA as "an interoperability mechanism for ensuring trust across disparate domains." In practice, this is a mix of the bridge CA model and elements of the cross-certification model:

> Successful cross certification with the FBCA asserts that the Applicant Public Key Infrastructure (PKI) operates in accordance with the standards, guidelines and practices of the Federal Public Key Infrastructure Policy Authority (FPKI Policy Authority) and of the Federal PKI Steering Committee (FPKISC).For cross-certifications internal to the US Federal Government community, the FBCA Certificate Policy requires entities to sign a cross certificate Memorandum of Agreement (MOA) formally describing the terms and conditions of the cross certification. Cross certifications with non-Federal entities require the implementation of formal cross certification formal agreements between the US Government and the external entity. The details of these agreements may vary based on the nature of the external entity and its relationship to the Federal Government.[23]

The FBCA began operating in 2002. It appears to be working well, and there have been clear advantages from the development of this central organisation to coordinate and promote PKI interoperability. The bridged government departments include Defence, Treasury and NASA, and will soon include the Canadian Government, the Patents & Trademarks Office and the education sector's own bridge (EDUCAUSE). One bridged application has used certificates issued by university faculties to authenticate employees of the National Institutes of Health.

The FBCA lets subscribing CAs develop their own policies and procedures, and then provides interoperability by managing equivalence tables for those policies. This allows relying parties to assess themselves whether or not the certificate provides the requisite level of trust.

> The FBCA is an information system that facilitates an entity accepting certificates issued by another entity for a transaction. The FBCA functions as a non-hierarchical hub allowing the "relying party" entity to create a certificate trust path from its domain back to the domain of the entity that issued the certificate, and then to test that path using the requirements set forth in X.509 to determine whether the offered certificate contains the requisite level of trust to allow the transaction to consummate.[24]

Participation in the US Bridge is not mandatory, and parties in a PKI may use other methods to determine trust:

> The FBCA does not add to and should not subtract from trust relationships existing between the transacting parties. At their discretion, agencies may elect to interoperate among themselves without using the FBCA. Those agencies that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP.[25]

[22] <http://www.cio.gov/fbca/>

[23] Federal Bridge Certification Authority, *US Government PKI Cross-Certification Criteria and Methodology*, October 2004 <http://www.cio.gov/fbca/documents/crosscert_method_criteria.pdf>.

[24] Refer to footnote 23.

[25] National Institute of Standards and Technology: Computer Security Resource Center, *Federal Bridge Certification Authority* <http://csrc.nist.gov/pki/fbca/welcome.html>.

Several other sectors, such as the aerospace industry and the pharmaceutical industry, are establishing their own PKI bridges in the USA.

Bridge CA working example: European Bridge CA (EBCA)

The EBCA[26] is a privately run initiative of Deutsche Bank and Deutsche Telekom, and is a "pure" implementation of the bridge model, providing a central CA which cross-certifies with each CA domain. It has provided interoperability among a few major EU companies. However the European Commission has rejected this as too simple[27] because it does not include a mechanism for providing detailed information on CAs. It has modified this model in the newer IDABC Bridge/Gateway Project, discussed below under certificate trust lists.

4.4. Cross-Recognition Model

Cross recognition is where an individual CA or an entire PKI domain agrees to recognise another CA or domain, rather than building from a lower lever technical solution.

> A relying party in one PKI domain can use authority information in another PKI domain to authenticate a party in the other PKI domain, and vice-versa.[28]

This requires close co-operation among either the CAs at an administrative level or accreditation agencies (and governments) at a higher level.

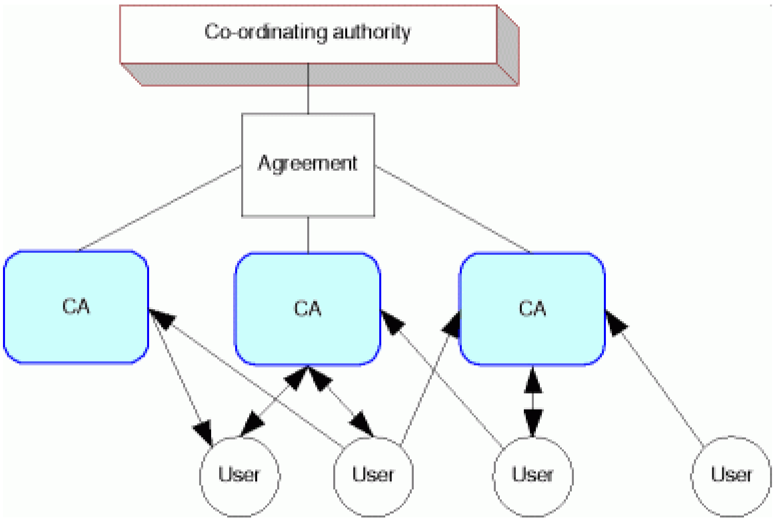

Figure 7. Cross-Recognition Model

In practice, cross-recognition means that certificates issued in a domain that has been recognised may be relied upon with some confidence by relying parties in the recognising domain:

[26] <http://www.bridge-ca.org>

[27] Refer to footnote 8, page 125.

[28] Business Facilitation Steering Group, Electronic Authentication Task Group, And Cross-Certification Expert Group, *Achieving PKI Interoperability*, APEC Telecommunications Working Group, 30 August 1999 <http://www.apectelwg.org/apecdata/telwg/eaTG/eatf06.doc>.

> Cross-recognition amounts to a formal and reciprocal recognition by the competent PKI authorities (top trust point) in one recognising PKI domain of the authority and capacity of the competent PKI authorities in another recognised PKI domain, to impose, manage and enforce PKI standards and trust processes appropriate for confident acceptance of those certificates in the recognising domain. A community of interest is thereby able to rely upon certificates issued from an external PKI for use in certain applications, within the limits of the accredited certificate policy for those certificates. As stated, however, the recognising domain would not be guaranteeing the status and reliability of foreign certificates.[29]

Cross-recognition is the basic trust model that is being pursued by the Asia Pacific Economic Cooperation (APEC) Telecommunications (TEL) Working Group.

Cross-recognition differs from cross-certification in several respects. For example, there is no mutual (or even unilateral) recognition between CAs. Cross-recognition is based on the notion that independent CAs would be licensed or audited by a mutually recognised trusted authority. The foreign CA may be regarded as trustworthy if they have been licensed/accredited by a formal licensing/accreditation body or they have been audited by a trusted independent party. This can be accomplished by the development of a mutually recognised set of criteria at the domain level. The end result is that as long as the user trusts the accreditation authority, they can trust certificates from any recognised CAs.

Cross-recognition is an attractive model because it avoids some of the technical interoperability issues. However, it still shares the administrative and management problems of all such networks of trust, and in many high-value applications it may not be seen as providing enough assurance.

Cross-Recognition working example: Pan-Asian E-Commerce Alliance (PAA)

A significant cross-recognition scheme is being organised by the Pan-Asian E-Commerce Alliance (PAA)[30] which has members from nine different economies[31] and co-ordinates a variety of e-commerce harmonisation activities to encourage regional trade. The PAA first authored a Certificate Policy Statement and, using that as a standard, has now accredited a CA from six of those nine economies to join the scheme. Cross-recognised certificates have now been used in several cross-border applications, especially customs and shipping.[32]

[29] Australian Government National Office for the Information Economy, *Interoperability between Gatekeeper and Foreign Digital Certificates through Cross-Recognising PKI Domains*, May 2003 <http://www.agimo.gov.au/__data/assets/file/18913/crossRecPolicyV2.3.pdf>.

[30] <http://www.paa.net/>.

[31] Singapore, Hong Kong, Taiwan, China, Korea, Japan, Malaysia, Macau, Thailand.

[32] PKI Forum Singapore, *Launch of final report on legal issues in cross-border e-commerce transactions*, 2003 <http://symposium.pki.or.kr/04%20WG%20Presentation%20I%20-%20Evelyn%20Ong.pdf>.

4.5. Certificate Trust List Model

The Certificate Trust List (CTL) is a list of CAs' certificates from a trusted authority. The list itself is electronically signed to ensure its integrity. While CTLs are simple, they provide a very useful device for communicating trust and replace the need for the more complex process of cross-certification. They are employed in a wide range of different administrative structures, such as the cross-recognition model used by the Pan-Asian Alliance (discussed above).

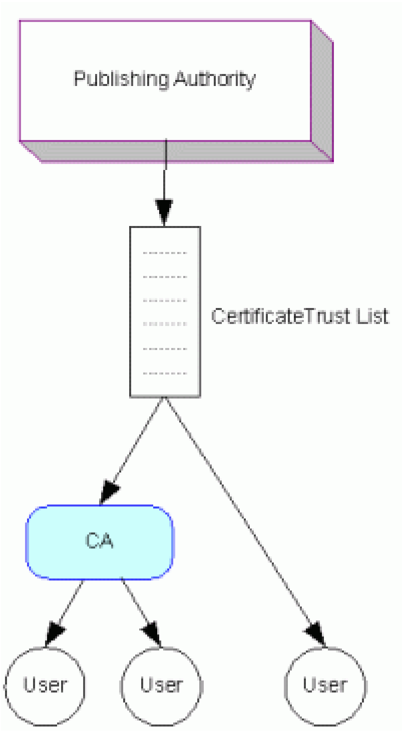

Figure 8. Certificate Trust List Model

Trust lists have also given rise to the 'browser' model - the most widespread interoperable PKI by virtue of web browser applications (such as Internet Explorer, Netscape or Firefox). These browsers use a list of pre-loaded certificates from several dozen of the largest and most reputable CAs such as Verisign, RSA and Thawte. Almost all e-commerce websites such as www.ebay.com or www.hotmail.com display a certificate issued by those particular CAs. When a browser visits their site, their certificates are automatically recognised and the user has some assurance that the web site is from the organisation it claims to be.

> From an inter-domain interoperability perspective, the CTL essentially replaces the cross-certificate pair… The key is that the relying party trusts the issuer of the CTL, which then allows the relying party to trust the CAs conveyed within the CTL. … Like any of the other alternatives, acceptable practices and procedures are required in order for this mechanism to be a viable alternative for achieving inter-domain interoperability. Specifically, what constitutes a trusted CTL issuer and the criteria that the CAs must adhere to before they can be considered "trusted" must be established.[33]

[33] Refer to footnote 10.

In the feasibility study[34] for the EU IDABC project discussed below, a different model was suggested where each participating PKI domain – in this case, each EU Member State – would exchange CTLs of government-accredited CAs. This is essentially a cross-certification mesh model that uses trust lists instead of cross-certifications. It is a simple solution in a technical sense, but it retains the administrative and management complexity of the cross-certification model.

Certificate Trust List working example: The EU IDABC Bridge/Gateway CA

The EU IDABC Bridge/Gateway CA[35] (BCA) has proposed a model that uses the centralised administrative structure of a bridge, and distributes trust using both cross-certifications and CTLs.

The BCA will be operated by the European Commission itself. The focus of the project is to allow interoperability between the PKIs of EU governments and their agencies, and the model assumes in each Member State there will be a national CA that operates that government's PKI. The BCA will bridge together each of these national CAs. It will perform a number of functions:

- It will publish a CTL of national CAs. Those national CAs can retrieve the list themselves and are free to add and subtract CAs from the list and republish it to their government's users according to their own national preferences.
- It may also publish CTLs of CAs in particular sectors – for example, a list of CAs accredited to provide health certificates.
- It will cross-certify with each national CA and make that certificate available to other CAs to perform their own cross-certifications.
- It will provide a directory service listing each national CA and maintain a CA Revocation List and Certificate Revocation List.
- It is also suggested that the bridge might provide an OSCP (Online Certificate Status Protocol) service, to route requests to the appropriate CA to determine if a foreign certificate has been revoked.
- It will provide a test bed service to help new CAs ensure they are integrated correctly.

[34] Refer to footnote 6, page 31.

[35] Europa – IDABC, *Bridge/Gateway Certification Authority*, September 2004 <http://europa.eu.int/idabc/en/document/2318>.

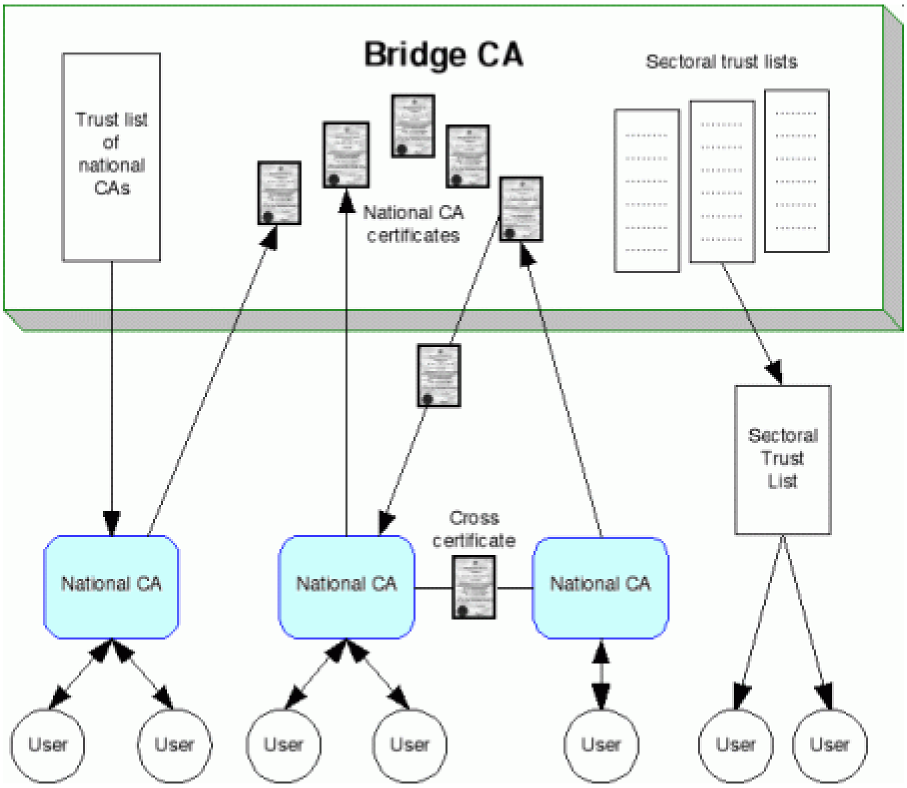

Figure 9. EU Modified Bridge CA Model

The feasibility study for this project[36] also considers the options for managing the variety of Certificate Policies (CPs) used by different CAs. It notes that the US Federal Bridge CA accepts the CPs as submitted by the CAs and maintains equivalence tables, allowing relying parties to make their own judgments about whether or not the CP provides a sufficient level of trust.

The EU study rejects this option, noting the administrative burden it would place on the BCA, and declares its preference for creating a limited set of standard CPs. Individual CAs could then be accredited to use these standard CPs by their national co-ordinating CAs. The individual CAs can combine the most demanding terms of their own policy stated on the certificate and the standard BCA CP to derive a set of procedures, usages and profiles that satisfy the BCA requirements as well as their own.

This EU project is still in a pilot phase, but it could be suggested that it represents the most mature theoretical approach to interoperability, taking lessons from the various international projects and adapting the best aspects of each model. At the same time it must be noted that it has the advantage of being placed in the tightly integrated and developed economies of the EU. Indeed, it is an expensive model with significant initial and ongoing costs, but provides a balance between the autonomy of its members and the efficiency of integration.

[36] Refer to footnote 34, page 37.

5. Comparative analysis

This section provides a brief comparative analysis of the available PKI interoperability models.

	Root CA / Hierarchy	Cross Certification (Mesh)	Cross Recognition	Bridge CA	Certificate Trust List
Brief Description	An organised chain of CAs, run from the top down.	CAs certify each other as peers	CAs/PKI domains agree to recognise each other's certificates	A central bridge CA manages interoperability between all other CAs	A list of trusted CAs is distributed
Role	Technical mechanism to convey recognition.	Technical mechanism to convey recognition. May also have role in establishing recognition.	Political and contractual process of establishing recognition.	Technical mechanism to convey recognition. May also have role in managing recognition.	Technical mechanism to convey recognition.
Working examples	Global – Identrus Germany – RegTP		Asia – PAA Australia – Gatekeeper / Angus	US Federal Bridge EU – Commercial Bridge	EU – Government Bridge
Agreement required	Tight agreement from the beginning	Only between CAs as needed	Political co-operation	Consensus of CAs to use bridge	Only useful if publisher already has authority
Technical interoperability – design stage	Yes – fully interoperable	Yes – but may require significant modifications	PKIs remain separate at technical level	Bridge can play a role in managing interoperability	Requires another mechanism to establish recognition (eg Cross Recognition)
Technical interoperability – real time operation	Yes – fully interoperable	Yes – fully interoperable	Requires use of other tools (eg Trust Lists) to achieve technical interoperability	Partial technical interoperability only – stronger if used with other tools (eg Trust Lists)	Yes – fully interoperable
Costs	Low – simple, easy system	High – each pair of CAs must go through expensive process to cross-certify	Low-Medium – co-ordinating body must enforce rules and audit participants	Medium – bridge CA has significant workload	Low, but varies with modes of use
Scalability	Medium – short and certain certification paths back to trusted root	Low – full mesh has n^2 pairs, certification paths may be long	Medium – no technical barriers, but challenging administrative co-ordination	Medium-High – limiting factor is bridge workload	High – simple, direct trust
Security risks	High – single breach of root brings down network, subordinate CAs must be re-certified	Low – single breach may have no effect on others, or may fragment network	Low – depending on level of technical integration, probably no effect on network	Medium – breach of bridge brings down network, but participants can still operate on their own	Medium – depending on implementation, may be lag between security breach and list update

6. Conclusion

There is a clear trend in the current PKI interoperability discussions to move towards the bridge CA model[37]. However, within the bridge model there are numerous variations for how interoperability is actually achieved. The bridge may be sitting above a cross-certification mesh, a cross recognition model, a series of certificate trust lists, or even a combination of all of these. It would appear that the main advantage of the bridge is the provision of a stable third party to co-ordinate and promote PKI interoperability by whatever means necessary.

In the absence of a bridge, interoperability may fall between the cracks. Individual governments, accreditation agencies and CAs do not have sufficient motive, skills or resources to deliver and maintain interoperability. In addition, the creation of a bridge allows interoperability to be achieved through staged testing and upgrades – perfect interoperability does not need to be achieved at once.

There does not appear to be a clear consensus on the best interoperability model below the bridge. Cross recognition is a broad brush approach that could be suitable for cross-border recognition – where governments are involved in the recognition of trusted domains. For many other aspects of PKI interoperability the certificate trust list model appears to deliver practical benefits.

[37] Stillson K D, *Public Key Infrastructure Interoperability: Tools and Concepts*, The Telecommunications Review 2002, <http://www.mitretek.org/publications/2002_telecomm_review/stillson_07.pdf> at p79.