SMART PAYMENT ASSOCIATION

shaping the future of payment technology

# The Instant Payment Card:

# Initiating a SEPA Credit Transfer at the Point Of Sale

## An SPA Paper

April 2020

# Table of Contents

# 1. Introduction and context

The European payment landscape is rapidly evolving through changes brought by regulation, technology innovation and digitization thanks to smart phone ubiquity.

In this context, European initiatives are emerging, driven both by the private and public sector, pushing for a pan European payment scheme based on instant payments (SCT Inst).

Such a scheme needs to address in a satisfactory way payments at the Point of Sale in physical stores. Face to face payments have requirements in terms of customer convenience, transaction speed and reliability.

**This SPA paper proposes an approach to payment at the POS relying on the existing EMV® standard and the use of a physical or digital EMV card interacting in the usual way with a payment terminal to initiate an (instant) credit transfer.**

The solution differs from existing card-based payments in that their clearing and settlement rails are not used anymore. The EMV (digital) card is a means of identification and authentication of the customer and the terminal is used to transmit payment and user authentication information.

The proposed solution fits within the new open banking framework defined by the Second Payment Services Directive (PSD2) and makes use of the Open APIs with instant payments initiated by a PISP. Another approach could make use of existing transaction authorisation circuits and SPA will be glad to participate in comparative discussions.

The paper contains a high-level view of this "Instant Payment Card" approach, describing the principle and the interactions between its components and highlighting the many advantages the solution offers.

**SPA's intent is to create interest in the approach and contribute to the on-going discussions. SPA welcomes feedback from stakeholders of the European payment ecosystem.**

# 2. Glossary

| | |
|---|---|
| ASPSP | Account Servicing Payment Service Provider. In most cases, the customer's bank |
| EMV | Europay Mastercard Visa: The standard for smart payment cards and terminals |
| IBAN | International Bank Account Number |
| IIN | Issuer Identification Number (the first 6 or 8 digits of the PAN) |
| KYC | Know Your Customer – the identification step when the customer is not yet known to the bank |
| PAN | Primary Account Number |
| POS | Point of sale. May be short for POS terminal |
| PISP | Payment Initiation Service Provider |
| PSD2 | the 2nd Payment Services Directive |
| QR code | Quick Response (2 dimensional) code |
| RTS | Regulatory Technical Standard. In this document refers to the RTS on Strong Customer Authentication under PSD2 |
| SEPA | Single Euro Payment Area |
| SCT | SEPA Credit Transfer |
| SCT Inst | Instant SCT. Also referred to as Instant Payment |

# 3. The Instant Payment Card

## 3.1. Principle

The Instant Payment Card is a card, or digital card in a mobile wallet, issued by a bank to its customer. When used at a point of sale terminal in store, the payment transaction results in an instant payment (SEPA Instant Credit Transfer).

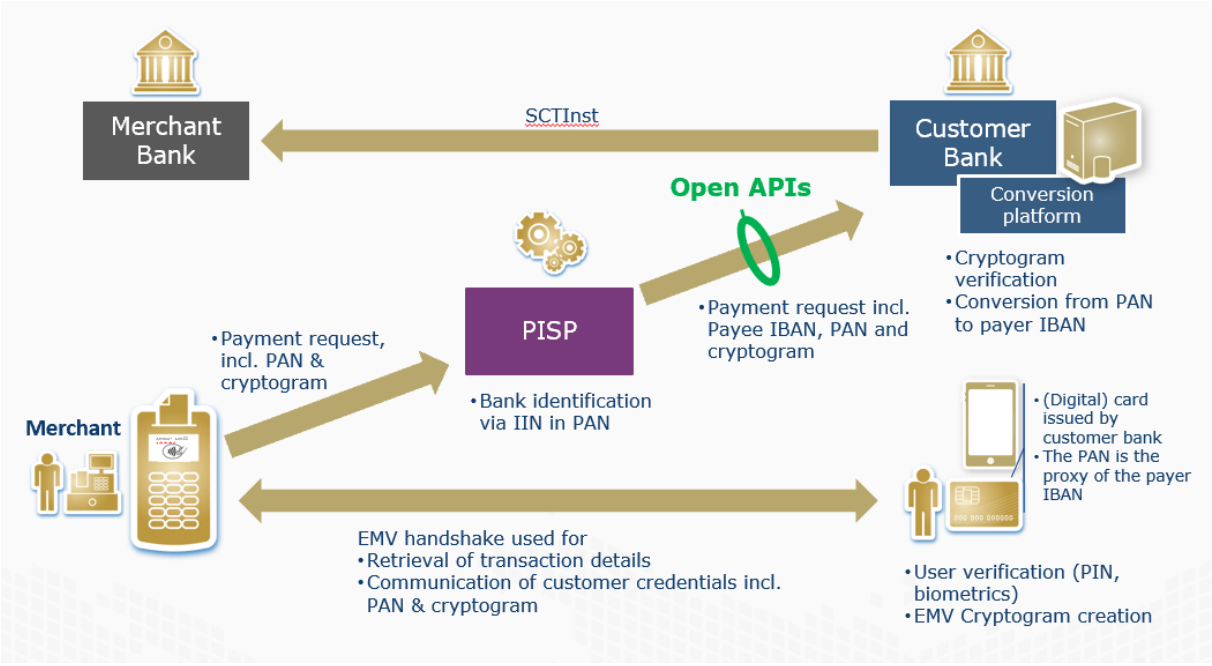
When paying at the point of sale, the customer follows the exact same user experience as with conventional payment cards: he/she inserts the Instant Payment Card in the terminal or taps it in contactless mode and enters a PIN. For mobile wallets, the customer verification method could be handled on the phone, for example using the supported biometric modalities.

Behind the scenes, the terminal connects on-line to a dedicated platform operated by a service provider that may also serve the role of a PISP as described in PSD2. For simplicity, this provider is referred to as a PISP in this document.

The PISP identifies the bank that issued the card and sends, through the Open APIs, a payment initiation request processed by the bank to perform an instant payment.

In this solution, the Primary Account Number (PAN) of the Instant Payment Card is a proxy of the IBAN of the customer. It is transmitted by the terminal to the PISP and provided by the PISP to the bank where it must be converted back to the actual IBAN of the customer.

This principle is illustrated in the following diagram:




**Instant Payment Card principle**

## 3.2. (Digital) Card content

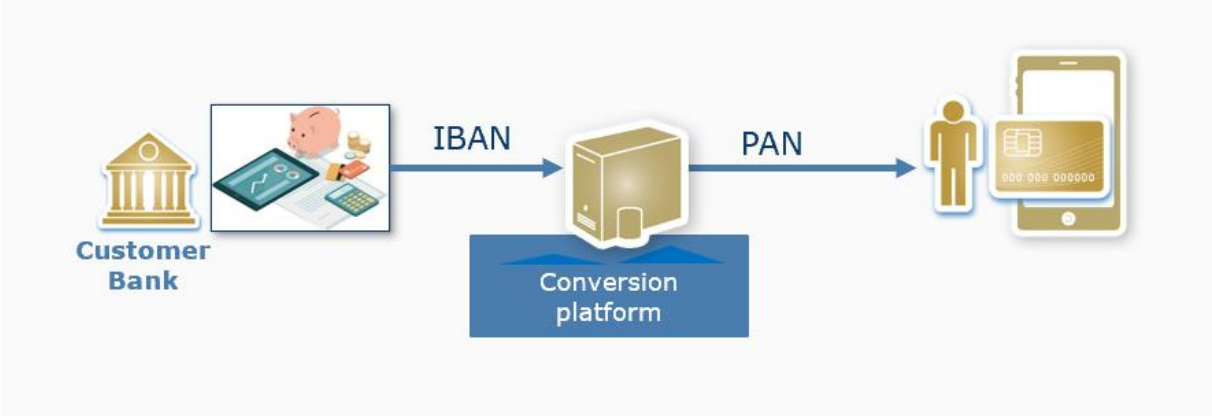
The (digital) Instant Payment Card contains the usual bank and user credentials, amongst them:

- a PAN – Primary Account Number
- an expiry date
- EMV parameters that control the (digital) card behavior at the POS
- issuing bank cryptographic keys
- user verification data: PIN or biometrics

This data is personalized in the card in a usual personalization center or provisioned over the air to a mobile wallet using the existing industry solutions and services.

The PAN conforms to the ISO/IEC 7812 standard and contains an Issuer Identification number. However, unlike for conventional cards, the PAN here is a proxy of the customer IBAN.

The PAN associated to the customer's IBAN is generated by a system of the bank or a provider of the bank and sent to the personalization bureau or mobile wallet provisioning solution.




**Conversion of the customer IBAN into a PAN during personalization / over the air provisioning**

The customer identification or KYC step, which is a pre-requisite to the issuance of the (digital) Instant Payment Card, is outside the scope of this document.

## 3.3. Customer authentication and payment

When paying at the point of sale, the customer pays with the (digital) Instant Payment Card in the same way as usual: she/he inserts the card or taps the (digital) card in/on the payment terminals and enters a PIN. On a mobile wallet, the customer would use biometric verification on the mobile phone.

The user verification step (PIN or biometrics) may also serve the purpose of obtaining customer consent provided the transaction details are displayed by the terminal at the same time as the user verification request.

The (digital) Instant Payment Card interacts with the payment terminals using the standard EMV communication protocol. This protocol allows the (digital) card to:

- receive the transaction details from the terminal
- verify the customer by means of a PIN code or biometric modality for a mobile wallet
- generate a cryptogram that signs the transaction using the issuing bank keys stored in the card. The cryptogram also signs the fact that the customer was positively identified by means of the PIN or biometric modality
- provide the customer credentials (PAN, expiry date…) and cryptogram to the terminal.

The payment terminal will then connect to the PISP platform sending merchant identification, transaction details, customer credentials and cryptogram (the payload). An existing authorization request protocol may be used for this purpose.

The PISP identifies the customer's bank from the Issuer Identification Number present in the PAN, connects to this bank using the open APIs and provides the payload, including merchant IBAN to the bank.

The bank verifies the cryptogram thereby authenticating the customer, subsequently retrieves the customer IBAN from the PAN and performs an instant payment to the merchant identified in the payload.

As can be seen, customer authentication is embedded in the payment process.

## 3.4. Confirmation

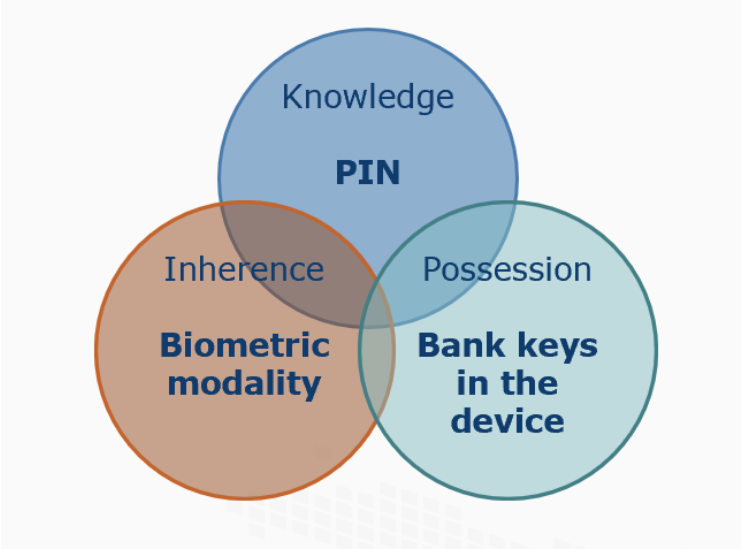
Once the Instant Payment is performed, the customer bank informs the PISP of the result. The PISP then communicates this information back to the payment terminal which displays the result on its screen. An existing authorization response protocol may be used for this purpose.

Communication of the result to the customer may be done via a receipt printed on the terminal or directly from the customer bank via an SMS or notification message to the customer's mobile phone.

A high-level payment transaction flow is provided in the appendix.

# 4. Compliance with PSD2

EMV (digital) Instant Payment Cards used at the POS comply with the Strong Customer Authentication mandate described in the RTS. They combine the possession factor with a knowledge or inherence factor:




- the knowledge factor is the PIN of the card,
- the inherence factor is the fingerprint scanned by a biometric card or whatever biometric modality supported by the smart phone in which a digital card has been provisioned,
- the possession factor is materialized by the bank keys personalized in the (digital) card and checked through the verification by the bank of the cryptogram generated by the (digital) Instant Payment Card.

The cryptogram generated by the (digital) card may be the authentication code described in the RTS.

# 5. Advantages of this model

## 5.1. Re-use of the existing POS infrastructure

Existing terminals already deployed at merchants may be used with the Instant Payment Card solution.

A new payment application making use of an EMV kernel must be downloaded to the target terminals. This payment application will send instant payment requests to the platform of the PISP and, for this purpose, could use existing authorization protocols supported in the country (ISO 8583 based, ISO 20022 based, Nexo based).

## 5.2. User convenience

The solution does not change customer habits and provides a convenient user experience. In particular, no redirection of the customer to the bank user interface is required for authentication. Authentication is embedded in the payment process which is very streamlined.

The reliability of the solution is the same as for conventional cards. In particular, the solution does not require over the air connectivity in the store. This is a significant advantage in situations where connectivity to the mobile network is poor.

As with any instant payment method, the speed of the transaction will depend on how fast the SCT is processed in real time.

## 5.3. Reach and inclusion

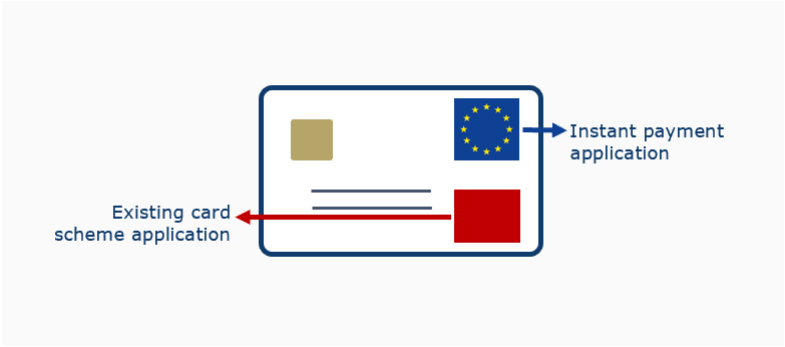
Not all users will have an adequate smart phone or want to use a smart phone for payment. An inclusive European instant payment scheme will therefore have to address that fraction of the users that will need an alternative method.

The card form factor has a robust image of security and is trusted by consumers. And cards are accepted in payment terminals in a vast number of stores across Europe.

This makes them an ideal method to maximize reach to all the customers of the bank.

## 5.4. Co-badging

The instant payment application could be combined, in a (digital) card, with existing card scheme applications.




Indeed, banks will continue to issue payment scheme cards whether for domestic or international purposes and will support the costs of issuing these cards. Combining a card scheme application with a European SCT Inst scheme application leverages the investment of banks in such cards and their issuance infrastructure.

A co-badged card bearing both a card scheme application and the instant payment application will require application selection at the point of sale. Particular care will be needed to educate customers on their choice of payment method as the instant payment application will cause the customer account to be debited in a few seconds whereas the card scheme payment application could result in the account being debited later, for example at the end of the month. Other differences may need highlighting such as refund capabilities.

## 5.5. Migration path to instant payments

The use of (digital) cards well known to customers in Europe provides an ideal path to move to a new scheme based on instant payments. While customers should be aware of the differences introduced by instant payments, their introduction would not require changes in payment habits and user experience. The consistency in the payment experience will facilitate the move to instant payments.

## 5.6. Extension to remote payment

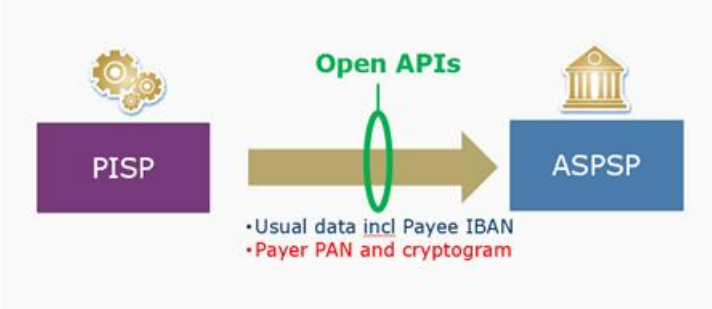
The Instant Payment Card is not a solution restricted to proximity payments at the POS. Indeed, the EMV standard provides for a means of authentication of the customer which can be extended to e-commerce use cases.

For example, an Instant Payment Card based mobile wallet used to pay in store in contactless mode could also be used for remote payments, out of band if shopping on a PC or through app to app redirection if shopping on a smart phone.

The PAN and expiry date of an instant payment plastic card could be used manually at the checkout page and possibly stored on file for frequent shoppers. For these use cases, the bank will have to have provided the customer with a suitable means of strong customer authentication.

# 6. Impact on the Open APIs

The Instant Payment Card solution described in this paper proposes to send authentication data to the bank via the Open APIs. To use terminology found in Open API literature, the Instant Payment Card uses an embedded authentication model.




The bank's APIs need to support the transmission of this authentication data. While the Open API specifications of the Berlin Group, or of STET, support the embedded model, further work is required to verify if changes are needed or not to support the Instant Payment Card method. Other API specification bodies would have to fully specify the model.

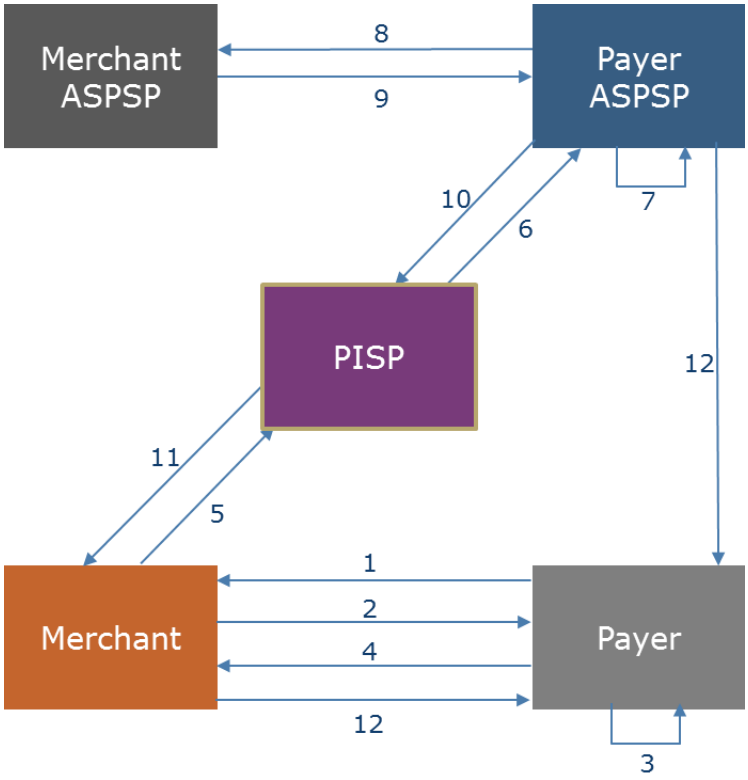
As the PISP will have to connect to many banks, standardized APIs for this use case would be highly desirable to reduce set up costs.

# 7. Conclusion

This paper presented a means of initiating instant payments at the POS using a (digital) EMV card. SPA believes this method provides benefits to the customer in terms of fluidity and convenience, to the merchant in terms of infrastructure re-use and reliability and to banks in terms of reach and co-existence with today's card schemes.

The paper is meant to raise interest and trigger discussions as there is no doubt that many questions arising from reading this paper will need answering. SPA will be glad to engage with interested parties to pursue these discussions and contribute to the creation of a pan European payment solution based on instant credit transfer.

# 8. Appendix: Proximity payment Transaction flows




1. Payer views transaction details and inserts/taps (digital) card in/on terminal
2. Payer (digital) card receives merchant/transaction data using EMV handshake
3. Payer verifies PIN /biometrics and (digital) card generates cryptogram
4. Payer (digital) card presents its data to the merchant using EMV handshake (including PAN, authentication cryptogram…)
5. Payment request including payer authentication data
6. Payment initiation request, including payer authentication data
7. ASPSP verifies cryptogram, thereby authenticating the Payer and converts PAN to IBAN
8. SCT or SCT Instant (Payer's ASPSP transfers fund to merchant ASPSP)
9. Confirmation that transfer was processed
10. Confirmation that transfer was processed
11. PISP sends SCT transaction confirmation to merchant (displayed on terminal)
12. Merchant sends SCT transaction confirmation to Payer (e.g. via printed receipt) and/or
12. ASPSP sends SCT transaction confirmation to Payer on mobile device

## Contact for the Smart Payment Association

Stéphanie de Labriolle : stephanie.delabriolle@smartpaymentassociation.com

## About the Smart Payment Association

The Smart Payment Association (SPA) is the trade body of the smart payments industry. The Smart Payment Association addresses the challenges of the evolving payment ecosystem, offering leadership and expert guidance to help its members and their customers realize the opportunities of smart, secure and personalized payment systems & services both now and for the future.

https://smartpaymentassociation.com/