entersekt
The Financial Authentication Company.

White Paper

An FI's Guide to Digital Wallet Fraud Prevention

Mike Cobley
Ellezane Williams
SOLUTIONS ARCHITECT TEAM

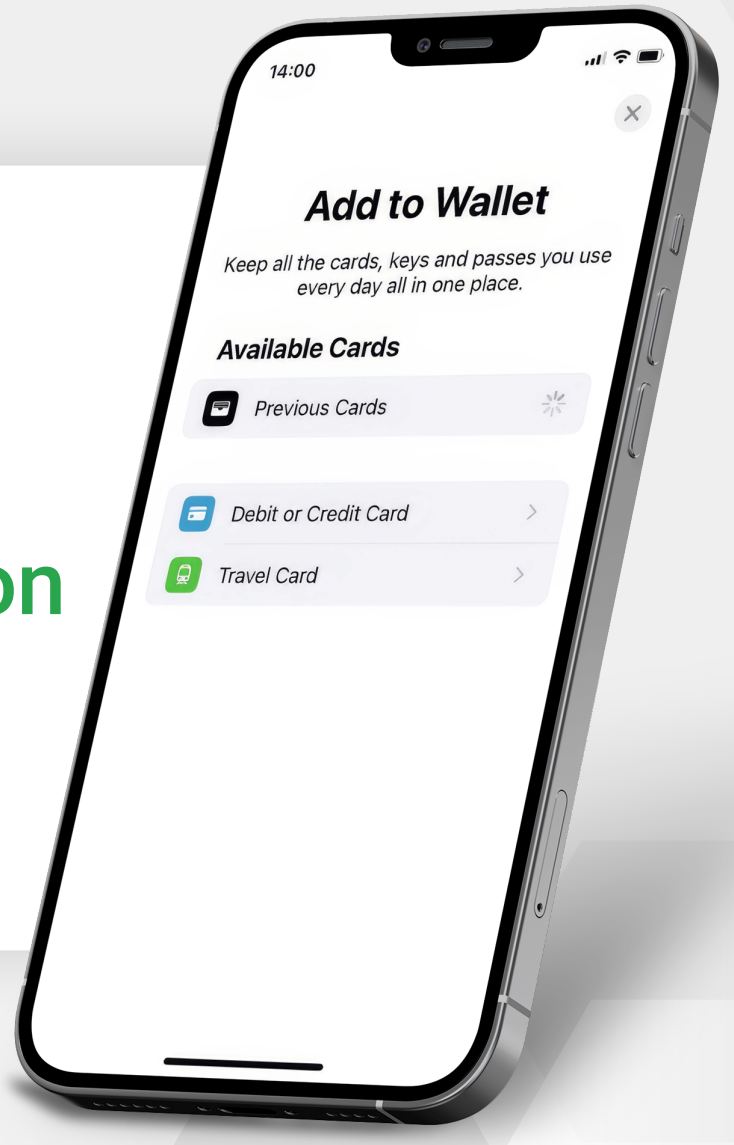


Table of contents

Introduction

Digital wallets have been gaining traction over the past few years. When we look at the numbers, they have clearly become mainstream as consumers have embraced the convenience and security benefits, and businesses have increasingly begun accepting them as a type of payment. In 2022, according to Capital One, there were 3.4 billion digital wallet users in the world, with 65% of U.S. adults reporting that they used a digital wallet at least once in the past month. In fact, 32% of global point-of-sale transactions that year were made using digital wallets, more than any other payment type, while digital wallets also led in global online purchases, the payment type of choice for 49% of transactions in 2022.

In 2022, according to Capital One, there were 3.4 billion digital wallet users in the world, with 65% of U.S. adults reporting that they used a digital wallet at least once in the past month.

What is a digital wallet?

Digital wallets securely hold payment information, such as credit and debit card details, allowing users to make electronic transactions. They are a method of payment from financial accounts via a computer, smartphone or smart device. To some extent, they eliminate the need to carry around a physical wallet. Some of the most popular digital wallets are Apple Pay, Google Pay, Samsung Pay, PayPal and Venmo. For issuers, it is important that the cards available in a digital wallet have already been authenticated at the time the card is added to the digital wallet.

How does digital wallet fraud occur and how can it be prevented?

As with any digital transaction, digital wallets are susceptible to fraud when an imposter makes an unauthorized transaction using someone else's card. For example, the fraudster has hacked into someone's account to use funds available via the victim's accounts in their digital wallet. Alternatively, a bad actor might add stolen cards to a digital wallet. And once a card is added to the wallet, authentication for individual transactions occurs entirely between the device security and the person who uploaded the card, presumably, the cardholder.

> As with any digital transaction, digital wallets are susceptible to fraud when an imposter makes an unauthorized transaction using someone else's card.

For this reason, it is critical that issuers have effective security measures to ensure that the legitimate cardholder is authorizing the setup of the card in the digital wallet. Further, it is essential to have a seamless verification process to ensure the cardholder does not abandon the setup leaving their card out of the wallet. A user-friendly process increases the likelihood of your card maintaining top of wallet status. Entersekt's Customer Authentication mobile SDK enables clients to authenticate cardholders across various digital wallet channels. By verifying the accountholder during the process of adding a card to their digital wallet, the issuer can reduce digital payment fraud.

In this white paper, we will discuss the capabilities and merits of a modern authentication process to protect cards during digital wallet setups, and a range of authentication options an issuer can utilize to create a more secure and customer-friendly card verification experience.

To understand how authentication works in this scenario, let's begin by reviewing how a card gets added to a digital wallet and then we will discuss the options for authenticating that interaction.

Authenticating card setup in digital wallets

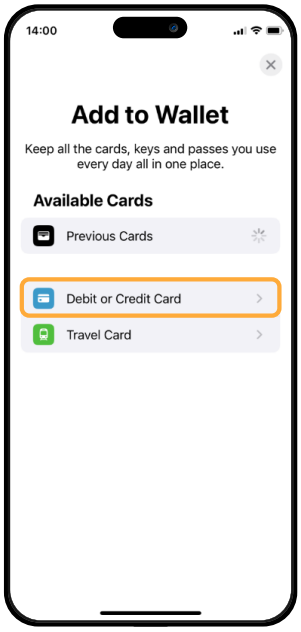
Adding a card to a digital wallet

To understand how the digital wallet authentication process works, a review of the setup steps is useful. Below is an example of how a payment card can be set up for Apple Pay, the mobile payment and digital wallet service developed by Apple Inc. While our example shows Apple Pay and an iPhone, the steps to add a card to other digital wallets and using Android phones are very similar.

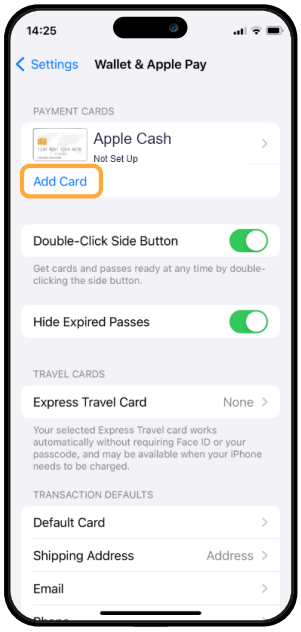
How to add a debit or credit card on an iPhone.

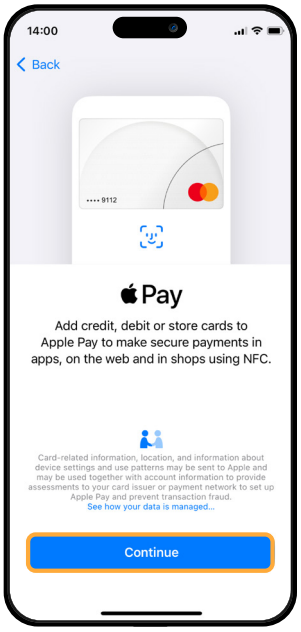
In the Settings, open “Wallet & Apple Pay,” and under “Payment Cards” click on “Add Card” (exact wording may vary by device model).

1. Tap Debit or Credit Card option to add a new card.

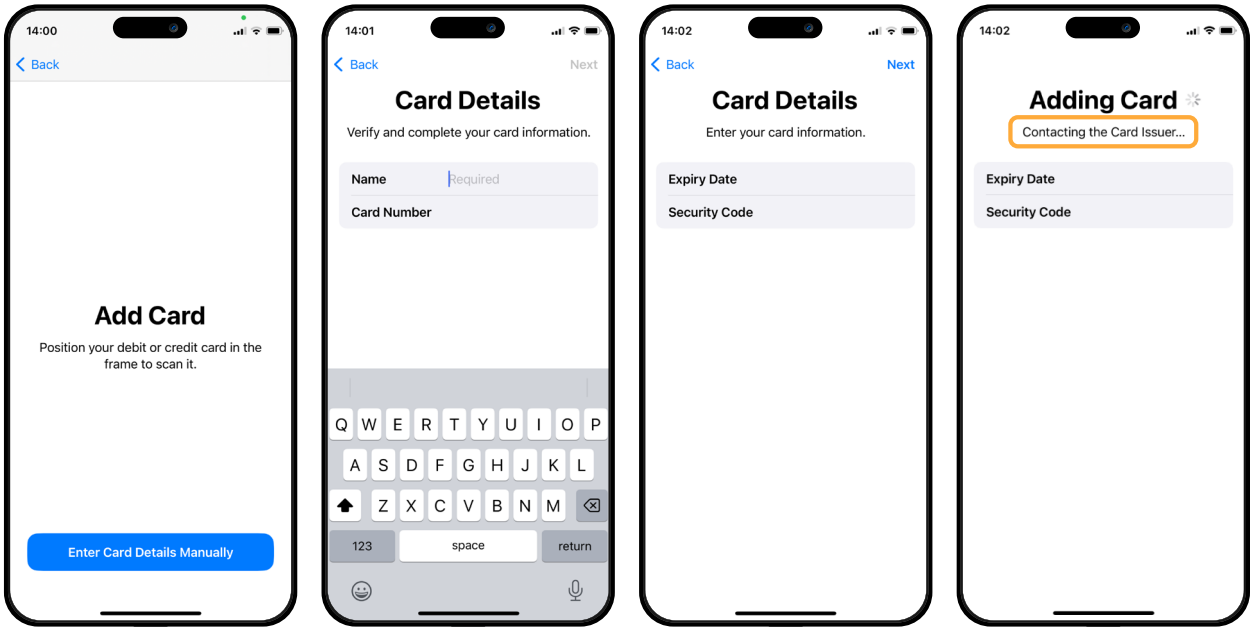


2. Under Payment Cards, click Add Card, then Continue.





3. Follow the steps on the screen to input the new card.



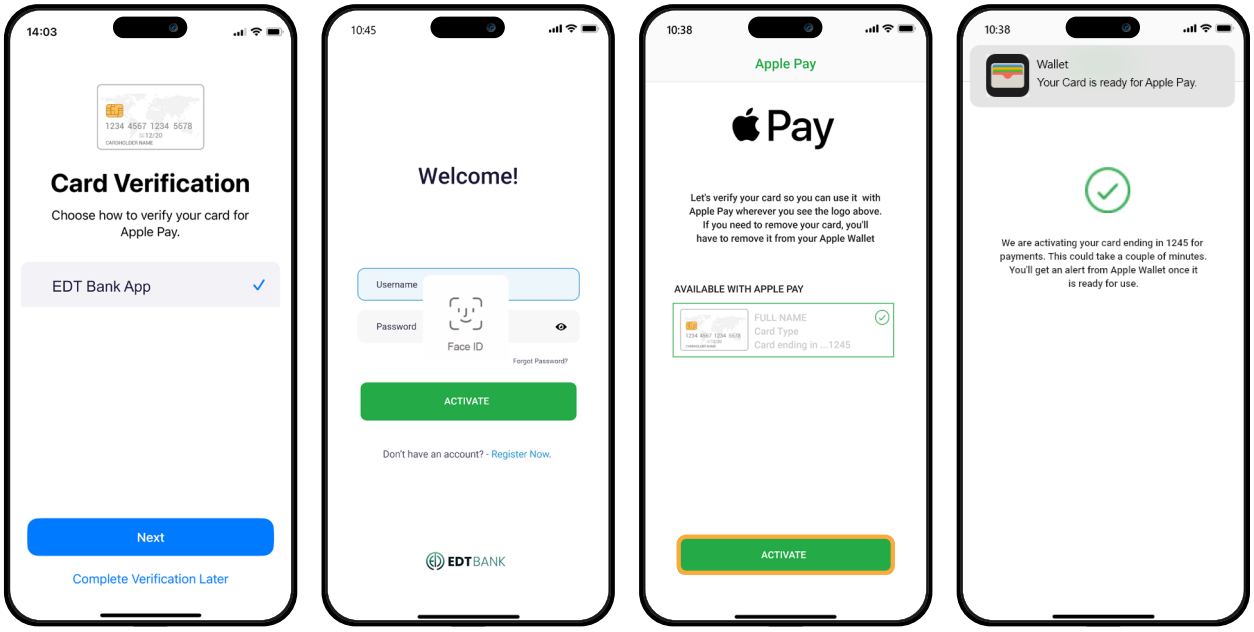
4. Before the setup is complete, Apple Pay prompts the cardholder to verify the card with their card issuer. This is where the Entersekt authentication solution fits in.

At this point in the setup process, FIs can leverage Entersekt's Customer Authentication solution to verify the customer with the card issuer. All actions up to this step are related to the digital wallet provider's process to input a card. Entersekt Customer Authentication provides strong customer authentication across browser and mobile applications. Authentication using a bank's mobile application will require an integration with the Entersekt mobile SDK. Browser authentication will require an integration with REST service APIs.

The steps that follow illustrate the continuation of the user journey above for a cardholder adding the card to their digital wallet and using their banking app to verify the card.

1. Cardholder selects *EDT Bank App* and *Next*, and the app automatically opens, using the authentication method the customer has set up for the app, in this case, the phone's face scan.

2. The cardholder is prompted to *Activate*, and even though the message says it could take a couple of minutes, the response is immediate and there is a notification at the top confirming that the card is ready to use in Apple Pay.



The authentication steps are completed in a matter of seconds, creating a seamless, secure experience.

In the "Sample use cases" section that follows, we describe and illustrate the backend steps and user journeys for four different authentication methods.

Digital wallet authentication: Sample use cases

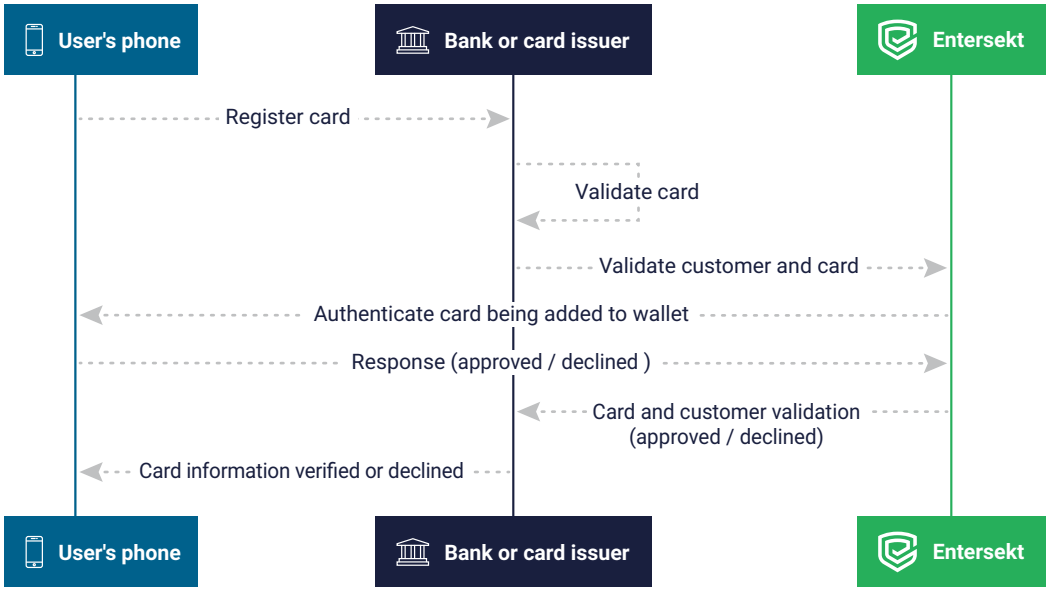
Below are four options for authenticating the addition of a debit or credit card to a digital wallet. There are many considerations issuers can assess, including user experience, security effectiveness and authentication methods currently in use to protect other channels. Entersekt experts can support issuers to assess which methods are the best fit.

Mobile banking app as the authenticator

In this scenario, you can see the backend diagram below, showing the flow of what transpired in the mobile app journey described previously, illustrating adding a card to a digital wallet and authenticating with the mobile banking app.

The key steps are:

- The card issuer has implemented the Entersekt mobile SDK into their mobile banking application.
- A customer is adding a credit or debit card to the digital wallet application.
- The user follows the steps to input the card details.
- Digital wallet provider contacts the card issuer to verify the user adding the card to the wallet.
- Having integrated to the Entersekt solution, the card issuer makes a secure web service call to initiate the authentication process.
- The Entersekt Secure Platform sends a secure authentication request to the user's mobile device via a push notification.
- Multi-factor authentication is applied, using their phone as the possession factor and device biometrics to provide the inherence factor.
- The user approves or declines the authentication request.
- The result is relayed back to the bank or card issuer that initiated the request and then returned to the digital wallet provider.

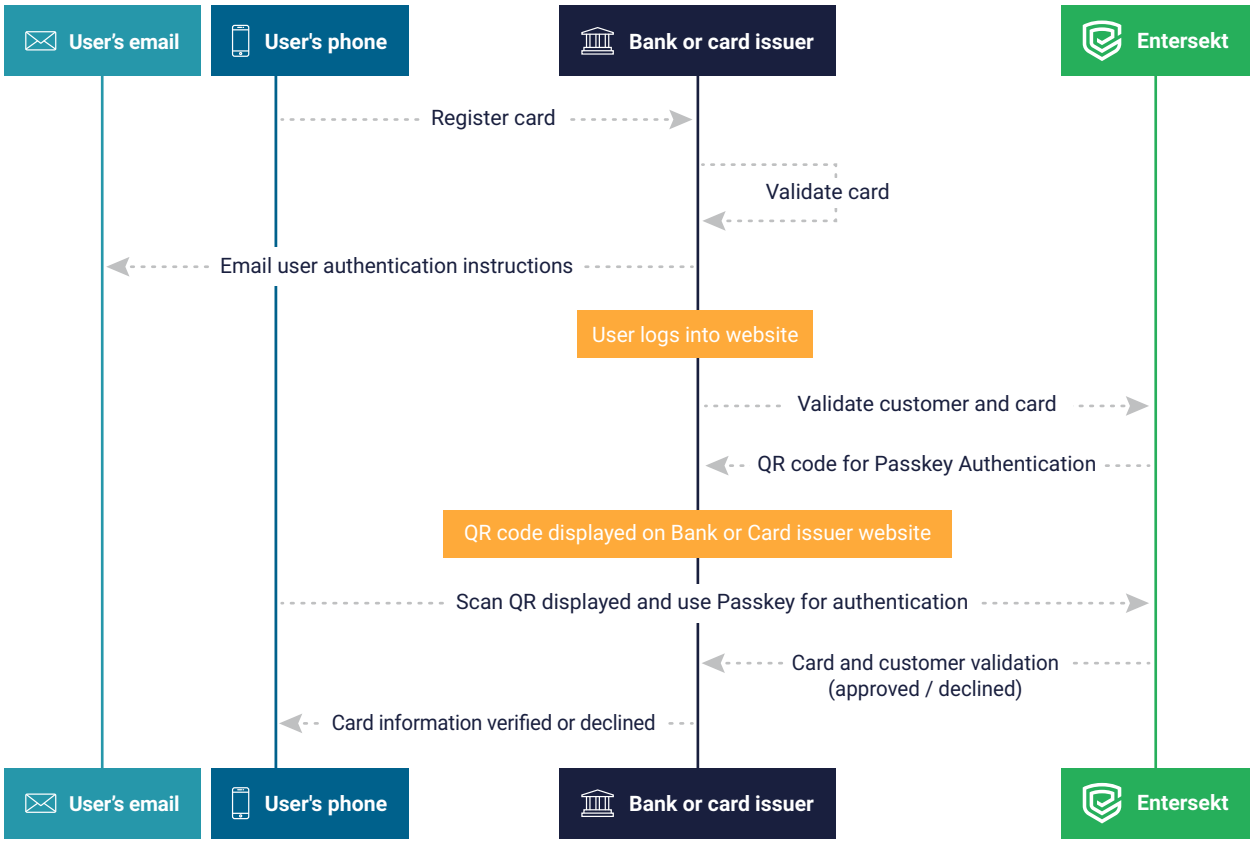


Passkey as an authenticator

In this example, we're assuming that the user has previously registered a passkey for authentication.

The key steps are:

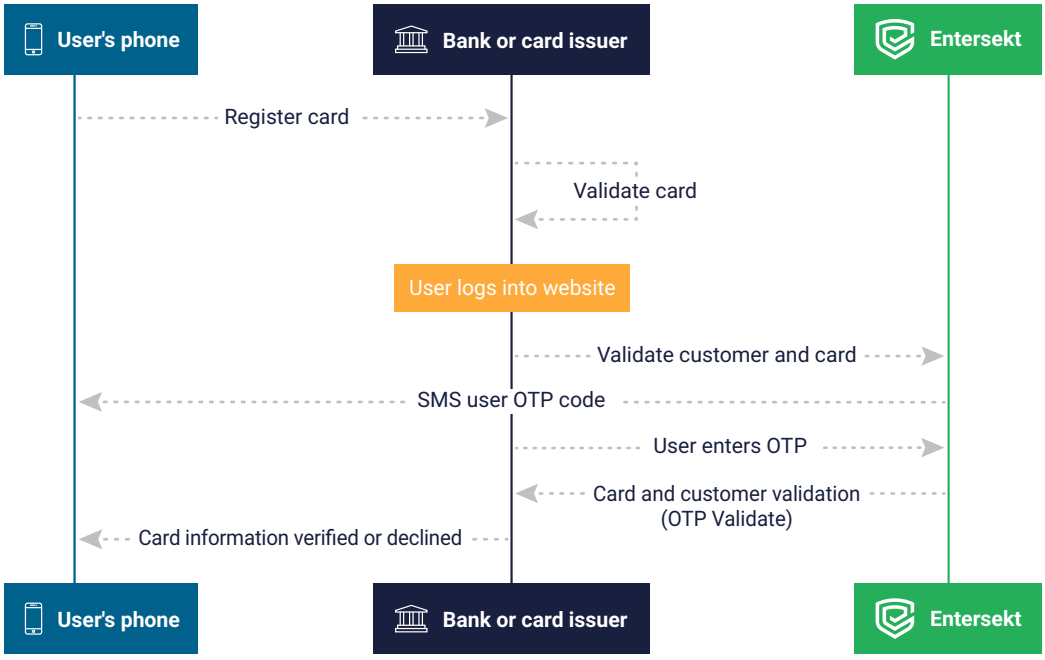
- A cardholder is adding a credit or debit card to the digital wallet application.
- Digital wallet provider contacts the card issuer to verify the user.
- The card issuer sends an email to the customer with instructions on how to authenticate using a passkey.
- Card issuer makes a secure web service call to Entersekt to initiate the passkey authentication process.
- The Entersekt Secure Platform generates a unique one-time URL.
- The card issuer displays this to the user in a QR code on their website. The cardholder uses their phone (or computer, if capable) to authenticate with the passkey-enabled device serving as the possession factor, and device biometrics to provide the inherence factor.
- The cardholder approves or declines the authentication request.
- The result is relayed back to the card issuer and then to the digital wallet provider.



SMS OTP for authentication

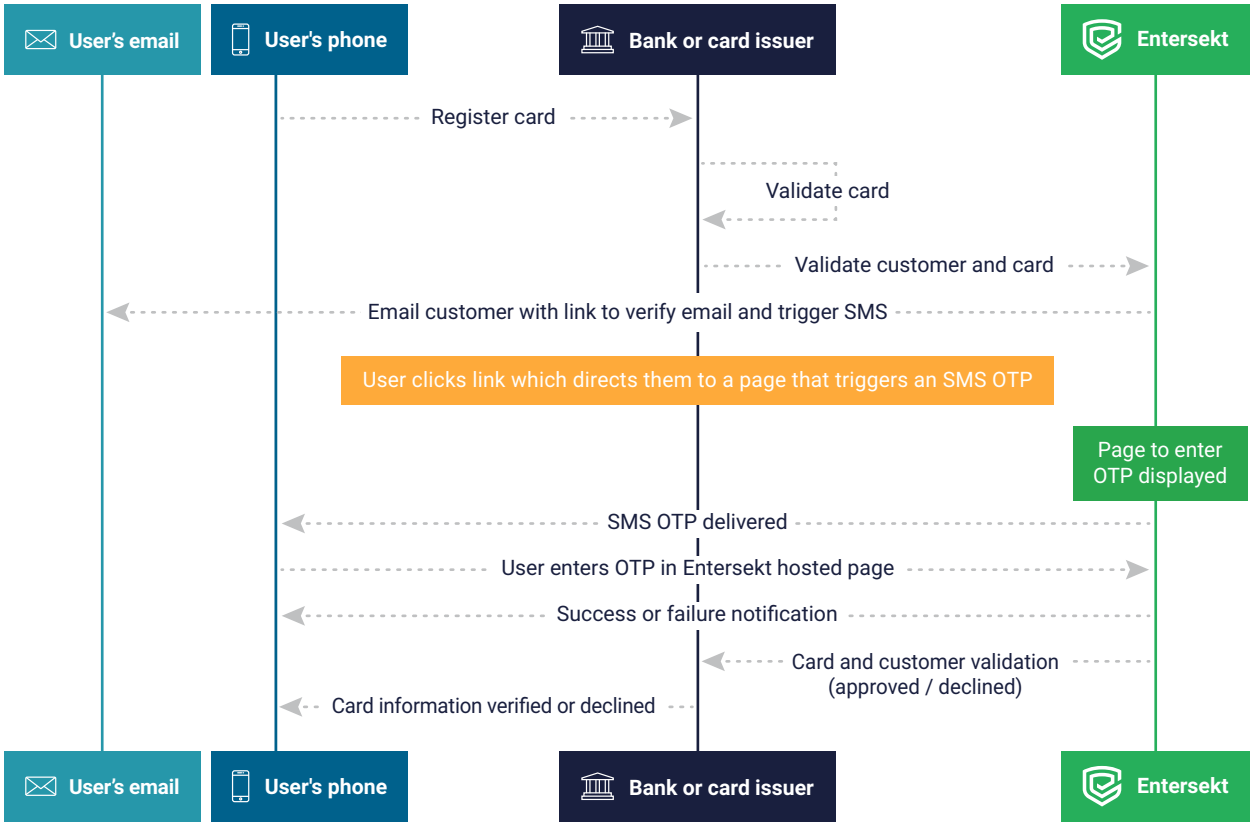
The following two scenarios are solutions that use SMS OTP-based authentication, which Entersekt supports although it is not the recommended authentication method. There are other options that provide more secure, reliable and user-friendly options. Entersekt experts can assist issuers to weigh the options.

- A cardholder is adding a credit or debit card to the digital wallet application.
- The digital wallet provider contacts the card issuer to verify the user adding the card to the wallet.
- The card issuer makes a secure web service call to Entersekt to initiate the SMS authentication process.
- The Entersekt Secure Platform generates and delivers an OTP to the cardholder's phone. Issuer can opt to add a layer of security by having Entersekt assess the SIM risk score of the device receiving the OTP.
- The card issuer displays a form to capture the OTP on their website.
- The cardholder enters the OTP, which is sent to Entersekt for validation.
- The result is relayed back to the card issuer and then to the digital wallet provider.



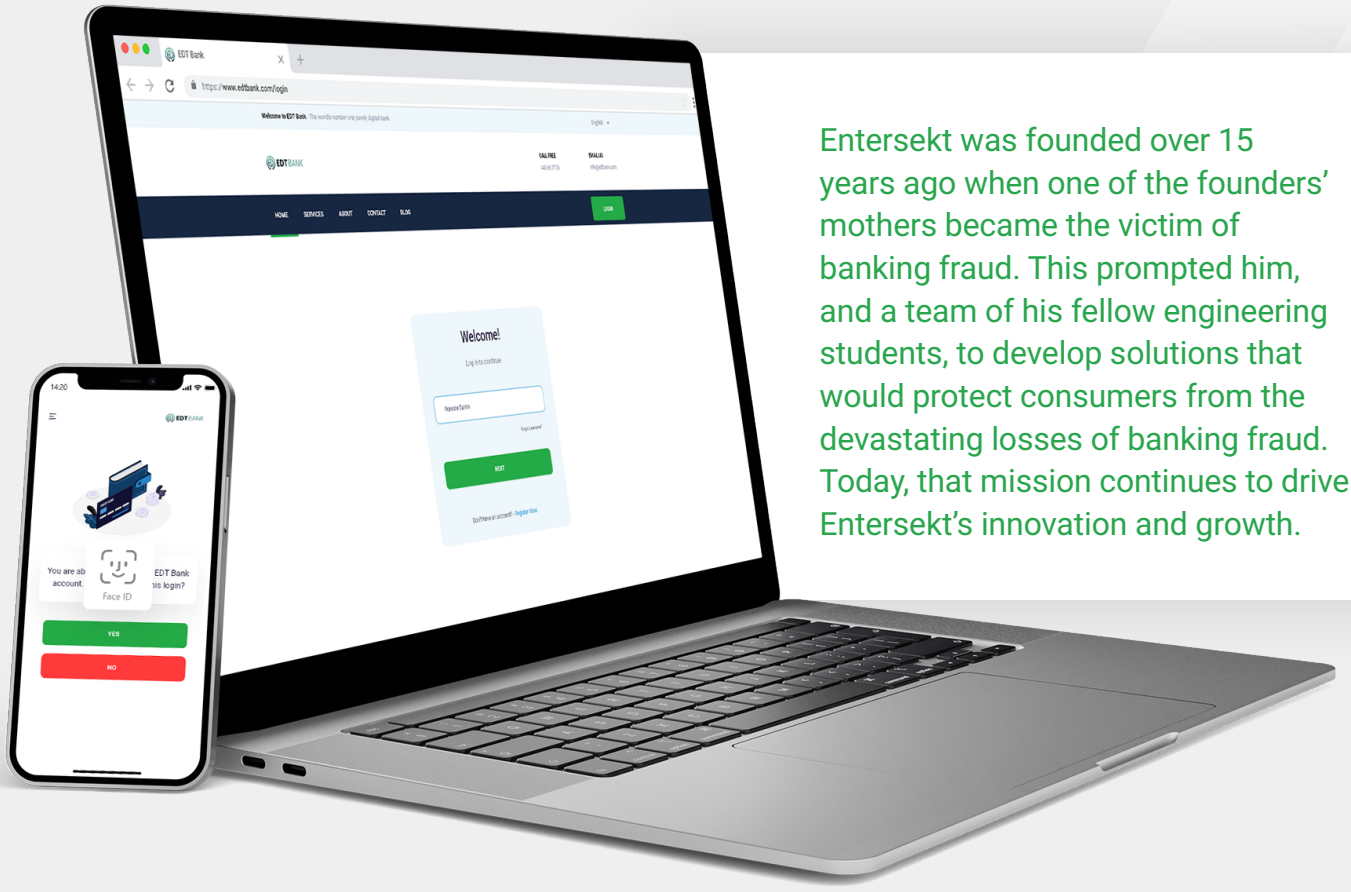
Email plus SMS for authentication

- A cardholder is adding a credit or debit card to the digital wallet application.
- The digital wallet provider contacts the card issuer to verify the user adding the card to the wallet.
- The card issuer makes a secure web service call to Entersekt to initiate an email to the customer.
- The email contains a link that validates the user's email and initiates an SMS OTP when clicked.
- The cardholder is sent to an Entersekt-hosted page prompting them to enter the SMS OTP.
- The cardholder enters the OTP, which is sent to Entersekt for validation.
- The result is relayed back to the card issuer and then to the digital wallet provider.



Why Entersekt Customer Authentication

While the focus of this white paper is to illustrate the effectiveness and positive customer experience when using Entersekt's Customer Authentication to verify credit and debit cards for digital wallets, the Entersekt mobile SDK enables clients to authenticate customers across various channels by verifying digital transactions and mitigating digital security threats. The SDK uses REST APIs to standardize authentication. The API enables orchestration and customizable user journeys for user identification and authentication.



Entersekt was founded over 15 years ago when one of the founders' mothers became the victim of banking fraud. This prompted him, and a team of his fellow engineering students, to develop solutions that would protect consumers from the devastating losses of banking fraud. Today, that mission continues to drive Entersekt's innovation and growth.

Key features of Entersekt Customer Authentication

At Entersekt, we understand the value that innovation has for FIs and their customers. With over 120 patents, we continually deliver modern fraud prevention measures that help our clients stay ahead of emerging fraud. Entersekt has a robust authentication solution that provides silent and active authenticators, able to secure all banking channels. Some of the essential features in the Entersekt solution that ensure effective authentication include:

Strong device identification

A unique identity, independent of any customer or device attributes, is bound to each customer's device using trusted cryptography standards. This identity cryptographically attests to the certainty of the customer's device during any digital interaction by leveraging its hidden private key. This key cannot be tampered with and is never disclosed.

Device context

The authentication technology checks the mobile software environment on which it is deployed to determine whether the device is emulated, rooted, or jail-broken. Emulated, rooted, or jail-broken devices provide significantly fewer security assurances than standard devices and are often a risk flag for malicious activities.

Out-of-band security channel

A bi-directionally authenticated and end-to-end encrypted security channel is formed between the customer's device and the Customer Authentication solution's backend. This isolates the transaction channel, such as mobile app to app server or web browser to web server, from security functions, such as identity verification, context analysis and authentication. This isolated out-of-band channel counters man-in-the-middle risk on the transaction channel and reduces the security impact on the transaction experience.

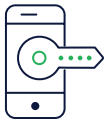
Multi-factor authentication

The solution improves the security position of a digital interaction by enabling transaction authorizations using a combination of multiple authentication factors. These include:

- Possession factors - Identifying an authorized customer device
- Knowledge factors - Verifying a customer's endpoint PIN
- Inherence factors - Verifying a customer's biometrics

Entersekt's hosted Customer Authentication solution supports:

- APP endpoints
- BROWSER endpoints
- SIM endpoints (in South Africa only)



Non-repudiation

Each authentication is digitally signed using the unique private key on the customer's registered device. Combined with a PIN or identifying biometrics, the digital signature provides the foundation necessary for proof of the origin, authenticity and integrity of data that transpired in the authentication process.

Efficiency

HTTP JSON API with support for OpenAPI enables efficient backend API generation and integration.

Key benefits

- A consistent customer experience across all digital channels
- Fast integration
- One API to standardize banking and payment authentication
- Entersekt-managed maintenance, monitoring, and upgrades
- Limited-to-zero downtime
- Strong customer authentication, based on solid security principles

The Entersekt advantage

Entersekt is a leading financial authentication company. Our exclusive focus is to meet the digital banking and payment authentication needs of financial services organizations. This focus provides clarity of purpose and allows us to concentrate investment in capabilities that serve the financial services industry.

Some of the key advantages of Entersekt's Customer Authentication include:

Data-driven fraud prevention

Reducing the impact of threats posed by phishing, man-in-the-middle, man-in-the-browser, and keylogging attacks. Our Customer Authentication solution creates a secure, encrypted, out-of-band authentication channel that ensures authentication requests and responses cannot be compromised.

Compliant

Entersekt ensures continuous compliance with industry requirements and security standards, supporting FIs to address key global and regional regulations.

Scalability

The API to the Entersekt Secure Platform provides access to the full range of capabilities and scales easily to accommodate new channels and banking services.

High availability

Entersekt's Customer Authentication solution employs Amazon's Elastic Compute Cloud (EC2) infrastructure to scale with the load and ensure successful live deployments. Entersekt implements live maintenance and updates to the system without downtime.

Balanced and consistent customer experience

Entersekt delivers security with a seamless customer experience by supporting multiple use cases, which all contribute to increased transaction success and app usage. We apply silent authenticators to minimize friction, only issuing challenges when data indicates risk, according to the FI's rules.

Fast time-to-market

Product go-to-market timelines for the hosted service are significantly reduced compared to deploying an on-premise solution. The API-based solution reduces the need to configure services or excessive firewall rules. When you embed the service SDK into the banking mobile app, you get access to Entersekt's full range of features. A dedicated authentication app with an implemented SDK is also available for even faster implementation.

Minimized security effort

By providing a robust platform that mitigates pressing security threats, Entersekt reduces your security implementation efforts, allowing technical teams to focus on innovation and other priorities.

Summary

With the rise in popularity of digital wallets, fraudsters will be working overtime to find ways to intercept the funds flowing through this channel. In this white paper, we've described several options for securing cards as customers add them to their digital wallets. Some of the options are more secure and more future-proof than others. Entersekt experts can advise you on the most suitable option for your organization.

The bottom line is, it is critical that financial institutions implement strong, proven authentication measures to prevent widespread losses. Those that don't will not only be exposed to direct financial costs, but risk losing the confidence of cardholders, and the coveted top of wallet status.

About Entersekt

Entersekt, The Financial Authentication Company, provides financial institutions with digital banking fraud prevention and payment security solutions through it's cross-channel, Context Aware™ Authentication platform that secures digital transactions and optimizes user experiences. Founded in 2010, Entersekt serves financial institutions around the world, and holds 120+ patents for its security innovations. In 2023, Entersekt acquired Modirum, a 3-D Secure solutions provider, positioning Entersekt as a global industry leader in authentication solutions for financial services. Entersekt processes 2.5bn+ transactions for 250m+ cardholders and 450,000+ merchants from 850 banks+ in nearly 70 countries. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions.

For more information, visit entersekt.com.