



Payment Gateway Services (PGS)

Cryptographic Key Custodian Authorization

EPR ID: 113309

Revised: 6/7/2011

Author: Amy Dall

CONTENTS

Version Control.....	2
PCI-dss 1.2 - Requirement 3.6.8 – Overview	3
section 1 – Policy	3
section 2 – Authorization	4



VERSION CONTROL

Prepared by	Change	Date	Reviewed by	Date
Amy Dall	Initial Version	6/7/2011	Greg Andrews	6/7/2011
	Initial Review and Approval		Nat Mokry	6/7/2011

INSTRUCTIONS

As part of the PCI documentation process, we are required to obtain a signed document from each individual that has PRO server level access to PGS (i.e. completes builds, troubleshoots or directly accesses servers for PGS, reviews logs, access to PGS Database, develops code, etc.)

If you meet any of the above guidelines, please complete the following:

- Review the entire document below
- Sign in the Employee Section
- Have your manager sign the Manager Section
- Have your manager return the completed document to [PGS PCI Inquiry@hp.com](mailto:PGS_PCI_Inquiry@hp.com)

Summary: By having access to PGS PRO servers or code, you have access to portions of cryptographic key information and are therefore required to sign this document as part of PCI compliance for HP.



PCI-DSS 1.2 - REQUIREMENT 3.6.8 – OVERVIEW

Requirement :- PCI Requirement 3.6.8

Requirement Details :- Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key custodian responsibilities

SECTION 1 – POLICY

Below is a representative subset of the HP IT Cryptography Policy:

Protecting Private Keys and Secret Keys

- The private key associated with any asymmetric key pair must never be transmitted on any network in clear form.
- Secret keys must never be transmitted on any network in clear form.
- The private key associated with any asymmetric key pair must never be stored on any media in clear form.
- Secret keys must never be stored on any media in clear form.
- Private keys and secret keys stored on media such as hard disks, CD-ROMs, or floppy disks must be encrypted using a symmetric cipher with an effective key length of at least 112 bits. If the symmetric cipher's key is derived from a passphrase, the passphrase must meet the complexity requirements of the Password Management Standard.
- When private keys and secret keys must be temporarily in the clear, such as in volatile memory for purposes of computation, they must be cleared immediately after use such that no residue exists for possible disclosure.
- Private keys and secret keys stored on hardware devices such as smart cards must require a user PIN of at least 4 digits and must have a user lockout feature or a device reset feature after no more than 5 failed PINs.
- The private keys associated with any certificate authority issuing certificates to which product liability may attach must be stored in an HP IT Security approved hardware device.

For more information please refer to HP IT Security Policies listed below:

- HP IT Cryptography Policy: <http://enhanced1.sharepoint.hp.com/teams/EA/Lists/Policy/DispForm.aspx?ID=80>



Other References from the HP IT Cryptography Policy listed below:

- [Cryptography Usage Standard](#)
- [Trusted Certificate Authorities \(CAs\) Specification](#)
- [Network Security Policy](#)
- [White Paper: On the Development of Security Policy for the use of Cryptography](#)
- [Considerations for Selecting Appropriate Information Security Controls Best Practice](#)
- [HP Standards of Business Conduct](#)
- [Privacy Office](#)

For details regarding how to label information, please see the HP Legal web pages at <http://legal.hp.com/legal/pages/labels.aspx>

SECTION 2 – AUTHORIZATION

All Hewlett-Packard staff that holds responsible authorized positions where they manage or handle encryption keys of the Payment Gateway Services (PGS) System must sign the following document.

As a condition of continued employment with Hewlett-Packard, and as an employee that has access to key management tools and equipment, you are obligated to sign the following to indicate acceptance of your responsibility.

The signatory of this document is in full employment with Hewlett-Packard on the date shown below and has been afforded access to key management devices, software and equipment, and hereby agrees that, he or she:


- Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of his/her ability, and has been trained in security awareness and has had the ability to raise questions and have those questions answered satisfactorily.
- Understands that non-compliance with the key management procedures can lead to disciplinary action including termination and prosecution.
- Exceptions to compliance only occur where such compliance would violate local, state, or federal law, or where a senior officer of the company or law enforcement officer has given prior authorization.




- Agrees to never divulge to any third party, any key management or related security systems; passwords, processes, security hardware or secrets associated with the Hewlett-Packard systems, unless authorized by an officer of the Hewlett-Packard or required to do so by law enforcement officers.
- Agrees to report promptly and in full to the correct personnel (immediate management or CITSIRT@hp.com), any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

I agree to the above and understand that this original copy will be held on my personnel record and kept by the company indefinitely.

EMPLOYEE:

Signature: 
Print Name: Fang, Can
Date: 2011.06.14

MANAGER:

Signature: 
Print Name: Ji, Li-chun
Date: Jun 14, 2011