WIZZIT DIGITAL

A FINTECH COMPANY DEVELOPING & IMPLEMENTING SECURE FRICTIONLESS PAYMENT TECHNOLOGIES.

www.wizzitdigital.com

What lies behind the technology that securely authenticates customers?

WHITE PAPER - Encrypted Mobile Authentication

- **Contact Centre Authentication**
- **Secured Payments over IM**
- **Digital Pin Setting**
- **Chat Banking Authentication**

The Evolution of The encrypted mobile 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 (e.g. A PIN) in a secure, encrypted and known format (e.g. via a POS device).

In the world of payments this is not complex where a POS device exists in the physical world, but gets really complicated in the e & m-commerce world when the card is not present and a PIN cannot be securely entered. Various methodologies emerged to counter this such as 3DS. However, this introduced new complexities such as managing the performance of an out of band SMS. This comes with the weakness that the OTP can be intercepted when MNO/Telco networks are involved through a simple SIM swap. This has become a global problem.

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. Solutions were 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. Further iterations evolved with similar security methodologies for use in the App world and this has so far proved successful.

Parallel to these developments the world of mobile channels has also evolved. Customer usage of Apps has grown but at the same time 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 WiFi has seen many mobile phone users push towards chat making less use of SMS or USSD.

According to Forbes

- There has been a 680% increase in global fraud transactions from mobile apps from October 2015 to December 2018, according to RSA.
- 70% of fraudulent transactions originated in the mobile channel in 2018.

The global increase of 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
- The amount of credit card data available on the dark web has increased by 153 percent over the past year
- Card-not-present fraud is now 81 percent more likely to occur than in-store, or card-present, fraud.
- By 2023, retailers will lose about $130 billion in revenue on fraudulent card-not-present transactions if they fail to keep up with digital fraud prevention measures

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!

Encrypted Mobile authentication

The 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 the ability to securely authenticate their customers using their own credentials. It can however be delivered through other channels such as SMS, in App or email. Our solutions have been built as SDK's and therefore easily embedded into any existing Apps without the need for changes to any existing infrastructure.

- ☑ Our Patented Technology
- ☑ API driven, suitable for many services
- ☑ Meets SCA (Strong Customer Authentication) standards
- ☑ PCI DSS Certified
- ☑ Fully secure, bank standard authentication
- ☑ Out of band, end-to-end encrypted authentication
- ☑ Authentication can be delivered through any chosen channel and forms part of our Tap2Pay solution {WhatsApp, Viber, Telegram, Facebook Messenger, Email, SMS}

Our authentication can be used for multiple purposes, along with the secure benefits, customers do not need to download anything to their mobile device for the authentication.

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.

WIZZIT Digital being at the forefront of mobile technology acknowledged the importance of having to keep up with customer trends and offer services in channels customers use. It was important that with the move to chat channels we offered a convenient and secure way of authenticating customers. The combination of high level of security and customer convenience was critical to our technology design.

Some of the use cases and new opportunities our Authentication will offer:

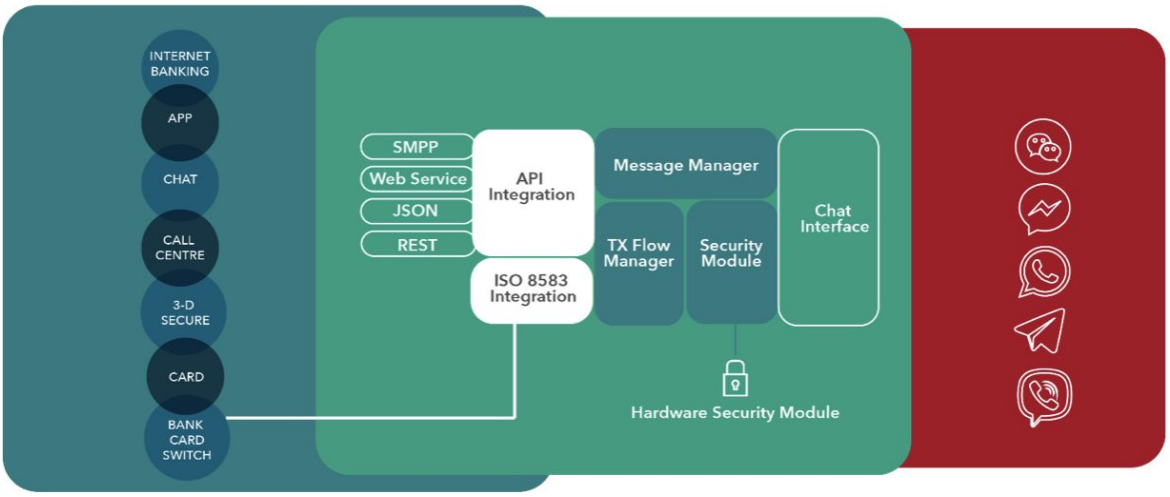
- Secured Payments – SCA compliant therefore offering a PSD2 solution
- Contact Centre Authentication - Establish customer identity via IM, eliminate the security questions
- Fraud alert authentication
- Chat Banking Authentication - Give your customers a new channel to transact and communicate with your bank (payments, bill payment, balance enquiry, etc) all on the platform they spend most of their time
- Digital PIN issuing/changing - Replace your pin mailers with pin selection via app

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

The Authenticator is PCIDSS certified.

Architecture

The Architecture is designed as a stand-alone application that can be accessed by the development team via a set of API interfaces. An example of this shown below would be the integration of the solution into a banking environment.



The API Integration that can be used to access the Authentication services is as follows:

- SMPP to replace the SMS gateway and send request and authorisations via Chat
- Web service, JSON and REST API for the integration of the Chat application and other services that may require authentication.

The system has an ISO 8583 Host to host node that allows for the connection of the authenticator to the banks card system to do the following for example:

- Debit and Credit card PIN authorisation
- PIN Selection by the customer on the issue of a new card
- Changing of the card PIN.

The message manager takes the input from the API and manages the format of the message and OTP or if required directs this to the ISO 8583 Interface.

The transaction flow manager, as the name suggests manages the sequence and the response based on the specific transaction type.

The security module interfaces to the Hardware security module and ensures that the encryption of the sensitive data is handled correctly.

The Bank will load their security keys on the HSM to ensure that all secure transactions are end to end encrypted.

The Chat Integration allows the system to push and receive messages from the various chat platforms. It also manages the interaction of the secure PIN pad for the capturing of sensitive data.

The following Chat interfaces are supported:

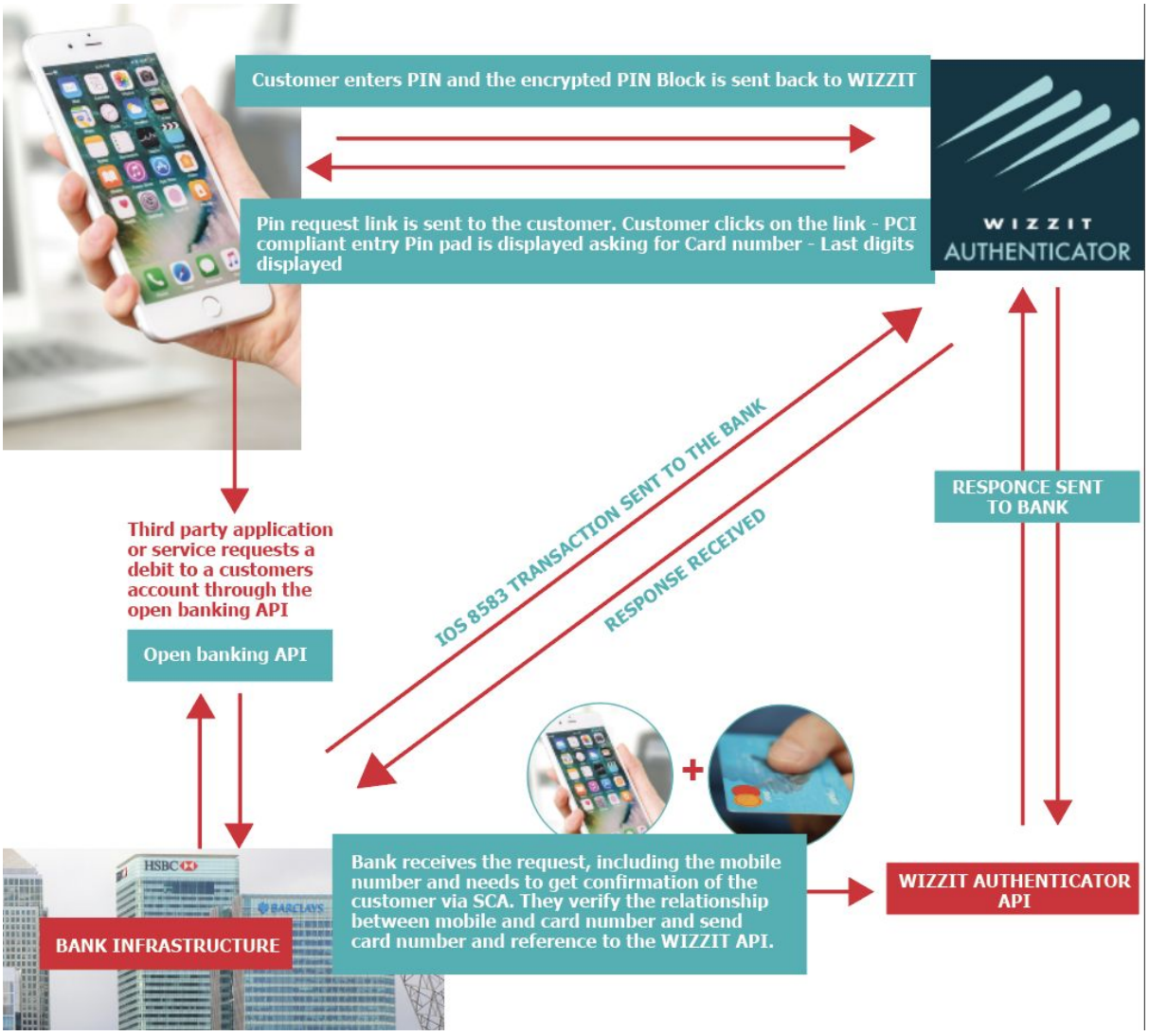
- WhatsApp
- Facebook Messenger
- Telegram
- Viber

On PSD2

Product definition

With the requirement for SCA (Strong Customer authentication) for Payment Services directive 2 (PSD2) WIZZIT Digital has developed an authentication mechanism that allows the bank where the account is held to do a full verification of the customer using the card PIN.
The customer may use a vendor app supplied by a third party that now requires payment. The third party vendor is connected to the banks Open API and does a request to debit the customer's account allows the bank to send through a request for confirmation to the customers device.

View the Process Below:



Infrastructure

Two separate Data centres are required to host the application. Both data centres need to be PCI DSS Compliant. Each data centre will host the application in its own secure VLan behind the banks firewall.

The following is required for each data centre:

- Safenet Protectserve HSM
- x86 4 Core server with 64 gig ram and 500 Gig storage

Transaction scenario

The following transaction flows are indicative of what can be done using the authentication channel.

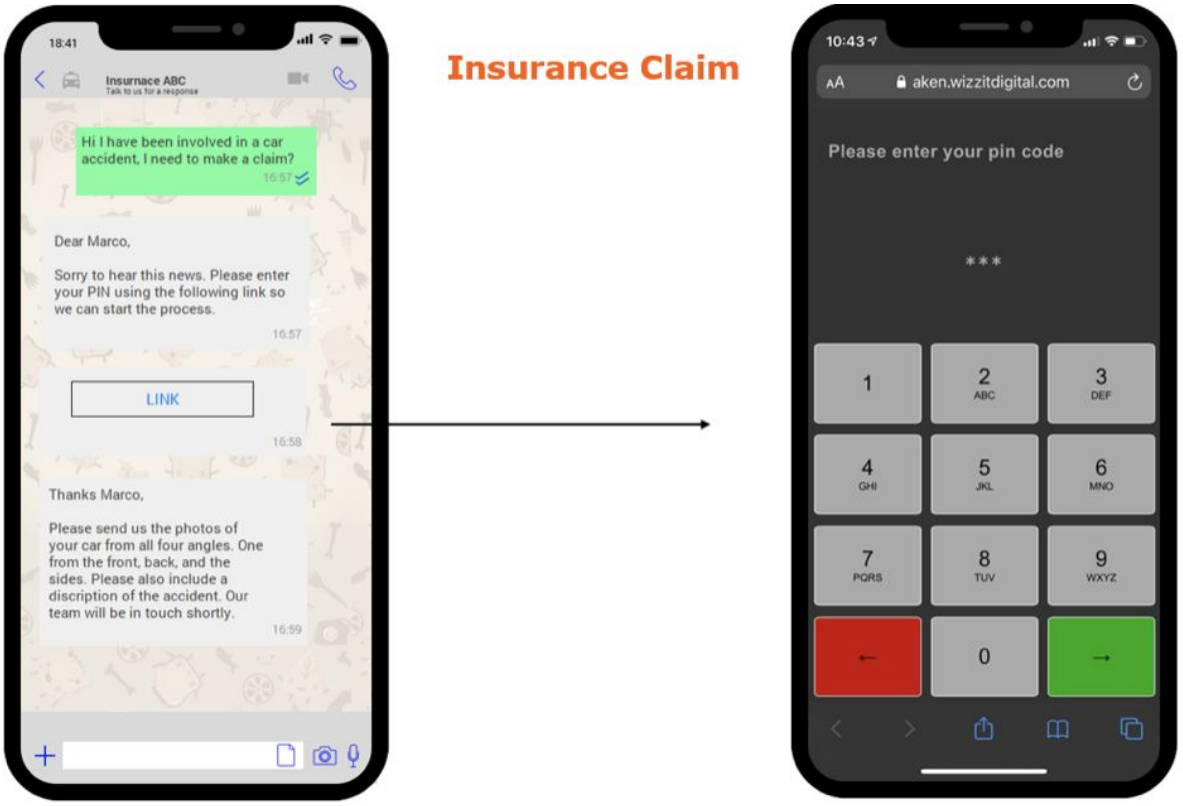
Scenario 1:

Contact Centre Authentication

- Reduce call centre staff by authenticating through your App/Chat channels
- Reduce SLA levels
- Eliminate the security questions

- Improve customer satisfaction by not having to ask a number of security questions
- Allow for your chatbot to implement/call our our authentication and provide personal data to your customers without the need of an agent
- Call centre agents will be able to authenticate your customers over the phone by sending (pushing) a link which contains our secure authentication Pin Pad {This can take place in WhatsApp/SMS or other chat channels}
- We can authenticate your customers by any method you currently use or want to use (Account number/ID number/PIN) with our secure Pin Pad

Authentication call centre contacts & any required person documentation



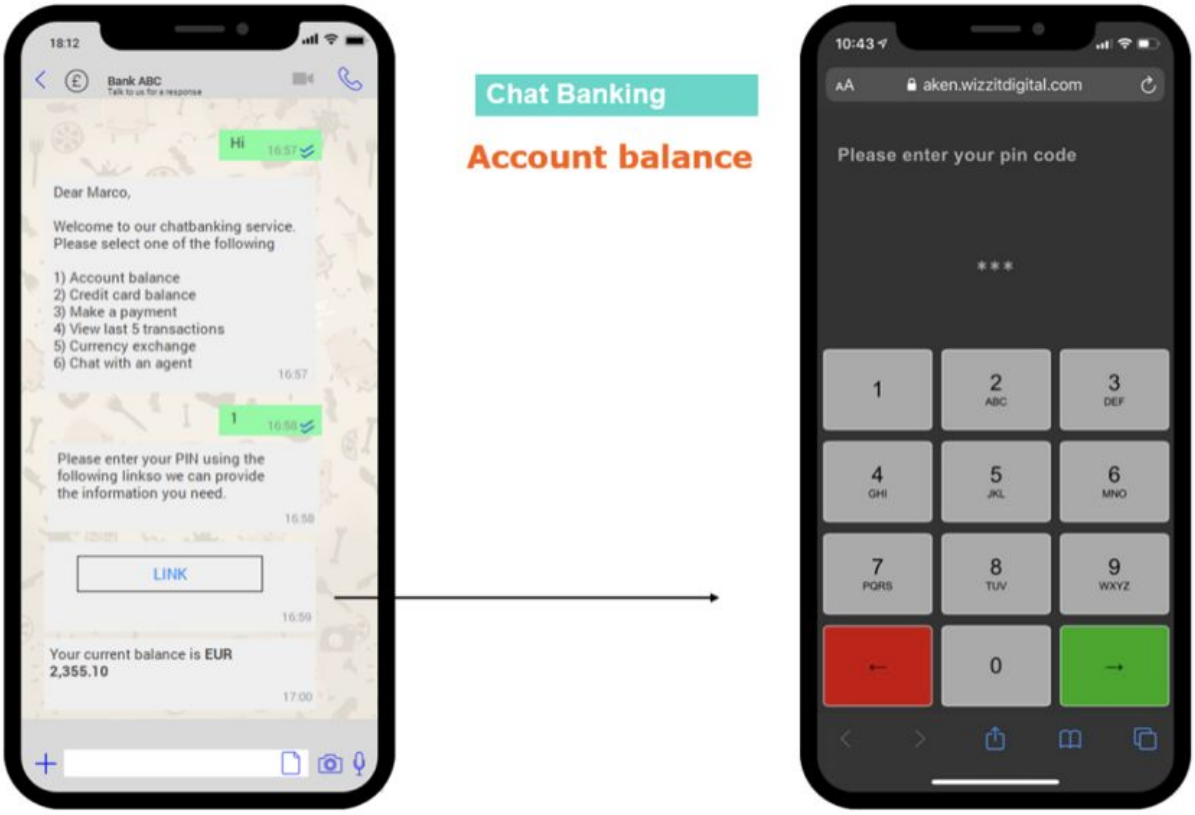
Scenario 2:

Chat Banking Authentication

Chat Banking Authentication

- Your bank can now offer a new payments channel
- Authentication accepted through chat; WhatsApp, Viber, Telegram, FB Messenger
- Give your customers an exciting opportunity to transact (P2P payments, pay bills) through their channel of choice

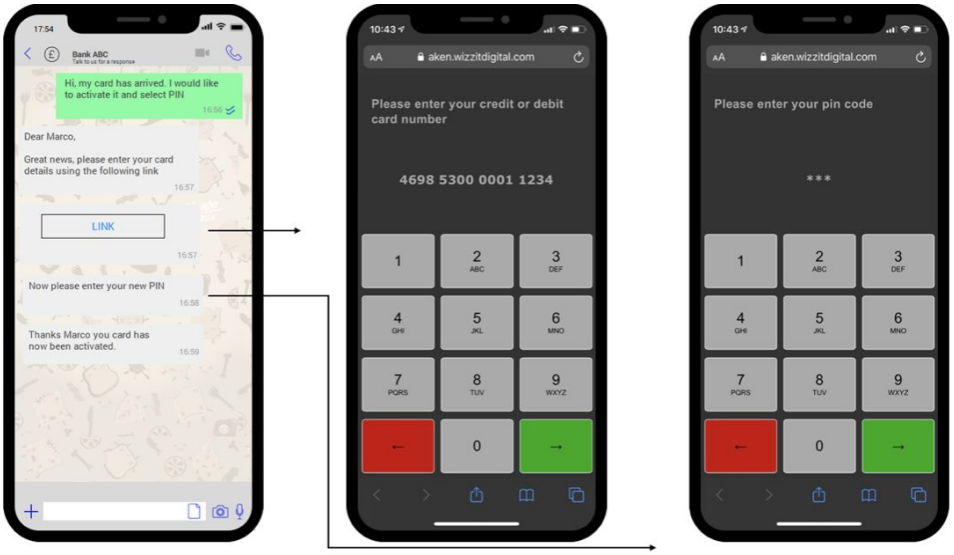
PIN Issuing or PIN Changing:



Scenario 3:

Digital Pin Issuing

- Customers now do not need to wait for an extra post-delivery with their Pin
- Saving money, time and a safer method
- Increase customer satisfaction
- We can integrate our Authentication into existing App's without changing any current infrastructure
- Can be done through a Chat channel



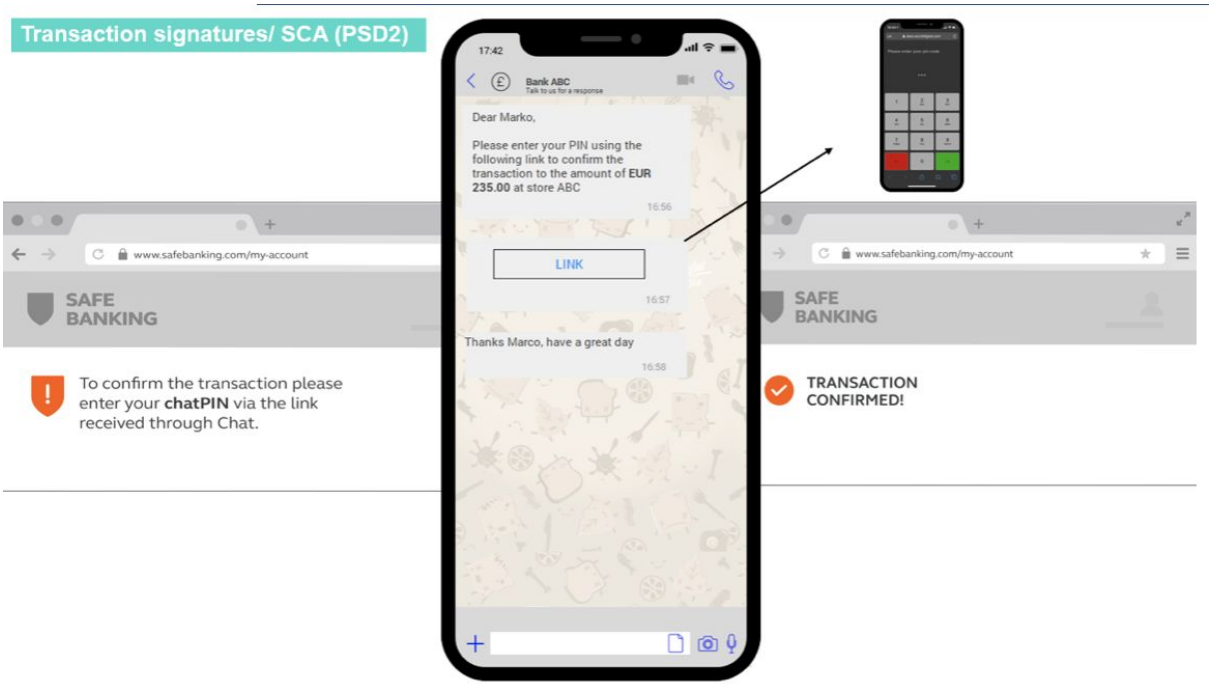
Scenario 4:

Enabling Secure Payments

- Replace your OTP (one-time pin) with our secure authentication methodology
- Safer, eliminating SIM Swap fraud
- Complies with SCA standards by sending the link to:

-something you have (mobile)

-something you know is your Pin



Tap2Pay

Based on the Encrypted Mobile Authenticator, we have developed a payment product with the ability to deliver two main solutions:

1. SoftPOS Solution
2. eCommerce Solution

Our object is to enable institutions to securely authenticate customers or payments as well as grow card acceptance and product use.

Scenario 1

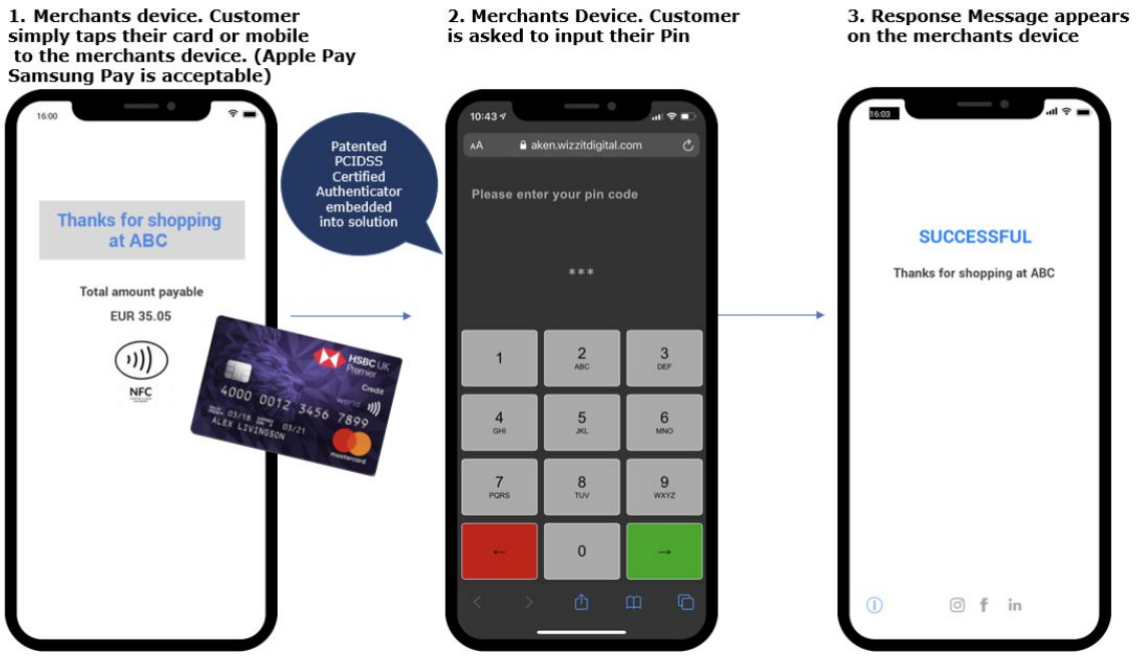
Merchant Solution: (Includes the built in Encrypted Mobile Authentication)

Where the mobile becomes the PoS. Thanks to the patented secure Pinpad, not only for low value transactions but all value transactions through contactless card payments are accepted. {creating the ability to replace the existing PoS, mPos, dongle solutions all together}

Benefits:

- Smaller merchants can accept card payments through their mobile
- Cheaper running costs, no POS hardware needed
- No maintenance or monthly fees
- Faster checkout process with multiple mobile devices being used as a SoftPOS
- Same process as what customers know today
- Our secure Authentication built into solution

Tap2Pay - SoftPOS Merchant Solution



eCommerce solution:

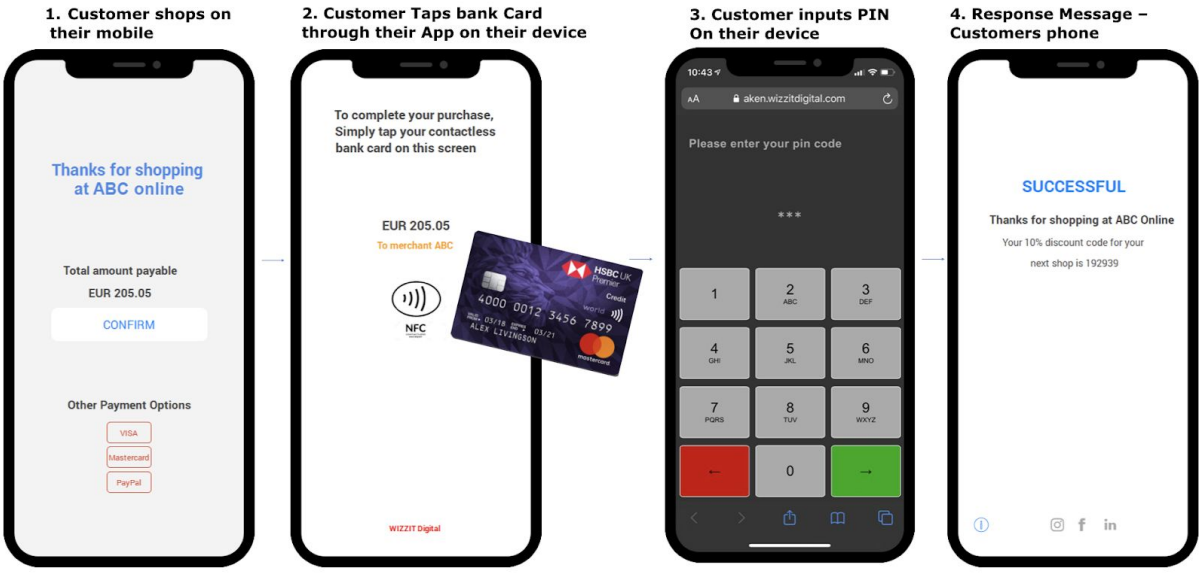
Where the technology functions to combat Card Not Present transactions for e-commerce payments since the solution can be installed on any Andriod phone or embedded in any other app.

Benefits:

- Dramatically reduces merchant costs– we enable Card Present EMV transactions
- Safer payment environment, transactions can not be spoofed through data transmissions
- Allows all merchants to accept card payments online in a safe Card Present environment
- No OTP (One Time Pin) authentication required due to a Card Present Purchase
- Customers do not need to give their card details away online

See Diagram Below:

eCommerce CNP moved to CP



For further information or to arrange a demonstration and discussion, please call contact us:

CONTACT US

South Africa, Africa, Central America

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

Europe

- Gideonv@wizzit-int.com

London & Australasia

- Nicholasr@wizzit-int.com
- Leonards@wizzit-int.com