PUBLIC

Implementation Guide

TransLink.iQ SmartPOS TETRA v1.1.x Implementation Guide

ASHBURN International

Version: 1.0

2019-10-17

Written by:	Date	_____	Signature	_____
Approved by:	Date	_____	Signature	_____

Change Log:

Version No.	Date	Author	Comment
0.9	2019-10-16	Linas Paukštė	Initial version
1.0	2019-10-17	Daniilas Farberovas	Minor changes and initial version release

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 SmartPOS TETRA v1.1.x payment application (refred to as TransLink.iQ SmartPOS TETRA further in this Implemnetation 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)*. In order to facilitate a successful PCI DSS assessment the TransLink.iQ SmartPOS TETRA v1.1.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 SmartPOS TETRA version 1.1.x running on Telium TETRA platform, using Ingenico Desk and Move device families. TransLink.iQ SmartPOS TETRA 1.1.x application has no other dependencies but Ingenico's Telium TETRA platform.

TransLink.iQ SmartPOS TETRA v1.1.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 installation and operation of the TransLink.iQ SmartPOS TETRA 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 is considered "PCI DSS compliant" by default. Each merchant is responsible for creating a PCI DSS compliant environment in its control.

Versions of TransLink.iQ SmartPOS TETRA software covered by this document can be found on the PCI SSC website in the "List of Validated Payment Applications" section. If version currently running on POS can't be found on this list, please contact your vendor or service provider in order to upgrade the terminal's software.

4 What is important to know

TransLink.iQ SmartPOS family of applications can be used in two ways – either, as stand-alone payment application (running on a dedicated POS / POI device), or as components of a larger payment acceptance

system such as a POS payment terminal integrated with an electronic cash register (ECR). Your data security obligations as a merchant extend to the payment acceptance system in its entirety.
For example, if you created a custom interface to your TransLink.iQ SmartPOS 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 engineers who prepare the POS terminals prior to moving them to production, and also be a part of information source for Service Providers who use a TransLink.iQ SmartPOS family of products as standalone and/or as integrated solution (such as POS + ECR).

5 Requirements and guidelines

Below is the list of security requirements that are related to any environment of a POS application, their interpretation, and how they are handled by TransLink.iQ SmartPOS TETRA in particular. The section also explains the actions merchants must take as well as security requirmenets that merchants must ensure themselves.

5.1. Protect Sensitive authentication data

PA-DSS requires not to retain the Sensitive Authentication Data (PA-DSS Requirement 1.1) that includes:

- Full magnetic stripe data or equivalent data from the chip,
- CAV2/CVC2/CVV2/CID,
- PINs/PIN blocks.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Sensitive Authentication Data is handled in volatile memory prior to authorization and is deleted immediately after the authorization is performed. Sensitive Authentication Data is never stored by the TransLink.iQ SmartPOS TETRA.

Actions required from Merchant and/or Service provider
No special action is required. However, when manual key entry transaction is performed, the CAV2/CVC2/CVV2/CID data must never be written down or otherwise recorded and stored outside the POS terminal by the merchant and/or service provider.

5.2. Deletion of Historical Sensitive authentication data

PA-DSS requires to securely remove and delete any Sensitive Authentication Data stored by previous version of POS Application (PA-DSS Requirement 1.1.4), if any.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA never stores the Sensitive Authentication Data in non-volatile memory. The data required for processing a transaction that is currently in progress will be irretrievably lost when terminal is turned off (or looses power) or TransLink.iQ SmartPOS TETRA application is restarted/reinstalled. So, no action is required, even if POS terminal hardware was previously loaded with an older, non-PA-DSS compliant, version of the application.

Actions required from Merchant and/or Service provider
You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) is removed from all other storage devices used in Your systems (ECRs, PCs, servers etc.) that might have been collected prior to the deployment of *TransLink.iQ SmartPOS TETRA.* For further details please refer to the

appropriate vendor. Removal of historical Sensitive Authentication Data is necessary for PCI DSS compliance.

5.3. Deletion of Sensitive authentication data collected for troubleshooting

PA-DSS permits collection of the only for solving a specific problem. Locations of Sensitive Authentication Data storage must be known and must have a limited access. The amount of data must be limited up to the required for solving a specific problem. Storage must be encrypted. All collected data must be deleted immediately after it has served its purpose (PA-DSS Requirement 1.1.5).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Debugging or troubleshooting mode/tools are not implemented in TransLink.iQ SmartPOS TETRA. So, TransLink.iQ SmartPOS TETRA never collects the Sensitive Authentication Data for debugging/troubleshooting purposes.

Actions required from Merchant and/or Service provider
No actions required.

5.4. Protect stored Cardholder data

PA-DSS permits storage of Cardholder Data only in encrypted, truncated or hashed formats. In case of encryption - only strong encryption algorithms can be used. Storage of Cardholder Data is permitted only when absolutely necessary. Hashed and truncated versions (if stored together) of PAN cannot be correlated to reconstruct the original PAN. The encryption keys used for encryption must be securely stored (PA-DSS Requirement 2.3).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not store the PAN and card expiration date for any type of transactions. Trace file does not contain Cardholder Data. Authorizations performed offline are sent to host immediately upon connection to the host. In case of no connection with the host, terminal holds the queue of unsent frames encrypted by communication transport layer and fully prepared for secure sending through a public networks (as it described in Chapter 5.22 of this document) in non-volatile memory. When connection to host is established, and before proceeding to any other action, POS terminal transmits all data from the queue to the host.
In addition, all PAN outputs implemented in TransLink.iQ SmartPOS TETRA, are limited on software level to first 6 plus last 4 digits. There are no configuration options, which allow modification of PAN storage or output settings.
Moreover, PAN output outside the payment application is always in one of two ways:
- truncated to the fisrst6/last 4 numbers of PAN or
- encrypted in the messaged to the host for authorization.

TransLink.iQ SmartPOS TETRA does not utilize debugging functionality or logs at all. There is no way to turn debugging mode and application logging on in a way that would contain PAN.

Actions required from Merchant and/or Service provider
If payment card is processed using magnetic stripe or chip, then no actions are required.
If Manual key entry authorization is performed, then any cardholder data must never be written down or otherwise recorded and stored by Merchant and/or service provider.
Merchant and/or Service provider must make sure that it did not capture network traffic on POS terminal network/subnet/segment intentionally or unintentionally (in order to avoid encrypted PAN storage contained in communication with the authorization hosts).

5.5. Purging the Cardholder data

PA-DSS requires that all Cardholder Data must be purged after it exceeds the customer-defined retention period (PA-DSS Requirement 2.1).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not store any Cardholder data in terminal's flash memory or underlying software or system. Only truncated PANs (first 6 and last 4 digits) are retained/stored till end-of-day process
Underlying platform vendors does not provide functionality to configure inadvertent capturing or retention of cardholder data.

Actions required from Merchant and/or Service provider
No further action is required form Merchant and/or Service provider to prevent inadvertent capture or retention of cardholder data, because there is no possibility to capture or storage of such data.

However, Merchant and/or Service provider must make sure that it did not capture network traffic on POS terminal network/subnet/segment intentionally or unintentionally.
Prior to removing the terminal from production the Settlement process must be executed manually to ensure the transmittion of all unsent data to the host. Then please reload the terminal with newest version of TransLink.iQ SmartPOS TETRA software. After that a terminal could be placed in a warehouse and be stored as long as it is needed.

5.6. Mask PAN when displayed

PA-DSS requires that any appearance of PAN whether it is on display, receipt, log file or any other screen or media must be masked (the first six and last four digits are the maximum number of digits to be displayed). Only personell with a legitimate business need can see the full PAN (PA-DSS Requirement 2.2).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA displays only masked PAN (max. first six/last four digits) in all instances where PAN is displayed: transaction details section on POS terminal screen, prints masked PAN on receipts. TransLink.iQ SmartPOS TETRA does not store PAN in TransLink.iQ SmartPOS TETRA trace files or transaction history. PAN is stored in truncated form only, thus masking is not available/needed.

Due to the above, display of more than the first six/last four digits of the PAN (full PAN) is not possible using TransLink.iQ SmartPOS TETRA.

Actions required from Merchant and/or Service provider
No actions required.

5.7. Protect the keys used to secure Cardholder data

PA-DSS requires ensuring necessary protection of encryption keys used to secure the Cardholder Data. It is required to restrict access to keys to the fewest number of custodians, and to store keys securely in the fewest possible locations and forms (PA-DSS Requirement 2.4).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not store any Cardholder data in terminal's non-volatile memory. So, no encryption keys are required to ensure the protection of Cardholder Data, and no Key Custodian forms need to be used.

Actions required from Merchant and/or Service provider

No actions required.

5.8. 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 SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not store any Cardholder data in terminal's non-volatile memory. So, no encryption keys are required to ensure the protection of Cardholder Data, and no Key Custodian forms need to be used.

Actions required from Merchant and/or Service provider
No actions required.

5.9. Render irretrievable cryptographic key material or cryptograms

PA-DSS requires rendering irretrievable cryptographic key material or cryptograms stored by previous payment application versions (PA-DSS Requirement 2.6).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Previous TransLink.iQ SmartPOS application version and current TransLink.iQ SmartPOS TETRA application version does not store any Cardholder data in terminal's non-volatile memory, thus no cryptographic key material or cryptograms are present.

Actions required from Merchant and/or Service provider
No actions required.

5.10. Support of User IDs and secure authentication for administrative access

PA-DSS requires usage of unique user IDs and secure authentication for administrative access and access to cardholder data (PA-DSS Requirement 3.1). Unique ID for each user, together with support for access rights hierarchy, must guarantee that each person, who has access to application, is identified, authenticated, authorised and all his/her activities are logged with a goal to ensure the required protection of cardholder data.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not utilize user accounts. There is no user access to administration or card data at all.
TransLink.iQ SmartPOS TETRA does not allow users any access to cardholder data and card data is not stored. No administrative functions are accessible from application user interface. No administrative access to the TransLink.iQ SmartPOS TETRA is possible.

Actions required from Merchant and/or Service provider
No actions required.

5.11. Support of User IDs and secure authentication for access to servers and DBs

PA-DSS requires usage of unique user IDs and secure authentication for access to PCs, servers, and databases containing payment application's and/or cardholder data (PA-DSS Requirement 3.2). Unique ID for each user together with supportfor access rights hierarchy, must guarantee that each person, who has

access to external components used by payment application, is identified, authenticated, authorised and all his/her activities are logged with a goal to ensure the required protection of cardholder data.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS is not installed on or used with PCs, servers, and databases.
TransLink.iQ SmartPOS does not store cardholder data on PCs, servers, and databases.
TransLink.iQ SmartPOS does not allow users to access servers, DBs and any other external components with cardholder data.

Actions required from Merchant and/or Service provider
No actions required.

5.12. Log payment application activity

PA-DSS requires to implement the audit trail that must include a logging of events such as access from application to cardholder data, all actions taken by individuals using administrative level access, attempts of invalid logical access, etc. (PA-DSS Requirement 4.1)

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not allow any user/administrative access, therefore it does not have the user rights management, making it impossible to affect the POS system.

As a result, there is only a tracing functionality and it is limited to saving the initialization events and application failures. This minimum set of tracing events is enabled by default and cannot be disabled.

Actions required from Merchant and/or Service provider
No actions required.

5.13. Automated audit trail

PA-DSS requires to implement an automated audit trail to reconstruct the following events: individual user accesses to cardholder data, actions taken by any an individual with administrative privileges, access to application audit trails managed by or within the application, invalid logical access attempts, changes to the application's identification and authentication mechanisms, initialization, stopping, or pausing of the application audit logs, creation and deletion of system-level objects within or by the application (PA-DSS Requirement 4.2)

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not utilize user/administrator access. TranslLink.iQ SmartPOS does not allow access to cardholder data. TransLink.iQ SmartPOS does not have any configurable options which affect application identification and authentication mechanisms. TransLink.iQ SmartPOS TETRA does not have audit logs.
TransLink.iQ SmartPOS TETRA does not create or manage system level objects except its own configuration file and its own executable update. Executable update and configuration file creation is logged in trace file and submitted to the host as described in "TL-PoSInterface.docx". Logging facilities are enabled by default in the application code and cannot be disabled or configured during or after installation.

Actions required from Merchant and/or Service provider
No actions required.

5.14. Centralized logging

PA-DSS requires to facilitate the centralized logging. Requirement means providing the capability to incorporate the payment application logs into centralized logging server (PA-DSS Requirement 4.4).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not utilize user/administrator access and logging functionality at all, but has tracing mechanism.

The ability to transform the traces to centralized server format is incorporated into TransLink.iQ SmartPOS TETRA. Traces are sent to the host automatically, in a form of text file, without user/operator interaction via already established secure channel with the host. Interface and implementation procedures are described in document named "TL-PoSInterface.docx" that can be requested separately. Usage of centralized tracing service might be necessary to ensure qualified analysing of the cause of problems, if any.

Actions required from Merchant and/or Service provider
No actions required.

5.15. Using of services, protocols and additional software components

PA-DSS states that payment application must only use or require use of necessary and secure services, communication protocols, daemons, components, and dependant software and hardware, including those provided by third parties, for any functionality of the payment application (PA-DSS Requirement 8.2).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA is intended to use only simple TCP/IP socket for connection to the authorization host. IP address and port are configurable. Implemented communication protocol does not affect protection of transferred data and data encryption is implemented in the application itself and does not rely on communication rotocol. All required functionality is incorporated into TransLink.iQ SmartPOS TETRA application and is used independently from any external software and/or hardware.

Actions required from Merchant and/or Service provider
No actions required.

5.16. Using of wireless technology

PA-DSS states that wireless technology must be implemented securely (PA-DSS Requirement 6.1). It means that:

- vendor's defaults including but not limited to default wireless encryption keys, passwords, SNMP community strings, must be changed before moving the terminal to production,
- Firewall must be installed between any wireless network and systems that store cardholder data. Firewall(s) must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA is designed to operate in any network – behind the firewall or in firewall-free environment. TransLink.iQ SmartPOS TETRA by default, at application layer, encrypts all traffic sent to the authorization host and uses a strong encryption for this purpose. That capability guarantees required protection of cardholder data independently from type of communication medium. Therefore, compliance with this PA-DSS requirement will help to protect the authorization host incoming interface from unauthorized connections and DoS attacks.

There are no wireless applications bundled with TransLink.iQ SmartPOS TETRA.

TransLink.iQ SmartPOS TETRA does not manage wireless functionality.
There are no wireless components provided with or controlled by the TransLink.iQ SmartPOS TETRA.

Actions required from Merchant and/or Service provider
When wireless technology is used, Merchant together with his Service provider must ensure the following:

1. Default wireless encryption keys and passwords are changed;
2. The procedure for emergency change of the encryption keys, passwords (including SNMP strings) must be implemented and activated in case of a compromise and/or if anyone who knows the keys leaves the company or changes his/her position;
3. Default SNMP community string is changed;
4. Default passwords are changed;
5. The firmware of wireless module is kept up to dated and supports strong encryption for authentication and transmission. To fulfil this requirements please contact wireless equipment vendor's support;
6. Other security-related wireless vendor defaults are changed,
7. Usage of firewall to protect the traffic inside of the wireless network and permit only authorized traffic between the wireless environment and the cardholder data environment.

5.17. Secure transmission of cardholder data over wireless network

PA-DSS requires to secure the transmission of cardholder data over wireless networks (PA-DSS Requirement 6.2). It means that payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission of cardholder data. The use of WEP as security control is prohibited.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Prior to being forwarded to wireless interface (or rather TCP/IP socket, indipendant from the medium), the cardholder data is encrypted twice by TransLink.iQ SmartPOS TETRA – using AES-128 algorithm with DUKPT and another DUKPT key that encrypts all communication traffic sent to the host and received from it. Each DUKPT key is derived from a different base derivation key.

There are no wireless applications bundled with TransLink.iQ SmartPOS TETRA.
TransLink.iQ SmartPOS TETRA does not manage wireless functionality.
There are no wireless components provided withor controlled by the TransLink.iQ SmartPOS TETRA.

Actions required from Merchant and/or Service provider
When wireless technology is used, Merchant together with his Service provider must ensure the following:

1. Default wireless encryption keys and passwords are changed;
2. The procedure for emergency change of the encryption keys, passwords (including SNMP strings) must be implemented and activated in case of a compromise and/or if anyone who knows the keys leaves the company or changes his/her position;
3. Default SNMP community string is changed;
4. Default passwords on access points are changed;
5. The firmware of wireless module is kept up to dated and supports strong encryption for authentication and transmission. To fulfil this requirements please contact wireless equipment vendor's support;
6. Other security-related wireless vendor defaults are changed;
7. Industry best practices are used to implement strong encryption for authentication and transmission.

5.18. Secure use of wireless technology

PA-DSS states that customer should be aware of secure use of wireless technology even if payment application is not intended for use in wireless environment (PA-DSS Requirement 6.3), it means that:

- Vendor's defaults including but not limited to default wireless encryption keys, passwords, SNMP community strings, must be changed;
- Wireless encryption keys, passwords, and SNMP strings must be changed anytime anyone with knowledge of the keys/passwords leaves the company or changes positions;
- Firewall must be installed between any wireless network and systems that store cardholder data. Firewall(s) must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment;
- Industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission must be used.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA payment application is intended for use in wireless and non-wireless environment. TransLink.iQ SmartPOS TETRA by default, at application layer, encrypts all traffic sent to the authorization host and uses a strong encryption for this purpose.

There are no wireless applications bundled with TransLink.iQ SmartPOS TETRA.
TransLink.iQ SmartPOS TETRA does not manage wireless functionality.
There are no wireless components provided with or controlled by the TransLink.iQ SmartPOS TETRA.

Actions required from Merchant and/or Service provider
When wireless technology is used, Merchant together with his Service provider must ensure the following:

1. Default wireless encryption keys and passwords are changed;
2. The procedure for emergency change of the encryption keys, passwords (including SNMP strings) must be implemented and activated in case of a compromise and/or if anyone who knows the keys leaves the company or changes his/her position;
3. Default SNMP community string is changed;
4. Default passwords are changed;
5. The firmware of wireless module is kept up to dated and supports strong encryption for authentication and transmission. To fulfil this requirements please contact wireless equipment vendor's support;
6. Other security-related wireless vendor defaults are changed,
7. Usage of firewall to protect the traffic inside of the wireless network and permit only authorized traffic between the wireless environment and the cardholder data environment.
8. Industry best practices are used to implement strong encryption for authentication and transmission.

5.19. Secure installation of patches and updates

PA-DSS requires to deliver and install patches and updates in a secure manner (PA-DSS Requirement 7.2.3). Including proper communication of notifications of new patches and updates, delivery of them in a secure manner with known chain of trust, and installation in a manner that maintains the integrity of the patch and update code.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not allow receiving any fixes and/or partial updates remotely except loading of full solution in single module.

TransLink.iQ SmartPOS TETRA checks daily if new updates are pending on the host. Due to that a separate communication and information to customers about new updates is not needed, as it is done automatically.

New version of TransLink.iQ SmartPOS TETRA is delivered from the host in fully automated way using secure update mechanism. Updates are signed by POS terminal vendor tools that guarantees integrity and authenticity of the package. Package is checked using POS vendor mechanisms on installation. Each software release is electronically signed using procedure and protected algorithm developed and supported by POS terminal vendor.

Actions required from Merchant and/or Service provider
No actions required.

5.20. Required protocols, services, components, and dependant software and hardware

PA-DSS demands that TransLink.iQ SmartPOS TETRA required protocols, services, components, and dependant software and hardware that are necessary for any functionality of the TransLink.iQ SmartPOS TETRA itself, including those provided by third parties are documented (PA-DSS Requirement 8.2).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA requires the following:

- TCP/IP stack.
- Port 6125 for establishing connections with host.
- 7015 for establishing connections with POS till computer (ECR).
- Telium TETRA platform.

DNS and DHCP are optional configurations.

Actions required from Merchant and/or Service provider
Merchant or Service provider must ensure that firewall(s), if used, is/are configured correspondingly to requirements mentioned above to allow communication from/to TransLink.iQ SmartPOS TETRA to the host.

5.21. Using of servers connected to the Internet

PA-DSS instructs not to store cardholder data on public-facing systems (for example, web server and database server must not be on same server as web server) (PA-DSS Requirement 9.1).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA is a POS payment application and does not require use of servers, database servers, web-servers, DMZ servers (other public facing systems) that would require Internet connection. Moreover, TransLink.iQ SmartPOS TETRA does not store card data at all.

Actions required from Merchant and/or Service provider
No action required.

5.22. Remote access to payment application

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

be implemented by using user ID and password together with additional authentication method such as a token.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not allow any remote access.

Actions required from Merchant and/or Service provider
No action required.

5.23. Remote access for updates of payment application

PA-DSS requires to activate the remote-access technologies for payment application updates only when needed for downloads, and turn off immediately after download completes. In additional, if computer is connected via VPN or other high-speed connection, receive remote payment application updates via a securely configured firewall or personal firewall (PA-DSS Requirement 10.2.1).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not allow any user type remote access. TransLink.iQ SmartPOS TETRA updates are handled by the host, delivered and installed automatically.

Actions required from Merchant and/or Service provider
No actions required.

5.24. Using of remote access software

PA-DSS requires implementartion ofadditional security features/settings in case a remote access software is used for accessing to payment application (PA-DSS Requirement 10.2.3). Such security features/options can be, but are not restricted to:

- Change the default settings in the remote access software,
- Allow connections only from specific (known) IP/MAC addresses,
- Use strong authentication and complex password for logins,
- Enable encrypted data transmission,
- Enable account lockout after certain number of failed login attempts,
- Use a VPN connection via firewall,
- Enable the logging,
- Restrict access to customer environments to authorized reseller/integrator personnel,
- Implement passwords management as it is required by PA-DSS standard.

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not allow any remote access.

Actions required from Merchant and/or Service provider
No action required.

5.25. Encrypt sensitive traffic over public networks

PA-DSS states that if the payment application sends, or facilitates sending, cardholder data over public networks (the Internet, Wireless including Bluetooth, GSM, GPRS technologies, Satellite communications), the payment application must support use of strong cryptography and security protocols (such as TLS, Internet protocol security (IPSEC), SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. SSL and early TLS are not considered strong cryptography. Applications that use or support TLS must not allow fall-back to SSL (PA-DSS Requirement 11.1).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Prior to sending the cardholder data over network, TransLink.iQ SmartPOS TETRA encrypts it using AES-128 algorithm with DUKPT. In addition, whole communication traffic sent to the host and received from it, is encrypted using AES-128 algorithm with DUKPT. DUKPT keys, used for each encryption event, are derived from a different base derivation key. Thus, any instance of cardholder data sent over network is encrypted twice. Aforementioned data encryption scheme is built-into the payment application and cannot be changed or disabled by the end customer.

Keys used for encryption of transmitted data are generated by HSM and forwarded to POS terminal in encrypted format using asymmetric RSA encryption with 2048 bit key. Each key has its own retention period that is controlled by POS terminal and host automatically. If all or any portion of data cannot be decrypted, then TransLink.iQ SmartPOS TETRA application receives the instruction to renew an actual key. It means that the keys' lifecycle is fully automated, therefore there is no need to have and use any Key Custodian form.

Actions required from Merchant and/or Service provider
No action required. Encryption is always enabled and cannot be disabled by parameterization or user options.

5.26. Using of end-user messaging technologies

PA-DSS states that if the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, 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 SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA does not support sending of PANs by end-user messaging technologies.

Actions required from Merchant and/or Service provider
No action required.

5.27. Encrypt all non-console administrative access

PA-DSS requires encrypting all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. SSL and early TLS are not considered strong cryptography. Applications that use or support TLS must not allow fall-back to SSL (PA-DSS Requirement 12.1).

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
Web-based management or other non-console administration access are not implemented and are not supported by TransLink.iQ SmartPOS TETRA. Any type of non-console administration access to TransLink.iQ SmartPOS TETRA is not allowed.

Actions required from Merchant and/or Service provider
No action required.

6 Versioning methodology

PA-DSS requires description of the vendors versioning methodology for customers and integrators/resellers (PA-DSS Requirement 5.4.4)

How the TransLink.iQ SmartPOS TETRA fulfils this requirement
TransLink.iQ SmartPOS TETRA payment application version consists of MAJOR.MINOR.PATCH parts. 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 wild card identifying any subsequent PATCH. By specification of MAJOR and MINOR version numbers any API, PA-DSS or Security changes will be reflected in exposed version numbers and only insignificant fixes and non-related changes can be hidden by a wild card.

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

Each time software version is built it has an associated BUILD data, which is not a part of 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. See *Strong Cryptography* also.

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 – Card Verification Value, 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 to terminal. The authorization performed with data obtained in such 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.

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.

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.

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 – 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.

Service provider - any company that buys or receives the TransLink.iQ SmartPOS application to install it on POS terminal and use in complex with host solution for authorizing of payment 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 SmartPOS 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 terminal instruction document, which is always distributed with a terminal itself.

3. It is published on Vendor's website.

In case of changes to this document related to TransLink.iQ SmartPOS TETRA application security or compliance with PCI PA-DSS requirements or any other significant changes which affect users of TransLink.iQ SmartPOS TETRA application, updated document will be sent via e-mail 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 SmartPOS TETRA application is updated and its new version is issued by vendor. Because 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.

Initial version of TransLink.iQ SmartPOS TETRA Implementation Guide can be found on vendor's site using following instructions:

1. Go to http://www.ashburn.eu/en,
2. Go to "PRODUCTS",
3. Go to "Solutions for financial and other transactions",
4. Find and use the "Download TransLink.iQ SmartPOS TETRA Implementation Guide" link.

The latest version of this document also can be downloaded using the direct link:
http://www.ashburn.eu/ASHBURN_International_SmartPOS_TETRA_IG_V1.0.pdf

10 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.