Certificate Practice Statement

For the

Bureau of the Public Debt

Certificate Authority

Prepared By: The Internet Services Group

Office of Information Technology
Division of Technical Services
Distributed Systems Branch

Certificate Practice Statement
For the Bureau of the Public Debt Certificate Authority

Table of Contents

Certificate Practice Statement for the Bureau of the Public Debt Certificate Authority (BPD CA)

1.0 Introduction

The Bureau of the Public Debt (BPD) operates a Certificate Authority (CA), which issues public key certificates to a set of external BPD business customers for use in securing BPD web based business applications. This document will describe for users and stakeholders in web based BPD business applications the practices and procedures that the Bureau of the Public Debt Certificate Authority (BPD CA) utilizes in the conduct of CA service and operations. These practices consist of business and operational practices associated with the issuance and management of certificates.

The services and operations of the BPD CA are intended solely for BPD users and applications. The BPD CA is not intended to provide general certificate services for the general public, nor for any applications other than BPD applications.

1.1 Scope

This Certificate Practice Statement (CPS) document pertains solely to the business and operational practices of the Certificate Authority operated by the Bureau of the Public Debt for the purpose of authentication of web-based BPD business customers. This CPS does not pertain to any other Bureau of the Public Debt certificate authority system that may be in operation or contemplated in the future.

1.2 Purpose

The purpose of this CPS document is to objectively define the practices and procedures that the BPD CA utilizes in the conduct of CA service and operations. This CPS also defines the obligations and responsibilities that involved entities have in the conduct of creating and using certificates issued by the BPD CA. The intent of the CPS is to allow involved entities, such as the BPD business customers, to understand and review the practices of the BPD CA.

1.3 General Trust Model

The services of the BPD CA will support secure electronic Web (World Wide Web (WWW)) access to certain BPD business applications. To accomplish this the BPD CA provides a trusted service for issuing and revoking, when duly notified, certificates in accordance with these published practices. The BPD CA provides a service that BPD business customers may rely on for the provisioning of certificate management services.

1.4 General Discussion of Certificate Issuing and Management

The BPD CA provides a service to facilitate the confirmation of the relationship between BPD business customers, BPD business management, and the BPD CA. The management process for certificates involves the acceptance of certificate requests, the appropriate authentication of requester identity, issuance of certificates, publishing of certificates into a repository (Directory), revocation of certificates and audit trail creation and maintenance.

1.5 Definitions

BPD CA - BPD Certificate Authority.

BPD Business Management - BPD office that owns the BPD application and its data.

BPD Security Contact - Personnel designated by the BPD business management as points of contact for the BPD CA and the BPD business customer.

BPD Business Customer - A Customer who has established a business relationship with BPD.

Customer Security Contact - Personnel designated by the BPD business customer as points of contact for the BPD CA and the BPD business customer.

Applicant - A potential user of a BPD application that requires a BPD certificate. A BPD business customer will submit certificate requests on behalf of an applicant.

Subscriber - A user of a BPD application that have been issued a BPD certificate

1.6 Certificate Types

The BPD CA supports the following certificates:

1.6.1 Customer Web Browser certificate. This type of certificate is intended for Web browsers to facilitate the establishment of Secure Sockets Layer connections between client browsers and BPD operated Web servers.

1.6.2 BPD Web Server certificate. This type of certificate is intended for Public Debt Web servers to facilitate the establishment of Secure Sockets Layer connections between BPD operated Web servers, other devices, and client browsers.

1.6.3 BPD Code Signing certificate. This type of certificate is intended for Public Debt's use to apply a digital signature to BPD written applications.

2.0 Obligations and Responsibilities

The BPD CA, BPD business management, and the BPD business customers have obligations and responsibilities with respect to the various facets of handling and using public key certificates and the supporting systems associated with certificate usage. These obligations and responsibilities are described below.

2.1 CA Obligations and Responsibilities

The BPD CA will have the following obligations and responsibilities:

2.1.1 Provide appropriate security for the certificate management process (including certificate issuance, certificate revocation and audit trails) and the protection of the CA signature key.

2.1.2 The BPD CA will ensure that there is no collision of the subscriber's name (as defined in the Distinguished Name on the subscriber's certificate) with that of any other BPD CA subscriber.

2.1.3 Certificates will be issued and available within a reasonable time after a properly formatted and validated Certificate Request is received by the BPD CA. There are subscriber obligations that affect the time required to validate the Certificate Request.

2.1.4 Notify the BPD security contact (via email and hardcopy) after a certificate has been approved for retrieval by the subscriber.

2.1.5 Publish the certificate in the Directory System. The Directory System serves as the certificate repository, or storage location for public key certificates, for the BPD CA.

2.1.6 The BPD CA will publish the Certificate Revocation List (CRL) to the BPD Directory System. BPD business applications will check the CRL before accepting a certificate.

2.2 BPD Business Management Obligations and Responsibilities

The management of a BPD business application, that requires a certificate, will have the following obligations and responsibilities:

2.2.1 Identify in writing to the BPD CA the names and contact information for two (2) BPD Security Contacts. Update the information as events warrant (due to employee reassignment, termination, etc)

2.2.2 The BPD security contacts will initially process incoming BPD customer applications for certificates. After identifying the applicant as an authorized user of a BPD business application, forward the application to the BPD CA.

2.2.3 The BPD security contacts will notify the BPD CA when a subscriber's certificate is to be revoked.

2.3 BPD Business Customer Obligations and Responsibilities

The management of the BPD business customer, have the following obligations and responsibilities:

2.3.1 Identify in writing to the BPD security contacts the names and contact information for two (2) Security Contacts. Update the information as events warrant (due to employee reassignment, termination, etc)

2.3.2 Notify BPD security contacts when any of the following events occurs:

2.3.2.1 A subscriber's employment or affiliation with the customer is terminated.

2.3.2.2 A subscriber no longer requires access to any BPD web based business application.

2.3.2.3 A subscriber forgets or no longer knows the password for their web browser.

2.3.2.4 A subscriber suspects his private key has been compromised.

2.4 Subscriber Obligations and Responsibilities

Subscribers to the BPD CA will have the following obligations and responsibilities:

2.4.1 The subscriber shall not divulge the value of any private key associated with that subscriber's certificate issued by BPD CA to any other entity.

2.4.2 The web browser used by the subscriber shall provide for password protection of the subscriber's private key. The subscriber must utilize password protection of the private key.

2.4.3 The subscriber shall notify the customer security contacts once any of the following conditions occurs:

- 2.4.3.1 The subscriber no longer requires access to any BPD web based business application.
- 2.4.3.2 The subscriber suspects his private key has been compromised.
- 2.4.3.3 The subscriber forgets or no longer knows the password for their web browser.

2.4.4 The subscriber shall destroy any private key that has been reported to the customer security contact to be compromised.

2.4.5 The subscriber shall follow the official procedures and instructions distributed by the BPD business management related to requesting and retrieving of certificates.

2.4.6 The subscriber shall use any and all certificates issued by the BPD CA solely for official business communications with the BPD.

3.0 Certificate Processing Procedures

This section of the CPS describes the procedures used by the BPD CA to authenticate and validate the identity of the subject named in a certificate request or revocation request received by the BPD CA.

3.1 Generating the Certificate Request

The applicant will submit a completed Internet application via US mail to the BPD security contact responsible for serving as the primary contact for Internet business application.

3.2 Certificate Request Authentication

Once a certificate request submitted by the applicant has been received by the BPD security contact for processing, the BPD security contact will verify that the applicant's name is on the list of authorized business customers.

3.3 Processing Applications

The BPD security contact will forward all authorized applications to the BPD CA for processing. The BPD CA will prepare a sealed envelope containing the applicant's authorization information for certificate retrieval. The BPD CA will give the sealed envelope to the BPD security contact. The BPD security contact will mail the following to the applicant: the sealed envelope, a processed application with a reference number for certificate renewal, and instructions on how to retrieve and protect the certificate.

3.4 Certificate Revocation

Certificates will be revoked if any of the following events occurs:

3.4.1. The private key value or the password protecting the subscriber's private key is compromised (known to any other entity other than the subscriber)

3.4.2. The subscriber's employment or affiliation with the customer is terminated.

3.4.3. The subscriber no longer requires access to any BPD web based application

The BPD CA shall take immediate action to revoke a certificate for which the BPD CA is notified that the associated private key has been or might have been compromised. Once the BPD CA is notified of a known or suspected private key compromise, a certificate will be revoked within 2 hours.

4.0 CA Operational Practices

4.1 Official BPD CA Contact Point

Contact information (names of personnel, including several layers of backup, along with telephone numbers and e-mail addresses) will be supplied to subscribers by the BPD security contact in written documentation, which will be updated as required.

4.2 Audit Logs

The BPD CA maintains audit logs, which are updated in real time. These audit logs are protected from tampering. These logs are also backed up to physical media (digital tape). Copies of these audit log backup tapes are stored both onsite and off-site to facilitate recovery if necessary. Audit logs contain the full history of the operational activities of the BPD CA.

4.3 Disaster Recovery and Business Continuity

The BPD CA provides a backup capability to restore BPD CA functioning in the event of a system failure at BPD CA. It is anticipated that in the event of a full system failure, the BPD CA can be restored to service within 4 hours elapsed time.

4.4 Physical Security

The BPD CA server computer is protected by a variety of physical security controls which include card key access to the physical computer data center at multiple, layered entry points

4.5 Technical Security Controls and Key Management

4.5.1 Key Length

BPD CA uses a private key/public key pair that is 1024 bits long.
The subscribers are required to use private key/public key pairs that are 1024 bits long.

4.5.2 Validity Period for Certificates (Key Life)

The validity period for certificates issued by the BPD CA is 2 years (24 months).
The signing private key lifetime is seventy (70) percent of the verification key lifetime.
The certificate of the BPD CA is valid for twenty (20) years from date of issue.

4.5.3 Certificate Revocation List Management

The BPD CA produces an updated Certificate Revocation List (CRL) every four (4) hours.
The CRL is distributed to the BPD Directory System. When certificates are revoked due to
private key compromise, an updated CRL is generated immediately at that time and published to the BPD Directory System.

5.0 Certificate Usage Policy and Limitations

5.1 Bureau of the Public Debt Certificate Usage Policy Statement

X.509 public key certificates issued by the Bureau of the Public Debt are to be used solely for official business communications with the Bureau of the Public Debt. Use of Bureau of the Public Debt issued certificates for other than official business communications with the Bureau of the Public Debt is expressly prohibited by the issuer. Any use of a Bureau of the Public Debt issued certificate for other than official business communications with the Bureau of the Public Debt is undertaken at the sole risk of the user.

5.2 Certificate Warning

As a official limitation on the authorized use of BPD CA issued certificates, the following statement is contained in all BPD CA issued certificates:

Browser certificate authorized by issuer solely for official business communication with BPD.

This statement is part of the certificate data structure itself, and is digitally signed by the BPD CA digital signature key.