WHITE PAPER

March 2001

PKI Interoperability Framework

The purpose of this PKI Forum White Paper is to define interoperability from the perspective of the PKI Forum, and to develop a framework that can be used to discuss the many facets of interoperability in an appropriate context using consistent terminology.

1 Introduction

1.1 Background and Scope

Interoperability — or more specifically, multi-vendor interoperability — is viewed by customers and industry analysts alike as a critically important issue for Public-Key Infrastructure (PKI). Interoperability helps to support transactions between parties that do not use technology supplied by the same vendors, offers greater flexibility and freedom of choice between vendors, and lowers the risk of deploying a PKI-based solution. To some, lack of interoperability is perceived as the leading barrier to wide-scale deployment of PKIs. Indeed, one of the fundamental reasons for the formation of the PKI Forum in December 1999 was to identify and resolve existing barriers to multi-vendor interoperability.

2 Interoperability Defined

Multi-vendor interoperability is a critical issue for PKI. But what does "interoperability" really mean?

In many cases, interoperability is used to describe the ability for one application to communicate seamlessly with another. Other aspects of interoperability include the ability to mix and match various PKI components from one vendor with those of another. Interoperability can also refer to the interaction between one enterprise domain and another (e.g., in order to conduct secure business-to-business transactions).

In summary, it is fair to say that PKI interoperability can mean different things to different people. Therefore, the purpose of this section is to define a generic framework for discussing interoperability issues.

Acknowledgements

PKI Interoperability Framework White Paper 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 review.

Editor:

Steven Lloyd
Entrust

Contributors:

Derek Brink
RSA Security

Andrew Nash
RSA Security

Gordon Buhle
Oracle

Nada Kapidzic Cicovic
Entegrity

Special thanks to Tim Polk, NIST, whose interoperability presentation during the PKI Forum meeting in Foster City, CA, March, 2000, inspired this document.

Contents

PKI forum

2.1 Interoperability Framework

At its highest level, interoperability is a broad topic that covers technology, business and (sometimes) legal issues. One can think of interoperability as a jigsaw puzzle comprised of several integral pieces, each of which may, in turn, be comprised of smaller pieces.

The PKI interoperability framework adopted by the PKI Forum is based on a presentation offered by Tim Polk of NIST at the first PKI Forum Members Meeting in Foster City, CA, USA on 6-8 March 2000, in which he identified three major interoperability areas as follows:

1. Component-Level Interoperability;
2. Application-Level Interoperability; and
3. Inter-Domain Interoperability.

Using the jigsaw puzzle analogy, these three areas can be considered as the three major pieces of the PKI interoperability puzzle, with each major piece consisting of several smaller pieces. Each of these three interoperability areas is discussed further in the subsections that follow. Note that it is assumed throughout this discussion that any vendor-specific dependencies that might have an impact on interoperability are to be avoided.

One can think of interoperability as a jigsaw puzzle comprised of several integral pieces, each of which may, in turn, be comprised of smaller pieces.

2.1.1 Component-Level Interoperability

As illustrated in Figure 1 (see next page), component-level interoperability deals with interaction between systems directly supporting and/or consuming PKI-related services. For the sake of simplicity, we are only considering intra-domain[3] interoperability here, as the typically more complex issues associated with inter-domain interoperability are addressed in Section 2.1.3. Note that Figure 1 allows for the possibility of more than one Certification Authority (CA) that would represent, in this context, intra-domain relationships (e.g., peer-level trust relationships or superior/subordinate trust relationships[4]).

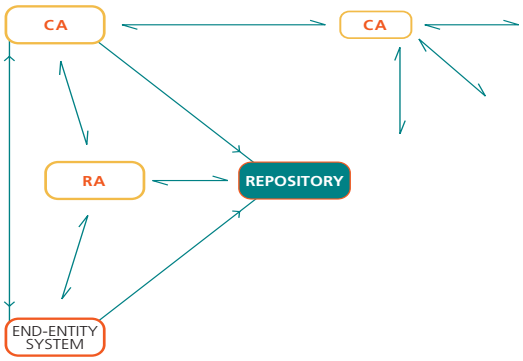


Figure 1.

Component-Level Interoperability

[3] "Intra-domain" interoperability refers to interoperability between components that belong to the same enterprise or fall under the control of a common administrative authority. This can be contrasted to "inter-domain" interoperability as discussed in Section 2.1.3.

[4] The meaning of "trust" or "trust relationship" is 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.

Component-level interoperability includes the following considerations:

1. Common protocols, message formats, and certificate formats must be implemented between applicable PKI components – this applies to CA-CA, CA-RA, End-Entity System[3]-CA, and End-Entity System-RA interaction;
2. Common algorithms must be implemented for entity authentication and the protection of the data exchanged between PKI components;
3. A method to facilitate the storage and retrieval of certificates and certificate status information between the Repository[4] and the PKI components must be supported (this includes the protocol(s) and any underlying authentication scheme(s));
4. Private keys must be accessible by authorized End-Entities in a secure manner regardless of storage method (e.g., software, smart card, or hardware token); and
5. One or more certificate status mechanisms must be supported.

Component-level interoperability deals with interaction between systems directly supporting and/or consuming PKI-related services.

In some cases, a standard cryptographic interface in support of a hardware security module at the CA may also be required (as dictated by local policy).

2.1.2 Application-Level Interoperability

The traditional notion of application-level interoperability is concerned with compatibility between two peers, regardless of the supplier of the application or any ancillary infrastructure components used to support the application. For example, two S/MIME-based e-mail clients must be capable of interoperating with one another, even when the application software is supplied by two different vendors, the applications run on two different platforms, and each S/MIME client uses PKI technology supplied by different vendors.

Note that the term "application" is not meant to limit this category of interoperability to the Application Layer as traditionally defined for a network architecture. For example, IPsec is considered to be an application in this context. Figure 2 helps to illustrate what is meant by Application-Level Interoperability. In addition to the issues discussed in Section 2.1.1, application-level interoperability includes the following considerations:

1. Certificate and certificate status information must be compatible (at least to the extent that any incompatibilities will not affect interoperability);
2. Business controls must be implemented to ensure certificates are being used consistent with intended key usage and any associated constraints;
3. Algorithms (including cryptographic algorithms and key sizes) must be compatible;
4. Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible;

Another aspect of application-level interoperability involves support for multiple applications from different vendors on the same end-system.

[3] We use "End-Entity" to denote a user, process or device that is enrolled into the PKI and consumes the services enabled by the PKI. The "System" is the combination of hardware and software that is used to support the End-Entity.

[4] The generic term "Repository" is meant to represent any remote storage facility where PKI-related information can be stored and easily retrieved. Examples of repositories include Web servers, FTP servers, LDAP-compliant repositories and X.500 Directory System Agents (DSAs).

5. Underlying communications protocols used to exchange information between peers must be compatible; and
6. Any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible.

Another aspect of application-level interoperability involves support for multiple applications from different vendors on the same end-system. This requires (often simultaneous) access to the same PKI credentials (i.e., private keys and public-key certificates). The PKI Forum is addressing this issue as part of the Token Interoperability and Portability project.

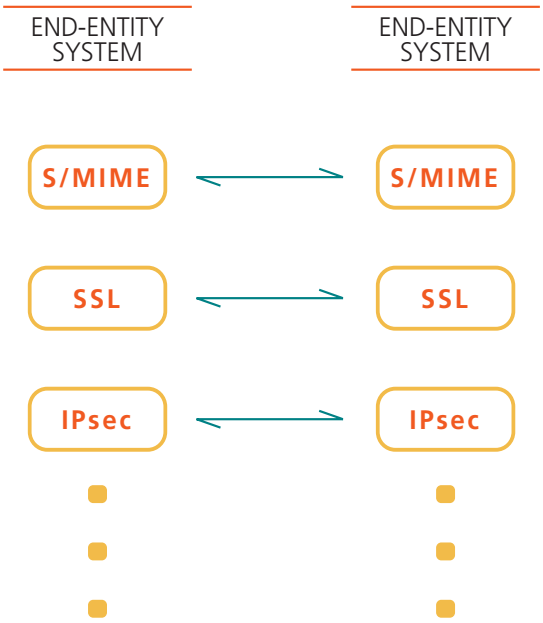


Figure 2.
Application-Level Interoperability

2.1.3 Inter-Domain Interoperability

Inter-domain interoperability deals with the issues and options associated with achieving interoperability between two otherwise isolated PKI domains[5]. This is in contrast to the interoperability issues encountered within the same PKI domain as discussed in Section 2.1.1.

Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the cooperation of multiple administrative domains.

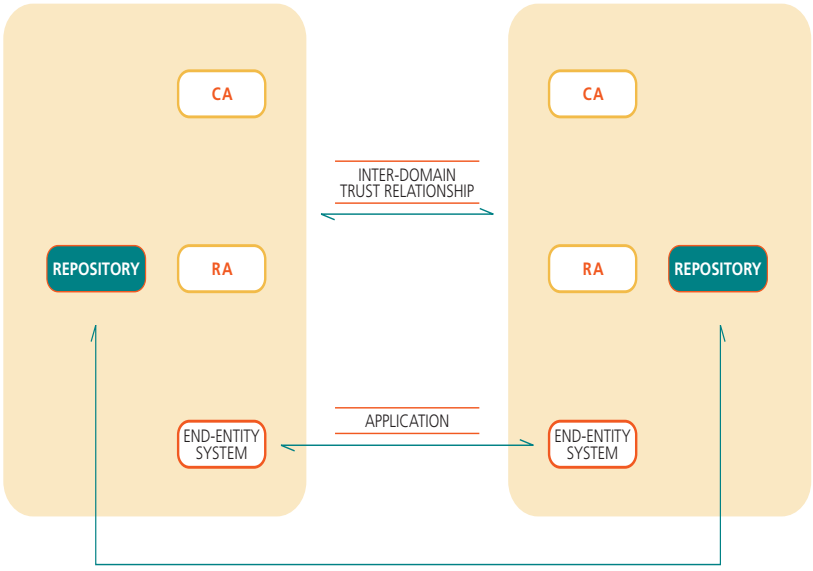
Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the cooperation of multiple administrative domains. Figure 3 (below) helps to illustrate what we mean by inter-domain interoperability. Note that the bi-directional arrow between Repositories does not imply that the internal Repository of one enterprise must be able to communicate directly with an internal Repository of the other enterprise (although this might be a desirable option in some cases). Rather, it represents the requirement to exchange PKI-related information between the

[5] 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 essentially constitutes interoperability between two enterprises.

two PKI domains (which can be accomplished in a variety of ways). Also note that the bi-directional arrow between the two domain boundaries can be facilitated in a number of ways, as discussed in the PKI Forum's CA-CA Interoperability White Paper, March 2001.

Figure 3.

Inter-Domain Interoperability



Inter-domain interoperability involves a number of challenges, both technology- and policy-related. All of the considerations outlined under section 2.1.2 necessary to facilitate application-level interoperability also apply here (i.e., it is assumed that the rationale for establishing the trust relationship is based on the need to support one or more applications between domains). In addition, the following issues must also be addressed:

1. A method for establishing trust relationships between the PKI domains is required (see the PKI Forum's CA-CA Interoperability White Paper, March 2001 for a discussion of options);
2. Appropriate PKI-related information in one domain must be made available to the other, and vice versa (as applicable based on the associated trust relationship); and
3. Each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed-upon policies.

3 Summary and Conclusions

Multi-vendor interoperability is an important consideration in virtually any technology area. This paper describes the framework adopted by the PKI Forum that will be used as the basis for discussing and addressing the interoperability issues specifically related to PKI technology in an easier, more consistent manner. Table 1 (see following page) summarizes the technical aspects that apply to each of the interoperability areas as discussed within this paper.

Figure 3.

Table 1: Summary of Interoperability issues

TECHNICAL ISSUE	COMPONENT-LEVEL INTEROPERABILITY	APPLICATION-LEVEL INTEROPERABILITY	INTER-DOMAIN INTEROPERABILITY
Common protocols, message formats, and certificate formats must be implemented between applicable PKI components.	✓	✓	✓
Common algorithms must be implemented for entity authentication and the protection of the exchanged data between PKI components.	✓	✓	✓
Protocols and underlying authentication schemes must be supported to facilitate the storage and retrieval of certificates and certificate status information between the Repository and the PKI components.	✓	✓	✓
Private keys must be accessible by authorized end-entities in a secure manner regardless of storage method (e.g., software, smart card, or hardware token).	✓	✓	✓
One or more certificate status mechanisms must be supported.	✓	✓	✓
Certificate and certificate status information must be compatible (at least to the extent that any incompatibilities will not impact interoperability).		✓	✓
Business controls must be implemented to ensure certificates are being used consistent with intended key usage and any associated constraints.		✓	✓
Algorithms (including cryptographic algorithms and key sizes) must be compatible.		✓	✓
Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible.		✓	✓
Underlying communications protocols used to exchange information between peers must be compatible.		✓	✓
Any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible.		✓	✓
A method for establishing trust relationships between the PKI domains is required.			✓
Appropriate PKI-related information in one domain must be made available to the other.			✓
Each PKI domain must agree to adhere to certain policies and mechanisms should be in place to enforce adherence to the agreed-upon policies.			✓

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