IT-SECURE.COM

The Swiss E-Security Company.

PKI POLICY DOCUMENTATION

Crafting Certificate Policies and Certification Practice Statements

Introduction

A Public Key Infrastructure (PKI) is a collection of hardware, software, processes and personnel to support the provision of security services based on digital certificates. The certificates themselves are used to encode parameters for a type of cryptography known as public key cryptography, which can be used as the underlying mechanism for security services such as confidentiality, authentication, integrity and non-repudiation.

A PKI will potentially effect many aspects of the IT environment where it is deployed. For example, within a given enterprise, the a directory infrastructure will need to be introduced or an existing structure modified; additional naming structures may need to be defined; employee desktops will need to be updated with certificate-enabled software; smart cards may need to be issued and managed; applications will have to be integrated with certificate-enabled services. At a minimum employees, and ultimately customers, will need to be educated on the use and benefits of a PKI.

Because of the pervasive nature of a PKI, the PKI itself must operate within a well-defined set of security practices and policies. Naturally, the PKI must adhere to established security policies and practices that exist within an enterprise IT environment as a whole. However, a PKI introduces several new policy issues that would not normally be addressed in standard security policies to any level of acceptable detail. Naturally there are technical issues associated with certificates (such as key lengths and certificate lifetimes) but perhaps the main issue is to supply enforceable policies that will define an acceptable trust model for the creation and use of certificates.

Several regulatory and (de facto) standards bodies, notably the Internet PKI working group (PKIX), are promoting the use of two categories of documents to describe various characteristics of a PKI, including trust models. The first category is a *certificate policy* (CP), originally defined in the X.509 standard, which is a policy statement associated with a certificate. The second category is a *certification practice statement* (CPS), defined by the American Bar Association, which is a policy statement associated with a certification authority (CA) that issues certificates. While the exact purpose and meaning of these policy documents will vary from one PKI to the next, it is generally agreed that a CP describes high level requirements on a certificate, while the CPS describes the low level operational details of a CA and they the CA conforms to one or several CPs.

Certificate Policy (CP)

A certificate is a signed data structure issued by a CA and identified with the *subscriber* named in the certificate. Basic information pertaining to the certificate is given in its mandatory fields which include administrative details (version number, serial number and validity period), the name and public key of the subscriber (referred to as the subject in the certificate), and the name and signature of the issuing CA. Additional information relevant to the certificate and the subscriber, such as restrictions on the usage of the public key and alternate names for the subscriber (for example an email address),

may be optionally provided in extension fields. We note that the definition and processing of certificate extensions is a major source of interoperability problems between PKI vendors.

X.509 certificates represent a comprehensive *certificate format specification,* suitable for facilitating the transport and processing of certificates by PKI-enabled software and hardware. However, the actual trust semantics that can be ascribed to a certificate must be defined by a distinct mechanism, which we define as a certificate policy (CP). A CP will typically articulate in detail the conformance requirements pertaining to

- The subscriber population (entities such as employees, customers, business associates, devices and applications).
- The relying party population (those entities that may trust a CSG certificate) .
- The obligations of all CSG PKI entities (including certificate authorities, registration authorities) that may be issued with, may rely on or may manage conforming certificates.
- The trust model implied by the relationships between CSG CAs (strict hierarchy, distributed trust, mesh, hub-and-spoke, web model) issuing conforming certificates.
- A definition or list of suitable applications that may process conforming certificates.
- Procedures for the issuance and management of conforming certificates.
- Additional profile information on conforming certificates.

A CP is typically a general document that may apply to more than one CA and even more than one PKI. It is the responsibility of a given CA to tailor its practices to meet a given CP it wishes to support.

Certification Practice Statement (CPS)

A CPS is a policy document which describes in detail the operational practices of a CA, as well as the responsibilities that the CA is willing to accept with respect to certificates it issues in accordance with these practices. If a CA operates according to the practices and responsibilities of a specific CPS then the CA is said to *governed* by this CPS. Sometimes the governing CPS of a CA is simply a description of how the CA is implemented. On the other hand, a CPS may be written independently of any specific CA, and CAs wishing to claim governance by such a CPS are required to be audited for this purpose. Such a CPS is written with the intention of establishing a community a CAs, potentially linked in some hierarchy, based on a common practices and responsibilities for certificate services. For example, several governments have written a single CPS to govern all CAs implemented within various government departments.

A CPS will typically be tailored to satisfy the conformance requirements of one or several CPs, and such CPs are said to be *supported* by the CPS. For example, a CP may require that the signing key of a CA which creates certificates conforming to the CP be securely stored at the CA. A CPS supporting this CP may then state that all CAs that are to be governed by the CPS must generate and store signing keys in tamper-resistant hardware modules that have passed FIPS 140-1 testing. Thus the actual practices of a CA, as expressed through its governing CPS, will depend to a large extent on the conformance requirements of CPs that the CPS intends to support. Ultimately there must be an audit of a

CPS to determine if its practices and responsibilities comply with the conformance requirements of each CP it claims to support. Similarly an audit will be required to verify that a CA can reasonably claim to be governed by its published CPS. If it is verified that a CPS supports a given CP, and further that a CA is governed by that CPS, then the CA is entitled to issue certificates that claim conformance with the CP. If a CA is governed by a CSP which supports a particular CP, then the CA may issue certificates which carry an extension field to indicate that the certificate conforms to the stated CP.

IT-Secure PKI Policy Documentation

Staff at IT-Secure are experienced with developing comprehensive PKI documentation including CPs, CPS and other ancillary documents including Subscriber and Relying party Agreements to enhance the legal standing of a given PKI. Our policy documents are based on the industry standard PKIX RFC 2527 format which permits a comprehensive description of the policies and practices of a PKI, and provides a solid basis for the audit a given PKI if required. These policy documents are used to define the basis architecture and processes of a PKI, and also the legal boundaries within which the PKI operates. The policy documents can be crafted to describe a closed PKI, say within a given enterprise; a semi-open (networked) PKI between cooperating partners and enterprises, or a totally open PKI which provides general certification services.

Please contact IT-Secure for more information on the development of policies for your PKI.