Entrust White Paper

Certificate Policies and Certification Practice Statements

Author: Sharon Boeyen
Date: February 1997
Version: 1.0

Entrust®
Securing Digital Identities & Information

1. Background

The automation of business processes introduces requirements for security services, such as confidentiality, integrity, authenticity and non-repudiation that can be satisfied by the Entrust™ range of products.

Use of a Public Key Infrastructure (PKI) to support business processes within a single organization requires no more policy and procedures preparation than that required for any Information Technology (IT) infrastructure. Prudent businesses routinely prepare a system security policy, and the special provisions required for a PKI can be easily accommodated within such a policy. When security services involve independent organizations or security domains, they should be qualified by an explicit "quality of service". This ensures that a user of the service does not anticipate a high quality of service or degree of assurance from a provider whose operating procedures are consistent with a lower degree of assurance. This situation could lead to what appears to the user to be a breach of security, even though the service provider has operated entirely within its own operating rules. Aspects of the system's operation that affect the degree of assurance are commonly documented in a system security policy.

Where the system includes a PKI, users need to be able to determine the degree of assurance or trust which can be placed in the authenticity and integrity of the public keys contained in certificates issued by the Certification Authority (CA). Information upon which such determinations can be made is documented in the relevant Certificate Policy and Certification Practice Statement.

2. Overview

A Certificate Policy, as defined in X.509, 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 any organization that operates a PKI, a Policy Authority is required to select or develop and maintain the Certificate Policy. The Policy Authority is generally the same group as that which is responsible for the organization's IT security policy. It should include representatives from the human resources, finance, legal, audit and IT organizational units, to ensure the Certificate Policy is defined and maintained in conjunction with related policies in the organization. At some time in the future, industry forums are expected to establish standard Certificate Policies for their respective business sectors. At such time, a Policy Authority may simply adopt or adapt a model Certificate Policy from such an association. In the meantime, the Policy Authority must develop a Certificate Policy on its own.

A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in managing the certificates that it issues. The Operating Authority (usually an individual within the IT unit) is responsible for preparing and maintaining the CPS. The CPS should describe how the Certificate Policy is interpreted in the context of the system architecture and operating procedures of the organization.

While a Certificate Policy is defined independently of the specific details of the operating environment of the PKI, the corresponding CPS should be tailored to the organizational structure, operating procedures, facilities and computing environment of the Operating Authority. Use of a standard structure for Certificate Policy and CPS documents will help ensure completeness and simplify the assessment of the corresponding degree of assurance by users and other CAs.

The following example illustrates the relationship between components of a Certificate Policy with the corresponding components of a CPS. The Certificate Policy generally states ***what*** is to be adhered to, while the CPS states ***how*** it is adhered to.

The following Certificate Policy component

> *"Users will inform the Operating Authority immediately upon discovery that their private key has suffered unauthorized disclosure"*

may be transformed by an Operating Authority into the following CPS component:

- *"All users (including end-users and operators of CAs) will be informed of the requirement to report unauthorized disclosure of their private key in an agreement, which they will sign prior to their being issued a certificate.*
- *Upon discovery of the unauthorized disclosure of the private key, users will be required to contact their CA, within one working day. The method of contacting the CA will be one of those listed in the CPS.*
- *When not in use, users will be required to keep all copies of their private key either on their person, or in a locked place."*

3. Structure and Components

Although a standard format for a Certificate Policy or CPS has not yet been finalized, a framework which includes a checklist of policy components has emerged. The items included in this checklist should be considered when establishing an organization's Certificate Policy and CPS. These components are outlined below.

3.1 Community and Applicability

The CPS should identify the:

- Certificate Policies with which it claims to conform;
- order of magnitude of the user community that it is intended to serve, including the number of CAs and Registration Authorities (RAs);
- standards to which its external interfaces conform;
- name form used in its certificates; and the
- name-space (e.g. X.500 subtree) in which the CA intends to issue certificates.

3.2 Identification and Authentication

The CPS should describe the mechanisms used to authenticate the identity of all principals, including Security Officer, Security Administrator, Directory Administrator and User. A brief statement of the privileges allocated to each role should be provided.

3.3 Key Management

The key management component should describe how the key life-cycles of each of the system components (including the CAs, RAs and end-users) are managed. Additional components in the area of key management include choice of:

- certificate signing algorithm;
- certificate validity periods; and
- data signing algorithm.

3.4 Local Security Practices

Local security practices are those that relate to the environment in which the major components of the PKI operate including:

- physical controls;
- personnel controls; and
- procedural controls.

3.5 Technical Security Practices

Technical security practices deal with the required technical standards for the components of the system, including:

- computer security controls;
- network security controls; and
- cryptographic module engineering controls.

3.6 Operational Practices

The operational practices describe the operating procedures for the CAs, RAs and end-entities, including the topics of:

- registration of unique names;
- de-registration/revocation;
- key compromise;
- dismissal for cause;
- certificate update;
- disaster recovery;
- private key recovery;
- audit practices; and
- non-disclosure of personal information.

3.7 Legal Provisions

The Certificate Policy may explicitly identify the statutes to which the PKI must conform, including data protection, privacy, access to information and legal wiretap legislation. The Certificate Policy should also state the purposes for which private keys are constrained to be used.

Any limitation of warranty, requirements for acknowledgment of limitations by the certificate user and acceptance of obligations by the principal should be stated. Legal provisions need to be included for each of the following:

- CA liability;
- CA obligations;
- certificate user obligations;
- principal obligations;
- acceptance of limitation; and
- informed consent.

3.8 Cross-certification Agreements

Independent organizations that wish to use one another's certificates should establish a cross-certification agreement between them. This agreement should formally commit both organizations to adhere to the CPS and clarify how disputes should be arbitrated in the event that loss is incurred as a result of a failure to comply.

3.9 Certificate and CRL Profile

The CPS should include a profile of the certificates and CRLs and the directory schema. The profile should indicate which certificate and CRL extensions are present, whether they are marked critical or non-critical, which optional fields are included, what value ranges are allowed, and what action is expected of verifiers in response to any non-standard extensions. The location of these attributes in the directory should be described.

3.10 CPS Administration

The CPS should describe the procedures for development and maintenance of the CPS document. These should include the procedures for approving the CPS and the nature of those changes that should lead to the issuance of a new policy identifier.

4. Deployment and Use

X.509 version 3 format certificates include a number of extension fields, some of which are useful in conveying information about Certificate Policy and the corresponding CPS. Given that both the specification of a Certificate Policy as well as the CPS may be lengthy, it is not generally feasible to include the full description of either directly in the certificate. The description of Certificate Policy and CPS can be made available in the same repository as that used for certificates and CRLs or through other means.

A Certificate Policy is represented in the certificate by a policy identifier in the *certificatePolicies* extension . This identifier is in the form of a registered Object Identifier (OID) assigned by the Policy Authority responsible for its development. In future, some OIDs for Certificate Policies agreed by business sector industry forums, are expected to be registered and become widely understood, eliminating the need for users to evaluate the full policy statement .

The *certificatePolicies* extension is used to ensure that certificate users have an authentic and non-repudiable indication of the policy under which the certificate was issued, and hence the applications for which it is suitable. This extension helps to prevent a verifier from using a certificate for a purpose other than that intended by the issuing CA. This also prevents a signer from repudiating a signature on the grounds that he/she did not intend the associated signature to be used for that purpose . If the PKI is to be used solely for internal corporate confidentiality and integrity/authenticity services, then this extension may be omitted from certificates issued to corporate users. Furthermore, if the Certification Authority operates a single policy, then the extension can be omitted, as the policy implied by the certificate is the declared policy of the issuer. However, even if only one policy is required today, it may be prudent to include this extension, as it will ease the transition to a multi-policy environment in the future.

The *certificatePolicies* extension also makes provision for policy qualifiers to further clarify the details of the policy identified by the policy identifier. Although standard syntax for these qualifiers is not yet set, the intention is that they will either contain a terse text description of the policy, or a pointer to the location of the full text of the Certificate Policy and/or CPS. If pointers use the *GeneralizedName* syntax defined in X.509, retrieval of these documents from a Web page or X.500 Directory system would be quite straightforward. The CPS can be presented as a single document, or it can be presented as a set of documents with one being a brief, user-friendly summary for end-users.

When trust relationships are established between CAs, the Certificate Policies supported by each may not be identical. In support of cross-certification, the X.509 version 3 certificate format includes an extension field *policyMappings* for CA certificates. This field is used to indicate that a particular policy supported by one of the CAs is considered equivalent by the other CA to a policy that it supports. The OIDs of the two policies are included in the extension field.

5. Summary

Certificate Policies and Certification Practice Statements are key components in establishing the degree of assurance or trust that can be placed in certificates issued by CAs. In a restricted, single security domain environment, formalizing these policies and practices may not be required. However, if future plans are to expand beyond this restricted scope, more formal policy and procedure definition is required, through the use of Certificate Policy and CPS documents. This will help ensure that policies and practices can be easily interpreted and assessed by the users and administrators who need to determine the degree of assurance in certificates issued by a Certification Authority. The

planning, development and maintenance of a Certificate Policy as well as a CPS should be conducted in close cooperation with, and with input from, many organizational units to ensure consistency throughout the organization. Establishing this framework within an organization at the early stages of setting up a PKI will help simplify the task and ease its integration with the related business processes of the organization.