Guidelines for Payment Service Provider Porting of Merchant Payment-Related Data

.

Version 0.1

25.11.2024

Australian Payments Network Limited
ABN 12 055 136 519
Suite 2, Level 17, 225 George Street
Sydney NSW 2000

Important Information

Responsibility

These Guidelines were developed by Australian Payments Network Limited (**AusPayNet**) and may be amended from time to time.

Current versions of Standards and Guidelines developed by AusPayNet are available on the AusPayNet website [link].

Feedback

Stakeholders may submit suggested updates, edits, changes, additions, or other feedback on the Standard or any related Guidelines by sending an email to [insert contact details]

Legal liability

To the maximum extent permitted by law, in no event shall AusPayNet be liable for any direct or indirect loss, damage or expense (irrespective of the manner in which it occurs), which may be suffered due to any person's reliance on this document.

Copyright

Written and published in Sydney, Australia by AusPayNet.

Amendment Certificate

The responsibility for amending this document rests with AusPayNet.

AMENDMENT			
Version	Date	Status	Author / Comments
0.1	25.11.2024	DRAFT	AusPayNet

Introduction

Payment gateway services provided by Payment Service Providers (PSPs) enable secure online transactions between merchants and their customers. These services connect a merchant’s website or application to their payment processing system through a secure online portal.

A PSP that is PCI-DSS compliant can hold customers’ sensitive card details, such as the Primary Account Number (PAN) and/or funding PAN (FPAN) on file on the merchant’s behalf. This prevents customers from having to re-enter their card details each time they make an online purchase with the merchant.

A PSP may also tokenise the PAN to protect sensitive data by replacing it with random, non-sensitive alphanumeric data, known as a *Token*. If intercepted by an unauthorised party, the tokenised PAN holds no exploitable value or meaning, as it can only be reversed (detokenised) to the original data by the tokenisation system that created it.

There are two main types of payment Tokens:

- **Scheme tokens** are issued by the domestic and international payment networks / card schemes that are registered with EMVCo, and are for use across the entire payment ecosystem. These are also referred to as Network Tokens.
- **Proprietary tokens** are issued by either a merchant or the PSP that provides the merchant with the ability to process online payments. These tokens are limited to the merchant and/or PSP ecosystem and are not used for sending card-related data to the card schemes.

The ‘*Standard for Payment Service Provider Porting of Merchant Payment-Related Data*’ (Standard) was developed in consultation with industry stakeholders to address friction faced by merchants attempting to switch PSPs that hold their customers’ sensitive card data. In some cases, this friction can be significant enough to prevent switching (i.e. it prevents merchants from moving away from PSPs holding the Merchant Payment-Related (MPR) Data).

1. Preliminary

Definitions

Capitalised terms used in these Guidelines have the same meaning ascribed to them in the ‘*Standard for Payment Service Provider Porting of Merchant Payment-Related Data*’ (‘Standard’).

Interpretation

These Guidelines should be read in conjunction with the Standard and are designed to help Applicable Entities interpret the Requirements and comply with them. If there are any inconsistencies between these Guidelines and the Standard, the Standard will take precedence.

2. Purpose, Application, and Scope

Purpose

In the RBA's Issues paper on '*The Australian Debit Card Market: Default Settings and Tokenisation*'[1] the RBA stated in Section 3.1 that it:

"expects tokenisation to be implemented [for online payments], since it can substantially reduce the amount of sensitive card details being stored – sometimes with minimal security – across the payments ecosystem. However, it needs to be implemented in a way that does not impede the adoption of LCR[2] or competition in the acquiring market more generally."

The Payment System Board's (PSB) May 2024 update reiterated the need to improve the security of card transactions in the online environment. Based on feedback from an industry working group convened by AusPayNet, the PSB decided to adjust and clarify the RBA's tokenisation expectations[3] for the industry. The PSB also endorsed AusPayNet undertaking further work to develop potential technical standards to support token portability.

Expectation 4.ii) of the RBA's tokenisation expectations states that "*Gateways should ensure that their proprietary tokens do not impede merchants switching payment service providers*". Expectation 4.iii) states that "*Token-holding entities should provide, in a secure way, any reasonable data to any 'authorised' third-party required to support token migration, and token migration should be executed in a timely manner*."

Supporting the industry to meet the RBA's portability expectations, the Standard aims to reduce the friction that can impede a merchant switching PSPs. An incumbent PSP being unwilling to send or sending incomplete customer payment-related data to a merchant's new PSP may result in the merchant needing to recollect sensitive card payment details from their customers, or an increase in payment declines. The Standard prescribes a set of requirements for the Porting of MPR Data that:

- details the mandatory payment-related data to be Ported between the Sending and Receiving Parties;
- establishes a common, repeatable process that addresses best practice data Porting security requirements that PSPs can adopt rather than having to build bespoke solutions to Port between different PSPs.

The Standard accommodates both the current prevalence of non-tokenised PAN in the merchant payment-related data to be Ported, but also tokenised data that may be held by a PSP as either a Scheme Token or Proprietary Token.

[1] The Australian Debit Card Market: Default Settings and Tokenisation

[2] Least-cost routing (LCR), also known as 'merchant choice routing', enables merchants to select the card network to process their debit transactions made by a dual-network debit card.

[3] Expectations for Tokenisation of Payment Cards and Storage of PANs - May 2024 | RBA

Application

Entities Holding Merchant Data Approaching End of Life

It is acknowledged that entities holding a merchant's MPR Data approaching end-of-life may choose not to adopt the Standard. However, these entities are still encouraged to follow the practices outlined in the Standard for Porting MPR Data, to enable the merchant to port their data with minimal issues.

Scope

Sending and Receiving Parties can either agree to apply the Standard or will be required to do so where they are unable to reach mutual agreement on the parameters of the data to be Ported between them.

Out of Scope

In addition to the items listed in **clause 2.4.1** it was determined that the Standard would not consider or address:

- **Pricing** related to the porting of MPR Data. However, Applicable Entities subject to the Standard are expected to note the RBA's tokenisation expectation 4.iv that '*only the reasonable costs of processing a token migration should be passed on to merchants'*.
- **Interoperability of Proprietary Tokens**. For example, the Standard does not enable a Proprietary Token issued by the Sending Party to be processed by the Receiving Party.
- **Interoperability of Scheme Tokens**. The Standard does not enable a Scheme Token from one card scheme (e.g. card scheme A) to be processed by a different card scheme (e.g. Card scheme B).

Departing from the Standard

Clauses 2.3.3 and 2.5.1 make clear that the Requirements of the Standard apply when the Sending Party and Receiving Party are unable to mutually agree on the parameters of the data to be ported by the Sending Party. To that end the Standard does not seek to address or supersede any commercial arrangements between those parties.

3. Common Requirements

Requirement #1: Merchant Payment Related Data

Clause 3.1.1 outlines the MPR Data to be ported by the Sending Party, ensuring that the Receiving Party receives the necessary payment-related data to enable future transactions by the merchant's cardholder, without requiring the cardholder to provide sensitive card data, such as the PAN, again.

While the MPR Data indicated in **Table 1: Data Elements**, is payment-related, it is important to note that the Sending Party may also hold non-financial customer data on behalf of a merchant (e.g. customer email, customer billing address etc.). In such cases, the Primary Parties are expected to mutually agree on the Porting of this additional information to prevent the cardholder from needing to resupply it.

Implicit in the Standard is that both the Sending Party and Receiving Party be PCI-DSS[4] compliant, and that the merchant has obtained cardholder consent to store the customer's payment related data.

Absence of the PAN

In some cases, the PAN may no longer be held by the Sending Party, having been purged and replaced with one of more Scheme Tokens. **Clause 3.1.1** of the Standard addresses this by specifying data fields in the minimum data to be ported, which can be defined by the Schemes to support their Token Migration Services. These services are expected to facilitate the porting of TPANs when the PAN is no longer held by a PSP.

Data Elements - Schema Design Key Notes

- The data structure in the **JSON Schema,** outlined in **Annexure A** of the Standard, consists of three distinct, independent entries: merchant records, customer records, and credential records. Each entry is optional, but they include 'child' relationship attributes for association where applicable, allowing the Receiving Party to use these associations. This structure is designed to accommodate the different approaches that may be used by the entity holding the data. For example, a file could contain only the 'credentials' data type without any customer/merchant ID fields, or it could include a single Merchant ID entry with associated credentials. Alternatively, it could feature a more complex structure with multiple merchants, each with their own customer set, and each customer having multiple credentials.

- The Standard does not state the "additionalProperties = false" rule, allowing for additional customisation. This enables the base schema to be extended through bilateral agreement to include any additional data points that are mutually agreed by the parties.

- Validation has been applied against the PAN/expiry fields only, as the other data points are either free-form strings, or are of formats which may vary between organisations, and are thus unable to be standardised.

- The only required parameter for a credential is the credentialID, which is most likely to be the PSP's token ID. The PAN/Expiry data was not made mandatory, to future-proof

[4] PCI Data Security Standard (PCI DSS)

the standard, allowing for the potential migration of a token using the SchemeCustomData sets.

- In **Table 1: Data Elements**, the Customer ID is shown as mandatory if the CustomerID forms part of the primary key of the Sending Party's credential data. This is to accommodate the different data structures used across the PSP ecosystem for those scenarios; in particular, where entities use a primary key which includes the customerID as part of that key structure. For example, if the Sending Party uses a key structure that includes both the CustomerID and Credential ID (e.g. for merchants, customers and multiple customer credentials) while the Receiving Party uses a simpler, credentials-only list with a unique key based on CredentialID alone, the CustomerID is required to allow the Receiving Party to reconstruct unique identifiers in their 'CredentialID' fields.

Requirement #2: Data Transfer Mechanism – Data Encryption

Clause 3.2.1 requires that the entire data file be encrypted using the OpenPGP standard. At this time, field-level encryption for data points such as PAN has not been specified. However, a future version of the Standard may incorporate this requirement if this additional security is considered necessary.

Clause 3.2.2 requires that the Sending and Receiving Parties must either verify Public Keys used for encryption before use, or ensure that they have been received through a trusted communications mechanism. The purpose of this clause is to prevent malicious parties modifying the Public Keys during electronic transmission which would result in the malicious party being able to decrypt the message. Many options exist for addressing this clause, including:

- Send the Public Key to the recipient over email. Sender and receiver verify fingerprint of the Public Key via a phone call.
- Convey the Public Key in an encrypted zip file using AES encryption and a password with a minimum length of 12 characters consisting of uppercase letters, lowercase letters, numbers and symbols. The password shall be transferred using an out-of-band communication channel.
- The Public Key is stored on a thumb drive and couriered to the recipient using a tamper evident package. The serial number of the tamper evident package is conveyed to the recipient using a separate communication channel (e.g. email).
- The public key is stored in a FIPS 140-2/140-3 approved encrypted drive and couriered to the recipient. The PIN/password shall be conveyed to the recipient using a separate communication channel.

Other techniques are acceptable. All techniques must detect or prevent attempts to manipulate the Public Key during transfer from sender to receiver.

Requirement #4: Data Transfer Mechanism – Data Delivery

Clause 3.4.1 requires that the files are transferred via SFTP, and the expectation is that the Sending Party will either operate its own SFTP solution or have access to one.

Requirement #5: Third Party Authorisation and Access

Clause 3.5.1 specifies that when third-party involvement is necessary to support the Porting process, the Primary Party with the direct relationship to the third party is responsible for either obtaining the information required to complete the generation of the MPR Data from the third party, and / or authorising the third party to directly transfer the MPR Data held by the third party to the Receiving Party. For example, if the Sending Party has a direct relationship with a third-party vault provider to store the MPR Data, then the Sending Party is responsible for either obtaining the MPR Data from the vault provider or authorising the vault provider to send the MPR Data directly to the Receiving Party.

It is acknowledged that the involvement of third parties not covered by the Standard creates a risk they may not comply with the data migration requirements. This risk can be mitigated if Applicable Entities seek to incorporate compliance with the Standard in their commercial agreements with relevant third parties.

4. COMPLIANCE MONITORING AND REPORTING

Annual Reporting Requirements

Clause 4.4.1 requires Applicable entities to complete and submit to AusPayNet an Annual Compliance and Monitoring Survey by 31 January each year. This will enable AusPayNet to monitor the effectiveness of the Standard's application and identify any areas of the Standard that may need to be amended.

5. ADMINISTRATION

Implementation timeframe

Clause 5.1.2 outlines a Transition Period to give Applicable Entities time to complete any necessary development work to enable compliance with the Standard's Requirements by the Effective Date.