PSD2 Customer Authentication & Payments In Chat

# WIZZIT Authenticator

November 2019

www.wizzit.com

## 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 (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 can not 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

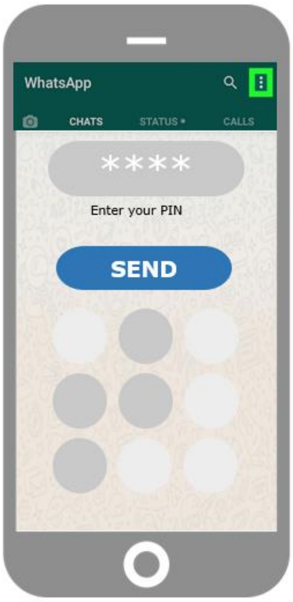
## THE INTRODUCTION OF CHAT

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!

## OUR SOLUTION AND HOW WE HELP COMBAT FRAUD

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 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.



Customers can receive a link in their chat channel where they can enter their PIN safely, securely and easily –

**WITHOUT the client having to download anything onto their mobile device.**

The creation of a fully end-to-end encrypted out of band channel, allows for the secure bank standard authentication, enabling sharing of secure information, payments or to simply authenticate customers.

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 market issues our authentication will help with:

- Decreasing SIM Swap fraud levels
- Complying with SCA (strong customer authentication) regulations
- Fraud alert authentication
- Digital PIN issuing/changing

Some new opportunities our authentication will offer:

- Providing a new payment channel for customers

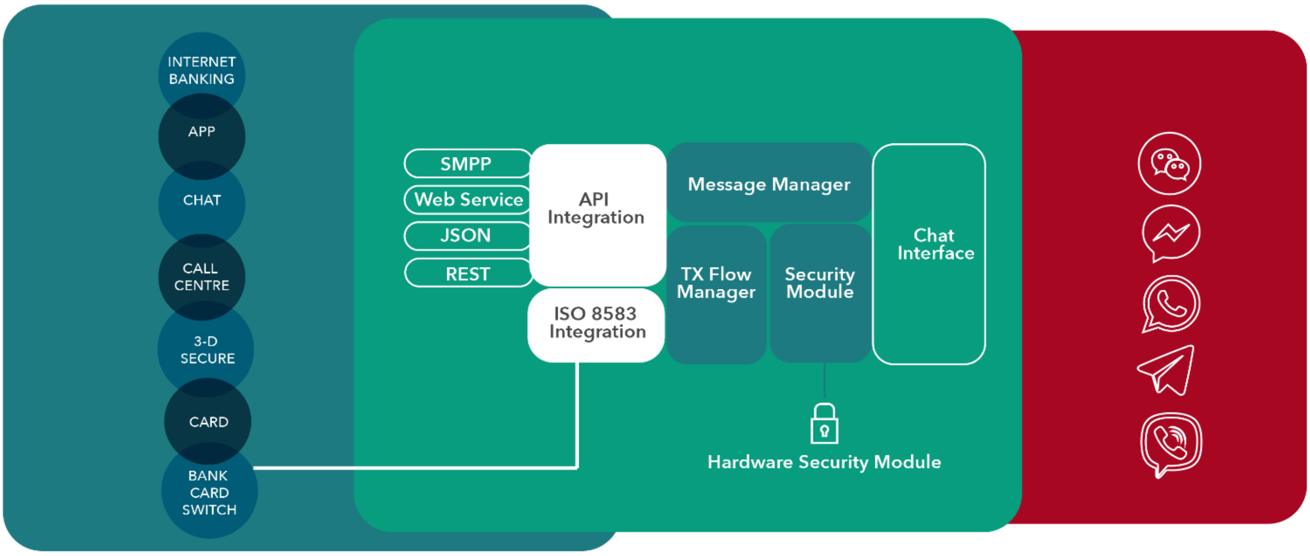
- Call centres to can now authenticate and chat to customers in their channel of choice
- Chat banking is now here

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. It can be provided as a turnkey service offering – hosted and operated by WIZZIT or it can be hosted by the customer.

The WIZZIT 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
- WeChat

## 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.

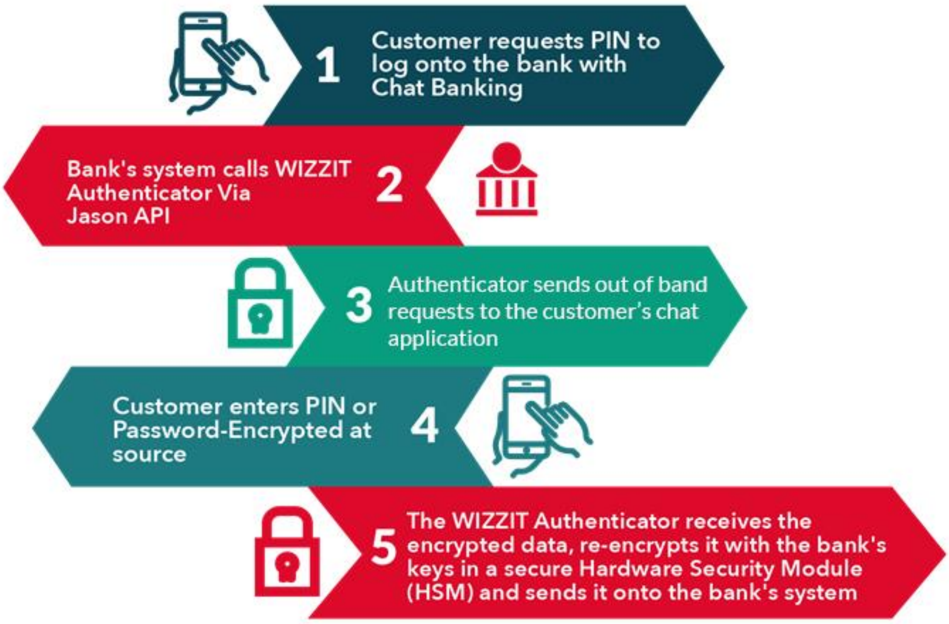
### Scenario 1:

### Customer Logon

This method is useful for

- Chat logon
- Internet banking logon

## The Process below shows the interaction between the Customer, the Bank and the WIZZIT Authenticator when a customer wants to login to their Chat banking or internet banking platform



1 Customer requests PIN to log onto the bank with Chat Banking

2 Bank's system calls WIZZIT Authenticator Via Jason API

3 Authenticator sends out of band requests to the customer's chat application

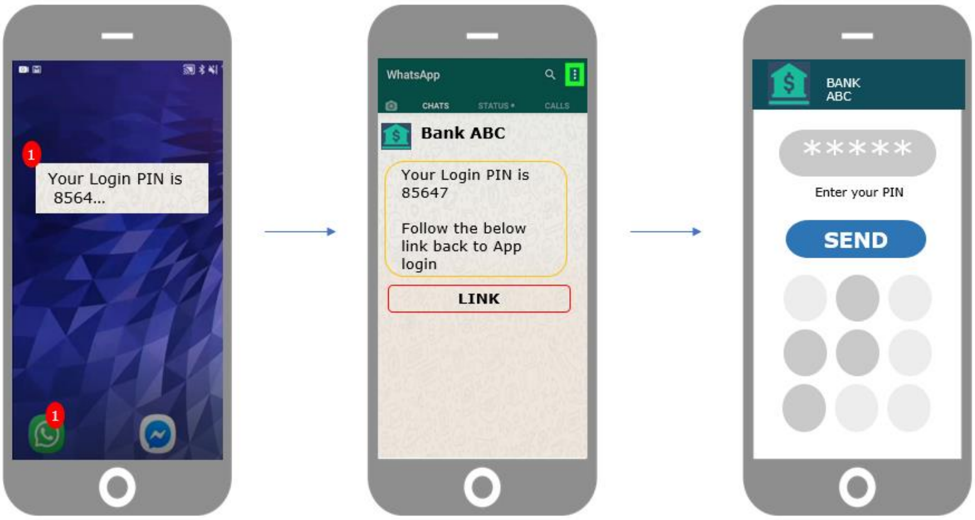
4 Customer enters PIN or Password-Encrypted at source

5 The WIZZIT Authenticator receives the encrypted data, re-encrypts it with the bank's keys in a secure Hardware Security Module (HSM) and sends it onto the bank's system

## A customer requests a PIN to login to their chat application:

1. The Banks chat application sends a request for the PIN to the Chat application server.
2. The bank responds from the chat server via the API to the WIZZIT Authenticator.
3. The Authenticator Pushes an out of band push request containing a keypad. This allows the transaction to be encrypted at source.
4. The customer enters the PIN / Password which is encrypted using a DUKPT (Derived Unique Key Per Transaction) Method as well as the Authentication of the device, to counter the Man in the middle attacks.
5. The Authenticator receives the encrypted information. This information is sent to the HSM (Hardware Security Module) and encrypted with the Banks keys. The re-encrypted information is then sent to the bank. The bank at this stage can now decrypt or validate this information to allow the logon to proceed.

## The customer experience:



Your Login PIN is 8564...

Bank ABC

Your Login PIN is 85647

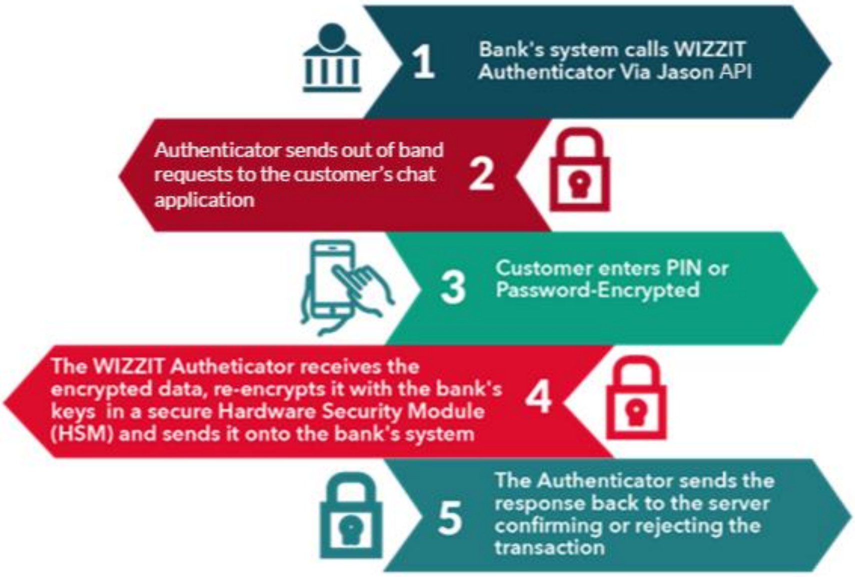
Follow the below link back to App login

### Scenario 2:

### System pushes to customer for authentication on chat

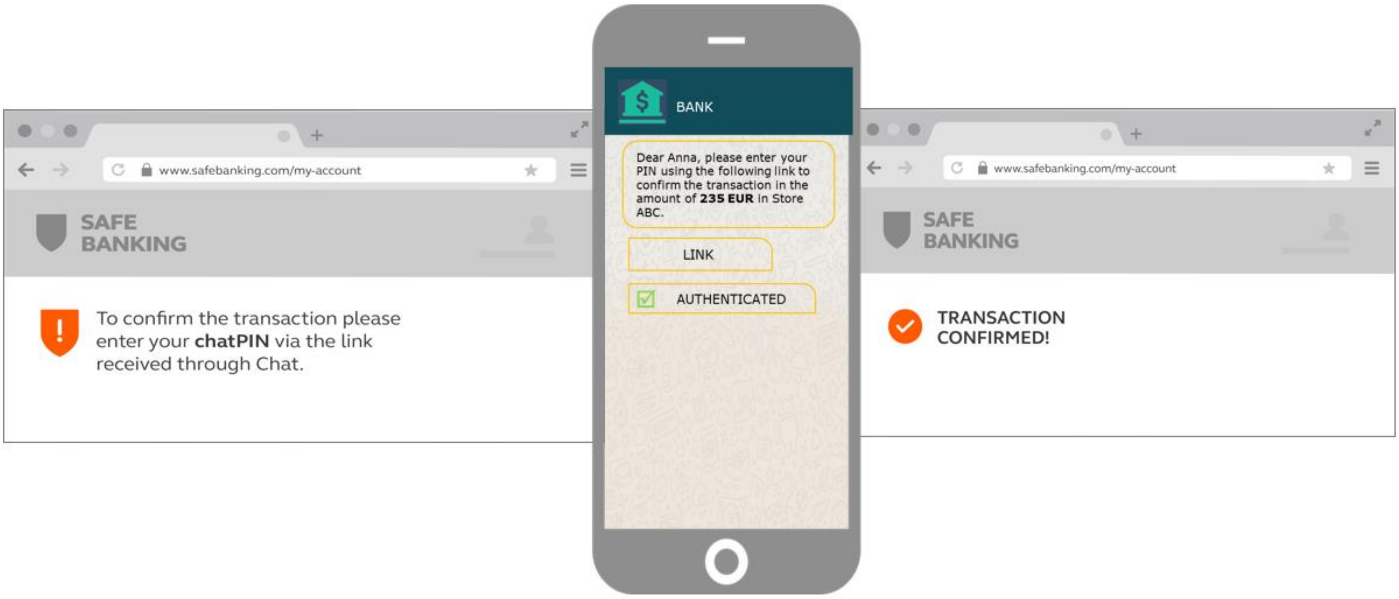
The scenario is the same as the one above except that the transaction is not initiated by the user. The initiation of the transaction is from the system. This method is useful for:

- Alerts for verification where a transaction is done over a certain limit.
- Alerts raised by the Fraud engine and, an authentication request is required, an authentication request can be pushed automatically to the customer.
- Where a call centre agent needs to verify the identity of a customer.
- Where a password needs to be changed by the user.


1
Bank's system calls WIZZIT Authenticator Via Jason API
Authenticator sends out of band requests to the customer's chat application
2
3
Customer enters PIN or Password-Encrypted
The WIZZIT Autheticator receives the encrypted data, re-encrypts it with the bank's keys in a secure Hardware Security Module (HSM) and sends it onto the bank's system
4
5
The Authenticator sends the response back to the server confirming or rejecting the transaction

1. The organisations application that requires authentication will, at that point call the WIZZIT Authenticator via the API to trigger the request for Authentication to the client.
2. The Authenticator PIN pad is then sent to the customer handset and displayed on their handset.
3. The customer enters the PIN or Password required in the PIN pad. The information is then encrypted using the Organisations keys in the HSM.
4. The Authenticator receives the encrypted data and sends it on the bank or organisation for validation.

### The customer experience:


www.safebanking.com/my-account
SAFE BANKING
BANK
LINK
AUTHENTICATED
www.safebanking.com/my-account
SAFE BANKING

To confirm the transaction please enter your **chatPIN** via the link received through Chat.

Dear Anna, please enter your PIN using the following link to confirm the transaction in the amount of **235 EUR** in Store ABC.

TRANSACTION CONFIRMED!

### Scenario 3:

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

This process is useful wherever the card PIN is required to authenticate a client, or a card PIN needs to be changed or issues. The push transaction can be system or call centre initiated. The same process is followed for Push transactions mentioned above but has the ability to do authentication of credentials to the bank's card switch.

The API allows for the bank to provide the Customer's mobile phone details as well as the card that needs the number validated.

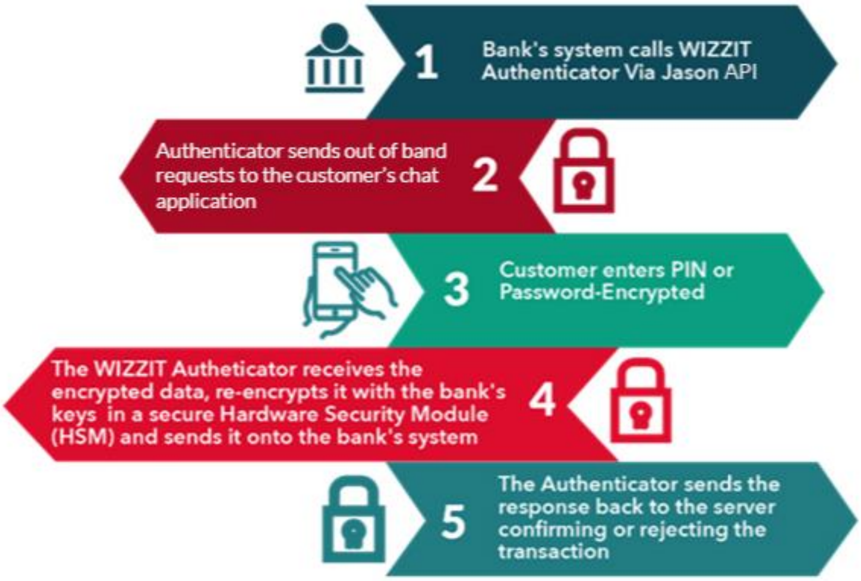
The Bank will have loaded their session keys on the WIZZIT HSM as well as the PIN block utilised. Once the customer is requested to authenticate a transaction or authorise using their PIN, The WIZZIT Authenticator will process the transaction directly to the bank's card switch allowing for the authentication of the customer's PIN.

The benefits of this are that the customers already have a pin number that they already know which will enable identification and authorisation.

### Examples of where this can be used are as follows:

- Enable the customer to change customer 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 an authentication method in addition to the ACS for 3-D Secure



1 Bank's system calls WIZZIT Authenticator Via Jason API

2 Authenticator sends out of band requests to the customer's chat application

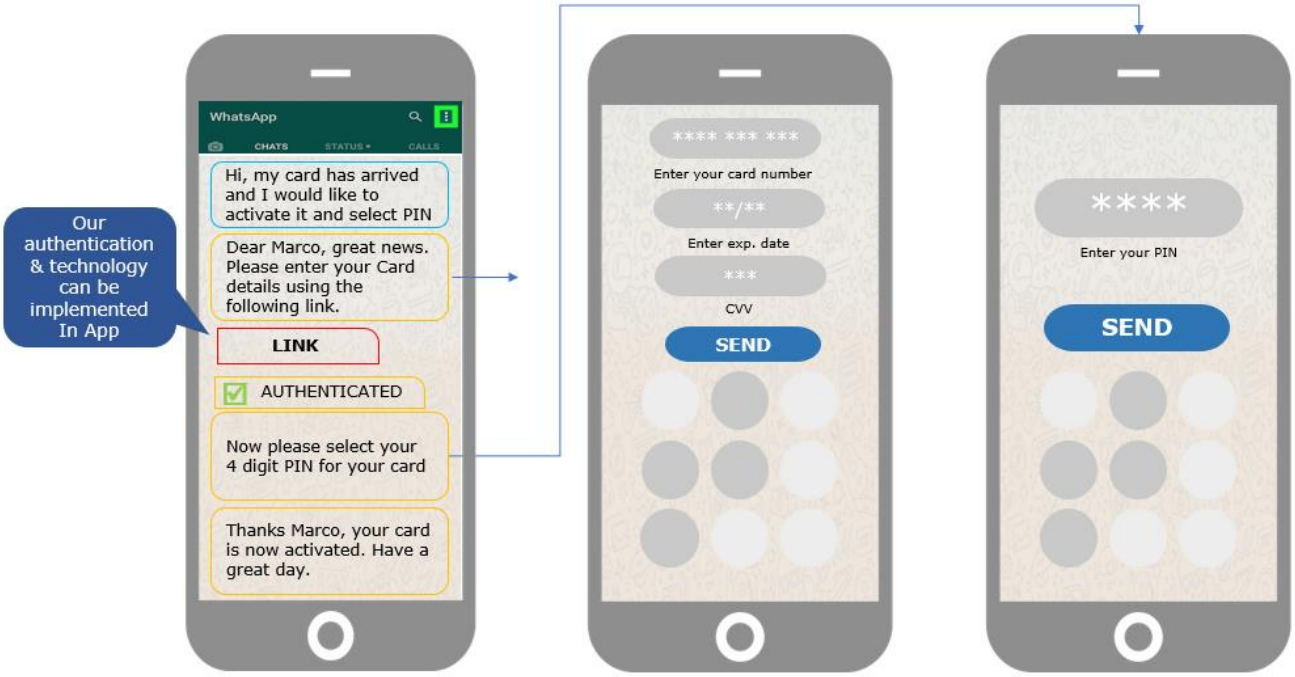
3 Customer enters PIN or Password-Encrypted

4 The WIZZIT Authenticator receives the encrypted data, re-encrypts it with the bank's keys in a secure Hardware Security Module (HSM) and sends it onto the bank's system

5 The Authenticator sends the response back to the server confirming or rejecting the transaction

1. The API is called by the Banks system when the Authentication is required.
2. The Authenticator pushes the message to the customer containing the PIN pad
3. The Customer opens the PIN pad and enters the Pin which is then encrypted under the banks keys.
4. The Authenticator receives the encrypted PIN. Creates an ISO 8583 AVI transaction and sends this to the Banks Switch

## The customer experience:



Our authentication & technology can be implemented In App

Hi, my card has arrived and I would like to activate it and select PIN

Dear Marco, great news. Please enter your Card details using the following link.

LINK

☑ AUTHENTICATED

Now please select your 4 digit PIN for your card

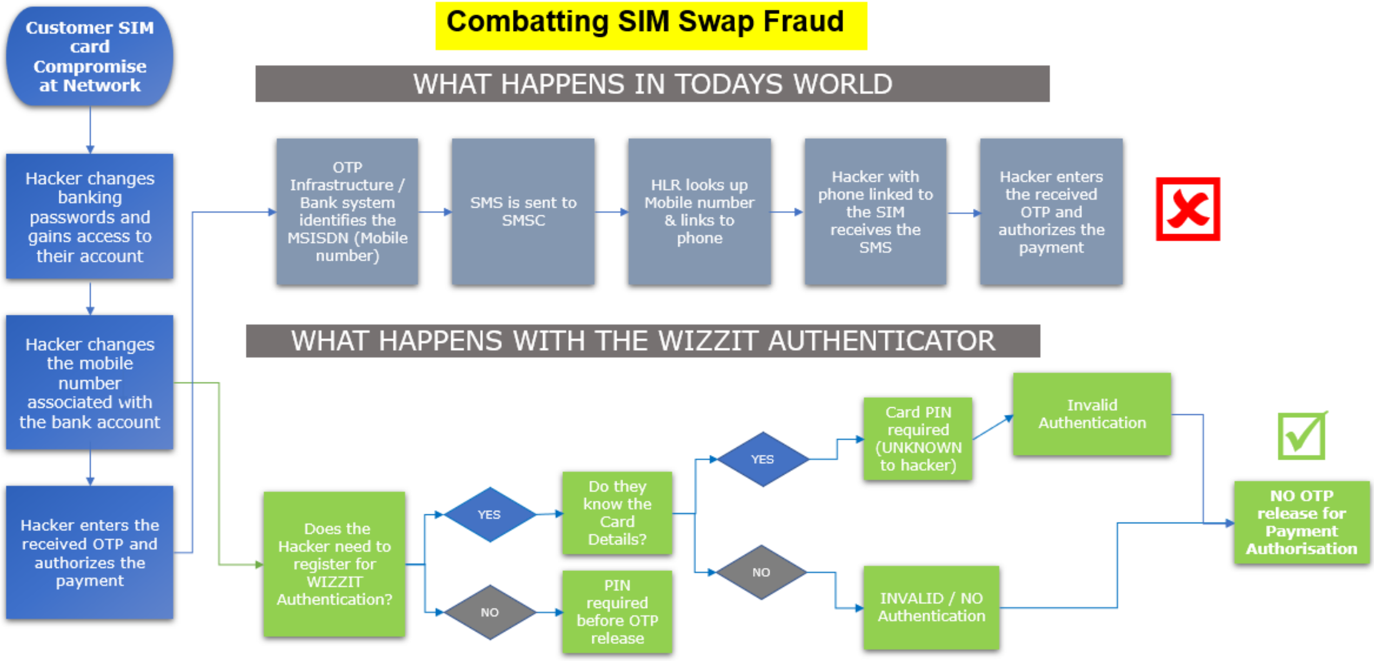
Thanks Marco, your card is now activated. Have a great day.

### Scenario 4:

### Internet banking login – eliminating issues around Sim Swap

Logon will allow a developer to call the API to present the PIN pad. The SMPP 3.3, 3.4 and 5.0 are supported in order for the institution to 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.

An example of this integration would be the integration of the solution in the internet banking and transaction environment of a bank to eliminate the risk of SIM Swap fraud.


Combatting SIM Swap Fraud
Customer SIM card Compromise at Network
Hacker changes banking passwords and gains access to their account
Hacker changes the mobile number associated with the bank account
Hacker enters the received OTP and authorizes the payment
WHAT HAPPENS IN TODAYS WORLD
OTP Infrastructure / Bank system identifies the MSISDN (Mobile number)
SMS is sent to SMSC
HLR looks up Mobile number & links to phone
Hacker with phone linked to the SIM receives the SMS
Hacker enters the received OTP and authorizes the payment
WHAT HAPPENS WITH THE WIZZIT AUTHENTICATOR
Does the Hacker need to register for WIZZIT Authentication?
YES
NO
Do they know the Card Details?
PIN required before OTP release
YES
NO
Card PIN required (UNKNOWN to hacker)
Invalid Authentication
INVALID / NO Authentication
NO OTP release for Payment Authorisation

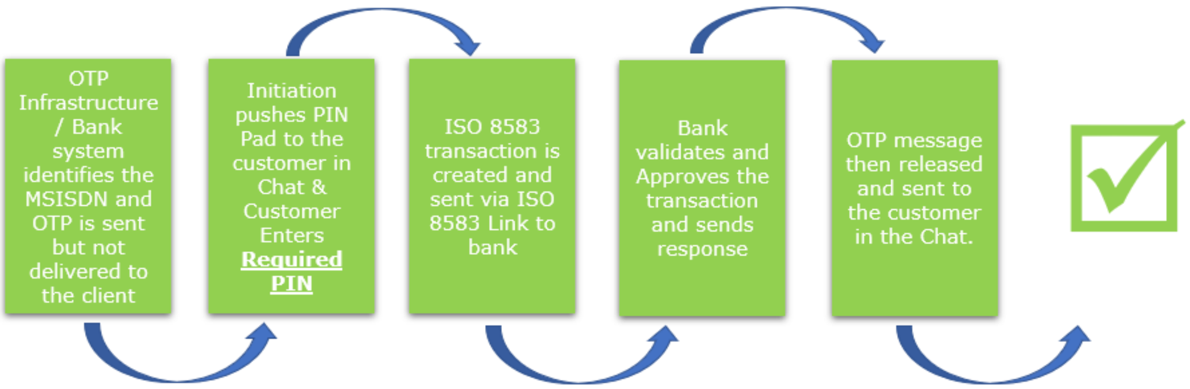
**HLR** - Home Location Register

**OTP** – One Time PIN

**SMSC** - Short message Service Centre

**MSISDN** - Mobile Station International Subscriber Directory Number

# THE WIZZIT AUTHENTICATOR FLOW



OTP Infrastructure / Bank system identifies the MSISDN and OTP is sent but not delivered to the client

Initiation pushes PIN Pad to the customer in Chat & Customer Enters **Required PIN**

ISO 8583 transaction is created and sent via ISO 8583 Link to bank

Bank validates and Approves the transaction and sends response

OTP message then released and sent to the customer in the Chat.

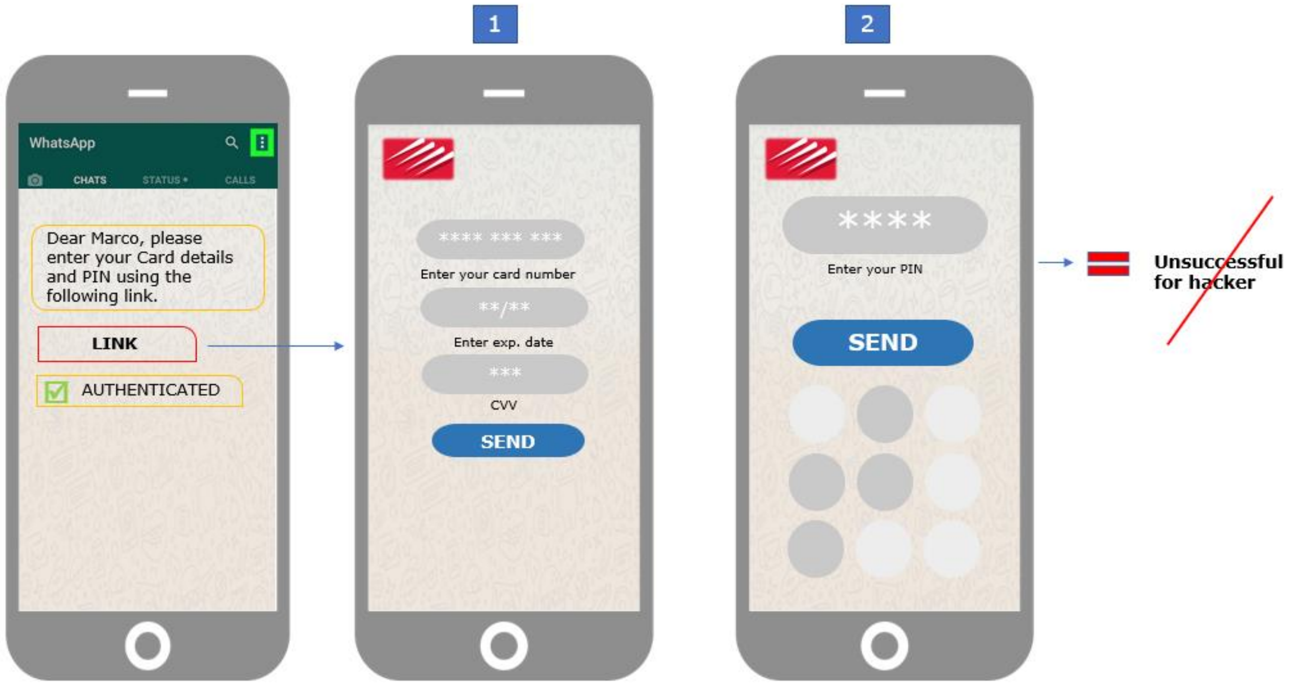
**SMSC** - Short message Service Centre

**MSISDN** - Mobile Station International Subscriber Directory Number

**HLR** - Home Location Register

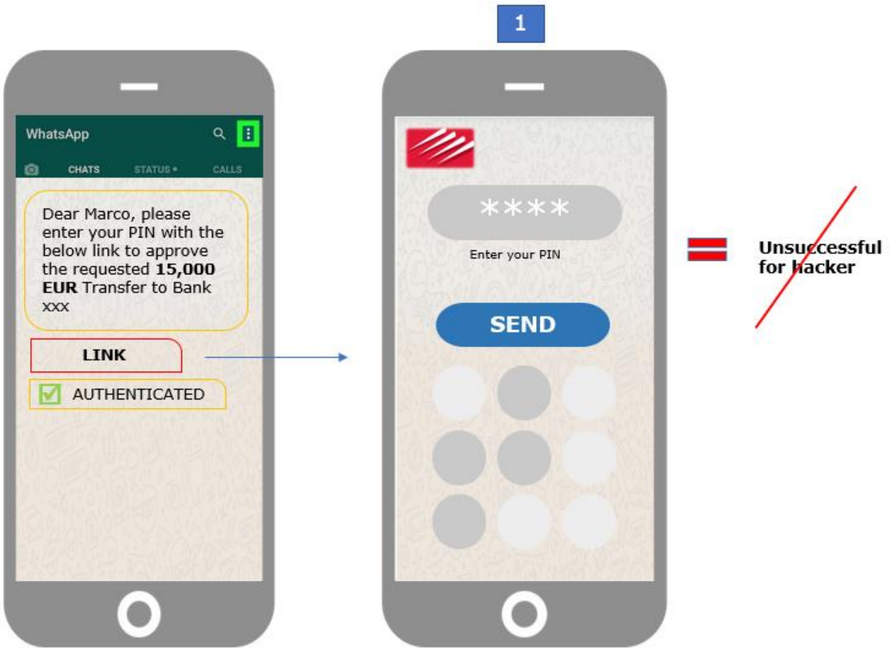
**ISO 8583** - is an international standard for financial transaction card originated interchange messaging

## New User to WIZZIT Authentication



Dear Marco, please enter your Card details and PIN using the following link.

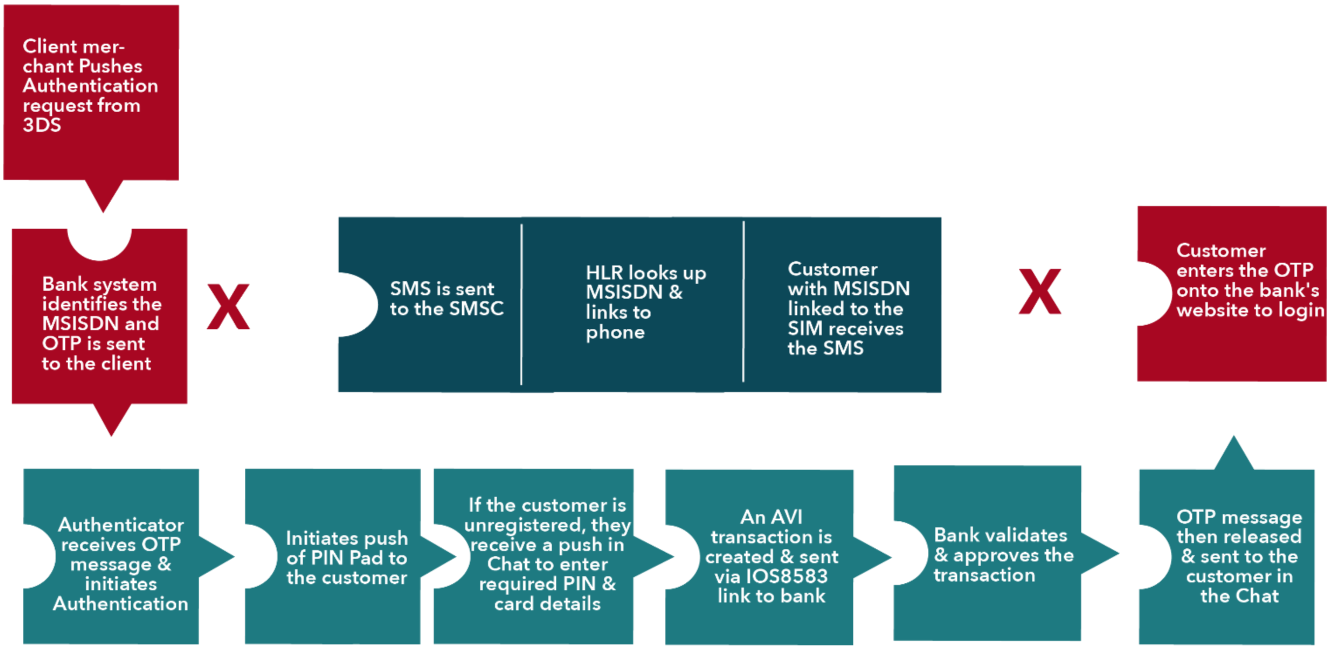
## Current Customer of WIZZIT Authentication



Dear Marco, please enter your PIN with the below link to approve the requested **15,000 EUR** Transfer to Bank xxx

### Scenario 5: Account Verification Instruction

An additional application could also be the validation of Authenticated Credit Transactions via an AVI (Account verification Instruction) transaction. The same process can be used for any validation that is done for 3D secure to directly replace the OTP or PIN validation.



Client merchant Pushes Authentication request from 3DS

Bank system identifies the MSISDN and OTP is sent to the client

SMS is sent to the SMSC

HLR looks up MSISDN & links to phone

Customer with MSISDN linked to the SIM receives the SMS

Customer enters the OTP onto the bank's website to login

Authenticator receives OTP message & initiates Authentication

Initiates push of PIN Pad to the customer

If the customer is unregistered, they receive a push in Chat to enter required PIN & card details

An AVI transaction is created & sent via IOS8583 link to bank

Bank validates & approves the transaction

OTP message then released & sent to the customer in the Chat

For the ACH transactions a process authentication can also be used for this purpose. If an OTP or in app validation is used this can be used as a direct integration to the authenticator to replace this process with a more secure option.

## CONCLUSION

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

### London & Australasia

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