Implementation Guide

TransLink.iQ Manager v3.0.x Implementation Guide

ASHBURN International

Version: 1.2

2020-11-18

Written by: Date ______________________ Signature ______________________________________

Approved by: Date ______________________ Signature ______________________________________

Change Log:

Version No.	Date	Author	Comment
0.9	2019-11-15	Linas Paukštė	Initial version
1.0	2020-09-21	Daniilas Farberovas	Minor changes and initial version release
1.2	2020-11-18	Daniilas Farberovas	Minor changes: typo corrections

Table of content

1 Introduction

The *Payment Card Industry Data Security Standard (PCI DSS)* defines a set of requirements for the configuration, operation, and security of payment card transactions. The requirements are designed for merchants and service providers who must validate compliance with the PCI DSS.

The Payment Card Industry has also set the requirements for software applications such as ASHBURN International's TransLink.iQ Manager v3.0.x payment application (referred to as TransLink.iQ Manager further in this Implementation Guide document) that store, process or transmits cardholder data. These requirements are defined by the *Payment Card Industry Payment Application Data Security Standard (PA-DSS further in the document)*. In order to facilitate a successful PCI DSS assessment the TransLink.iQ Manager v3.0.x application has been validated and listed in PCI SSC list of validated payment applications as compliant with the PA-DSS v3.2 requirements.

Failure to comply with these standards can result in significant fines should a security breach occur. For more details about PCI DSS and PA-DSS, please see the following link:
http://www.pcisecuritystandards.org

2 Scope

This payment application implementation guide applies to TransLink.iQ Manager version 3.0.x application running on Microsoft Windows Server 2016 Standard.
The Windows Server 2016 Standard, Thales payShield 9000 HSM and TransLink.iQ proxy are the only dependencies required for the full functionality of the TransLink.iQ Manager v3.0.x and in order for it to be configured in a PCI DSS compliant manner.

Since TransLink.iQ Manager does not implement encryption for data in transit between itself and processing host(s), it depends on third party solutions:

- Site-to-site VPN (any secure VPN technology or vendor)
- TLS tunnel provided by stunnel

TransLink.iQ Manager v3.0.x has no other dependencies.

TransLink.iQ Manager v3.0.x's compliance to PA-DSS is important to your business, as performing credit and debit card transactions in a non-PCI DSS compliant environment can result in financial sanctions issued by Card Associations and/or Banks Acquirers, or even the loss of your business.

3 Document use

The purpose of this Implementation Guide is to provide the information needed during deployment and operation of the TransLink.iQ Manager in a manner that will support a merchant's PCI DSS compliance posture.

Usage of PA-DSS validated software solution does not guarantee the that the merchant will be considered to be "PCI DSS compliant" by default. Each merchant is responsible for creating a PCI DSS compliant environment in its control.

Versions of TransLink.iQ Manager software covered by this document can be found on the PCI SSC website in the “List of Validated Payment Applications” section. If currently running version can’t be found on this list, please contact ASHBURN International (the vendow) in order to upgrade the software.

4 What is important to know

TransLink.iQ Manager application typically is used as host based transaction switching and TMS application. Your data security obligations as a merchant, service provider or reseller and/or integrator extend to the payment acceptance system in its entirety.
For example, if you created a custom interface to your TransLink.iQ Manager product, you need to assess your own software code and computer infrastructure for compliance with data security standards.

IMPORTANT:
This document must be read by customers (merchants, service providers, processing centers, banks) and reseller and/or integrator staff who deploy and/or manage PCI DSS in-scope systems prior to moving them to production environment.

5 Requirements and guidelines

Below is the list of security requirements in PA-DSS that are related to any card switching and TMS environment, their interpretation, and how they are handled by TransLink.iQ Manager in particular. The section also explains the actions customers and resellers and/or integrators must take as well as security requirements that customers and resellers and/or integrators must ensure themselves.

5.1. Deletion of historical sensitive authentication data

PA-DSS requires to securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application (PA-DSS Requirement 1.1.4).

How the TransLink.iQ Manager fulfills this requirement
No version of TransLink.iQ Manager has ever stored the Sensitive Authentication Data in non-volatile memory. The data required for processing of transaction that is currently in progress will be irretrievably lost when service is stopped or restarted.

Actions required from Customers and Resellers and/or Integrators
No action is required.

5.2. Deletion of sensitive authentication data collected for debugging and troubleshooting

PA-DSS demands the following when SAD data is used in troubleshooting processes (PA-DSS Requirement 1.1.5):

- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.

PA-DSS instructs that if debugging logs are ever enabled and the logs include PAN, they must be protected in accordance with PCI DSS, disabled as soon as troubleshooting is complete and securely deleted when no longer needed (PA-DSS Requirement 2.3).

How the TransLink.iQ Manager fulfills this requirement
Troubleshooting and debugging tools are not implemented in TransLink.iQ Manager. So, TransLink.iQ Manager never collects the sensitive authentication data or cardholder data for troubleshooting and debugging processes or otherwise.

Actions required from Customers and Resellers and/or Integrators
No actions required.

5.3. Deletion of the cardholder data

PA-DSS requires that all cardholder data must be securely deleted after expiration of customer-defined retention period (PA-DSS Requirement 2.1).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager stores cardholder data until the day is closed.
After day close is processed, all cardholder data is deleted. There is no option to specify a different retention period as this functionality is hardcoded in to the application.

All cardholder data is stored in the .dd file only. File location is configurable.

Actions required from Customers and Resellers and/or Integrators
No actions required. However, do make sure that .dd file is not moved to a new location without changing TransLink.iQ Manager configuration file.

Make sure to exclude or delete the .dd file from your backup or snapshot systems. However, if .dd file is included in the backup or snapshots, systems and processes must be configured in such a way, that .dd file is securely removed from backups and snapshots after retention period (i.e. after day close procedure has succeeded). Moreover, make sure to wipe or physically destroy media that stored the .dd files before discarding the media.

Ensure that hibernation functionality and crash dumps are disabled on any underlying system.
If hibernation and crash dumps are used, make sure to use secure deletion tools to wipe hibernation or dump files should they be generated.

5.4. Secure PAN storage and masking for display

PA-DSS requires to mask PAN when displayed (the first six and last four digits are the maximum number of digits allowed to be displayed to unauthorized people), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN (PA-DSS Requirement 2.2, 2.3).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager displays a masked PAN in the following instances:

- Operator's built-in web-interface.
- .dd file.
- Daily history file.
- Log file.

In all these locations PAN is truncated to 6x4 format and cannot be revealed in full.

PAN masking, truncation and encryption is a hard-coded feature that cannot be changed trough configuration.
In any location where PAN is stored it is stored in either HSM encrypted using AES128 algorithm or 6x4 truncated.

TransLink.iQ Manager is not capable of outputting any cardholder data in a format that customer of TransLink.iQ Manager could use to store outside TransLink.iQ Manager.

Actions required from Customers and Resellers and/or Integrators
No actions required.

5.5. Protect the keys used to secure cardholder data

PA-DSS requires to address the following (PA-DSS Requirement 2.4):

- Restrict access to keys to the fewest number of custodians necessary.
- Store keys securely in the fewest possible locations and forms.

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager depends on HSM encryption and key management functionality.

Actions required from Customers and Resellers and/or Integrators
Restrict access to keys to the fewest number of key custodians necessary and store keys securely in the fewest possible locations and forms using an HSM corresponding manuals. Never export full keys from an HSM device.

5.6. Implement key management processes and procedures

PA-DSS requires to implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data (PA-DSS Requirement 2.5).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager fully depends on HSM encryption and key management functionality.

Actions required from Customers and Resellers and/or Integrators
Please refer to HSM manual for the details on key management, key rotation, key expiration (cyptoperiod) settings of your particular device.
Customer must define a specific cryptoperiod in line with NIST Special Publication 800-57 or other industry best practice. Current best practice for symmetric encryption keys is to set cryptoperiod to 1 calendar year.

If integrity of your encryption key is weakened or is suspected to be weakened (for example key custodian has left the company, changed position, key was compromised or there is a suspicion of any of previous mentioned events, etc.), please follow HSM vendor instructions to retire or replace such keys.
Ensure that retired and superseded keys are never used for encryption again.

5.7. Secure authentication

PA-DSS requires that the payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data.

Software vendor must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication (PA-DSS Requirements 3.1, 3.2).

How the TransLink.iQ Manager fulfills this requirement
Web-based built-in interface is not for administrative purposes and cardholder data cannot be accessed through it.
There only instance where cardholder data can be accessed is .dd file on the file system of the host operating system.
Changes to the configuration (administrative access) of payment application can be performed through changes to configuration file only. Access to configuration file is controlled by the host operating system.

Actions required from Customers and Resellers and/or Integrators
Ensure that the following is addressed on host operating system where .dd file and TransLink.iQ Manager configuration file is located:
Control access to any PCs, servers, and databases with payment applications or cardholder data via unique user ID and PCI DSS compliant secure authentication.

5.8. User access logging, centralized logging

PA-DSS requires that at the completion of the installation process, the “out of the box” default installation of the payment application must log all user access and be able to link all activities to individual users (PA-DSS Requirement 4.1).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager does not utilize any administrative access and cardholder data cannot be accessed by its interfaces. Therefore, it does not have corresponding user rights management and logging.

Actions required from Customers and Resellers and/or Integrators
Ensure that underlying operating system uses PCI DSS compliant configuration settings for audit logs that includes logging logical access to the .dd file. Ensure that centralized logging (central log server accumulating all relevant audit log entries) is implemented for underlying system logs.

5.9. Using of wireless technology

PA-DSS requires to provide instructions for customers about secure use of wireless technology (PA-DSS Requirement 6.3). Customers and resellers and/or integrators must be instructed on PCI DSS compliant wireless settings, as follows:

- Instructions to change all wireless default encryption keys, passwords and SNMP community strings upon installation.
- Instructions to change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager does not use wireless technologies itself, and there are no other applications bundled with the TransLink.iQ Manager that use wireless technologies.

However, *TransLink.iQ Manager is medium agnostic (i.e. it is not aware if data is being sent via physical medium, such as copper wire, or wirelessly as a radio frequency)*. If wireless technologies are used for data transmission to or from the TransLink.iQ Manager or other processing hosts the below listed instructions must be followed and wireless security must be implemented.

Actions required from Customers and Resellers and/or Integrators
When wireless technology is used, Client must:

- change all wireless default encryption keys, passwords and SNMP community strings upon installation;
- change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions;
- install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment;
- use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

5.10. Delivery and installation of patches and updates

PA-DSS requires the following to be provided for customers and resellers and/or integrators (PA-DSS Requirement 7.2.3):

- How the vendor will communicate notifications of new patches and updates.
- How patches and updates will be delivered in a secure manner with a known chain of trust.
- How to access and install patches and updates in a manner that maintains the integrity of the patch and update code.

How the TransLink.iQ Manager fulfills this requirement
We, as the vendor, will inform relevant customer personnel (email addresses defined in legal contract) via email about all TransLink.iQ Manager patches/updates.
Only predefined customer representatives (email addresses defined in legal contract) will have access to the OneDrive account and will be authorized to download patches/updates.
All the patches/updates will be digitally signed in order to ensure integrity of the product.
Software is released as a single monolith binary executable file which is not installed but simply copied onto the file system overwriting the previous file.
Executable files are digitally signed and digital signature can be checked manually to verify integrity before copying the file over to a production system.

Actions required from Customers and Resellers and/or Integrators
Always check the digital signature of patches and updates and make sure it is valid before deploying he update.
Provide and maintain the current and up to date list of email addresses that will have access to our OneDrive account.

5.11. Required services, protocols and additional software or hardware components

PA-DSS requires to document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application, including those provided by third parties (PA-DSS Requirement 8.2).

How the TransLink.iQ Manager fulfills this requirement

TransLink.iQ Manager is developed to be run on Windows Server 2016 Standard operating system. The simple TCP/IP socket is used for connection to TransLink.iQ Proxy. IP address and TCP port number are configurable. Connection with authorization/processing hosts depends on third party requirements. Thales payShield 9000 HSM and TransLink.iQ proxy are the only dependencies required for the TransLink.iQ Manager to be configured in a PCI DSS compliant manner.

Actions required from Customers and Resellers and/or Integrators
Make sure that above listed versions of hardware and software are used in production environment(s).

5.12. Cardholder data storage on public-facing systems

PA-DSS requires the following instructions to be addressed (PA-DSS Requirement 9.1):

- Instructions not to store cardholder data on public-facing systems.
- Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data.
- A list of services/ports that the application needs to use in order to communicate across two network zones.

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager does not require using any web and/or database servers.

Actions required from Customers and Resellers and/or Integrators
Ensure that storage component is implemented in the internal network zone when installing the product. Deploy and use TransLink.iQ Manager with TransLink.iQ Proxy product. TransLink.iQ Manager must be installed in the internal network zone and TransLink.iQ Proxy must be installed in the DMZ. Do make sure not to place the .dd file on any DMZ system.

List of services and ports:
TransLink.iQ Manager is a self-contained software and does not rely on host operating system services and no services need to be enabled. However, there are several TCP ports that must accessible. Port numbers are configurable, so make sure to set your ACLs accordingly, where non default ports are used. Default ports are:
- TCP/6121 from TransLink.iQ Manager to TransLink.iQ Proxy (to retrieve transactions)
- TCP/2080 from operator to TransLink.iQ Manager (operaror’s web interface)
- TCP/6125 from internet to TransLink.iQ Proxy (to receive transactions from POS payment terminals)
Other ports will depend on your infrastructure. For example, TransLink.iQ Manager will need to be able to connect with downstream processing entity, however, specifics will depend on the processing entity.

5.13. Remote access to payment application

PA-DSS requires usage of a multi-factor authentication for all remote access to the payment application that originates from outside the customer environment (PA-DSS Requirement 10.1).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager by design is developed to be accessible from internal networks only. Setting up remote access to TransLink.iQ Manager would violate PA-DSS and PCI DSS requirements.

Actions required from Customers and Resellers and/or Integrators
Do not deploy TransLink.iQ Manager in DMZ and access it from internal segments only.

5.14. Sending CHD over public network

PA-DSS requires that vendor specifies protocols and cryptography for use when cardholder data is sent over the public Internet (Requirement 11.1).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager relies on third party solutions to encrypt cardholder data in transit between it and processing host(s). Two protection methods are accepted:

- Site-to-site VPN connection
- TLS tunnel (stunnel)

Actions required from Customers and Resellers and/or Integrators
No mater which method (site-to-site VPN or stunnel) is selected, it must be configured to use strong cryptography. Sine there are several different VPN technologies, the rule of thumb is to use encryption algorithm ensuring no less that 112bit of effective key strength. Vendor advised to use at least AES128 symmetric encryption algorithm for data encryption in transit. Please refer to the latest release of NIST SP 800-113 and SP800-77 for more in depth details on configuring VPN connections.
In case of stunnel - same rule of thumb applies - use algorithm ensuring at lease 112bit effective strength and again use of at AES128-GCM encryption algorithm is advised. In case if stunnel, it must be configured to use at least TLS v1.2. For more details on secure cipher suites for TLS please refer to the latest release of NIST SP 800-52.
In either case - do ensure that connection is authenticated either through validation of certificate (such as X.509) or other means (such as securely exchanged secret).

5.15. Using of end-user messaging technologies

PA-DSS requires that if the payment application facilitates sending of PANs by end-user messaging technologies (for example, email, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs (PA-DSS Requirement 11.2).

How the TransLink.iQ Manager fulfills this requirement
TransLink.iQ Manager does not support sending of PANs by end-user messaging technologies.

Actions required from Customers and Resellers and/or Integrators
No action required.

5.16. Non-console administrative access

PA-DSS requires the following: if the payment application facilitates non-console administrative access, encrypt all such access with strong cryptography (PA-DSS Requirement 12.1, 12.1.1, 12.2).

How the TransLink.iQ Manager fulfills this requirement
Web-based administrative management or other non-console administration access is not implemented in TransLink.iQ Manager. Administrative level access is through host operating system functionality only.

Actions required from Customers and Resellers and/or Integrators
Ensure that non-console access used to access operating system hosting TransLink.iQ Manager provides strong cryptography to secure remote access session.

5.17. Not applicable requirements

A certain number of PA-DSS requirements where deemed not applicable to TransLink.iQ Manager, either due to its design, intended use or other technological characteristics. Below is a list of those not applicable requirements for the attention of the intended end client, resellers and/or integrators, or other entities involved in managing, deploying or maintaining TransLink.iQ Manager, in case the product is deployed in environment or a fashion not foreseen by the vendor and certain requirement become applicable and must be addressed:

- 2.6 Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.
- 6.1 Securely implement wireless technology.
- 6.2 Secure transmissions of cardholder data over wireless networks.
- 10.2.1 Securely deliver remote payment application updates.
- 10.2.3 Securely implement remote-access software.

6 Versioning methodology

PA-DSS requires description of the vendor's versioning methodology for customers and resellers and/or integrators (PA-DSS Requirement 5.5.4).

How the TransLink.iQ Manager fulfils this requirement
TransLink.iQ Manager payment application version consists of MAJOR.MINOR.PATCH numeric parts. Each part separated by a dot. Increments of 1 are made to the:

- MAJOR version when incompatible API/Protocol changes are made (up to 2 digits).
- MINOR version when adding functionality in a backwards-compatible manner, or change affecting PA-DSS requirements or security is made (up to 3 digits).
- PATCH version when backwards-compatible bug fixes that do not affect PA-DSS scope or security are made. (up to 4 digits).

Wildcard usage. Software version may be referred to by MAJOR and MINOR application versions using wildcards. For example, 1.0.x where x is the wild card identifying any subsequent PATCH. By specifying MAJOR and MINOR version numbers any API, PA-DSS or Security changes will be reflected in exposed version numbers and only insignificant fixes and changes not relted to security of PA-DSS requirements can be hidden by a wild card.

In case of any other type of update not mentioned above, it will be classified above prameters and assigned to either MAJOR, MINOR or PATCH category.

Each time software version is built it has an associated BUILD data, which is not a part of the version number.

- BUILD (optional) data. (up to 16 alpha numeric and symbols, such as - @ + $ % # &).

7 Terminology

3DES – Triple Data Encryption Standard. It describes the symmetric algorithm used for strong data encryption. Also see *Strong Cryptography*.

Cardholder – non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder data – at a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

CVV2/CVC2 – Card Verification Value/ Card Verification Code, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip. Supplying this code in a transaction is intended to verify that the card is present at the point of sale when PAN entered manually or when a voice referral is performed.

ECR – Electronic Cash Register.

EOD – the process called End-of-Day when terminal sends to host the final confirmations of each performed authorization since last EOD. When EOD procedure is finished, terminal purges the data of stored transactions.

Manual key entry – the process when payment card's data (at least PAN and card expiration date) are manually entered into POS payment terminal. The authorization performed with data obtained in such a way is named Manual key entry transaction.

Merchant – any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

PCI SSC – Payment Card Industry Security Standards Council. The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI SSC's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

PA-DSS – Payment Application Data Security Standard created by the PCI SSC. PA-DSS was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications. The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant with the PCI DSS.

PAN - Primary Account Number also referred to as "account number." It is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

PCI DSS – Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Defined by the PCI SSC, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure.

PIN – Personal Identification Number. It is a Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system.

POS – Point of Sale. Hardware and/or software used to process payment card transactions at merchant locations.

Sensitive authentication data (SAD) – security-related information including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks, used to authenticate cardholders and/or authorize payment card transactions.

Strong Cryptography - Cryptography based on industry-tested and accepted algorithms, along with strong key lengths (minimum 112-bits of effective key strength) and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or “one way”). Examples of industry-tested and accepted standards and algorithms for minimum encryption strength include AES (128 bits and higher), TDES (minimum triple-length keys), RSA (2048 bits and higher), ECC (160 bits and higher), and ElGamal (2048 bits and higher).

Vendor – Ashburn International UAB, who develops TransLink.iQ Manager application.

8 Document distribution

This document is delivered in three ways:

1. It is included in the welcome package distributed to customer together with signed contract.
2. It can be downloaded from a publicly accessible web link, included in product instruction document, which is always distributed with a product itself.
3. It is published on Vendor's website.

In case of changes to this document related to TransLink.iQ Manager application security or compliance with PCI PA-DSS requirements or any other significant changes which affect users of TransLink.iQ Manager application, updated document will be sent via email to customers, resellers and/or integrators.

Additional information is provided in Chapter 9.

9 Document reviews and updates

This document is reviewed annually and/or when the TransLink.iQ Manager application is updated and its new version is issued by the vendor. Because the vendor supports the application in accordance to PA-DSS requirements, the new version of the document will be issued when PA-DSS standard is updated, or at any time when it is necessary. Therefore, please be sure that you are using the latest version.

The latest version of TransLink.iQ Manager Implementation Guide can be found on the vendor's web site using following instructions:

1. Go to http://www.ashburn.eu/en,
2. Go to "PRODUCTS",
3. Go to "TransLink.iQ",
4. Find and use the "Download TransLink.iQ Manager Implementation Guide" link.

The latest version of this document also can be downloaded using the direct link:
http://www.ashburn.eu/ASHBURN_International_Manager_IG_V1.2.pdf

10 Key custodian form

Below is vendors proposed form template to be used for key custodians to acknowledge and accept their duties and responsibilities as key custodians.

By signing the below, I thereby confirm that I have read the key management policy and procedures, I have been explained duties and responsibilities of the key custodian, I do understand both procedures and responsibilities and dully accept them.

Role	Name, Surname	Signature	Date
CFO	John Doe		YYYY-MM-DD
CEO	Jane Doe		YYYY-MM-DD

11 References

This document is based on publications listed below:

- PCI DSS (Payment Card Industry Data Security Standard). Version 3.2.1.
- PA-DSS (Payment Applications Data Security Standard). Version 3.2.