Transport for Greater Manchester

Transport for Greater Manchester Policy

P09 Key Management Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	26th March 2020	Document Reference no.	Key Management Policy P09
Version No.	4.0	Prepared by:	Claire Styler, Catherine Burke & Rohan Mendis
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim **Date:**		Full Impact Assessment completed: YES **Validated by Equality Officer signature:** **Date:**
Authorisation Level required:	Executive Group/Director		Staff Applicable to: All Staff
Authorised by: Date:	Head of IS Operations (Ricard Fuertes) 31st March 2020		Implementation date: 31st March 2020 Annual review date: 31st January 2021

Table of Contents

1 Policy Aims

a) This document is intended to detail **TfGM's** policy in relation to Cryptographic Key Management for networks that store, process or transmit Cardholder Data.

b) This document outlines the security standards and procedures required for effectively handling and managing keys.

c) This document should be viewed in conjunction with **TfGM's** top level security policy: P01 - IS Policy.

2 Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by the **TfGM IS Operations Team** to ensure:

   i) the business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS), and

   ii) it maintains its relevance to the business' current and planned payment card processing operations.

b) The **IS Operations Team** will undertake the review of this policy statement and associated company policies.

c) Any changes to this policy must be communicated to all members of **TfGM's IS Operations Team** and to all affected parties.

3 Purpose

a) This document outlines in broad terms the Key Management procedures used at **TfGM**. This document is not intended to replace any training materials for data security roles but should be an aid to day-to-day operations.

b) Procedures and guidelines will feed directly into **TfGM's** annual PCI compliance programme.

4 Scope

This document is intended for those members of staff who are key custodians at **TfGM**.

5 Policy Delivery

This policy will be delivered to all staff by internal communication and will be situated on the **TfGM** Intranet.

6 Accountability

- **Responsible to the Board:** Head of IS Operations
- **Compliance:** IS Department
- **Awareness:** All Staff

7 Enforcement /Monitoring / Compliance

a) Key Management Policies & Procedures will be monitored daily and reviewed annually.

b) This policy will be enforced by the Executive.

c) Should a breach or violation of this policy be identified, it may result in disciplinary action in accordance with **TfGM** disciplinary policy.

8 Policy

8.1 Key Management

TfGM shall put technical measures in place to track and log changes to encryption, keys used to protect cardholder data, and to prevent and alert upon unauthorised key substitution.

8.2 Key Storage

a) **TfGM** shall ensure that data decryption keys are not stored on the same machine as the one holding the data that the key decrypts.

b) **TfGM** shall ensure all keys used to protect cardholder data will only exist in one or more of the following formats at all times:

c) **TfGM** shall ensure all keys are stored in a strongly encrypted format.

d) **TfGM** shall ensure encryption with a key-encrypting-key is stored separately from the data encrypting key.

e) **TfGM** and its Service Provider shall ensure that keys are stored in the fewest possible locations and stored securely at all times, for example, by using encryption/passwords to protect the keys.

f) **TfGM** shall ensure that a secure cryptographic device such as a host security module (HSM) or PTS approved point-of-interaction device.

g) **TfGM** shall ensure that key components or key shares, are in accordance with an industry-accepted method. For all uses of cryptographic keys, they keys shall be stored in fewest locations and forms.

8.3 Key Usage

TfGM and its service provider shall limit the number of staff with access to the decryption keys, to as few staff as possible, for business use. All key custodians are required to sign F12 - Key Custodians Form and acknowledge their key custodian responsibilities.

8.4 Cryptographic Key Schemes

8.4.1 Split Password

a) A split password shall be used where **TfGM's** and Service Provider's key holders have a partial key that is joined in order to create a complete decryption key.

b) Where a key is accessed using a split password scheme, the following policy rules shall apply.

   i) The password holders must be senior member's staff (chosen by the Head of IS Operations.

   ii) Passwords for Encryption Keys must remain secret and not disclosed to any other member of staff.

   iii) Clear-text key-management procedures require split knowledge and dual control of keys.

iv) The Key Custodians shall record their password on paper and seal it in a tamper-proof envelope. These envelopes shall be held in escrow by an independent 3rd party. Should any of the elected key holders no longer be available, the Escrow Agent shall return the relevant key envelopes to a Company Director.

v) In the event of the keys being returned by the Escrow Agent, the Encryption Key must then be changed.

vi) Technical measures shall be put in place to ensure that keys can only be changed with authorisation by the relevant **TfGM's** Service Provider.

vii) Passwords shall be generated by the use of an elected password generation utility (e.g. pwgen on UNI X systems).

viii) Each key holder will generate his or her own 20-character key creating a combined key of 40-characters

8.4.2 Symmetric Keys

a) Where a symmetric key is used, the following policy rules shall apply:

i) If the key designed for use in a pre-shared environment, it shall be longer than 40 characters, and meet the complexity requirements as outlined in the **TfGM** password policy.

ii) Technical measures shall be put in place to ensure that keys can be changed or substituted with authorisation

8.4.3 Asymmetric Keys

a) Database Encryption System

i) **TfGM's** Service Provider shall employ a custom key generation technique for encrypting unique rows within the database system:

ii) **TfGM's** Service Providers do not use Asymmetric Keys for encryption of databases deployed in its' CDE.

iii) Where a public & private key scheme is used, the following policy rules shall apply to the public key:

- The public key can be distributed without restriction as it may only be used to encrypt data for decryption via the private key.

iv) The following policy rules shall apply to the private key:

- The private key shall itself be protected by a key-encrypting key.
- The private key shall not be stored in a widely accessible location.
- The private key shall not be stored in plaintext.
- The private key shall not be stored along with the key encrypting key.

Technical measures shall be put in place to ensure that keys can only be changed or substituted with authorisation.

b) Pre-Shared Key (PSK)

The pre-shared key (PSK) used for IPSEC VPN on **TfGM** firewalls deployed for provisioning connectivity to Ticket Vending Machines (TVM) is 43 characters, key with uppercase and lowercase alphabetical letters, numbers and extended characters.

8.4.4 Key Encrypting Keys

a) If key encrypting keys are in use, then **TfGM** shall ensure that they are stored separately from data encrypting keys. The keys shall be stored in the fewest possible locations and forms, and will be at least as strong as the data-encrypting keys they are protecting.

b) For the purpose of this policy, key encrypting keys are used to associate a password with a key within the following example systems. This list is not exhaustive:

i) SSH client keys.

ii) SSL server certificates.

iii) SSL client certificates.

iv) RSA tokens.

Technical measures shall be put in place to ensure that keys can only be changed or substituted with authorisation.

Note that the firewalls and switches deployed in the TfGM multi service Network generate a 2048 bit Secure Socket Layer (SSL) key.

8.5 Key Strength & Ciphers

a) Where **TfGM** is not using a recognised key-generation tool, the key shall be generated using a source of strong entropy such as a pseudo random generator within the host operating system.

b) It is essential that no cryptographic solution protecting cardholder data employs a non-standard or closed, proprietary cipher. The types of ciphers supported will vary depending upon the software or hardware implementation. **TfGM** shall ensure that it uses strong ciphers in all cases.

c) Firewall IPSEC encryption should be set to AES256 and authentication will be MD5 hashing algorithm.

8.6 Key Changes & Distribution

a) **TfGM's** Service Provider will ensure that keys are encrypted using a recognised, non-proprietary encryption algorithm during distribution and are never distributed in plaintext.

b) The Encryption Key will be changed every year unless circumstances require it to be changed before a year has elapsed.

c) Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimise the risk of someone being able to decrypt card data. If the encryption key was provided by the encryption application vendor, **TfGM** must follow the vendor's documented recommendations for periodic changing of keys. If guidance is not provided by the encryption application vendor, **TfGM,** the key custodian must refer to industry best practices on key management, e.g. *NIST Special Publication 800-57*, for guidance on appropriate cryptoperiods. If no application vendor or industry best

practice guidance is available, the encryption key should be changed every year unless circumstances require it to be changed before a year has elapsed.

d) In the event of an information security breach or if the integrity of the keys is weakened, the Encryption Keys must be retired and changed, regardless of whether or not the key itself has been compromised.

e) Keys may only be changed with the authorisation of the Head of Information Security. Staff found to have changed the key without written authorisation will be subject to disciplinary procedures.

f) Keys must only be changed with the authorisation of the Head of Information Systems. Staff found to have changed the key without written authorisation will be subject to disciplinary procedures.

g) Keys will be updated on each system affected as soon as the key has been changed.

h) Keys removed from the system will be destroyed using secure disposal methods.

i) In all cryptographic implementation, technical measures shall be put in place to ensure that keys can only be changed or substituted with authorisation.

8.7 Key Destruction

a) Upon a change of Encryption Keys, the keys held in Escrow will also be destroyed and replaced with the updated keys, following the same procedure.

b) Where applicable, once a key has been retired, it should be appended to **TfGM's** Certificate Revocation List or submitted to the appropriate key revocation process, as per the application. If the keys are retained ensure that they are not used for encryption operations.

8.8 In Scope Cryptographic Implementations

a) Cryptographic implementations that are the subject of this policy include, but are not limited to:

i) SSH access via client key.

ii) RSA tokens.

iii) VPN Client & Server or IPSEC implementations.

iv) SSL client & server certificates.

v) Custom solutions developed in-house.

vi) Disk encryption software such as BeCrypt, or PGPDisk.

vii) COTS software having a cryptographic component.

viii) Black Box solutions such as Ingrian or Protegrity.

ix) P2PE arrpvoed solution

x) PTS approved P01 devices

8.9 Service Provider's Sharing Keys with Customers

If **TfGM** (in a situation acting as a Service Provider) shares encryption keys with its customers for transmission or storage of cardholder data, then **TfGM** must provide documented guidance to its customers on how to securely transmit, store and update customer encryption keys, in accordance with PCI DSS requirements 3.6.1 through 3.6.8 (for service providers only).

9 Glossary & References

9.1 Glossary

See document P99 - Glossary

9.2 References

- P01 – Information Security Policy
- F12 - Key Custodians Form

Policy: IS Key Management				
Version	Change	Reason for change	Date	Name
1.0	Review, update.	Annual review, date & version change.	31/10/2013	C. Burke
1.1	Annual Review	Annual review	06/03/2014	C. Burke
1.2	Update	Updated to include Version 3.0 change variations	16/03/2015	C.Burke
1.3	Date and Version	Annual Review	31/03/2016	C. Burke
1.4	Date and Version	Annual Review	31/03/2017	C. Burke
2.0	Date and Version	Annual Review	31/03/2018	C. Styler
3.0	Date and Version	Annual Review	11/03/2019	C. Burke
4.0	Annual Review and Change	Annual Review and change of IS Team to IS Operations Team and Head of IS to Head of IS Operations	26/03/2020	C. Styler