WHITE PAPER

March 2001

CA-CA Interoperability

The CA-CA Interoperability Project is one of several major work areas being conducted under the auspices of the PKI Forum Technical Work Group (TWG) during calendar year 2000/2001. The purpose of this paper is to discuss the issues associated with establishing interoperability between otherwise isolated PKI domains, and to provide recommendations for the way forward.

1 Introduction

1.1 Background and Scope

The CA-CA Interoperability Project is one of several major work areas being conducted under the auspices of the PKI Forum Technical Work Group (TWG) during calendar year 2000/2001. The purpose of this paper is to discuss the issues associated with establishing interoperability between otherwise isolated PKI domains, and to provide recommendations for the way forward.

It is recognized that CA-CA Interoperbility is an area that is subject to some debate, and there are a number of different views that have yet to coalesce into a universally agreed position. Thus, the writers of this paper fully expect that some of the topics discussed herein might be controversial. It is also probable that some scenarios/options discussed herein will be appropriate in some contexts but not in others. It may therefore be unrealistic to expect one common approach will win out in favor of all others. Ultimately, the purpose of this paper is to stimulate discussion, eventually leading to a consolidated set of recommendations.

It should be noted that while standards serve a very important role in establishing compatible implementations, experience has demonstrated that standards alone are insufficient to guarantee multi-vendor interoperability. This is not something that is unique to the PKI industry; but it is something that the PKI industry must address. Indeed, one of the fundamental reasons for establishing the PKI Forum is to provide an environment where PKI vendors can work together in order to resolve interoperability issues.

Of course, not all interoperability issues are directly related to CA-CA interoperability. However, the interconnection of multiple PKI domains that are based on technology supplied by different PKI vendors does bring almost every conceivable facet of interoperability to the forefront. It is therefore appropriate to discuss these issues within the context of this paper. While the title of this project is "CA-CA Interoperability", emphasis is placed on what is best described as inter-domain interoperability. This term is defined later within the body of this report and it is also described in [SL].

Acknowledgements

"CA-CA Interoperability" is a deliverable from the PKI Forum's Technology Working Group (TWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews. Key contributors include:

Editor:

Steve Lloyd
Entrust Technologies

Principal Authors:

Steve Lloyd
Entrust Technologies

David Fillingham
NSA

Richard Lampard
CESG

Steve Orlowski
Chair APEC eSecurity Task Group

John Weigelt
Treasury Board of Canada

Reviewers and Contributors:

Michael Baum
Verisign

Rich Guida
US Department of Treasury

Martin Lindstrom
Entegrity

Takuya Tamura
Fujitsu

Udo Rockmann
Arthur Andersen

Martin Roe
Royal Mail

Ann Terwilliger
Visa International

PKI forum

1.2 Structure and Content

This paper is divided into five major sections as follows:

- Section 1 – Introduction;
- Section 2 – Setting the Stage – Issues and Options;
- Section 3 – Inter-domain Interoperability Initiatives;
- Section 4 – Role of CP, CPS and PDS; and
- Section 5 – Summary and Recommendations.

Section 1 identifies the purpose and scope of this paper, provides useful definitions and includes a list of references. Section 2 discusses the various issues associated with CA-CA interoperability with particular emphasis on inter-domain interoperability. Section 3 identifies and discusses a number of interoperability initiatives that are relevant to this topic and highlights some of the lessons learned as a result of some of these initiatives. Section 4 discusses the various schools of thought associated with the role of Certificate Policies (CPs), Certification Practice Statements (CPSs) and PKI Disclosure Statements (PDSs). Finally, Section 5 provides a brief summary and includes recommendations for moving forward.

2 Setting the Stage - Issues and Options

The main thrust of this section is to discuss the issues and options associated with inter-domain interoperability as defined in [SL]. Specifically, it deals with the issues and options associated with achieving interoperability between two otherwise isolated PKI domains[1]. For completeness, CA-CA interoperability within the same domain (or under a common corporate infrastructure) is also discussed.

Before describing the various options that are either available or are being proposed to facilitate inter-domain interoperability, it is important that we recognize that there are at least three areas that need to be considered when reviewing the pros and cons of the various alternatives that might be available.

The first area deals with technical considerations. Essentially, this area is concerned with the protocol, data structure and other aspects (e.g., sharing certificates and certificate revocation information) that are necessary to facilitate interoperability once all necessary business-level agreements are in place. This is probably the best understood of the three areas.

The second area deals with policy or business relationships. This encompasses non-technical details necessary to establish the relationship between two PKI domains. Ultimately, the rationale for establishing an inter-domain (or enterprise-to-enterprise) relationship will be based on the need to exchange information electronically. Stated another way – businesses typically establish a requirement to exchange information based on one or more applications[2]. This "electronic relationship" could be based on existing business requirements, or new requirements/relationships can be forged over time. In any case, it is the application(s) that typically drive items such as how certificates issued in a foreign domain will be used in the local domain. Naturally, these business-level agreements must be enforced technically, procedurally, or a combination of both.

[1] It is recognized that the meaning of the term "PKI domain" is subject to interpretation. For the purposes of this paper, a "PKI domain" or simply "domain" is an autonomous infrastructure that has been deployed within an enterprise. Therefore, inter-domain interoperability constitutes interoperability between two enterprises.

[2] An alternative view is that this could occur in the absence of a specific application, but it is asserted (in this paper) that ultimately it is the application(s) that drive the requirement for inter-domain interoperability.

Contents

The third area involves legal considerations. When one considers the current legal landscape surrounding PKI, this is probably the least understood of the three areas. Legal considerations include the following:

- One of the most fundamental interoperability issues rests on the acceptance of digital signatures in a multi-jurisdictional environment. The recently passed Electronic Signature legislation (referred to as E-Sign) within the United States is one of many attempts to help in this regard. Similar legislation has also been adopted in Europe. At a minimum, this legislation lends the same credibility to electronic signatures that hand-written signatures currently enjoy. However, this legislation is not without its problems. A good treatment of this topic relative to the recently enacted US E-Sign legislation can be found in [AC].
- Issues associated with responsibilities and liability need to be addressed/ understood. Some of the methods for facilitating inter-domain interoperability (discussed below) attempt to limit the liability of the CA by placing additional burden on the relying party. However, it remains to be seen if this orientation will be acceptable in every conceivable set of circumstances.
- Obligations surrounding the requirement for "user notice" need to be considered. Specifically, what constitutes legal notice, and how is legal notice conveyed to the relying party?

Note that all three of these areas are likely to apply to any inter-domain interoperability option in one fashion or another.
The primary focus of this paper is on the technical issues and, to a certain extent, business- and policy-related issues. Legal considerations are expected to be addressed separately by the PKI Forum Policy and Privacy sub-group.

When addressing the question of CA-CA interoperability in general, and inter-domain interoperability in particular, it is only fair to discuss all of the relevant alternatives – and to define (sometimes new) terminology in order to easily distinguish one option from another. Based on current literature and projects (since we want to take advantage of ongoing work in this area), there are a number of proposals for achieving inter-domain interoperability. Specifically, the following alternatives for achieving inter-domain interoperability have been suggested.

- cross-certification
- Bridge CA
- cross-recognition
- Certificate Trust Lists
- Accreditation Certificate
- strict hierarchy
- delegated path discovery and validation

Each proposal is discussed in more detail in the sub-sections that follow. As each proposal is discussed, it is worth noting the following observations:

- some of these options are not necessarily mutually exclusive, and
- a single solution may not be appropriate for all conceivable environments.

When addressing the question of CA-CA interoperability in general, and inter-domain interoperability in particular, it is only fair to discuss all of the relevant alternatives – and to define (sometimes new) terminology in order to easily distinguish one option from another.

2.1 Cross Certification

Simply put, cross-certification is the act of one CA issuing a certificate to another CA. This definition is entirely consistent with the X.509 [X509] where it is stated:

> "A certification authority may be the subject of a certificate issued by another certification authority. In this case, the certificate is called a cross-certificate…" and
> "Cross certificate – This is a certificate where the issuer and the subject are different CAs. CAs issue certificates to other CAs either as a mechanism to authorize the subject CA's existence (e.g. in a strict hierarchy) or to recognize the existence of the subject CA (e.g. in a distributed trust model). The cross-certificate structure is used for both of these."

The fundamental purpose of cross-certification is to establish a trust relationship[3] between two CAs. This is typically done to establish an interoperability path for one or more applications between two distinct PKI domains or between two CAs within the same PKI domain. The former is referred to as *inter-domain cross-certification* and the latter is referred to as *intra-domain cross-certification*[4].

Cross-certification may be mutual or unilateral. In the case of mutual cross-certification, a reciprocal relationship is established between the CAs - one CA issues a cross-certificate for the other, and vice versa. The cross-certificate issued by the local CA for a remote CA is referred to as a reverse cross-certificate (from the perspective of the local CA). The cross-certificate issued by the remote CA for the local CA is referred to as the forward cross-certificate (from the perspective of the local CA). The reverse cross-certificate and the forward cross-certificate are stored in the Directory as a Cross-Certificate Pair in accordance with X.509. Unilateral cross-certification simply means that one CA generates a cross-certificate for another CA, but the inverse is not true. Unilateral cross-certification would typically apply within a strict hierarchy where a superior CA issues a certificate to a subordinate CA[5]. However, there may be cases where unilateral cross-certification could apply in the inter-domain context as well.

One of the (largely unfounded) criticisms of cross-certification is that it could introduce an undesirable trust cascade[6] across multiple PKI domains. Stated another way, if A->B and B->C, then how do we prevent A->C (assuming that we want to)[7]? Fortunately, there are a number of extensions that are used within the cross-certificates that provide controls for preventing an unwanted trust cascade. These include:

- Name Constraints – can be used to specify one or more permissible name space(s) associated with subjects in the foreign PKI domain (e.g., A->B for

One of the (largely unfounded) criticisms of cross-certification is that it could introduce an undesirable trust cascade across multiple PKI domains. Stated another way, if A->B and B->C, then how do we prevent A->C?

[3] The meaning of the terms "trust" and "trust relationship" are not universally agreed. In the context of this paper, "trust" is used consistent with the definition provided in X.509 (i.e., "Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. ") It remains to be seen if refinement of this definition will be required.

[4] It is recognized that there are some who object to the use of the term "cross-certification" when describing the relationship between CAs within a strict hierarchy, and there are several sources where the very definition of "cross-certification" implies "inter-domain cross-certification" only. However, from a technical perspective, and consistent with X.509 [X509], cross-certification can apply in both an intra- and inter-domain context, and within a hierarchical or distributed trust model.

[5] The certificate issued by a superior CA to a subordinate CA is stored in the forward cross-certificate attribute of the subordinate CA. In this case, the corresponding reverse cross-certificate would be null. The issued certificate may also be stored in the *cACertificate* attribute of the subordinate. See X.509 [X509], Sections 11.2.2 and 11.2.3.

[6] This is also sometimes referred to as "transitive trust".

[7] The notation -> denotes a trust relationship. For example, A->B denotes "A trusts B".

subjects within the finance department of organization B) – also used to constrain (through exclusion or permission) subsequent issuers in a given certification path,

- Policy Constraints – can be used to limit the use of certificates issued to subjects in the foreign PKI domain (e.g., certificates issued to subjects in foreign domain B are to be used for non-committal e-mail only) and/or to prohibit policy mappings (to prevent the undesirable trust cascade across multiple PKI domains as discussed above), and

- Path Length Constraints (found in Basic Constraints certificate extension) – used to limit the number of cross-certificates in the certificate path (e.g., a path length constraint with the value of zero explicitly prevents the trust cascade between A and C in the example above).

From a technical perspective, the act of cross-certification is fairly straightforward once protocol-level interoperability has been established. However, there are other considerations that need to be taken into consideration such as sharing PKI-related information (e.g., end-entity encryption certificates and certificate revocation information) between PKI domains. In addition, methods to enforce the agreed business controls must be provided (e.g., desktop software may be necessary to ensure that certificates are being used consistent with their associated key usage and policy-related restrictions). But it can be argued that these issues also apply to other options that might be selected to facilitate inter-domain interoperability.

Of course, there are also a number of policy- or business-related issues that need to be addressed before the technical aspects associated with cross-certification are permitted to occur. This has been the source of most of the criticism associated with cross-certification, and this issue will be addressed later in this paper.

One of the primary advantages associated with cross-certification is that each PKI domain retains its autonomy. That is, external trust relationships can come and go without affecting the internal trust relationship between the relying parties and their trust anchor within a given PKI domain.

One of the primary advantages associated with cross-certification is that each PKI domain retains its autonomy.

2.2 Bridge CA

The Bridge CA is based on a special trust model sometimes referred to as the "hub and spoke" model. Current Bridge CA initiatives use cross-certification as the basis for inter-domain interoperability (although conceivably other methods could be used as well).

One of the early criticisms of bilateral cross-certification was that it could not possibly scale. It was argued that the number of bilateral cross-certification agreements in a worst case scenario (e.g., as required in a fully meshed orientation) is on the order of n^2, making the overhead involved even for a relatively small number of organizations unacceptable. This problem has been compounded recently in the sense that many feel that the cross-certification process itself is too complicated and laborious, making the overhead associated with bilateral cross-certification even worse than originally feared. However, it is also true that not everyone agrees on a common set of procedures for cross-certification, and some proposals are much less complicated and labor intensive than others.

Simply put, the Bridge CA essentially acts as a facilitator or introducer of one organization or enterprise to another. Since the Bridge CA serves to introduce one organization to another, it is no longer necessary for each organization to enter into a bilateral cross-certification arrangement with every other

The Bridge CA essentially acts as a facilitator or introducer of one organization or enterprise to another.

organization. Each organization can enter into a cross-certification arrangement with the Bridge CA under one or more certificate policies. Where the certificate policies overlap, the organizations now have a "trusted path" to each other via the Bridge CA.

From the perspective of each enterprise, the overhead associated with establishing these "trust relationships" can be reduced significantly. This is not to say that a given organization will always be able to rely on a single Bridge CA (and a single cross-certification) for every conceivable trust relationship. But it does illustrate how the Bridge CA can be used to significantly reduce the amount of overhead involved – especially when the number of organizations that fall under the umbrella of the same policy is significant.

2.3 Cross-Recognition

Cross-recognition is a concept that is being considered by the Asia Pacific Economic Cooperation (APEC) Telecommunications (TEL) Working Group. Cross-recognition is defined in [APEC] 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."

Cross-recognition is based on the notion that independent CAs would somehow be licensed or audited by a mutually recognized trusted authority.

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 somehow be licensed or audited by a mutually recognized trusted authority (e.g., an accreditation authority or an independent auditor). Specifically, [APEC] states that:

> "The (foreign) CA is regarded as trustworthy if it has been licensed/accredited by a formal licensing/accreditation body or has been audited by a trusted independent party."

Presumably, this would be accomplished under some sort of mutually recognized set of criteria.

Another significant difference is that the relying party is expected to make the trust decisions rather than the CAs. It is not yet clear how the relying party will obtain the necessary information to make an informed decision, although it has been suggested that this could be conveyed to the relying party through the use of certificate extensions or some other means[8]. In any case, [APEC] admits that this will place additional burden on the relying party, and that cross-recognition may not be viewed as an acceptable solution where high levels of assurance or trust are required.

2.4 Certificate Trust Lists

A Certificate Trust List (CTL) is a signed PKCS#7 data structure that can contain, among other things, a list of "trusted CAs". A "trusted CA" is identified within the CTL by a hash of the public key certificate of the subject CA. The CTL also contains policy identifiers and supports the use of extensions.

From an inter-domain interoperability perspective, the CTL essentially replaces the cross-certificate pair as described in Section 2.1. 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.

[8] The concept of cross-recognition is largely independent of technology, and one or more methods may be used to convey cross-recognition relationships.

It is expected that the distribution of the CTL to the relying party could be accommodated in a variety of ways, including one or more of the operational protocols defined within the IETF PKIX working group or via an out-of-band distribution mechanism.

Like any of the other alternatives discussed within this section, 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.

2.5 Accreditation Certificate

A discussion paper proposing a "Gatekeeper Accreditation Certificate" [UR] was circulated in conjunction with the Australian Government Gatekeeper project in March 2000. The proposal discusses issues associated with both cross-certification and cross-recognition, and it introduces the use of an *accreditation certificate* that could be used to indicate that a given CA is accredited by the Australian government. The concept of the Gatekeeper Accreditation Certificate (GAC) is also described in [GAC], which is a more recent publication from the Australian Government.

Essentially, each accredited CA would have their public key signed by the GAC. This signing process provides assurance to the relying party that the subject CA has met the accreditation criteria of the Australian government. As long as the relying party is willing to rely on the GAC as a source of trust, any CA accredited by the Australian government would also be recognized as trustworthy by the relying party.

On the surface, this orientation is similar to a rooted hierarchy concept. But there are two very important distinctions. First, each CA accredited by the Australian government could have a unique CP and CPS. Second, nothing prevents each CA from having their own self-signed public key certificate, something that is typically disallowed in a strict hierarchy. In a certain sense, the accredited CAs are autonomous entities that have been accredited by the same authority.

As in the case of cross-recognition, this does not require the issuance of cross-certificates. But unlike cross-recognition, CAs are involved in establishing the trust relationships. Accreditation would be accordance with criteria defined by the Australian government. Naturally, it is possible that a similar approach could be adopted by other national governments.

2.6 Strict Hierarchy

The idea behind a strict hierarchy is that all "trust" emanates from a common root CA. That is, the root CA is the trust anchor for all relying parties within that domain. Although subordinate CAs may be deployed, relying parties will not rely on any certificates issued by a subordinate CA unless a valid certificate path can be traced back to the root CA. A strict hierarchy is also characterized by the fact that a subordinate CA will have one, and only one, superior. Further, subordinate CAs are not permitted to have their own self-signed certificates; only the root CA has a self-signed certificate[9].

Strict hierarchies are comprised of one root CA and zero or more subordinate CAs. Figure 1 illustrates one possible representation of a strict hierarchy. In this case, the root CA (labeled "Level 0") issues certificates to the two subordinate

A strict hierarchy is also characterized by the fact that a subordinate CA will have one, and only one, superior.

[9] It is recognized that "loose hierarchies" may also exist where some of the restrictions normally associated with a strict hierarchy would be relaxed. However, for the purposes of this paper this is not relevant.

CAs (labeled "Level 1"), and the Level 1 CAs can subsequently issue certificates to their subordinate CAs (labeled "Level 2"). The issuance of a subordinate CA certificate by the superior CA is essentially unilateral cross-certification as described in Section 2.1. In accordance with X.509 (see Sections 11.2.2 and 11.2.3), a subordinate will store its certificate in the *CA certificate attribute*[10] as well as in the forward element of the cross-certificate pair. Note that in a strict hierarchy, only the root CA has a self-signed certificate and, in accordance with X.509, the self-signed root CA certificate will be stored under the root's CA certificate attribute.

Strict Hierarchy Example

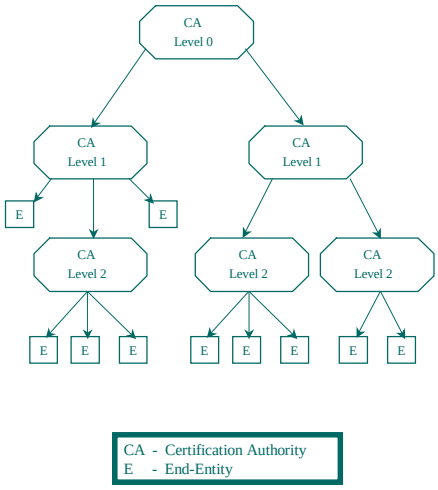

Chart 1: Strict Hierarchy

Strict hierarchies (or derivatives thereof) are appropriate for many enterprises, especially where policy controls are to be enforced in a "top-down" fashion. We are also seeing examples where a root CA has been established to support specific applications within a given industry vertical (e.g., Identrus).

One of the criticisms associated with strict hierarchies is that the consequences of root CA private key compromise can be catastrophic. In addition, there is no single root CA that applies to every PKI domain, so it is not possible to maintain a strict hierarchy across all conceivable domains. This means that one of the other methods discussed above must be used to establish a trust relationship between these otherwise isolated PKI domains.

Strict hierarchies (or derivatives thereof) are appropriate for many enterprises, especially where policy controls are to be enforced in a "top-down" fashion.

2.7 Delegated Path Discovery and Validation

Delegated path validation allows trust decisions to be partially or completely off-loaded from the relying party. This would involve client-side software, acting on behalf of the relying party, which would query a trusted third-party server when required. Essentially, the request to a trusted remote server could be as simple as "should I trust this certificate". Of course, more complex queries could also be supported. Any protocols defined to support this function should allow for different levels of granularity to be specified in the request.

[10] Assuming that the issuing CA is in the same "realm" as the subordinate CA.

There is ongoing work within the Internet Engineering Task Force (IETF) that is addressing this issue. One possible method for achieving this is through Version 2 of the On-Line Certificate Status Protocol (OCSP) and the associated path delegation and validation Internet Drafts. In competition with this work is the Simple Certificate Validation Protocol (SCVP). It is expected that one of these two alternatives will be adopted by the IETF. The relevant Internet Drafts can be found at "http://www.ietf.org/html.charters/pkix-charter.html".

While this option certainly looks attractive in terms of reducing the complexity associated with conveying and processing this information to/by the relying party, it is likely that the complexity of the back-end infrastructure needed to support this orientation would be as complex as any other of the alternatives discussed within this section. There are also bandwidth considerations and issues associated with catching replies that need to be explored further.

2.8 Summary Comparison

A comparison of the relative advantages and disadvantages of the various approaches described within Section 2 is provided in Appendix C, Table 1.

3 Inter-Domain Interoperability Initiatives

There are several national and international initiatives that are attempting to address the issues associated with inter-domain interoperability. The purpose of this section is to discuss some these initiatives[11] and, in some cases, to document the lessons learned as the result of these initiatives.

3.1 APEC TEL PKI Interoperability Expert Group

The PKI Interoperability Expert Group (which is part of the APEC TEL structure) is currently examining interoperability between a number of schemes in APEC economies. The project involves identifying the key elements of a PKI scheme and then mapping the various approaches against those key elements. The list of key elements is currently being discussed within the Expert Group and is largely based on RFC 2527. The process recognizes the existence of multiple levels of certificates and is focusing on trying to develop at least one certificate that will have legal effect in all APEC member economies regardless of its place of issue. Most of the schemes under consideration are either government licensing/accreditation schemes, either mandatory or voluntary, or standards based accreditation schemes such as that being developed by the Certification Forum of Australia. The existence of the accreditation schemes will facilitate the concept of cross-recognition previously put forward by the Expert Group.

The Expert Group is also working with the European Electronic Signature Standards Initiative (EESSI) to ensure that there are no inconsistencies between the two groups. One issue recently discussed at a workshop in Barcelona was the need for standards that could support the standard for qualified certificates. Also, the absence of standards for security aspects of the operations of a CA, as opposed to its technology, was highlighted in a recent attempt to compare the Australian Gatekeeper scheme with the scheme operated by the Controller of Certification Authorities in Singapore.

The PKI Interoperability Expert Group (which is part of the APEC TEL structure) is currently examining interoperability between a number of schemes in APEC economies. The project involves identifying the key elements of a PKI scheme and then mapping the various approaches against those key elements.

[11] This is not an exhaustive treatment of this topic area. Additional initiatives may be added to the discussion as appropriate. Possible examples include the ABA PKI Assessment Guidelines, the EEMA interoperability activity, and the ongoing work under the OECD.

In addition, discussions on interoperability pilots between a number of economies involving legal, technical and policy aspects are currently underway. These pilots range from government schemes to trade group schemes involved in the shipment of goods.

3.2 Australian Government Gatekeeper Project

The Australian Gatekeeper Project is described in [GKPR]. Interoperability is an important element of the Gatekeeper strategy. Interoperability within the Australian Government Certificate Infrastructure (AGCMI) is to be achieved via the Gatekeeper Accreditation Certificate (GAC). The GAC is intended to be a central 'trust point' for the Commonwealth and other jurisdictions or PKI schemes that may wish to accept it, but is NOT intended to be a national 'root' certificate. The GAC is intended to be the central 'trust point' for both the authentication and privilege management frameworks. Additional information regarding the Gatekeeper Accreditation Certificate can be found in [GAC].

The Gatekeeper Accreditation Certificate is intended to be a central 'trust point' for the Commonwealth and other jurisdictions or PKI schemes that may wish to accept it, but is NOT intended to be a national 'root' certificate.

3.3 CESG CLOUD COVER Interoperability Testing

The Communications-Electronics Security Group (CESG) of the UK Government Communications Headquarters is conducting a number of interoperability tests under the auspices of project CLOUD COVER. The CESG CLOUD COVER project "aims to set standards to foster the development by industry of Public Key Infrastructure (PKI) products and services to meet the electronic key distribution requirements of HMG" [CESG1].

The first phase of this interoperability initiative was completed in 2000. It was based on a rooted hierarchy, with four subordinate CAs representing four different Government departments. Each subordinate CA was based on products supplied by different PKI vendors. The results of this initiative were published in March 2000 (see [CESG1, CESG2]).

Many valuable lessons were learned regarding some of the problems that can be encountered when attempting to establish interoperability between products supplied by different vendors. Some of these lessons are summarized below. A more detailed treatment of the results can be found in [CESG1 and CESG2]. CESG also plans to conduct additional interoperability testing based on S/MIME Version 3 in February 2001, and it is expected that the results of that testing will also be made available to the PKI Forum.

The CESG CLOUD COVER project "aims to set standards to foster the development by industry of Public Key Infrastructure (PKI) products and services to meet the electronic key distribution requirements of HMG."

3.3.1 Encoding/Decoding Issues

A number of issues related to the encoding and decoding of information were encountered, including:

- Inconsistent use of date formats (UTCTime versus GeneralizedTime) between CAs which can make decoding and subsequent signature verification behave incorrectly;
- Differences in use of BER/DER encoding for extensions;
- Use of non-standard OIDs to denote algorithms which prevents another CA from generating cross-certificates;
- Differing assumptions about what should be supplied in the cross-certification request (e.g., one CA assumes that cross-certifying CA will determine certain values whereas the second CA assumes they will be provided in the request);
- Cross-certification requests may be encoded as binary ASN.1 or Base64 encoded; and
- Encoding of empty values (e.g., if no attributes are present in a request, some products assume that the request will contain encoding of empty set while others assume no encoding at all).

3.3.2 Boundary and Range Issues

A number of boundary/range problems were encountered, including:

- Assumptions about maximum value of certificate serial number (e.g., some cross-certifying CAs produce cross-certificates with a serial number greater than the cross-certified CA can handle);
- Assumptions about maximum length of names (e.g., the cross-certification request contains a distinguished name longer than cross-certifying CA can handle); and
- Arbitrary limits on maximum permissible path length, which make cross-certification fail.

3.3.3 Naming Conventions

A number of naming convention issues were encountered, including:

- Use of non-standard or legacy values in distinguished names (e.g., RFC822 address within Issuer Distinguished Name);
- Assumptions about the ordering of distinguished name attributes (e.g., assume common name is always encoded last in sequence), or arbitrary limitations upon the number of attributes (e.g., only one organizational unit attribute was allowed); and
- Where human intervention is required in cross-certification process (e.g., a request and cross-certificate are transferred via floppy), file naming conventions need to be agreed.

3.3.4 Certificates, CRLs and Certificate Paths

A number of issues related to certificates, CRLs, and certificate paths were encountered, including:

- Some vendors implemented arbitrary path length restrictions that would be insufficient for some environments;
- Inconsistent use of keyUsage and basicConstraints extensions;
- Inconsistent use of issuer name, serial number, authorityKeyIdentifier and subjectKeyIdentifier;
- Inconsistent use of nextUpdate field in CRLs;
- Inconsistencies in creating and responding to cross-certification requests; and
- In some cases, applications do not yet possess the ability to process complex certificate paths as they have been designed with simple hierarchical trust models in mind.

3.3.5 Directory Issues

A number of directory-related issues were encountered, including:

- In some implementations a CA entry can only be added to the X.500 LDAP directory when the directory is first configured. Therefore, a new entry for cross-certified CA cannot be added. Some implementations only check to see if CA is bound to the directory at log on, so any errors will not be reported.
- Some CAs use the same OID for different object classes.

3.4 GOC PKI

Currently, there appears to be very little available in terms of formal criteria for establishing inter-domain interoperability. One notable exception is the Government of Canada Public Key Infrastructure (GoC PKI) that defines a detailed cross-certification methodology as described in the "Government of Canada Public Key Infrastructure Cross-Certification Methodology and Criteria" [GOC].

The CESG CLOUD COVER project "aims to set standards to foster the development by industry of Public Key Infrastructure (PKI) products and services to meet the electronic key distribution requirements of HMG."

The cross-certification methodology defined by the Government of Canada (GoC) is by far the most detailed and formal set of procedures of all the publications examined. A step-by-step process is defined, including associated forms and explicit requirements for detailed documentation such as Certificate Policies and Certification Practice Statements. The process itself follows the normal steps or phases in arranging a contract as the model for the establishment of agreements between business partners. These phases are:

1. Initiation – The initiation phase is where a business requirement has been identified for the conduct of secure electronic service delivery where no electronic trust relationship currently exists. The CA that is not part of the GoC PKI petitions for cross certification.

2. Examination – The cross certification team reviews the Candidate CAs certificate policies and any other information that will provide a means to establish a level of assurance in the operation of the system. Likewise, the candidate CA has open access to the documentation created for the GoC PKI.

3. Arrangement – A contractual relationship is established between the GoC PKI and the candidate CA and cross-certificates are issued. The arrangement will mitigate any outstanding risks that were not addressed in the examination phase (i.e., where sufficient assurance is not obtained through the review process, alternative arrangements such as a Memorandum of Understanding or other form of contractual agreement is put in place to mitigate risk in the event of negligence on the part of the foreign CA).

4. Maintenance – As with other contractual mechanisms, there is a need for continued review of the CAs adherence to the obligations it sets out in its CPs. The fourth phase identifies those steps taken to maintain the trust established at the original signing of the agreement.

IT systems within the GoC are governed by the Canadian Government Security Policy and as such are subject to a certification and accreditation (C&A) process conducted by competent experts. This provides a basis for assurance in the internal government CAs. The C&A process cannot, however, be imposed upon external businesses. The philosophies related to securing IT systems can also vary between businesses, with some relying on an audit rich methodology and others on evaluated products. Nonetheless, the GoC PKI cross-certification methodology and criteria is intended to be applied equally across both communities of interest, those internal and those external to government. As a result, some guidance documentation has found its way into the annexes to provide some insight into those elements upon which the GoC relies upon to gain assurance. While the annexes provide a great deal of insight into the requirements for those CAs internal to government, external CAs need only to provide a subset of this documentation as part of the process. Specifically, only 7 of the 21 annexes are mandatory requirements where a legal arrangement (as discussed above) is used to mitigate risk.

The cross-certification methodology defined by the Government of Canada (GoC) is by far the most detailed and formal set of procedures of all the publications examined.

3.5 US Federal and DoD Bridge CA Initiatives

The US Federal Bridge Certification Authority is being developed by the General Services Administration under the auspices of the Federal Chief Information Officers' Council. The first objective of the Federal Bridge CA project is to provide interoperation across Federal department and agency public key infrastructures, of which there are dozens. Later, the US Federal Bridge CA is planned to provide mechanisms for Federal to State, cross government, and commercial sector PKIs.

The first objective of the Federal Bridge CA project is to provide interoperation across Federal department and agency public key infrastructures, of which there are dozens.

Achieving interoperation across the US Federal government presents a number of special challenges. In nearly every case, Federal public key infrastructures were developed for particular agency or department public key enabled applications. Without any Federal "top-down" design or interface specifications with which to conform, it was inevitable that various Federal agencies and departments would purchase a wide variety of PKI products, many of which were not designed to interoperate.

While there are many technical challenges in developing an interoperable Federal Public Key Infrastructure, there exist organizational challenges as well. Different Federal department and agency PKIs have different certificate policy requirements. Furthermore, the notion of subordination, found in interoperability concepts such as CA hierarchies, is very difficult to impose on an organization as large and complex as the US Federal government – and certainly would be completely inappropriate for international, Federal-State, and Federal-Commercial PKI relationships.

3.5.1 Alternative Approaches and the Bridge CA Concept

There are a number of alternative approaches to a strict hierarchy. For example, trust lists are supported in many public key enabled applications, and avoid the problems associated with single PKI hierarchies. However, they seem impractical, unwieldy, and difficult to manage securely when very large numbers of PKIs are being integrated, as is the case with the US Federal PKI.

Another approach to avoid both hierarchical PKIs and trust lists could be bilateral cross-certification among Federal agency and department PKIs. For example, if the Department of Defense and the Federal Aviation Administration wish to accept each others' certificates, their PKIs could directly cross-certify. But there are hundreds of PKIs within the Federal Government – to say nothing of State and international PKIs. As the Federal government PKIs become more richly cross-certified, the overhead costs associated with managing so many cross-agency certificates would increase exponentially.

Another approach to avoid both hierarchical PKIs and trust lists could be bilateral cross-certification among Federal agency and department PKIs. For example, if the Department of Defense and the Federal Aviation Administration wish to accept each others' certificates, their PKIs could directly cross-certify.

As a result, the Federal Public Key Infrastructure Technical Working Group, led by the US National Institute of Standards and Technology (NIST), has adopted the "Bridge CA" concept from commercial industry, which was facing similar problems associated with integrating large numbers of non-hierarchical PKIs. The Bridge CA concept allows a consolidation of cross-certificates that reduces the labor associated with their management, and makes administration of the Federal PKI much more feasible and economical. The Bridge CA involves deployment of a "trust nexus" – a CA that acts as a "bridge of trust" between different PKIs by cross-certifying with "Principal Certification Authorities" (PCAs) within the separate US Federal Department and Agency PKIs.

The Bridge CA differs from a hierarchical Root in that its public key does not serve as a "trust anchor." This is important for several reasons. First, trust anchor keys must be delivered by secure out-of-band mechanisms. Consequently, changing the trust anchor key becomes very difficult for a large, heterogeneous organization. Secondly, a relying party's Trusted CA is the root of trust decisions – the "starting point" for further trust decisions regarding which CAs are to be trusted, and to what degree. Were the Bridge CA a Federal Root, each agency's relying party community would be required to discard their existing trust anchor keys, and load the "Federal Root" key. In so doing, they would have to largely cede control of their PKI's to the Federal Root. Because of the diverse certificate policy requirements of the Federal government, it would be extremely difficult to formulate Federal government decisions regarding acceptable certificate policies and cross-certification in a hierarchical structure. By cross-certifying with subscriber PKIs as peers, each Department or Agency PKI retains control of

its local PKI and Certificate Policies, and can, by careful population of the cross-certificates it issues to the Federal Bridge, regulate the degree of trust it places in the certificates accepted via the Federal Bridge.

3.5.2 Certificate Policy Management

It is important to recognize that not all certificates are created equal. The "common security rules" enforced by a PKI to provide assurance in the certificates it issues is an important component of a certificate policy. Given that the Federal department and agency PKIs were developed largely independently, with different assurance requirements, they implement a wide range of Certificate Policies. A chain of cross-certificates from a low-assurance PKI to a high-assurance PKI would reduce the assurance of the high-assurance PKI subscribers, were no technical measures taken to prevent this trust-dilution. The Federal Bridge CA uses the policy mapping features of the ISO/ITU X.509 standard to prevent low-assurance certificates from "contaminating" the high assurance domains.

It is important to recognize that not all certificates are created equal. The "common security rules" enforced by a PKI to provide assurance in the certificates it issues is an important component of a certificate policy.

The policy mapping features of the X.509 standard allow a CA to assert in a cross-certificate that the certificate policies of a cross-certified PKI are equivalent to those of the local CA domain. Each Federal department or agency PKI has a certificate policy by which the department or agency issues and manages certificates. A body known as the "Federal Policy Authority" establishes the Federal Bridge CA Policy, which serves as the basis for issuing certificates from the Bridge CA. To serve this function, the Federal Bridge Policy has to address two issues – the rules for operating the Bridge CA itself, and the basis on which the Bridge CA will issue certificates to other CAs, and at which policy levels.

Currently, the Federal Bridge CA Policy describes four levels of assurance: Rudimentary, Basic, Medium and High. The Federal Policy Authority will evaluate the certificate policies of applicant PKIs, and map these agency policies to the Federal Bridge CA Certificate policy. For example, the Federal Policy Authority may evaluate the Department of Defense CLASS 4 Certificate Policy as being equivalent to the Federal High assurance policy, and the Treasury Department Certificate Policy as being equivalent to the Federal Bridge Certification Authority Medium Assurance certificate policy. Similarly, the Department of Defense Policy Management Authority may evaluate the Federal High Assurance certificate policy as being equivalent to the DoD CLASS 4 Certificate Policy. The resulting chains of certificates reflect these policy decisions, and allow the relying party applications to accept or reject certificates on the basis of these infrastructure policy analyses and local relying party requirements. Of course, the policy information embedded in the certificates is only of value if applications are capable of processing it.

3.5.3 Application Processing Requirements

The Federal Bridge Certification Authority provides the chains of certificates required to link separate Department and Agency PKIs, and the Federal Policy Authority provides a means to equate certificate policies – but these are not sufficient to provide PKI interoperability. Use of the Bridge CA imposes special requirements on client applications:

Use of the Bridge CA imposes special requirements on client applications:

- Certificate Path Development
- Certificate Path Processing

- Certificate Path Development – The Bridge CA combines both hierarchical and distirbuted PKI architectures into a single "mesh" style PKI. Applications built to develop certificate chains only from hierarchical certificate graphs – and at present this includes most PKI enabled applications – must be upgraded to develop certificate chains from mesh-style PKIs before they can validate certificates linked to their local CA domain via the Bridge CA.
- Certificate Path Processing – As was mentioned earlier, joining multiple PKIs implementing multiple certificate policies can reduce the assurance of cross-certified PKIs implementing more stringent certificate policies. This "trust

dilution" problem can be greatly mitigated by use of the policy related X.509 certificate extensions (certificatePolicies and policyMappings). There are other certificate extensions that are also important in preventing the Bridge CA concept from reducing the certificate assurance level of PKIs that subscribe to the Bridge CA. The nameConstraints extension is particularly valuable in preventing unwanted trust paths from being propagated through the Bridge CA. For example, if Agency A does not wish to accept certificates issued by Agency B, then Agency A could use the nameConstraints extension in the certificate it issues to the Bridge CA to exclude certificates issued by Agency B. Finally – the fact that the Bridge CA is expected to join many PKIs issuing certificates to many certificate profiles means that applications will need to process certificates containing a wide variety of extensions that they may not have encountered before.

While at present there are only a few applications that can build and process the certificate chains associated with the Bridge CA, there is a great deal of encouraging progress among major application and operating system providers in this regard, and it seems likely that several vendors will be offering "Bridge CA Capable" applications within the next two years.

3.5.4 The Directory System and the Bridge CA

The approach of cross-certifying PKIs via the Bridge CA establishes certificate chains – but the clients of the diverse PKIs linked via the Bridge CA must somehow obtain these certificates, and also obtain revocation status for each certificate in the certificate chain. Directories (sometimes called "repositories") are the most common method of sharing PKI certificates and revocation information.

While at present there are only a few applications that can build and process the certificate chains associated with the Bridge CA, there is a great deal of encouraging progress among major application and operating system providers in this regard, and it seems likely that several vendors will be offering "Bridge CA Capable" applications within the next two years.

Earlier, we mentioned that Federal Agency and Department PKI elements were often developed to serve a single "enterprise," without much thought being given to multi-vendor, cross-enterprise interoperability. Similarly, the directory products serving these "enterprise PKIs" were also often developed without much thought to later integration into multi-vendor PKI environments. If the Bridge CA concept is to work for the US Federal government, then the problem of multi-vendor directory interoperation must be solved.

The most commonly implemented open standards used for directory-to-directory interoperation are the ISO/ITU X.500 standards.[12] These standards define (among other things) the Directory System Protocol (DSP) which allows "chaining" between different directory systems. Chained Directory System Agents (DSAs) provide clients with the "illusion" of a single, integrated directory system. In theory, directory chaining among the various Federal department and agency directory systems could result in seamless directory interoperation. Indeed, several technology demonstrations have shown that X.500 directory chaining can support multi-vendor PKIs, using a diverse array of Directory Systems.

Unfortunately, some of the most commonly used commercial directory systems use proprietary protocols for inter-directory communications, so the simple approach of linking all Federal department and agency directories via X.500 DSP is not possible.

[12] Note that while X.500 is the most common open standard for getting directory systems to communicate with each other, the Internet Engineering Task Force (IETF) Lightweight Directory Access Protocol (LDAP) is by far the most common approach to providing client access to directory information. It is important to note that use of X.500 standards to achieve cross-directory interoperation does not in any way prevent use of LDAP for client directory access.

The IETF Lightweight Directory Access Protol (LDAP) provides for multi-directory interoperation by use of "referrals."[13] Referrals are a way for directories to "refer" clients from the directory the client has queried to another directory that is more likely to have the information the client has requested. LDAP referrals require applications to be able to process them, and at present, very few PKI-enabled clients process LDAP referrals.

Proprietary protocols and client limitations are technical barriers to directory interoperation, but there is a policy barrier as well. Enterprise directory systems are becoming important components of agency and department business processes. They often contain sensitive information about every employee associated with that enterprise. It is unacceptable to provide all of the information in the enterprise directory to every other enterprise associated with the Federal Bridge CA.

The technical and policy barriers to interoperation can both be addressed to some degree by use of a concept called "border directories." The border directory concept was originally developed by the Combined Communications Electronics Board (a working group of allied military communications experts) to solve the problem of securely making some directory information available to allies while maintaining other directory information strictly within the local directory.

The border directory concept involves placing an X.500 compliant directory outside the enterprise firewall. A subset of directory information (for example, perhaps only the CA certificates and CRLs) is exported from the internal directory system to the border, and is thereafter available through the network of chained X.500 border directories. Information from external PKI directories can be made available to relying parties using the "internal" enterprise directory by a number of mechanisms, including:

- "One way" knowledge references from the border directory into the local directory. This sort of relationship provides a kind of "data diode" that allows a flow of PKI information (certificates and CRLs) from the border directory into the local directory system, but not the other way around; and

- LDAP referrals, in which the local directory system refers clients to the chained border directory for information not available from the local directory system.

Smaller departments and agencies may not be able to deploy border directory systems, so it seems likely the Federal Bridge CA will, in addition to deploying a directory system agent for posting its own cross-certificates and CRLs, provide a "border directory service" for those departments and agencies not fielding their own border directory. Federal Departments and Agencies may use LDAP or X.500 protocols to transfer the data they wish to make available to the Federal Bridge CA system to the Bridge CA directory.

Directory interoperability, client capability limitations and CA interoperability are all significant challenges – but previous and ongoing technology demonstrations have shown that the technologies required to achieve multi-vendor, multi-PKI interoperability exist now, and that they do work.

Directory interoperability, client capability limitations and CA interoperability are all significant challenges – but previous and ongoing technology demonstrations have shown that the technologies required to achieve multi-vendor, multi-PKI interoperability exist now, and that they do work.

[13] X.500 also supports the notion of referrals.

As discussed in [CASL], the role of Certificate Policies (CPs) and Certification Practice Statements (CPSs) is not universally agreed. In addition, the notion of a PKI Disclosure Statement (PDS) has recently been introduced, and it may mean different things to different people as well. The purpose of this section is to discuss the various schools of thought regarding the role that these documents may have in relationship to achieving inter-domain interoperability.

4.1 Certificate Policy

As defined in X.509 [X509] and endorsed by RFC 2527, a Certificate Policy (CP) is defined as:

> "A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range."

Certificate policies are instrumental in forming the basis of interoperability between two or more PKI domains. Each CP will be associated with a unique identifier referred to as an Object Identifier (OID). Certificates, cross-certificates or any other vehicle for conveying certificate policy information will be populated with the appropriate OIDs so that end-entity certificates are used consistent with the applicable CP(s).

Certificate policies are instrumental in forming the basis of interoperability between two or more PKI domains.

4.2 Certification Practice Statement

As defined in [ABA] and endorsed by RFC 2527, a Certificate Policy (CP) is defined as:

> "A statement of the practices which a certification authority employs in issuing certificates."

As RFC 2527 points out, the 1995 draft of the ABA guidelines expands this definition as follows:

> "A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration.
>
> Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The certification authority's duties to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.
>
> Whether a certification practice statement is binding on a relying person depends on whether the relying person has knowledge or notice of the certification practice statement. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by

As defined in the ABA Guidelines, and endorsed by RFC 2527, a Certificate Policy (CP) is defined as:

"A statement of the practices which a certification authority employs in issuing certificates."

reference. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.

As much as possible, a certification practice statement should indicate any of the widely recognized standards to which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems."

Thus, a CPS is expected to address extremely detailed aspects associated with the operation of the CA or PKI. It is also expected that the CPS would be used as the basis of any third party audits that may be required in order to solidify an inter-domain interoperability arrangement.

4.3 PKI Disclosure Statement

A proposal for a model PKI Disclosure Statement (PDS) was submitted to the IETF as an Internet Draft in November 1999 [SSMB]. The purpose of a PDS is to provide more concise and user-friendly information regarding the "policies and practices employed by a CA/PKI". Essentially, it defines a model for representing subsets of information normally contained in a CP and/or CPS. In addition, the PDS may include pointers to the relevant portions of the CP and/or CPS. The idea behind the creation of a PDS is that it would serve as a more suitable basis to convey legal notice/disclosure to end-users (discussed further below). A good example of a PDS can be found at http://www.verisign.com/repository/disclosure.html.

The purpose of a PDS is to provide more concise and user-friendly information regarding the "policies and practices employed by a CA/PKI".

4.4 Relationship between CP, CPS and PDS

RFC 2527 describes the relationship between a CP and CPS for the Internet community as follows:

"A certification practice statement is a detailed statement by a certification authority as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life-cycle management of certificates, and more - a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

Although such detail may be indispensable for adequate disclosure, and for full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics, a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, multiple different CAs, with non-identical certification practice statements, may support the same certificate policy.

For example, the Federal Government might define a government-wide certificate policy for handling confidential human resources information. The certificate policy definition will be a broad statement of the general

characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate certification authorities with different certification practice statements might support this certificate policy. At the same time, such certification authorities may support other certificate policies.

The main difference between certificate policy and CPS can therefore be summarized as follows:

(a) Most organizations that operate public or inter-organizational certification authorities will document their own practices in CPSs or similar statements. The CPS is one of the organization's means of protecting itself and positioning its business relationships with subscribers and other entities.

(b) There is strong incentive, on the other hand, for a certificate policy to apply more broadly than to just a single organization. If a particular certificate policy is widely recognized and imitated, it has great potential as the basis of automated certificate acceptance in many systems, including unmanned systems and systems that are manned by people not independently empowered to determine the acceptability of different presented certificates."

Although it is implied that the CPS can be used as an agreement between a CA and a subscriber or that a CPS can be used as a vehicle for serving legal notice, many feel that a CPS is too voluminous and complex to be useful in this manner. As stated in Section 4.3, the purpose of a PDS is to provide more concise and user-friendly information regarding the "policies and practices employed by a CA/PKI" [SSMB]. Note that a PDS is not necessarily intended to eliminate the need for a CP and/or CPS, but it is intended to serve as a more useful vehicle for conveying the appropriate information to the end-user. Thus, the PDS may actually become the accepted basis for conveying legal notice and disclosure to end-users.

The role that each of these documents has (or should have) yields various schools of thought, as discussed in the following paragraphs.

Certainly in a service provider model, it is clear that the CPS is a publicly available document, and it serves (or attempts to serve) to convey responsibilities of the subscriber and to limit the liability on the CA.

In the enterprise context, the role of a CPS is not nearly as clear. There are organizations that use a CPS to document the operational aspects of their CA(s), but this document is not used as a basis for anything other than internal security audits. Specifically, the CPS would not be disclosed to the public, nor would it be disclosed in the context of an inter-domain interoperability arrangement with a partner or affiliate.

In addition, the use of a CPS to form the basis of an inter-domain interoperability arrangement (or more specifically, a cross-certification arrangement) is generally criticized from several perspectives. The first is that a CPS tends to be extremely detailed and voluminous, making a painstaking review of the CPS a tedious and labor intensive exercise. The second criticism is that terminology may differ from one domain to another, and what was thought to be an equivalent mapping might not be the same thing at all [PAG]. Third, the CPS may contain extremely sensitive information, and the organization may be unwilling to share the information contained with the CPS with anyone.

In a service provider model, it is clear that the CPS is a publicly available document, and it serves (or attempts to serve) to convey responsibilities of the subscriber and to limit the liability on the CA... In the enterprise context, the role of a CPS is not nearly as clear.

This tends to suggest that something other than a CPS needs to be used to form the basis of inter-domain interoperability arrangements when dealing with enterprise domains. In fact, there is a school of thought that suggests that the CP, not the CPS, should be used as the basis for inter-domain interoperability, especially in the specific case of cross-certification. However, the CP itself can be rather detailed (the distinction between what goes into a CP and what goes into a CPS isn't always clear to everyone). With the introduction of PDSs, some would suggest that this could form a suitable basis for inter-domain interoperability. Moreover, a recent proposal [TM] forwarded to the ABA as a contribution to the PKI Assessment Guidelines [PAG] suggests that a PDS is, in fact, a CP in accordance with the definition in X.509.

Yet another school of thought suggests that independent evaluation or audit of CAs/PKIs can be used as the basis for establishing inter-domain interoperability. Conceivably, this could be accomplished through mutual recognition of CA/PKI evaluation criteria (i.e., formal audits would be conducted against some set of internationally recognized criteria). This could also make sense in the case of cross-certification as well. Incurring a one-time (or periodic) fee for an independent and mutually recognized audit seems much more attractive than requiring individual reviews each time a new cross-certification arrangement is needed.

There is also at least one other school of thought, although it is unclear how many people actually subscribe to this position. Yet, it is interesting to note that some believe that most of the formalization of inter-domain interoperability procedures as discussed above is actually unnecessary. This centers around the question: "why can't I simply rely on my existing business relationships as a basis of interoperability?". In other words, organizations conduct business on a regular basis now so why does the introduction of PKI technology introduce this additional overhead/complexity. The tacit assumption here is that each business would be expected to operate as the other business dictates. But a business need not necessarily scrutinize the operational procedures of another as long as appropriate liability is assumed in the event of fraud or some other negative event due to negligence related to the operation of the PKI. Of course, this doesn't eliminate the need to agree on the certificate policies that would apply. Again, the use of a PDS to specify this level of agreement may be very attractive.

Arguably, each of the methods described above might form a suitable basis for establishing inter-domain interoperability in one context or another, regardless of which alternative is selected (e.g., cross-certification versus cross-recognition, etc.). More specific recommendations associated with the use and role of these documents are provided in Section 5.

It is interesting to note that some believe that most of the formalization of inter-domain interoperability procedures as discussed is actually unnecessary. This centers around the question: "Why can't I simply rely on my existing business relationships as a basis of interoperability?"

5 Summary and Recommendations

This report discusses a number of different options that can be used to facilitate inter-domain interoperability. The pros and cons of each are discussed. It has been noted that some of these alternatives are not necessarily mutually exclusive, and that there may not be one option that can be selected above all others in every conceivable set of circumstances.

In addition, a number of interoperability initiatives have been summarized. Some of these interoperability initiatives have adopted or are studying one or more of the options discussed in Section 2. While a number of interoperability issues have been discovered as a result of these activities, successful demonstrations have occurred, and overall the results are encouraging. Further, the ongoing cooperation within the PKI vendor community will help to ensure that interoperability issues will be discovered and resolved as expeditiously as possible in the future.

The role of documentation such as CP, CPS and PDS has also been discussed. Recommendations associated with these documents are included below.

The primary purpose of this paper is to explore the issues associated with achieving inter-domain interoperability and to provide a set of recommendations based on the resulting analysis. Based on the discussion provided within this paper, the following recommendations/observations are offered:

1. In general, a CPS does not form a suitable basis for forging inter-domain interoperability arrangements. However, there are likely to be exceptions to this. It may be appropriate to state that where resources allow (e.g., at the national government level) and circumstances warrant it may make sense to conduct a thorough evaluation based on a detailed CPS. However, this would only seem feasible in the case of large governments or corporations. In the absence of complete evaluations, the parties can enter into contractual agreements designed to mitigate any residual risk.

2. Independent trusted third party audits would appear to make sense for most of the inter-domain interoperability options described within this paper. A CPS may form a suitable basis for internal and third party audits. But it isn't clear if this is required in all cases, and it doesn't necessarily apply in all circumstances (e.g., to small companies that have deployed their own PKI, but can't afford the additional cost of an independent third party audit). Regardless, there are clearly circumstances where a more scalable, less intensive procedure to achieve inter-domain interoperability will be required.

3. In certain cases (e.g., Gatekeeper), the notion of an accreditation authority may be appropriate. For enterprise level interoperability, cross-certification (either bilateral or through a Bridge CA) would seem to be the most appropriate.

4. The use of a PDS to facilitate inter-domain interoperability appears to be attractive. It is recommended that this should be explored further by the PKI Forum Policy and Privacy sub-group.

5. An attempt to list and describe a generic set of steps/procedures that are required in order to facilitate inter-domain interoperability should be made. Note that certain aspects may differ with each methodology. Portions of the GOC PKI cross-certification methodology may serve as an appropriate baseline for this activity.

The ongoing cooperation within the PKI vendor community will help to ensure that interoperability issues will be discovered and resolved as expeditiously as possible in the future.

The primary purpose of this paper is to explore the issues associated with achieving inter-domain interoperability and to provide a set of recommendations based on the resulting analysis.

6. Given that standards are clearly not sufficient to guarantee multi-vendor interoperability, it is recommended that implementation agreements or profiles should be developed. It may be necessary to develop more than one (e.g., profiles may be required based on industry vertical and/or "type" of PKI). It is recommended that the PKI Forum explore this issue and determine if it should undertake the development of these profiles.

7. It is recommended that the PKI Forum Policy and Privacy subgroup coordinate with the appropriate organizations and/or industry initiatives in order to ensure legal/policy-related issues associated with multi-domain/ multi-jurisdictional interoperability are being addressed appropriately. This activity should be pursued in cooperation with the PKI Forum's Technology Working Group.

8. Processing requirements in association with certificate path construction and validation must be clearly identified. At least a portion of this should be addressed as part of the PKI Forum Certificate Path Construction white paper.

9. It is recommended that issues associated with the use of LDAP repositories identified within this report be included in the PKI Forum's Technology Working Group LDAP white paper activity.

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to under-stand and exploit the value of PKI in their e-business applications.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810

A. References

[ABA] Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, American Bar Association, 1995

[AC] Impact on E-Sign Legislation, PKI Forum contribution by A. Carlson (Preston|Gates) [PKI Forum members can retrieve this document from www.pkiforum.org/members_only/bwg/e-signDRAFT.pdf]

[APEC] Achieving PKI Interoperability, Technical Contribution to the APEC TEL WG, undated

[CASL] Understanding Public Key Infrastructure: Concepts, Standards and Deployment Considerations, C. Adams and S. Lloyd, 1999, ISBN 1-57870-166-X

[CESG1] Interoperability Testing Between Commercial PKI Products, Issue 1.E, CESG, 15 March 2000

[CESG2] CLOUD COVER PKI Implementor's Guide, Issue 0.A, CESG, 12 March 2000

[GAC] Gatekeeper Certificate Management Infrastructure Gatekeeper Accreditation Certificate Concept of Operations, Department of Communications Information Technology and the Arts, Version 0.9.1a, 6 October 2000

[GKPR] Gatekeeper: A strategy for public key technology use in the Government, Australian Office of Government Information Technology, 6 May 1998

[GOC] Government of Canada Public-Key Infrastructure Cross-Certification Methodology and Criteria, Draft Version dated April 2000

[PAG] PKI Assessment Guidelines, American Bar Association Information Security Committee, Version 0.14 dated May 4, 2000 (Distribution Restricted)

[SL] PKI Interoperability Framework,submitted by S. Lloyd, Version 1.4, March 2001. [SSMB]
Internet X.509 Public Key Infrastructure PKI Disclosure Statement, S. Santesson and M. Baum, IETF Internet Draft dated November 10, 1999

[TM] PKI Disclosure Statement, Contribution to ABA for consideration in PKI Assessment Guidelines submitted by T. Moses, undated (circa June 2000)

[UR] Discussion Paper: Gatekeeper Accreditation Certificate, Gatekeeper Contribution by U. Rockmann, 17 March 2000

[X509] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Joint Recommendation|Standard ITU-T X.509 and ISO/IEC 9594-8, 2000

B. Terminology

The following terms are defined and used within the context of this paper. They are provided here for ease of reference.

Bilateral cross-certification - used to establish a peer relationship between two CAs – each CA issues a public key certificate (referred to as a cross-certificate) for the other CA – may be used in both an intra- and inter-domain context.

Bridge CA - a component that facilitates or brokers trust relationships between multiple PKI domains.

Distributed Trust Model - a mutual trust relationship established between two or more otherwise isolated CAs or PKI domains.

PKI Domain - an autonomous collection of components (including one or more CAs, zero or more RAs, a collection of PKI-enabled end-entities, etc.) that operate under one or more certificate policy(ies) as specified by the governing body associated with that domain (e.g., a Policy Management Authority). In the context of this paper, a PKI domain is usually associated with a given enterprise or organization.

Strict Hierarchy - an "inverted tree" of CAs where all trust emanates from a single "root" CA.

Unilateral cross-certification - generally used to establish a superior/subordinate relationship where the superior CA issues a public key certificate to the subordinate CA, but not vice versa. This can be contrasted to bilateral cross-certification (see definition above).

C. Table 1. Summary Comparison

Approach	Relative Strengths/Advantages	Potential Disadvantages/Unknowns
Cross certification (Inter-domain only)	Effect of compromise is limited to EEs subordinate to the compromised CA. EEs can trust a local (well-known) CA. Trusted point rollover affects only local EEs. Certification paths are short between local users. Revocation of single trusted point is straightforward.	Certification paths can be very long between distant EEs. Revocation of multiple trusted points (if applicable) must be supported. Path construction may be complex - must be able to navigate multiple paths and find a path (not necessarily the optimal one) linking sender to relying party's trust point. Level of flexibility required for path construction and validation is not currently supported in all client products. Need access to revocation information from the cross-certified domain (implies repository connectivity or import of CRLs from other domain).
Bridge CA	No single point of failure. Bridge can enforce PAA policy on cross-certification. Amount of overhead normally associated with standard cross-certification can be reduced significantly.	Significant policy negotiation can be required for multiple cross certifications (although this can be reduced by appropriate PAA policy framework). Vulnerabilities can be introduced because of unintended trust paths (although this can be reduced by appropriate PAA policy framework and implementation of appropriate business controls). Conveyance of revocation can be complex (although it can be simplified as revocation information is held at the bridge. Must be able to navigate multiple paths through the PKI and find a path (not necessarily the optimal one) linking sender to relying party's trust point via the Bridge. Level of flexibility required for path construction and validation is not currently supported in all client products.
Cross-Recognition	Cross-certification agreements are not required.	Relying party expected to make trust decisions. Likely insufficient mechanism for high assurance transactions. If remote trust gained through licensing regime, presumably revocation of trust must be achieved through similar means. Criteria for establishing cross-recognition not universally agreed at present. Method to convey necessary information to relying party not yet defined.
Certificate Trust Lists	No single point of failure. Issuer of CTL can produce ARL to revoke a trusted CA, or can issue new CTL with revoked CA omitted.	Path needs to be established between sender and a CA in CTL. Similar processing requirements to other systems though greater choice of final trust point which may make paths quicker to find. There is some (yet to be quantified) level of system management workload associated with the management of multiple trust points. Client must trust issuer of CTL. Not clear how client obtains CTL. Level of support in products unclear.
Accreditation Certificate	Accreditation authority approach affords more autonomy to the accredited CAs than a rooted approach. Compromise of accreditation authority not as devastating as compromise of a root CA.	Compromise of accreditation authority negates previously established trust relationships. Roll-over of accreditation authority certificate affects all end-entities. Client needs to trace path to trust point, and then check if this trust point is accredited (presumably underlying PKI could still be a mesh). Path processing requirements thus similar to other trust models. Method to convey accreditation certificate to end-entities needs to be established. Accreditation criteria may be unique to a specific domain or set of domains.
Strict Hierarchy	Root can enforce adherence to a certificate policy by subordinate CAs. Within the confines of a rooted hierarchy, certification paths between remote EEs tend to be relatively short since it only needs to be traced back to the root. Allows inter-domain cross-certification with other jurisdictions to be controlled at a senior level. Path processing more straightforward than other models with better support in existing client products.	Root key compromise is catastrophic, affecting entire infrastructure – this is a single point of failure. Requires end-entities to ultimately trust a remote root authority. Trust point roll-over or revocation affects entire PKI domain. Cannot accommodate interoperability between isolated PKI domains (i.e., there is no single root CA that applies to every PKI domain).
Delegated Path Discovery and Validation	Burden of path discovery and validation can be removed from client, needs only to trust the trusted third-party.	Performance may be an issue - trade-off between how often to consult trusted third-party and how long to cache previous responses requires further study. Compromise of trusted third party affects all relying parties that depend on that third party. Back-end infrastructure unspecified – level of complexity unclear.