TIMS PKI

PKI Disclosure Statements

Effective Date: 10 Jan 2020

Version: 1.0

Important Note About this Document

The present document is the TIMS PKI public "PKI Disclosure statement" (PDS). Throughout this document, the use of the term "PDS" refers to the present document, unless otherwise specified.

The purpose of the PDS is to:

- summarize the key points of the CP/CPS for the benefit of Subscribers and Relying Parties
- provide additional details and further provisions that apply to the CP/CPS.

Contact Information:

Inland Revenue Services

DBS Building 4th Floor

P.O. Box 1877

Apia

Samoa

https://www.revenue.gov.ws

tims@revenue.gov.ws

Version Control:

Author	Date	Version	Comment
TIMS Committee	1/10/2020	1.0	Initial version

Table of Contents

1 TIMS PKI CONTACT INFO

TIMS Committee

DBS Building 4th Floor

P.O. Box 1877

Apia

Samoa

https://www.revenue.gov.ws

tims@revenue.gov.ws

2 CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

2.1 CERTIFICATE TYPE

Within the TIMS PKI, an Issuing CA can only issue Digital Certificates with approved Digital Certificate types.

Certificate Type	Description	Certificate type OID (EKU)	Certificate class OID (Certificate Policy)	token
3.1	Intend for Web Site server authentication	1.3.6.1.4.1.49952.3.6.3.1	1.3.6.1.4.1.49952.3.6.4.1	No
3.2	Intend for Web site client authentication	1.3.6.1.4.1.49952.3.6.3.2	1.3.6.1.4.1.49952.3.6.4.1	No
3.3	Intend for Invoice Signing outside TIMS	1.3.6.1.4.1.49952.3.6.3.3	1.3.6.1.4.1.49952.3.6.4.2	Yes
3.4	Intend for Web site client authentication (paired with type 3.3)	1.3.6.1.4.1.49952.3.6.3.4	1.3.6.1.4.1.49952.3.6.4.2	Yes
3.5	Intend for Invoice Signing inside TIMS	1.3.6.1.4.1.49952.3.6.3.5	1.3.6.1.4.1.49952.3.6.4.1	No
3.6	Intend encrypting messages for TIMS	1.3.6.1.4.1.49952.3.6.3.6	1.3.6.1.4.1.49952.3.6.4.1	No

2.1.1 Digital Certificate Type 3.1

All web traffic except invoice verification service both external and internal is protected using https and client certificates. This type of certificate is intended for server's authentication.

Web traffic for invoice verification service does not require authentication service and is https protected with public third-party certificates that is trusted by most used clients.

2.1.2 Digital Certificate Type 3.2

All internal services use this type of certificate to authenticate to web site services.

Organization authorized person can request this type of certificates for fiscalization solutions that use TIMS online service for signing invoices. This certificate is distributed to Organization in form of PKCS#12 and protected with password defined by Organization authorized person.

2.1.3 Digital Certificate Type 3.3

For fiscalization solutions that do not use TIMS online service, this is a signing invoices certificate. This type of certificate is smart card (token) mandatory for protecting private key and PIN for activating data. Prior to issuing of certificate, PIN is defined by Organization authorized person.

2.1.4 Digital Certificate Type 3.4

Certificate type 3.3 is not for authenticating to TIMS web site services. Type 3.4 fill in smart card usage for authenticating to TIMS web site services.

2.1.5 Digital Certificate Type 3.5

TIMS internal services use this type of certificate to sign invoices.

2.1.6 Digital Certificate Type 3.6

TIMS use this certificate type for communication with smart card holding certificate type 3.3 for audit purpose.

2.2 Enrolment Process and Responsibilities

2.2.1 Enrolment Process and Responsibilities for First Digital Certificate

1. Identification data preparation
    a. TIMS Enrolment officer is responsible to inform organization authorized person to update identification data held by TIMS system.
    b. Organization authorized person is responsible to update identification data.
2. Activation data and delivery method defining
    a. TIMS Enrolment officer is responsible to inform organization authorized person to set Digital Certificate activation data – PIN.
    b. Organization authorized person is responsible to set Digital Certificate activation data – PIN and choose delivery process
3. Approving Digital Certificate issuance
    a. TIMS Enrolment officer is responsible to approve Digital Certificate issuance
    b. TIMS Personalization officer is responsible to issue Digital Certificate on smart card
    c. TIMS Personalization officer is responsible to deliver smart card to chosen Delivery method
    d. Officers at delivery address are responsible to identify organization authorize person face-to-face and return cover letter signed by organization authorize person
    e. TIMS Enrolment officer upon returned cover letter signed by organization authorize person is responsible to enable organization authorize person Digital Certificate in TIMS system.

2.2.2 Enrolment Process and Responsibilities for other Digital Certificate

1. Identification data preparation
    a. Organization authorize person is responsible to add identification data for additional Locations and request addition digital certificates
2. Activation data and delivery method defining
    a. Organization authorize person is responsible to set Digital Certificate activation data – PIN and choose delivery process or set PKCS12 password and PKCS12 activation data for TIMS system
3. Approving Digital Certificate issuance
    a. TIMS Enrolment officer is responsible to approve Digital Certificate issuance

b. TIMS system upon approval is responsible to automatically issue Digital Certificate in PKCS12
c. TIMS Personalization officer is responsible to issue Digital Certificate on smart card
d. TIMS Personalization officer is responsible to deliver smart card to chosen Delivery method
e. Officers at delivery address are responsible to identify organization authorize person face-to-face and return cover letter signed by organization authorize person
f. TIMS Enrolment officer is responsible to enable organization authorize person Digital Certificate in TIMS system.

3 RELIANCE LIMITS

TIMS PKI is support process of TIMS system.

4 OBLIGATIONS OF SUBSCRIBERS

Certificate Holders are required to act in accordance with this CP/CPS. A Certificate Holder represents, warrants and covenants with and to TIMS PKI processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify TIMS PKI immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key.
- Immediately notify TIMS PKI in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever.

Following compromise, the use of the Certificate Holder's Private Key should be immediately and permanently discontinued.

- Take all reasonable measures to avoid the compromise of the security or integrity of the TIMS PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.

- At all times utilize the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.
- Discontinue the use of the digital signature Key Pair in the event that TIMS notifies the Certificate Holder that the TIMS PKI has been compromised.

5 CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Relying party cannot rely on a Digital Certificate issued by TIMS current set as revoked Digital Certificates published by TIMS. Certificates have pointers to URLs where TIMS publishes status information, including Certificate Revocation Lists (CRLs), and Relying Parties are required to check the most recent CRL.

5.1 Authorize Relaying parties

Authorize Relying parties are involved in signed invoices creation and are required to act in accordance with this CP/CPS. Any device or software used to create signed invoice must be accredited in accordance with current regulation.

5.2 Relaying parties involved in signed invoices receives

Any party receiving a signed electronic invoice may use publicly available service to rely on that Digital Signature.

Every signed invoice from accredited device or software contain QR code which is used in verification process. Verification service URL is under https://tims.revenue.gov.ws

6 LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

TIMS PKI is support process of TIMS system.

7 APPLICABLE AGREEMENTS

TIMS PKI is support process of TIMS system.

8 PRIVACY POLICY

The content of Digital Certificates issued by TIMS PKI is public information and deemed not private.

All information about Certificate Holders that is not publicly available through the content of issued Digital Certificates is part of TIMS system and will follow rules of TIMS system.

Except for reason codes contained in a Certificate Revocation List, the detailed reason for a Digital Certificate being revoked, (if applicable) remains part of TIMS system.

9 REFUND POLICY

No refund policy will be established.

10 APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

N/A

11 TIMS PKI AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

TIMS PKI is support process of TIMS system.