Important Notice

Dear Prism Customer,

Your new PCI HSM v3.0 TSM500i Hardware Security Module (HSM) is not shipped with default passwords for the Crypto Officer roles. Reset your HSM to Boot Loader state to query the Boot loader version.

- **BL50 v1.5.0.0 (or later)** Refer to section 2.8 of **TSM500i and TSM-Web User Guide (PCI HSM v3).pdf** to authenticate HSM and set initial passwords.

In order to receive certificates to enable passwords to be set, you will need to:

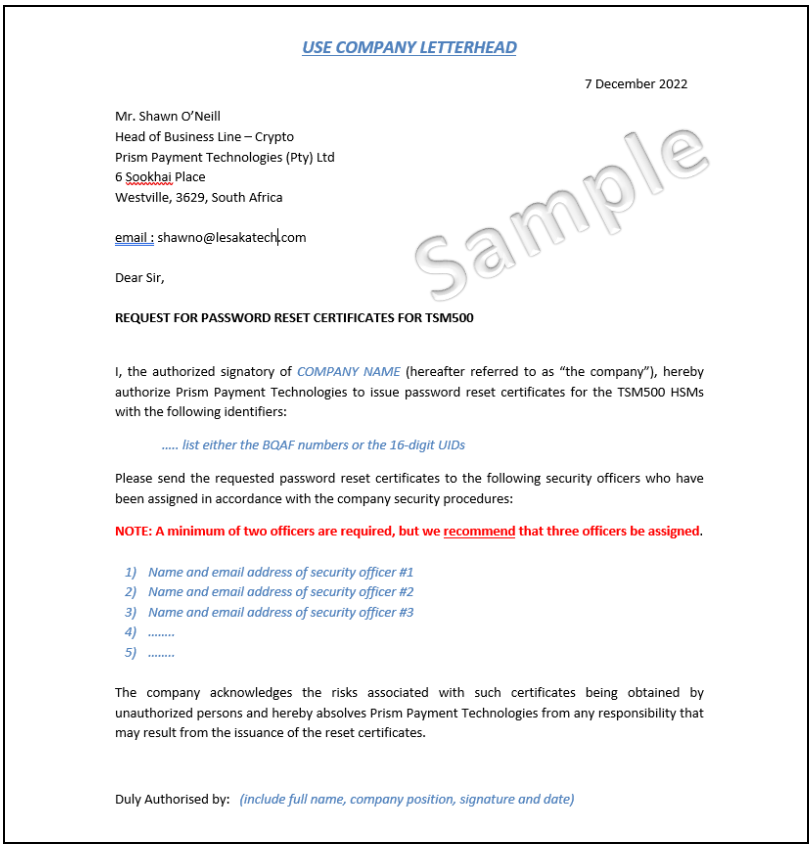
1) **Assign at least two crypto officers** in accordance with your company's security procedures. Crypto officers are expected to be familiar with the security requirements applicable to your application. Some minimum guidelines are provided in section 2.2 of the applicable TSM500i and TSM-Web User Guide (PCI HSM v3). HSMs with BL50 v1.5.0.0 (or later) require additional authentication steps as detailed in the above documentation.

2) **Send a letter to Prism Payment Technologies** requesting Password Reset Certificates for your HSMs. The letter must contain the content per the sample letter shown below. The letter must be signed by an authorized representative of your company. In most cases this should be the person who was responsible for negotiating the purchase of the HSMs from Prism Payment Technologies.

3) **Email the Device Authentication Token** to Prism so that the HSM can be authenticated before control is transferred to the Customer.

   The letter should be emailed to: **shawno@lesakatech.com** and **shailendras@lesakatech.com**

Initial password reset certificates for a new HSM will be supplied at no charge. Where Prism is required to generate and supply password reset certificates because a password has been forgotten, the customer will be charged for this service. A template for the SAMPLE LETTER may be found in the Documents/Help menu in TsmWeb



USE COMPANY LETTERHEAD

7 December 2022

Mr. Shawn O'Neill
Head of Business Line – Crypto
Prism Payment Technologies (Pty) Ltd
6 Sookhai Place
Westville, 3629, South Africa

email : shawno@lesakatech.com

Sample

Dear Sir,

REQUEST FOR PASSWORD RESET CERTIFICATES FOR TSM500

I, the authorized signatory of *COMPANY NAME* (hereafter referred to as "the company"), hereby authorize Prism Payment Technologies to issue password reset certificates for the TSM500 HSMs with the following identifiers:

..... list either the BQAF numbers or the 16-digit UIDs

Please send the requested password reset certificates to the following security officers who have been assigned in accordance with the company security procedures:

NOTE: A minimum of two officers are required, but we recommend that three officers be assigned.

1) *Name and email address of security officer #1*
2) *Name and email address of security officer #2*
3) *Name and email address of security officer #3*
4) .....
5) .....

The company acknowledges the risks associated with such certificates being obtained by unauthorized persons and hereby absolves Prism Payment Technologies from any responsibility that may result from the issuance of the reset certificates.

Duly Authorised by: *(include full name, company position, signature and date)*

The HSM requires dual control for all sensitive operations, so it is strongly recommended that the crypto officers add at least one more crypto officer during initial deployment. A minimum of two officers are required, but we recommend that three officers be assigned.

For information on security awareness, and the implication of lost passwords and components please refer to section 3.4 in TSM500i and TSM-Web User Guide (PCI HSM v3).pdf.