Bank of England

Point-of-sale proof of concept

Digital pound experiment report

May 2024

Contents

Summary

As part of the design phase for a digital pound, the Bank of England (the Bank) is conducting experiments and proofs of concept (PoC) in collaboration with private-sector innovators and a range of stakeholders. These aim to assess the technical feasibility and technology and policy implications of potential digital pound design features. No decision has been taken on whether or not to build a digital pound.

The purpose of this experiment was to assess the technical feasibility of using existing point-of-sale (POS) hardware, as currently used in the UK, to initiate digital pound payments. This involved a PoC that used EMV[1] standards to send payment instructions from smart cards to POS devices, and then to an application programming interface (the 'BoE API').

While the Bank did not build a digital pound infrastructure, and no real money payments were made, the experiment demonstrated the following from a technology perspective:

- Existing POS terminals in the UK could, in principle, be used to initiate digital pound payments.
- Those terminals do not appear to require modification in order to make digital pound payments.

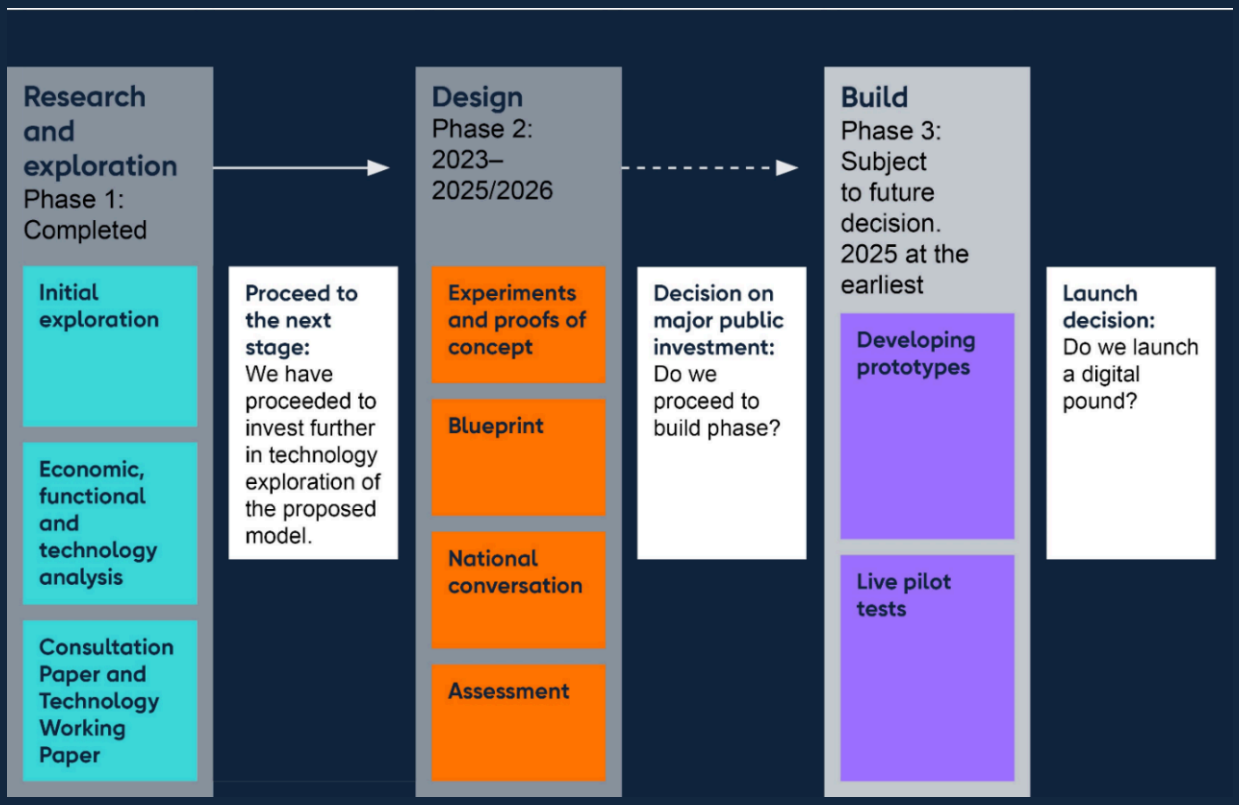
The experiment also concluded that it is technically feasible to implement offline payments functionality at points of sale using existing POS terminals. But this functionality might require that an offline payments application be deployed to those terminals in order to store offline balances. Therefore, while existing POS terminals may not need to be modified to make online digital pound payments, they might need to be modified for offline payments.

There are several other factors, such as operational, legal and commercial considerations, that will impact design choices around digital pound payments at points of sale. Those factors were not tested in this experiment.

Background

In February 2023, the Bank published a **Technology Working Paper**, which accompanied the Bank and HM Treasury's joint **Consultation Paper on the digital pound**. The Bank and HM Treasury **confirmed in January 2024** that further preparatory work was justified to enable us to respond to developments in the payments landscape and to reduce materially the lead time if there is a future decision to introduce a digital pound. The Bank and HM Treasury have therefore moved from the research and exploration phase of work on a digital pound to the design phase, which will result in a decision around the middle of the decade on whether to build a digital pound.

Figure 1: Roadmap for the digital pound project



The objectives of the design phase are to:

- cut lead-times on digital pound development and equip ourselves with the knowledge and capabilities to move into a build phase, if required;
- determine the technology feasibility and investment needed to build a digital pound;
- articulate, in detail, what the technology and operational architecture for a digital pound would look like;
- assess and evaluate the benefits and costs of a digital pound architecture;
- deepen the Bank's knowledge of central bank digital currency (CBDC) technology and support stakeholder understanding of our technology approach;
- support the development of the broader UK digital currency technology industry through collaboration, knowledge-sharing, experimentation and proofs of concept; and
- provide the basis for a future decision on whether to introduce a digital pound and move to a build phase.

As part of the design phase, the Bank is conducting experiments and PoC in collaboration with private-sector innovators and a range of stakeholders. These experiments and PoC do not indicate a decision to build a digital pound or a final digital pound design. They aim to assess the technical feasibility and technology and policy implications of a digital pound, in order to help the Bank and HM Treasury explore the design of a digital pound, and provide evidence to support a decision on whether to build one. By partnering on experiments and PoC, the Bank and HM Treasury seek to catalyse private innovation in digital currency technologies, encourage innovative digital money business models and support knowledge sharing across the UK fintech sector.

The point-of-sale feasibility study

As discussed in the Technology Working Paper, in order for a digital pound to meet its policy goals, it would need to be useful for everyday payments, including being able to make payments 'in store'. Today, in-store card payments are enabled through the sending of payment instructions from the merchant's POS terminal to the payer's card issuer. This is facilitated by the merchant's acquirer and the payment scheme associated with the payer's card.

If a digital pound were to utilise existing POS terminals, this would reduce, or potentially even eliminate the need for merchants to invest in new hardware. Existing POS terminals have wide adoption in the UK, and merchants often maintain the same terminals for several years without changing them. Those terminals are also familiar to merchants, their staff, and consumers, delivering a consistent user experience.

The Bank's POS feasibility work took place in two stages. First, the Bank commissioned a feasibility study to explore how digital pound payments could be made using existing POS infrastructure in the UK. The study concluded that it would be feasible, from a technology perspective, to use existing POS hardware to make digital pound payments, and highlighted different payment flows that could be used to deliver this. This report covers the second stage of the Bank's POS feasibility work, a PoC which aimed to validate the findings from the feasibility study.

Project overview

Consult Hyperion[2] developed this PoC to help us test digital pound payment initiation using existing POS hardware. We (the Bank and Consult Hyperion) used the following components to simulate in-store digital pound payments:

- POS devices, namely traditional POS terminals, mobile POS terminals, and a software POS application on an Android mobile phone;
- EMV-compliant contactless kernels;[3]
- Smart cards[4] with EMV applications[5] and different verification methods, namely Consumer Device Cardholder Verification Method (CDCVM)[6] and Online PIN;
- A proxy server developed by Consult Hyperion, referred to as the BoE API; and
- A web application dashboard showing balances, transactions and error logs.

In addition to the components listed above, we developed an application that could enable offline payments on the POS devices.

Figure 2: Mobile, traditional and software POS devices

Implementation

Payment flows

This PoC explored three different payment flows:

- PASSTHRU – where a request for payment is sent to the BoE API via the merchant's Payment Interface Provider (PIP);
- DIRECT – where a request for payment is sent directly to the BoE API, bypassing the merchant's PIP; and
- PEER – where a payment is made between two devices without network connection, supporting offline payments.

For each payment flow, we considered sale and refund transactions, and transaction queries.

PASSTHRU

> **This flow assumes that balance is stored remotely on the core ledger provided by the Bank.**

- The merchant's POS device requests payment.
- The payer taps their device on the merchant's POS device.
- The payer either authenticates to their device using CDCVM or enters their PIN on the merchant's POS device.
- A request for payment with payer authentication data is sent from the merchant's POS to the merchant's PIP.
- The merchant's PIP sends this request (authentication data is encrypted) to the BoE API, which routes it to the payer's PIP.
- The payer's PIP authenticates the payer using the authentication data in the request.
- Upon successful authentication, the payer's PIP sends the payment instruction to the core ledger to transfer digital pounds from the payer to the merchant.
- Digital pounds are transferred from the payer's wallet to the merchant's wallet and the transaction data is viewable on the web application.[7]

Figure 3A: Sale transaction at POS using the PASSTHRU payment flow

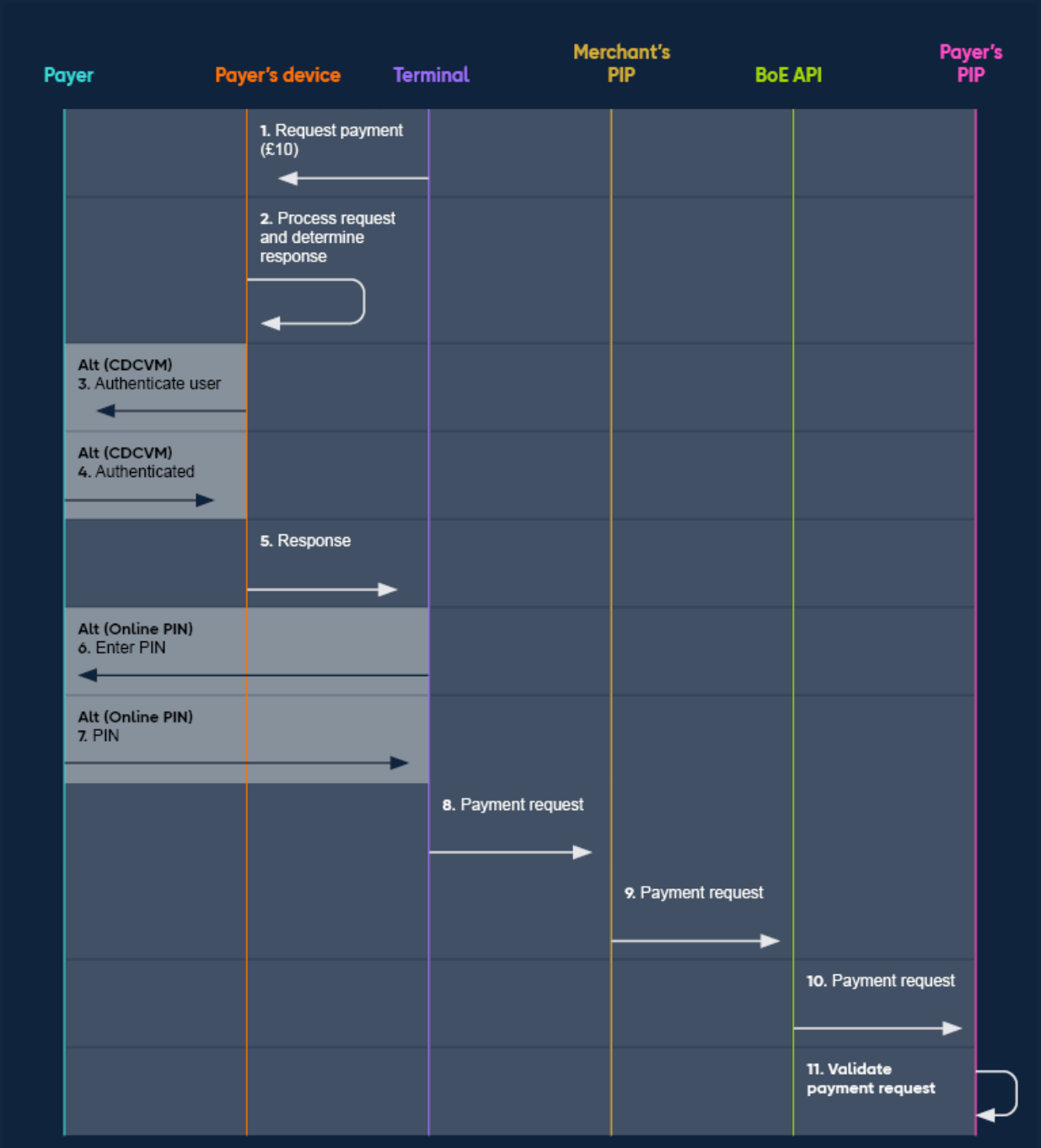
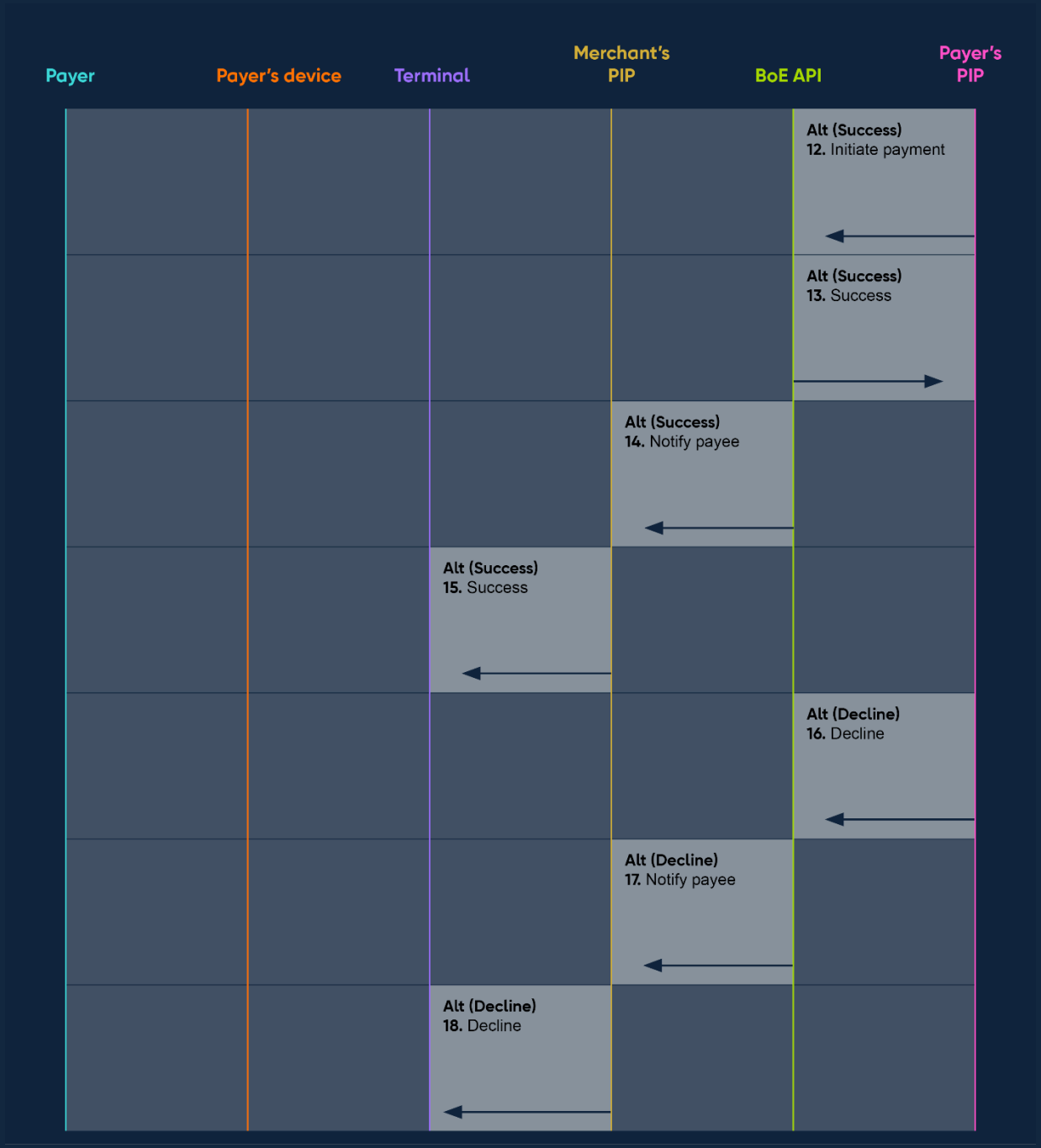


Figure 3B: Sale transaction at POS using the PASSTHRU payment flow



DIRECT

> **This flow assumes that balance is stored remotely on the core ledger provided by the Bank.**

- The merchant's POS device requests payment.
- The payer taps their device on the merchant's POS device.
- The payer either authenticates to their device using CDCVM or enters their PIN on the merchant's POS device.
- An encrypted request for payment, along with payer authentication data, is sent from the merchant's POS directly to the BoE API.
- The BoE API routes this request to the payer's PIP.
- The payer's PIP authenticates the payer using the authentication data in the request.
- Upon successful authentication, the payer's PIP sends the payment instruction to the core ledger to transfer digital pounds from the payer to the merchant.
- Digital pounds are transferred from the payer's wallet to the merchant's wallet and the transaction data is viewable on the web application.[8]

Figure 4A: Sale transaction at POS using the DIRECT payment flow

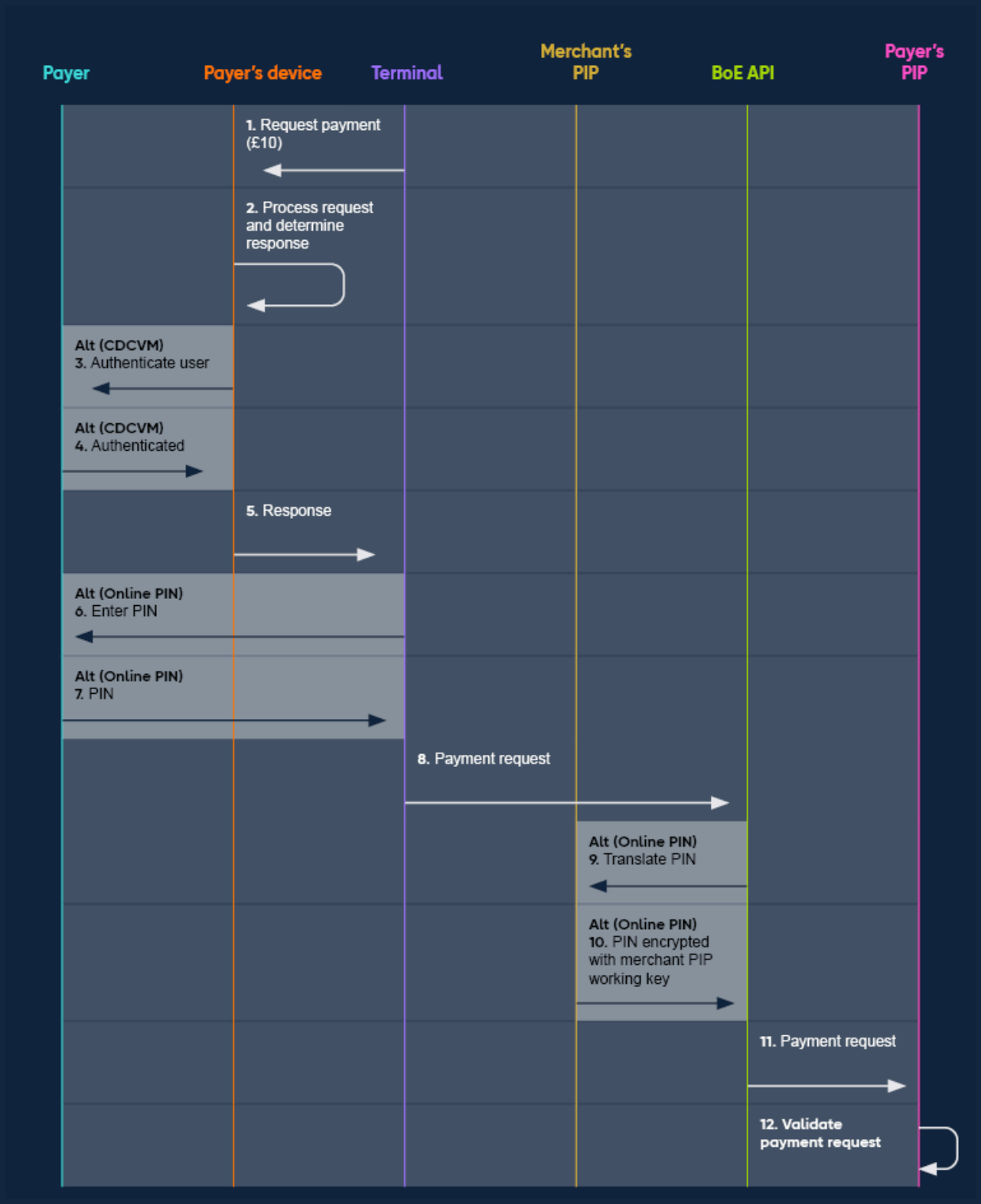
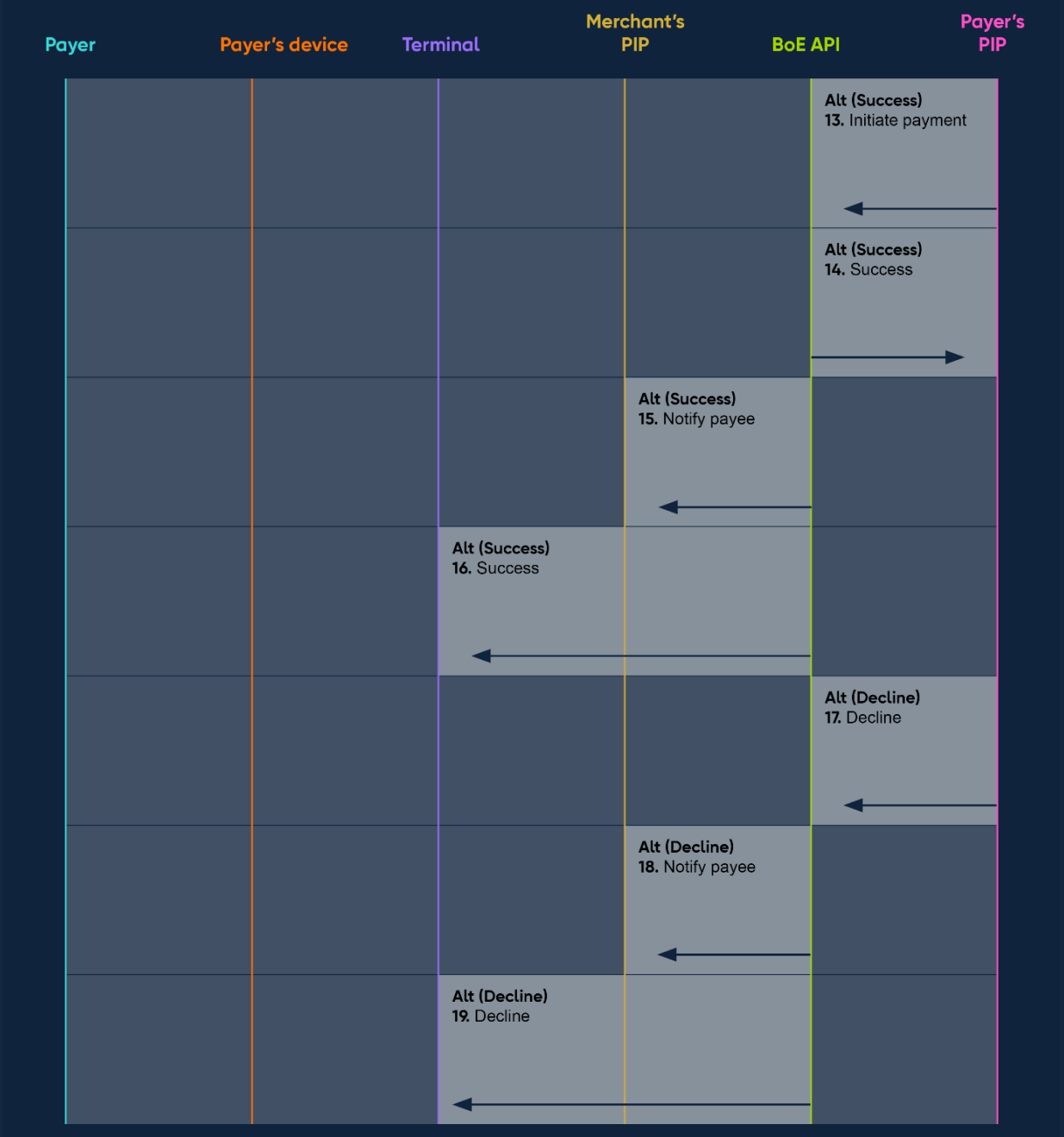


Figure 4B: Sale transaction at POS using the DIRECT payment flow



PEER

> **This flow assumes that balance is stored on the user's device. Therefore, payments can be made offline, with immediate confirmation and settlement.**

This flow also introduces the concept of a 'controller' and a 'server' of the transaction. The controller is the application that initiates the transfer. It can be in a merchant POS device or a consumer's device. The server is the application that receives the transfer request.[9] The controller or server can be either the payer or the payee.

- The controller initiates the transaction.
- The server device is tapped onto the controller device.
- Upon the controller's request, each device verifies that the other is valid to conduct a transaction and the payer carries out authentication using CDCVM.
- If authentication is successful, a payment request is sent from the controller to the server.
- If this payment request is accepted, digital pounds are transferred directly from the payer's device to the payee's device, with the payer's balance debited before the payee's balance is credited.
- If the devices were online, the transfer details would immediately be notified to the core ledger and made viewable on the web application.
- If the devices were offline, the transaction details would be stored on the devices until they reconnect to the network.

Figure 5: PEER sale transaction using the PEER flow, with payee's device as the controller

Figure 6: PEER sale transaction using the PEER flow, with payer's device as the controller

The EMV applications on the smart cards were not appropriate for storing offline balances, as they were primarily designed as risk management counters.[10] Therefore, we developed a new application that could store offline balances on the smart cards. This new application was not based on EMV standards so we also needed to deploy a new kernel to the terminals that could interact with it.

Authentication

We enabled two verification mechanisms for user authentication, CDCVM and Online PIN. CDCVM was enabled via a fingerprint sensor on the smart cards.[11] Although not widely adopted, fingerprint-enabled smart cards have been around for many years and are available today for POS payments.

To set up the card, the payer enrolled their fingerprint to the card. When used for authentication, the fingerprint on the sensor was checked against the enrolled fingerprint. The fingerprint data was stored on the user's card and was never transferred to the Bank or the user's PIP.

Online PIN verification was implemented through the exchange of cryptographic keys between the merchant's POS terminal, the payer's PIP, the merchant's PIP, and the BoE API. This process ensured that, similar to card payments and automated teller machine (ATM) transactions in the UK, the user's PIN was transferred securely. The BoE API held a shared key with the merchant's PIP (merchant PIP working key) and with the payer's PIP (payer PIP working key). No personal data was transferred to the Bank. Where Online PIN verification was selected:

- PIN values were captured on the POS terminals as encrypted PIN blocks.
    - If the PASSTHRU flow was used, the PIN block was immediately sent to the merchant PIP for PIN translation.[12]
    - If the DIRECT flow was used, the PIN block was sent to the BoE API, which passed it back to the merchant PIP for PIN translation.
- The merchant PIP translated the PIN block from the terminal working key to the merchant PIP working key, before sending it to the BoE API.
- The BoE API translated the merchant PIP working key to the payer PIP working key, before sending it to the payer's PIP.
- The payer's PIP checked that the PIN matched the payer's reference PIN, before approving authentication.[13]

Figure 7: Online PIN verification in the PASSTHRU payment flow

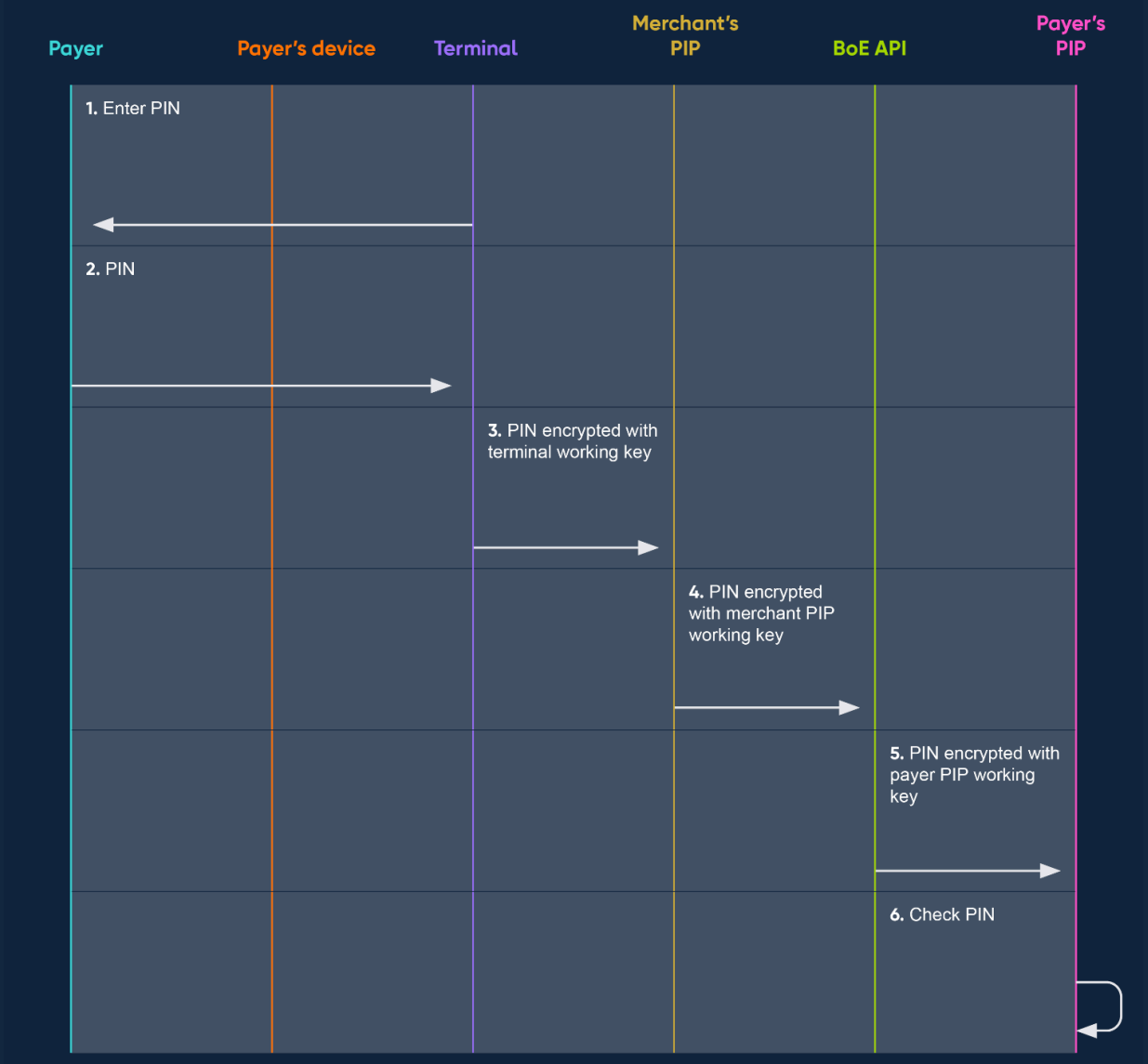
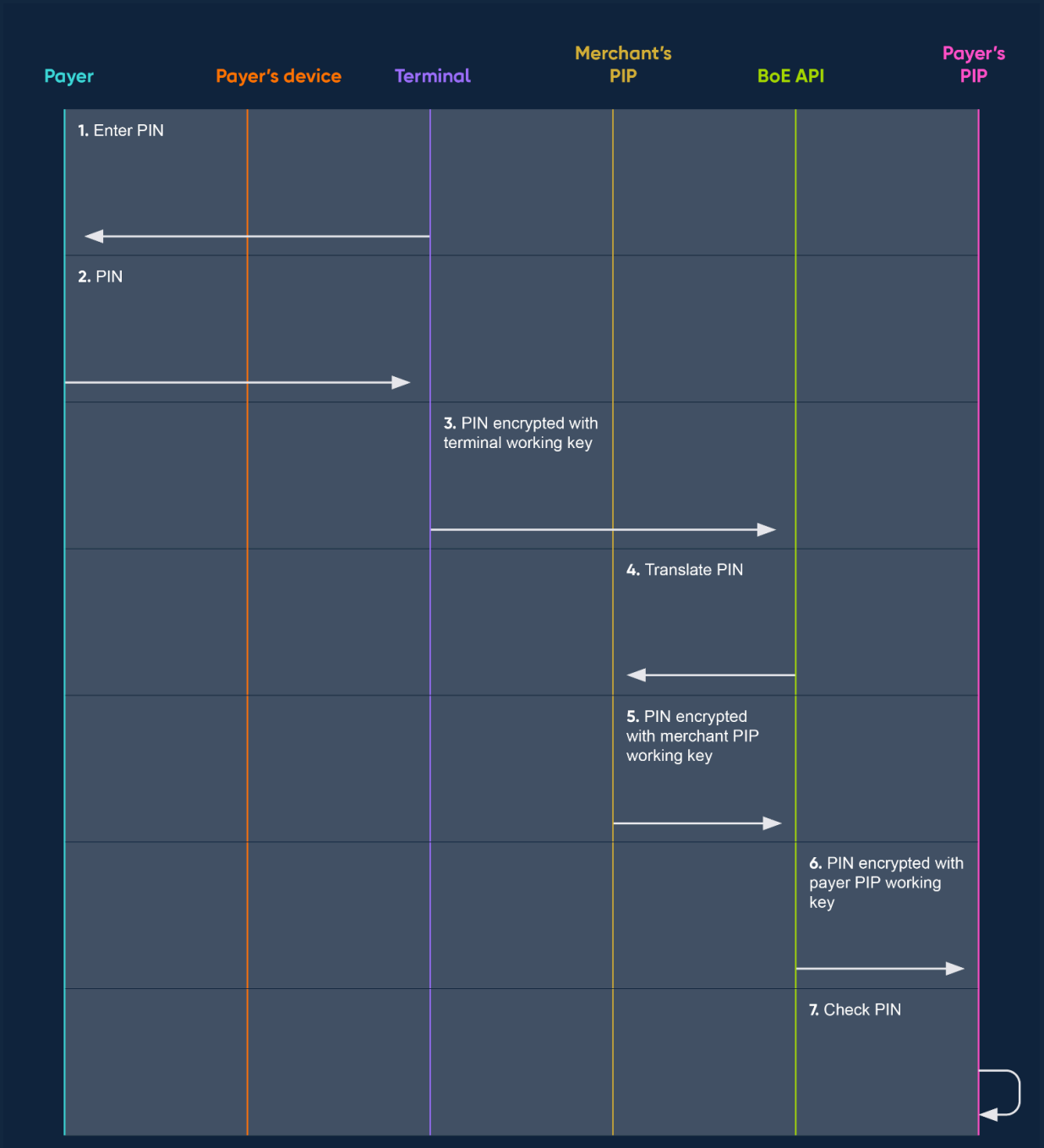


Figure 8: Online PIN verification in the DIRECT payment flow



Results

Payment flows

We successfully implemented the PASSTHRU and DIRECT payment flows using the traditional, mobile and software POS terminals.

The DIRECT flow required all POS terminals to be connected to the BoE API, which placed significant key management load[14] on the BoE API. Also, since payment instructions were sent directly to the BoE API, they were sent with a SHA256 hash of the primary account number (PAN), rather than the PAN.[15] This ensured that the PAN was not visible to the BoE API. This flow did not use the Association for Payment Clearing Services (APACS) 70 standard which is commonly used in the UK today.[16] PAN is a mandatory field in the APACS 70 file definition. Therefore, the APACS 70 standard was not appropriate for this implementation of the DIRECT flow.

While we successfully implemented the PEER flow using the traditional POS terminal and the software POS application. We were unable to implement it using mobile POS terminals because of restricted access to terminal's software development kit. Despite this limitation, we were able to demonstrate offline payments using this payment flow, as payments could be executed without an immediate connection to the BoE API.

Unlike the DIRECT and PASSTHRU payment flows, the PEER flow required that the POS terminals' software be modified or updated.

Authentication

We successfully implemented both CDCVM and Online PIN verification, enabling the payer's PIP to authorise the payer. CDCVM verification was possible for all payment flows, in both online and offline (PEER) transactions.

Online PIN verification was implemented in both the PASSTHRU and DIRECT flows. However, the DIRECT flow introduced complexities since it required the BoE API to send the encrypted PIN block to the merchant's PIP before routing the payment instruction to the payer's PIP. Also, since Online PIN verification required online approval, this verification mechanism did not work for offline (PEER) transactions.

Reflection and next steps

This PoC demonstrated the technical feasibility of using existing POS hardware to initiate digital pound payments. It was useful in developing the Bank's understanding of the requirements for initiating digital pound payments at POS, both online and offline.

This PoC made several assumptions about design choices for a digital pound, including what POS hardware to use, whether there would be cards and what type, where balance is stored and the applicable PIN translation mechanism. At this time, no such design choices have been made. There are a range of considerations, other than technical feasibility, that will impact design choices for in-store digital pound payments.

1. EMV (Europay, Mastercard and Visa) is a set of technical specifications which enable card-based payments to be consistently accepted across different payment schemes.
2. **Consult Hyperion** was awarded a **contract for point of sale consultancy services.**
3. EMV kernels are the software applications that implement the EMV functionality, enabling payment processing.
4. These smart cards were fingerprint-enabled, allowing us to test strong customer authentication without requiring users to authenticate to a smartphone. The user's fingerprint remained on their card and was not shared with other parties. See **Payment Services Regulations 2017** for information on strong customer authentication requirements.
5. We developed applications based on EMV standards that could interact with the EMV kernels on the POS devices.
6. CDCVM enables users to be authenticated on their own devices rather than on the merchant's POS device. This mechanism supports contactless payments.
7. The transaction data is viewable by the payer's PIP and the payee's PIP, but not by the Bank.
8. The transaction data is viewable by the payer's PIP and the payee's PIP, but not by the Bank.
9. The use of a controller allows transactions to be resumed in the event of an error. The funds may be locked if the transaction does not resume, but they would be unlocked when both devices return online.
10. They are designed to record how many transactions are completed offline and the transaction amounts approved offline.
11. Smart cards rather than smartphones were used in order to test providing strong customer authentication to users who do not have, or choose not to use, a smartphone.
12. From a technical perspective, another option would be to enable merchant PIP to translate PINs directly to the payer PIP working key.
13. Hardware Security Modules (HSMs) were not used in this PoC. HSMs are hardware security devices that store cryptographic keys and protect the keys from tampering or unauthorised access. They could be used in a production CBDC system to protect PINs from compromise.
14. This refers to the volume of keys that the BoE API was required to store.
15. PAN refers to the long number on a debit or credit card.
16. APACS 70 is a messaging standard used in the UK payments industry for passing payment instructions between the merchant's POS terminal and the merchant's acquirer.