PASA
3D Secure Implementation

Standard Bank Moving Forward™

Table of Content

Section A

1. Background and context

Card not Present (CNP) fraud has been on the increase in South Africa and has therefore been on the agenda of various PASA forums since 2011.

During February 2013 PASA made a decision to mandate the implementation of 3D Secure for all e-commerce merchants and a deadline of February 2014 was set.

Through interactions with merchants and integrators it became evident that there were implementation challenges and concerns that needed to be addressed at an industry level in order to ensure the efficient implementation of 3D Secure.

An action plan was formulated and executed accordingly.

2. Purpose of the document

The purpose of the document is to provide clarity on a number of key concerns raised during stakeholder engagement in 2013 as well as related actions agreed to address the concerns.

3. Terminology

3D Secure is the collective term used for various authentication services, as supported by each Card Scheme respectively, which allows only the cardholder to use the card. Example of these individual products are Verified by Visa or MasterCard SecureCode.

The term "3D Secure" is derived from the fact that enhanced security features are brought into the three primary domains inherent in a card transaction, namely the:

a. Cardholder – Issuer domain

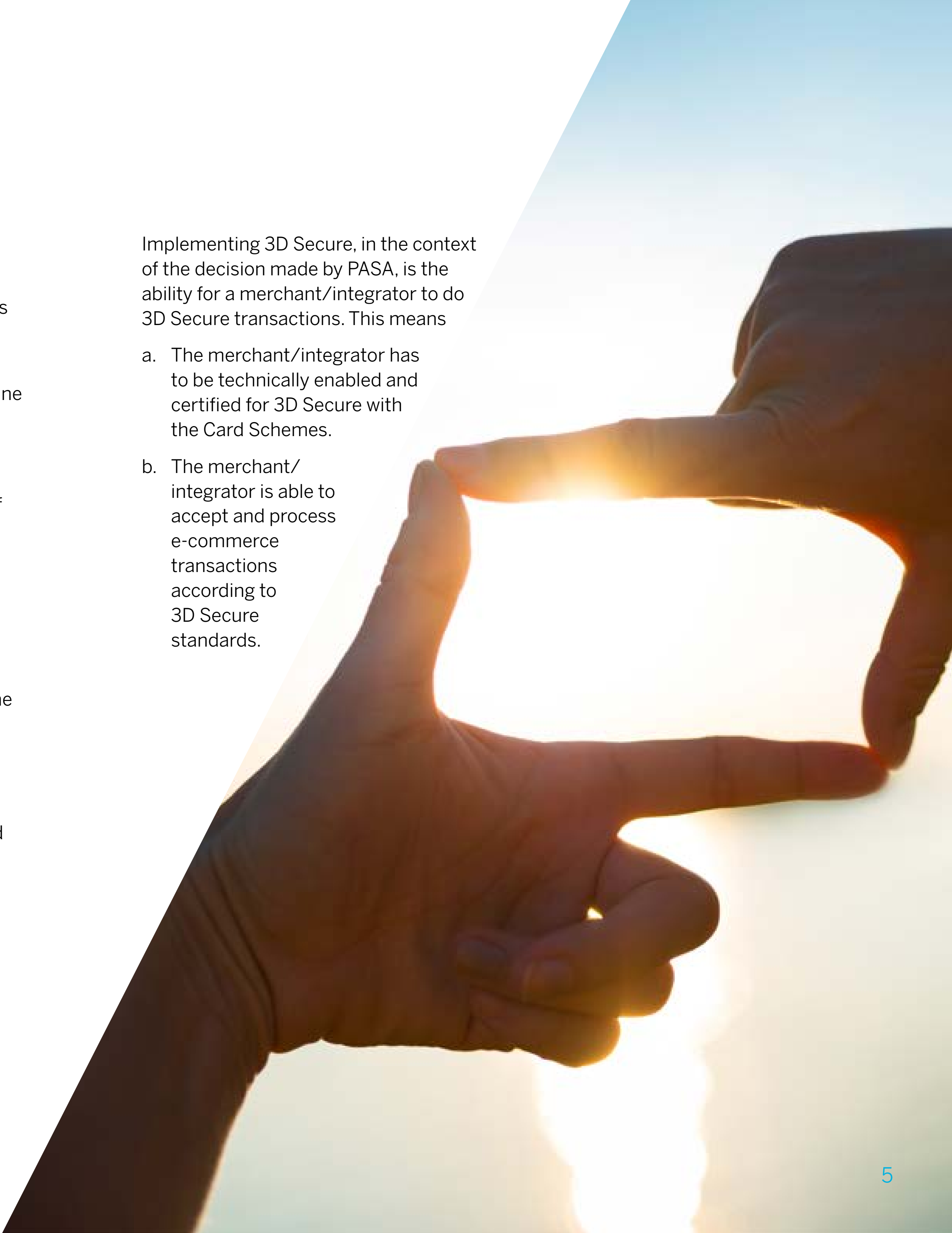
b. Merchant – Acquiring domain

c. Interoperability domain between the banks and their system operators or service providers.

Implementing 3D Secure, in the context of the decision made by PASA, is the ability for a merchant/integrator to do 3D Secure transactions. This means

a. The merchant/integrator has to be technically enabled and certified for 3D Secure with the Card Schemes.

b. The merchant/integrator is able to accept and process e-commerce transactions according to 3D Secure standards.



Section B

Concerns/challenges submitted by banks, merchants and integrators were categorised to enable a summarised view of the practical implementation landscape. This section aims to offer responses to each category.

1. Cardholder education and awareness

Cardholder education and awareness resides mainly with Issuing Banks and banks have constantly been communicating the 3D Secure service to their cardholders. There is, however, always a need for enhanced cardholder awareness and although it may not be merchants' responsibility to educate bank cardholders, it is equally important and beneficial for merchants to ensure cardholders are aware of updated processes and safety features on their websites. Merchants are encouraged to communicate the benefits and processes regarding 3D Secure to their customers accordingly.

Additionally, awareness is raised through focused industry efforts such as the media release and related Frequently Asked Question document for cardholders on 10 March 2014, SABRIC card fraud awareness campaigns and continued communication efforts by the Card Schemes.

2. Cardholder experience

Cardholder experience has been a major concern for many merchants. Over the past 12 months PASA has been working with Issuing Banks to ensure a more cardholder-friendly experience. For merchants, a big part of understanding 3D Secure and the cardholder experience is to understand the different phases and processes that enable 3D Secure. These processes are explained below.

2.1 Cardholder Registration and Activation

There are three distinct processes banks have to follow to enable their cardholders to transact in a 3D Secure manner.

a. **Firstly, all e-commerce enabled BINs have to be registered by banks with the Card Schemes.**

The majority of BINs that are e-commerce enabled are currently registered with the Card Schemes. In some instances Issuing Banks have opted not to register particular BINs, mostly for practical reasons, for example with many corporate cards where sending a One Time PIN to the company's registered mobile number will not be sufficient if there are multiple corporate cards linked to that account.

b. **Secondly, banks have to register/enroll their cardholders for the 3D Secure service. This allows most of the customer information required to be pre-populated, making the activation process more efficient, timeous, and less frustrating for the customer.**

All major banks have either already registered their cardholders for the 3D Secure services. Currently 94% of all e-commerce enable cards have been registered. Similar to the BIN registration process, there are instances where the Issuing bank chooses not to register specific cards, mostly for practical reasons.

c. **Thirdly, cardholders have to activate their cards to enable 3D Secure transactions to happen.**

Although activation processes differ between Issuing Banks, most banks who offer e-commerce transactions to their cardholders currently have processes in place to ensure that cardholders activate 3D Secure, or are automatically activated in most cases, when the first transaction is performed by the cardholder at a 3D Secure merchant.

In most instances cardholders would have been pre-activated by their bank and would merely receive their One Time PIN or relevant activation code. Only in exceptional cases will the cardholder be asked to activate for 3D Secure during the payment process.

Currently 87% of all cardholders have already been activated for 3D Secure, with an expected figure of 94% at the end of March 2014. This means the majority of cardholders will merely be prompted with one additional screen asking for a One Time PIN, static PIN or Password when making their online purchase.

2.2 Inconsistent customer experience

When talking about customer experience there are a number of factors to consider.

a. **It remains a bank's choice which cards/products it allows to perform e-commerce transactions.**

Bank products and the related ability to do e-commerce transactions may differ between banks and is not something that can be standardised.

b. **Banks choose to authorise or decline transactions based on business and product rules.**

The choice to authorise or decline any cardholder transaction is the prerogative of the bank. A bank could therefore approve an e-commerce transaction now and at a later stage decline a similar transaction on the same card, depending on a number of factors that the bank considers. Banks have fraud detection tools, cardholder behaviour rules, card limits, transaction limits and a number of other factors to consider before a transaction is authorised. Similarly, two banks may not have the same business rules in place to approve e-commerce transactions.

Inconsistent customer experience is not unique to the e-commerce environment. Face to face transactions are also subjected to system rules, business rules and processes and various limits, which may vary between products and also between banks.

It is however important to remember that banks do not want to inconvenience their cardholders in any way and would in most instances do their utmost best to rather approve a transaction, except if they have good reason not to.

c. **Banks differentiate themselves by the 'look and feel' of their client interfaces.**

It is recognised that the information requested to complete a 3D Secure transaction should be fairly standard (for example a customer should always be asked for his/her card number, CVV2/CVC2 and card expiry date). Different banks may however design the interfaces where clients enter their details to look different, for example to incorporate their logo or an additional message.

It is also important to understand that these screens are developed according to international standards.

Although all the above factors should be taken into consideration when referring to cardholder experience and the consistency thereof, PASA has confirmed through production testing during February 2014 that the core payment experience for the majority of cardholders are very similar.

3. Cards not eligible for or not technically capable of performing 3D Secure transactions

Although not all Card Schemes currently have a 3D Secure solution and, even within the Card Schemes who do participate, there are certain types of cards that cannot be 'technically enrolled' for 3D Secure, it shouldn't impact the merchant's ability to process transactions performed with these cards. When a card is unable to be enrolled/registered for 3D Secure, the transaction should simply go through the system without the additional layer of authentication and will therefore have an impact on the liability shift, as explained in point 5 below.

There are also two additional points to consider under this topic:

a. **At this stage the majority of e-commerce transaction volumes are derived from Visa and MasterCard products.**

b. **Amex is in the process of developing a 3D Secure solution and should be ready during 2014.**

4. Loss of transactions

There has been a general fear from the merchant community that 3D Secure may cause a loss in sales/transactions due to banks declining and cardholders abandoning transactions.

Although there certainly could be the initial risk of first time customers being anxious about the 3D Secure process, there are a number of different reasons why e-commerce transactions could be unsuccessful.

a. Banks declining transactions at the Authorisation level

Banks may decline transactions submitted for authorisation based on the 3D Secure (authentication) response as well as a number of other factors that may be considered by the bank, for example account status, fraud scoring of the transaction etc.

b. Failed transactions at Authentication level

There are a number of reasons why transactions can fail during the authentication request, however the main reason for this category is incorrect OTP or PIN entered, which include attempted fraudulent transactions.

c. Not completed transactions at Authentication level

This category is made up of a number of different conditions, including time outs and cardholders opting out of transactions. This could happen for a number of reasons, inter alia:

- Cardholders taking too long to enter OTP or PIN
- Delayed OTPs
- Fraudsters abandoning transactions due to not having the OTP or PIN to continue
- Cardholders opting out of transactions due to some merchants requesting non-related personal information during the purchase process

5. Liability Shift

Liability shift is covered by comprehensive Visa and MasterCard rules and have been adopted in the PASA Clearing Rules, but to summarise the position, in most instances the 'non-3D Secure party' in the transaction takes the liability. Therefore, if a merchant is 3D Secure enabled and active, and the cardholder is not, the liability for the transaction would reside with the Issuing bank.

A more comprehensive explanation of liability shift can be found in Annexure A of this document.

6. 3D Secure and Mobile

The mobile landscape is very broad and one has to distinguish between the use of mobile devices to access web and mobi sites and cardholders using a mobile application to perform an e-commerce transaction.

In both instances 3D Secure does not lend itself for use within these environments.

This has been a problem for many merchants and after careful consideration a decision was made to exclude e-commerce transactions that are concluded on a mobi site or native application from the February 2014 mandate for a limited period of 6 months.

This means that:

- E-commerce merchants would not be mandated to submit transactions that are concluded on a mobi site or native application for 3D Secure authentication;
- 'Exempted' transactions would have to be processed to the Issuer as non-authenticated e-commerce transactions; and
- The liability for transactions concluded on a mobi site or native application and not routed for 3D Authentication would remain with the merchant (as is currently the case).
- PASA will use the 6 month extension to conduct further consultation and analysis to formulate a way forward for mobile e-commerce transactions.

In the interim MasterCard has launched the MasterPass product in association with Standard Bank which does allow for 3D Secure on both the mobile site and within the mobile app.

7. Other fraud detection systems

Although there are a number of very effective fraud monitoring systems in the market, these systems serve a different purpose to the 3D Secure process and should be used as a supplement, not replacement, to 3D Secure.

Fraud and Risk detection systems are designed to monitor trends, behaviour and a number of other predefined criteria to ascertain the legitimacy of the transaction. The purpose of 3D Secure however, is to authenticate the cardholder, not the transaction.

Additionally, it should be taken into account that 3D Secure offers liability protection for the merchant, which no other fraud system does.

PASA has considered alternatives to 3D Secure and have found no other industry wide solutions/products comparable to 3D Secure at this stage.

8. International transactions and merchants

Similar to those local cards that cannot perform a 3D Secure transaction, any international transaction, where the Issuing institution does not subscribe to 3D Secure, should merely be processed through the system without going through the 3D Secure process. The transaction should not be declined or delayed and the cardholder should not be impacted at all.

Additionally, whilst Card Scheme rule apply across international jurisdictions, PASA rules only apply to domestic transactions (that is, where a domestic cardholder uses a domestic merchant). Similar to the face-to-face environment, international merchants are not governed by South African rules, except where such an entity is registered as a South African company, in which case it will be bound by local rules and regulations.

9. Technical specifications and standards

The correct population of e-commerce transaction messages are crucial for many reasons including to correctly authorise or decline a transaction, chargeback rights and statistical analysis by all parties in the payments value chain.

As with all payment transactions, e-commerce transactions are required to be compliant to the agreed industry specifications implemented by all banks, PCH System Operators (BankservAfrica, Visa and MasterCard) and all other relevant stakeholders. Where there are instances of non-adherence to these standards, specific examples would assist in resolving this matter and can be communicated to the relevant Acquiring banks.

10. Increased transaction time

It is expected that an additional authentication layer adds additional processing time to any transaction. It is however important to ensure this additional time is kept to a minimum and is included in the technical interpretation and processing of messages in order not to allow undue transaction time outs. The interbank technical specification and approval timeframes currently allow for the additional seconds of processing. Banks, integrators and merchants should ensure that business, operational and technical rules are in line with these timeframes.

It is also important that cardholders are educated about this process in order not be uncomfortable with the extra few seconds it takes. Customer education is addressed under point 1 of this document.

Currently, the average processing time entire 3D Secure authentication process is between 15 and 20 seconds.

Annexure A

3D Secure messages and high level liability shift

Verify enrolment (Directory Server)

(VEReq and VERes)

Y = BIN is registered to participate and a URL is provided

N = BIN is not registered to participate – authorisation process continues without 3D prompting – no impact to cardholder

N for US only Visa and anonymous prepaid cards, no liability shift to Issuer. The current understanding is that merchants are not able to identify when these cards are used, which could be problematic.
N for SA BINs, liability shift to Issuer (wef March 2014)

Verify payment (Access Control Server)

(PAReq and PARes)

Issuer ACS Responses – positive

Y with Cardholder Authentication Verification Value (V) or
Y with Accountholder Authentication Value (M)
These are fully authenticated transactions. An authorisation request may be generated.
Merchant is protected from FRAUD chargebacks [2/05]

Y with Cardholder Authentication Verification Value (V) or
Y with Accountholder Authentication Value (M)
These are fully authenticated transactions. An authorisation request may be generated.
Merchant is protected from FRAUD chargebacks [2/05]

Issuer ACS Responses – negative

U without Cardholder Authentication Verification Value (V) or
U without Accountholder Authentication Value (M)
The Issuer ACS is not able to complete the authentication request. Merchants may proceed with the above purchases as non-authenticated.
Merchant is NOT protected from FRAUD chargebacks [0/07]

N without Cardholder Authentication Verification Value (V) or
N without Accountholder Authentication Value (M)
The Issuer is not able to authenticate the cardholder. Merchants are not permitted to generate an authorization request.
Issuer may have a compliance case against a merchant generating such authorization requests.

For more information on MasterPass please contact 0861 001 200
or email us on merchantservice.cpc@standardbank.co.za or
StandardBank.co.za/MasterPass

Authorised financial services and registered credit provider (NCRCP15)
The Standard Bank of South Africa Limited (Reg. No. 1962/000738/06).
Moving Forward is a trademark of The Standard Bank of South Africa Limited. SBSA 241012 – 6/16