

PKI policy white paper

Published: July 2001

Table of contents

Policy in the traditional business environment	3
Policy in PKI	4
PKI Policy: The parties involved	5
PKI Policy: Certificate policy	5
PKI Policy: Certification practice statement	6
Certificate Policy—What is specified?	6
Supporting a CP with other documents	7
How policy is managed: Enterprise vs. trading partners vs. community of interest	7
Other PKI policy issues	8
Specific references included in this policy note.....	9

PKI policy white paper

By John T. Sabo and Yuriy A. Dzambasow

This PKI note provides general information about PKI policy, the role that policy plays in a PKI and how that policy applies to both traditional and PKI-enabled business environments. It also addresses the documentation required to support a PKI policy, what is specified in a PKI policy, and how a PKI policy can be managed, and it outlines some high level issues regarding PKI policy.

It is not intended to provide a detailed technical discussion of policy issues in PKI. The content of and approach to forming PKI policy is an evolving discipline, and there is much ongoing debate about it, especially as large PKI-based trust infrastructures begin to emerge. As a result, this paper is a positioning document rather than a definitive statement for policy makers.

ABOUT THE PKI FORUM

This document was made available to TechRepublic from [The PKI Forum](#), an international, not-for-profit, multi-vendor and end-user alliance. Its 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 understand and exploit the value of PKI in their e-business applications. This white paper is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance, and editorial reviews.

Policy in the traditional business environment

In the traditional world, the individual moves through differing process and policy environments in which varying policies govern their interactions with others. As one example, governments face the problem of enabling and managing cross-border travel and immigration. To address such requirements, government law and/or policy typically requires citizens crossing national boundaries to possess passports that establish citizenship and identity. A passport links or "binds" some information about the individual (photograph, height, weight, age) to a specially designed physical document having a unique issuing authority and control number.

The passport issuing authority follows policies for issuing passports. These policies may require that the individual seeking a passport appear in person at a designated office, complete a paper application, present several forms of identification, provide photographs, physically sign an affirmation with a pen-and-ink signature, and wait while all of this information is reviewed and verified. After a series of processes and controls (all set by policy) have been carried out, the individual will receive the passport—in a manner meeting policy requirements (in-person or by mail). Policies may control more than simply issuing a passport. Subsequently, the individual receiving the passport may have responsibilities to safeguard the passport, report its loss, make proper use of it, etc. Countries where the passport is presented have their own policies governing its acceptance and may require further documentation before authorizing entry, in the form of a visa. Additionally, the issuing country has a method of revoking or withdrawing a passport when necessary—and passports have built-in expiration dates to allow for change in both the passport holder and the policies of the issuing authority.

There are sets of policies at work in this example, some dictated by law and some by custom and tradition. Within each set—for example the issuing country's identification requirements—policies have been established to provide a certain level of risk management (in this case that the holder is properly entitled to the rights of citizenship whether at home or abroad).

At some point, however, the policies of the issuing authorities and those accepting the passport intersect. For example, a particular country's immigration authority may not merely accept the passport at face value but may conduct an online database check at the border. Others may not.

Policies and processes are also at work in nongovernmental environments, where identity credentials are issued by trusted third parties, such as financial institutions or commercial entities established specifically to facilitate trusted relationships, such as through value-added networks. It is also interesting that different policy jurisdictions are brought together as expedients in the realm of commerce.

For example, some merchants when cashing customer checks require presentation of a credit card as additional proof, on the assumption that the issuer of the credit card has verified and vouches for the financial identity of the card holder, even though there is no direct policy (or even contractual) connection from one realm to the other. In fact, we see widespread integration of private and public sector trust policies in traditional business environments, something to keep in mind as we explore PKI policy issues.

Policy in PKI

Why must PKI place such importance on policy? PKI is most often discussed purely in terms of its component technologies (the use of public key cryptography and underlying systems to enable digital signatures, strong authentication, data integrity, nonrepudiation, and confidentiality).

However, those supporting technologies require an infrastructure (the I in PKI), and that infrastructure encompasses much more than cryptographic technology and protocols. It includes the policies governing the use of PKI, the risk management controls and business processes needed to enable PKI-supported systems and the applications that serve the newly emerging digital analogues replacing and extending our traditional business, government, and interpersonal transactional relationships. In the realm of PKI, we generate a pair of mathematically related public and private keys.

While the private key is carefully safeguarded, the public key is linked to subject identifier information (e.g., name and other information) in a digitally signed public key certificate, where the subject is the owner of the public/private key pair. This linkage or “binding” is made possible by including specified data in the certificate, which is essentially a specially formatted file generated in accordance with industry standards.

The certificate itself and the public and private keys will then be used in systems and processes to represent the individual or entity that is the “subject” identified by the certificate. In some cases, they will be used in the process of creating and verifying digital signatures. Therefore, it is critical for a relying party application (i.e., an application that relies on the use of a certificate) to have confidence that the certificate correctly and accurately identifies the subject and subject’s public key, as well as the issuer of the certificate.

The distinguishing feature of PKI is the use of the certificate published by a Certification Authority to confirm the identity and other relevant information about the entity that holds the certificate. It is critical for a ‘relying party,’ that is, an application or another person who relies on the certificate, to be able to have confidence that the certificate correctly and accurately identifies the subject, the subject’s key, and the credentials of the issuer of the certificate.

The public key is linked to subject identifier information (e.g., name and other information) in a digitally signed public key certificate, where the subject is the owner of the public/private key pair.

Given the importance of correctly establishing the strong linkage of a private/public key pair to a subject, and in some cases warranting the ‘binding’, policies must be established. These policies must define the level of trust that can be placed in a certificate when it is presented to a relying party-application (e.g., Web server)—a level of trust that will be related directly to the assurances provided in the overall certificate issuance and management process. Policies must also define the rules and liabilities of the parties involved in issuing, managing, and processing certificates. The role of policy in PKI is critical, as it defines the level of risk for relying party applications in a given community of interest.

However, PKI policies are in no way mysterious. They, in fact, are directly related to trust policies already in place in the traditional world (and often taken for granted because they are so common and so integral to our traditional way of conducting business).

PKI Policy: The parties involved

In PKI-supported environments, PKI implementations reflect policy requirements tailored to the new world of network and integrated, high-velocity trust applications. As with the traditional business models, there are multiple parties, multiple interests, and multiple policy issues.

There are multiple parties directly involved in achieving the appropriate level of trust with respect to the creation and use of public key certificates, including:

- The individual or entity identified by the certificate (Subject or Subscriber).
- The issuer of the certificate, which includes identification and authentication of subject information contained in the certificate (Certification Authority/Registration Authority).
- The entity that provides certificate validation services in certain implementations (Validation Authority).
- The company, agency, or individual relying on the certificate (Relying Party).

At a minimum, three of the parties identified above are required to support a PKI policy: Certification Authority, Subject (or Subscriber), and Relying Party.

From this point forward, the term Subscriber will be used instead of Subject, as the term Subscriber is accepted in the legal and policy community. To assist the Certification Authority, a Registration Authority and Validation Authority may be deployed to perform subject registration and certificate validation functions, respectively. In either case, the responsibilities and liabilities of these parties are expressed in the PKI policy, and specifically, in a Certificate Policy

PKI Policy: Certificate policy

As a practical matter, it is the Relying Party who “creates value” by making use of the certificate, and so the Relying Party has considerable interest in the policy supporting the creation and use of the certificate. The policy is the principal vehicle for establishing whether a certificate is fit for the purpose for which it is presented.

It is critical for a ‘relying party’, that is, an application or another person who relies on the certificate, to be able to have confidence that the certificate correctly and accurately identifies the subject, the subject’s key, and the credentials of the issuer of the certificate.

A Relying Party, such as a governmental agency or a financial institution, accepts public key certificates in conducting transactions for such things as authenticating customers or accepting digital signatures. They do so in accordance with laws, regulations, generally accepted practices, audit requirements, and custom. As the value and/or sensitivity of the transaction increases, the strength of the underlying policy becomes more critical. These requirements will vary depending on the purpose for which the certificate is presented.

For example, a health care provider may establish policies regarding the issuance and management of certificates provided to physicians. Those requirements will differ greatly from requirements for issuing certificates to employees who do not prescribe controlled substances. Business uses for the certificates will vary, and in turn, the risk associated with their use must be addressed by the appropriate set of policy requirements.

Certification Authorities (CAs) play a major role in establishing Certificate Policies. For example, a CA may work with a group of companies or an industry in creating a certificate policy accepted as appropriate for use in that sector, and Relying Parties may simply write their individual policies to reflect this model. In other situations, CAs may have to set de facto policy. For example, the issuers of certificates used to authenticate Web sites using Secure Sockets Layer (SSL) may have established the policies and processes by which they will authenticate Web servers. In doing this, they may require letters of

incorporation or other formal documentation before issuing a server certificate. Relying parties, whether individuals or employees accessing Web servers they list, trust that the Web site actually belongs to that company but do not have oversight of the policies by which those certificates were issued or managed.

The set of policy requirements governing the creation and use of public key certificates is known as a Certificate Policy (CP), and a guideline which defines certificate policy has been established by the Internet Engineering Task Force: the “Certificate Policy and Certification Practices Framework” (also referred to as the IETF Framework). By IETF Framework definition, a certificate policy is “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.”

Once established, a CA can identify a policy, including qualifying information about the policy, in a certificate. By doing so, the CA is declaring the intended use of the certificate to a relying party who may process the certificate. Similarly, a relying party can simply look for the appropriate policy identifier information in a certificate to assist in processing certificates that are acceptable to that relying party.

PKI Policy: Certification practice statement

The IETF Framework defines the Certification Practice Statement as the “statement of practices which a certification authority employs in issuing certificates.”

A Certification Practice Statement is often confused with a Certificate Policy but in fact reflects a Certification Authority’s statement of practices which should establish conformance with relevant requirements of one or more Certificate Policies or enable relying parties and subscribers generally to assess the level of trust they may have in the CA and the certificates it issues. Generally, it is understood that a CPS contains much greater detail than a Certificate Policy and may in fact be used to support multiple CPs. In simple terms, one should view the Certificate Policy as the “what I need to do” document, and the Certification Practice Statement as the “how I need to do it” document.

Not all CAs publish Certification Practice Statements. In some situations, a Relying Party may also operate its own Certification Authority, in which case the Certificate Policy itself may embody both the rules related to the applicability of a certificate and reference the practices by which the rules are observed. For example, a government agency may publish a Certificate Policy, and its data center may manage the CA/RA operation within existing security and operational controls. These may be referenced in the policy itself but not separately published as a Certification Practice Statement.

By IETF Framework definition, a certificate policy is “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.” In simple terms, one should view the certificate policy as the “what I need to do” document and the certification practice statement as the “how I need to do it” document.

Certificate Policy—What is specified?

Certificate Policies are understood to encompass a range of specifications, including business, legal, and technical elements. In order to bring order to what could be an unmanageably large amount of information, the IETF Framework specifies the contents of certificate policies and provides a structure for their expression.

The Framework includes a large number of general policy and legal topics, such as the applications for which the certificates may be used; statements of liability, warranties, and liability limits; specific obligations of the parties; fees; and audit requirements. It includes detailed policy and procedural requirements for the identification and authentication of subscribers. It specifies a number of operational requirements for CAs and RAs, such as processes to be followed in issuing certificates and revocation procedures. The Framework also provides sections outlining detailed physical, procedural, and technical security controls needed to provide the desired level of trust in the certificate issuance and management process. Finally, the Framework specifies the format or profile of the actual certificate, including the

technical data elements that will be encoded into the certificate. This includes the actual certificate policy Object Identifier (OID) that, once registered, will uniquely identify the certificate policy and allow parties to access and read the policy.

Building Certificate Policies in accordance with the IETF Framework standard has an additional value. Registering policies that map to the Framework can simplify the development of “machine-readable” policy digests such as the proposed PKI Disclosure Statement and can facilitate the review and evaluation of policies by users of PKI, including relying parties, subscribers, CAs, and other parties.

Supporting a CP with other documents

A CP alone may not be legally binding depending on the event in question. Agreements such as Subscriber Agreements, Relying Party Agreements, Privacy Notices, etc. are also required to establish and maintain a complete infrastructure.

This is because the PKI policy has little value without explicit linkages to the existing legal, regulatory, and business policy infrastructure, which supports business and government transactions and other applications. For example, a policy may require a Subscriber to accept certain responsibilities with respect to the use of the certificate or with respect to the protection of the private key corresponding to the public key contained in the certificate. Although “policy” may state the requirements, enforcement of these policy conditions may in turn require the establishment of a legally binding contract between the CA and the Subscriber. Such a “Subscriber Agreement” may be necessary both to establish subscriber obligations as well as to establish an enforcement mechanism in the event those obligations are breached. Obviously, the liability of the subscriber would be established in part as a result of this agreement.

In order to bring order to what could be an unmanageably large amount of information, the IETF Framework specifies the contents of certificate policies and provides a structure for their expression.

Likewise, other parties in the PKI may be bound together by agreements and other forms of contract, thus establishing a legal basis for their obligations and any liability in the use of the PKI. For example, the Relying Party Agreement may specify a limit on the value of a transaction or the type of transaction for which the Relying Party will use a particular certificate. The Privacy Notice will specify the privacy policies observed by the CA, which in certain international jurisdictions, for example European Union countries or Canada, will be enforceable under law. Three basic PKI models:

1. Enterprise Model, used to issue certificates that are used solely within the enterprise
2. Trading Model, used to issue certificates to trading partner organizations that have a requirement to do business with the certificate issuing organization
3. Community of Interest Model, used to issue certificates that are used by Authorized Relying Parties (ARPs) within a large community of interest

How policy is managed: Enterprise vs. trading partners vs. community of interest

As noted in the above discussion, PKI reflects and supports existing business and governance models. We see three basic models for how policy can be managed. The first is an enterprise model. In this model, a PKI is used to issue certificates that are used solely within the enterprise (e.g., a corporation). An example of this is certificate issuance to employees to control access to corporate resources.

The second model is a Trading Partner model. In this model, a PKI is used to issue certificates to trading partner organizations that have a requirement to do business with the certificate issuing organization. An example of this is a wholesale electronic parts exchange PKI used by a limited set of business partners.

The third model is a Community of Interest (COI) model. In this model, a PKI is used to issue certificates that are used by Authorized Relying Parties (ARPs) within a large community of interest (e.g., healthcare, financial services). Examples of this include efforts such as GSA Access Certificate for Electronic Services (ACES), Identrus, American Bankers Association (ABA) TrustID, and products like Electronic ID Cards issued by The Finnish Population Register Centre and the Swedish Post.

In the extended world of e-commerce and e-business, either the Trading Partner or COI model needs to be used. In the Trading Partner model, disparate PKIs must determine a way to interact to allow business transactions to flow between various Trading Partner domains.

For example, Ford Motor Co., General Motors Corp., and Chrysler Corp. may each deploy a PKI that issues certificates to their trading partners. But these trading partners do business with all three of the manufacturers: Ford, GM, and Chrysler. Therefore, the trading partners must either obtain a certificate from each issuer (Ford, GM, and Chrysler), or a solution must be developed where Chrysler accepts a certificate issued by Ford. To date, the commonly accepted approach is for a relying party to trust multiple certificate issuers.

However, initiatives such as the U.S. Federal Bridge CA effort provide an alternative to trusting multiple certificate issuers. In this model, a Bridge is established to govern and cross-certify individual Root CAs used to issue certificates within their PKIs. This mechanism allows certificates issued by one organization to be used by other organizations for applications requiring equivalent levels of trust. Such cross-certification can also be done bi-laterally between any two organizations (e.g., Ford and Chrysler). One CA may choose to cross-certify with another when both CAs deem it in their interest to enable use of certificates across PKI boundaries. However, this poses an N^2 problem on certificate issuing organizations as the number of bi-lateral agreements increase over time.

In the COI model, a certificate issuer or set of certificate issuers are trusted by Authorized Relying Parties (ARPs) to issue certificates to subscribers within a given community. This is accomplished through the establishment of a common Certificate Policy (CP) and a contract infrastructure. The common CP and contract infrastructure define the rules (typically set by the ARPs, since they take on the most liability in accepting certificates) that bind all parties together: CA, Subscriber, and Relying Party. This model is very effective as it eases the decision making process on Relying Parties. However, creation of a common CP and contract infrastructure takes time and requires a consolidated effort of the part of the Relying Parties that make up the COI.

Implementers of PKI need to assess their policy requirements before selecting the appropriate model, as all have advantages and disadvantages. The pure enterprise model offers, among other things, simplified policy and technical manageability for those within the enterprise. But from a practical perspective, it will not always accommodate the various business and policy requirements demanded by the real-world institutions and individuals.

Other PKI policy issues

There are a large number of PKI policy issues being addressed today, and it is likely the number of issues will grow as PKI becomes widely adopted for more and more business and government applications and as these applications and supporting PKIs increasingly interact.

For example, a long-standing issue is the liability exposure for certificate authorities in instances where, despite the presence of policies limiting use of a certificate to a certain class of relying parties, a business or individual outside that class accepts and processes a certificate without authorization to do so. This issue has concerned some governments as well, who worry that government-issued certificates will become de facto requirements for nongovernmental business. As the format of certificates is based on IETF PKIX standards, and as we increasingly achieve PKI interoperability at the technical level, there may be no sure means to prevent improper reliance on a certificate. From a legal perspective, the use of disclaimers and limits on reliance and liability in a CP may not be adequate protections for CAs. In some communities (e.g., the work of the American Bankers Association, Identrus), the concept of Authorized

Relying Party (ARP) has been developed to address this issue. An Authorized Relying Party (ARP) is contractually bound to accept only certain types of certificates.

Another issue is the nature of the certificate itself. Emerging from European Commission work on electronic signature standards, the term "Qualified Certificate" has been developed to reflect a certificate specifically issued to identify an individual to provide nonrepudiation for high-assurance government transactions. An IETF work group has written an Internet Draft to define the profile for such a certificate.

Other areas at issue include differing governmental requirements for electronic signatures versus PKI-based digital signatures, the need for more "human understandable" policy statements, the appropriate protection of personal information collected in the certificate registration process, and even the data incorporated in the certificate as an individual identifier.

The next two to three years should be interesting. With electronic signature legislation being enacted globally, it is expected that online agreements that hold legal effect will increase dramatically over the coming years. This should provide an impetus for PKI implementers and Relying Parties to develop solutions that take advantage of this newly signed legislation.

A long-standing issue is the liability exposure for certificate authorities in instances where, despite the presence of policies limiting use of a certificate to a certain class of relying parties, a business or individual outside that class accepts and processes a certificate without authorization to do so.

Other areas at issue include:

- Differing governmental requirements for electronic signatures vs. PKI-based digital signatures.
- The need for more "human understandable" policy statements.
- The appropriate protection of personal information collected in the certificate registration process.
- The data incorporated in the certificate as an individual identifier.

Specific references included in this policy note

Internet Engineering Task Force (IETF), Request For Comment (RFC) 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999

Internet Engineering Task Force (IETF), Internet Draft, Internet X.509 Public Key Infra-structure Qualified Certificates Profile, August 200

General Services Administration, Access Certificates for Electronic Services (ACES) Certificate Policy, 3 September 1999

American Bankers Association (ABA) Trust ID Certificate Policy, December 13, 2000

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Draft Version 1.9, 27 May 2000

Authors include: John T. Sabo of Computer Associates Intl. and Yuriy A. Dzambasow of Digital Signature Trust Co. Contributors to this white paper include Gordon Divitt of FundSERV, Inc., Simon Corell of Smart Trust, and Michael Zolotarev of Balitmore Technologies.

Copyright statement

This White Paper and all other materials printed by the PKI Forum are property of the PKI Forum and may not be copied without express consent from the PKI Forum. 2001 PKI Forum, Inc.

This document is provided for informational purposes only and TechRepublic makes no warranties, either expressed or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of TechRepublic.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.