WIZZIT AUTHENTICATOR

AUTHENTICATOR INTRODUCTION

THE EVOLUTION OF AUTHENTICATION

At its most basic level, bank grade authentication is built around a simple concept of the person being authenticated having something unique that is known to the authenticator (e.g. a credit card) which is then combined with something only known to the person being authenticated (eg A PIN) in a secure, encrypted and known format (e.g. via a POS device).

In the world of payments this was not complex where a POS device exists in the physical world, but got really complicated in the e & m-commerce world when the card was not present and a PIN could not be securely entered. Various methodologies emerged to counter this such as 3-D Secure (3-DS) – a protocol to prevent fraud in transactions with credit and debit cards.

However, this introduced new complexities such as managing the performance of an out of band SMS - and besides it came with the weakness that the One Time Pin (OTP) delivered through an out of band SMS, could be intercepted when MNO/Telco networks were involved through a simple SIM swop.

Security methodologies evolved to allow the push of the OTP via more secure methodologies such as Push USSD but the issue is that the message was simply being pushed to a pre-registered device - ownership of which could not be proven and as such the key principle of involving “something I have with something only I know” was fundamentally broken.

Again new technologies emerged to address this– a solution was developed that used a secured MNO’s Wireless Internet gateway to talk directly to the keys of the SIM, allowing the customer to enter their actual ATM/POS PIN directly into the handset. This overcame the aspect of PIN entry and both Visa and MasterCard along with the local payment authority approved a new transaction type – called Authenticated Mobile Transactions (AMT) – which saw non-repudiation in a similar manner to that of a physical POS. Further iterations evolved with similar security methodologies for use in the App world and this has so far proved successful within Masterpass.

Parallel to these developments the world of mobile channels has also evolved. Customer usage of Apps has not been the much-touted success – with customers using a very limited subset of their downloaded Apps. In addition, the move towards Instant Messaging or Chat as it is known has come to dominate messaging – with dramatic declines in SMS and voice usage being noted.

The dependence on Wi-fi has seen many mobile phone users not even making use of an MNO/Telco network anymore – therefore not making use of SMS or USSD. With Chat maturing and able to provide a more relational interface without the requirement for a customer to download an App the next challenge of authentication arises.

THE INTRODUCTION OF CHAT

Most Chat applications provide some form of encryption of their messages, but this is not typically to the level that trusted entities such as banks, cards, governments and others will accept. Not as a result of the absolute technical ability of this encryption but because the encryption processes places control of credentials and keys outside of these entities. Banks for example, want to be able to be the final arbitrator of the authenticity of their own customers, using their own key structures and are not willing to pass this control on to the Chat providers. When it comes to matters of money - authentication is an absolute!

AUTHENTICATION IN THE CHAT CHANNEL

The WIZZIT Authenticator provides a bi-directional bank grade encryption process for the most popular Chat platforms such as WhatsApp, Facebook Messenger, Viber, Telegram and others giving trusted entities such as banks the ability to securely authenticate their customers using their own credentials. The two-way process allows encrypted data to now be sent to the customer as well to receive it – providing new methods of data sharing and authentication – whilst also making use of existing ones without the current worries and concerns.

With a highly flexible customer interface the WIZZIT Authenticator is designed to allow businesses to deploy a secure authentication interface quickly and very cost effectively. The WIZZIT Authenticator can be provided as a turnkey service offering – hosted and operated by WIZZIT or it can be hosted by the customer. WIZZIT can supply all the hardware required.

WIZZIT Authenticator has been patented and has been subjected to rigorous international penetration testing and provides a strong base for compliance requirements such as PCI-DSS. At its core is a bank grade authentication methodology allowing rapid payments, banking and other security applications to be deployed within the Chat world.

WHAT ARE THE CURRENT ISSUES EXPERIENCED?

Fraud Statistics

The increase in digital payments has the unfortunate consequence of attracting increasing levels of crime and fraud. Cyber criminals are a reality as more customers prefer the convenience of digital transactions to cash;

- 40% of the world's card holders have been subject to fraud
- 50% of card holders fear their cards will be hacked while shopping online
- Fraud is costing banks billions of dollars every year.

After a global study with financial institutions, McKinsey provided the following insights into security and the mitigation of risk:

- Vulnerabilities in payments services have increased as the shift to digital and mobile customer platforms accelerates.
- New solutions have also led to transactions being executed quickly, leaving banks and processors with less time to identify, counteract and recover funds.
- Increasingly agile fraud perpetrators have benefited from banks' and payments firms' limited ability to adapt.

It is also frightening to note that the last five years has seen a surge of attacks on the healthcare industry, with the largest breaches impacting as many as 80 million people. Today's challenge is to reduce current losses, detect and prevent emerging fraud, and enhance customer experience.

SIM Swap Fraud

The hottest new fraud trend which has crossed all areas of the globe and is rapidly increasing, involves what is called a "SIM-Swap" fraud. This is real and it will not disappear any time soon. It is done in highly professional and sophisticated way in that you may never see it coming until the last possible moment - the moment when your bank account/trading account/cryptocurrency wallet are compromised and drained.

This is becoming a global issue. This fraud is done by fraudsters who gather customers' personal information through phishing, vishing or any other scams. They proceed to approach/call your mobile operator and block your SIM card. The mobile operator de-activates the genuine SIM and issues a new one and or transfers your number to the new SIM already purchased by the fraudster. The OTP is then generated and sent to the new SIM card held by the fraudster which is required to facilitate payments.

Solution: Working both on an MNO's/Telco's network as well as Wi-Fi - the days of Sim swop and the associated fraud are a thing of the past …when using WIZZIT Authenticator.

OTP (SMS Driven) fraud

As mentioned above, OTP's can be hacked or intercepted. One needs to understand that channel fraudsters are regularly using this to gain access to financial transactions and manipulating or completing them without the customer knowing. Not only are they used by fraudsters, but OTP's are also costly for the bank/trusted entities to send to their clients.

Solution: WIZZIT's integration into the SMS gateway with a secure chat based encryption capability without needing to change any of the current OTP infrastructure that is in existence and reduce the integration timeframe for the bank significantly.

This will enable the bank to save dramatically on their OTP costs. As mentioned above, working both on an MNO's/Telco's network as well as Wi-Fi - Sim swop and the associated fraud will be highly unlikely… when using WIZZIT Authenticator.

Inability to use Chat Channels for payments due to authentication barriers

There have been attempts by institutions to implement chat banking however many of these solutions are clumsy and not user-friendly for the following reasons:

- To authenticate the transaction, the user must exit the bank's chat channel and sign into a third party, supposedly trusted third party APP and secure keyboard application.

- The user has to then enter their credentials before having to return back to the bank's chat channel to complete the transaction.

Solution: The WIZZIT Authenticator offers a fully secure, end to end encrypted PinPad for customers to be authenticated in their preferred channel of choice – their chat applications. Some of the features of the WIZZIT Authenticator are mentioned below:

- Secure issuing of PINs
- Out of band authentication
- Secure limit changing
- Secure messaging customers
- Step up authentication for transactions from another channel and many other applications

Biometric authentication risks

Biometric authentications are starting to become a daily part of our lives with the simple fingerprint or facial recognition authorisation in order to make the payment. In most cases biometric authentication only authenticates the device, but does not authenticate the actual payment. Most smartphones as we know can have more than one person's biometric loaded, hence further opening of the gate to potential fraud.

For micro payments and ongoing pressure from customers for fast, easy payments that tap & go provides, there is a place for biometric and facial recognition as part of the authentication process, being fairly low risk.

Solution: For higher value payments, we strongly believe our Authenticator is a product that will combine well with the biometric authentication which will include a simple push of the Pin Pad to the customers phone.

CONSEQUENCES OF DOING NOTHING

It is vitally important that we continue to beat fraudsters by innovating and ensuring that the right balance between security and customer experience is met. As cyber criminals and fraudsters become smarter and more sophisticated, so fraud costs continue to rise.

For today's digital savvy customers, the WIZZIT Authenticator is a solution for all institutions which will see the right balance between security and customer experience. The WIZZIT Authenticator not only meets but exceeds the banking technical and security requirements and regulations.

IN WHAT SITUATIONS CAN THE AUTHENTICATOR BE USED

The WIZZIT Authenticator can be used in a number of different scenarios which are mentioned below:

1. Customer Logon to Internet Banking and Chat Banking
2. System pushed to the customer for authentication on chat

   - Alerts for verification done over a limit
   - Alerts raised by a fraud engine
   - Call centre agent needs to verify the customer
   - Password change

3. Utilising the application for card authentication with integration directly to the Bank's card switch

   - To enable the customer to change PIN number via chat
   - To push a PIN pad to the customer to select their PIN on the first issue of a card
   - To use the PIN to validate card transactions done via a card
   - As a step-up authentication for tap and go transactions
   - Authorisation of Masterpass and mVisa
   - As a authentication method in addition to the ACS for 3-D Secure.

4. Internet banking login- eliminating issues around SIM Swap

   -The bank/institution can seamlessly replace their current SMS gateway integration with a secure chat based encryption capability without needing to change any of the current OTP infrastructure that is in existence and reduce the integration timeframe for the bank significantly.
   -This would eliminate the risk of SIM Swap Fraud.

OTHER APPLICATIONS/OPPORTUNITIES FOR THE WIZZIT AUTHENTICATOR

Imagine a world in the future where one can securely register for and vote using Chat - order my prescription medicine – pay using my bank PIN – have access to my bank data via a third party – get my bank updates in Chat – approve a debit order – manage my home automation – KYC myself – get my OTP (for anything) – get my PIN sent to me – receive my bills securely – and pay for them - imagine! After years of research, development and certification, the WIZZIT Authenticator makes this possible.

CONCLUSION

In the increasingly digital world, institutions cannot afford to take a chance or a shortcut on security.

However, customers insist on a frictionless experience. WIZZIT Authenticator solves this problem very cost effectively – and has to be balanced with the financial cost and reputational damage of doing nothing.

For further information or to arrange a demonstration and discussion, please call us Contact us.

WIZZIT INTERNATIONAL

- Dirkb@wizzit-int.com
- Davep@wizzit-int.com
- Charlesr@wizzit-int.com
- Brianr@wizzit-int.com

Europe

- Gideonv@wizzit-int.com

Australasia

- Nicholasr@wizzit-int.com

London

- Simonellis89@icloud.com