Deep Science Publishing
https://doi.org/10.70593/978-81-989050-1-7_6

DeepScience
Open Access Books

Chapter 6: Modernization of wallets, smart cards, and contactless payment interfaces

6.1. Introduction to Modern Payment Systems

As a part of daily shopping, both social and individual, at least some operations must be carried out for the exchange of goods or services for payment in currency form. From historical data, these currency exchanges have evolved from the barter method, where people's needs for goods and services matched each other, to the modern global markets through different stages including the use of metals, banknotes, and coins. Similar variations exist for settlement operations in e-commerce as well. The barter system, which had direct utility for trading parties for their common needs, had significant shortcomings for large populations, which were gradually overcome with the adoption of new payment methods and intermediaries. With the substantial growth in mobility of populations and commerce, and with the development of financial instruments and diverse goods and services provided by new suppliers, providing effective and secure payment methods becomes challenging. The evolution in payment systems began with the introduction of paper-based currency, subsequently for the digital form with the advent of computers, and recent developments include cryptographic mechanisms for the digital currencies in various forms (Khando et al., 2022; Moon et al., 2022; Mogaji & Nguyen, 2024).

In this development, for the concepts of efficiency, security, and privacy, the growth in digital payment methods contributed significantly. However, they also introduced new risks associated with centralization, which hackers could exploit for large-scale robberies. With the present trend towards consumerism in both goods and services, the payment system is at a pivotal position in enabling faster and flawless settlement of financial transaction overlays among business portals for e-commerce, for contactless smart card/e-wallet payment systems through point of sales terminals, and mobile applications. At the same time, consumers prefer convenient and effective payment through reduced risks for security and privacy breaches. It is against this backdrop that we present a review of the current developments in the world of modern payment systems, especially e-wallet, smart card, and contactless payment interface technologies.Digital tokens like frequent buyer credits and prepaid value held for tax refunds by merchants are not convertible to cash and, most importantly, cannot be transferred by consumers to other merchants. While private incentive programs are ubiquitous, prepaid value transfers and payments to others form a critical layer of our payment infrastructure and, through walletization, also of our monetary infrastructure. In this context, various payment implementers have begun to explore a silent revolution by embedding payment functions into smart cards and wallet devices most of which are mobile phones with contactless wallets that communicate to contact arrays on point of sale terminals (Patel et al., 2024; Shah, 2025).

Fig 6.1: Modernization of Wallets, Smart Cards, and Contactless Payment Interfaces

6.1.1. Background and Significance

Modern payment systems are both unaccountably ancient and yet astoundingly new. The credit card which we normally think of as the epitome of the modern payment device was only invented in the early 1950s. The spread of electronic money was only made possible by the widespread development of computerized databases, magnetic stripe, EMV chip, and contactless smart card technologies. Its first tangible manifestation was the ATM, which was pioneered amidst the hothouse conditions in Britain and Japan. After modest penetration in retail and eCommerce during the 1990s, the advent of mobile phones saw a second generation of electronic means of payment. The latest incarnations – mobile wallets which support remote and proximity payments and smart cards which allow for the storage of multiple prepaid value and prepaid debit applications – have incited an outbreak of public and private sector interest.

What is new about money? Quite simply, it must be authentication. If value stored in a prepaid account cannot be moved, it is not a danger to monetary sovereignty.

6.2. Evolution of Wallets

Wallets are essential for carrying things of high value such as money, cards, and personal identity. They are a component of a user's identity and as such reflect their values and preferences. How a wallet looks and what is inside shows the world who you are. Wallets have existed for millennia, typically made from animal hide or leather, and have evolved from simple pouches to sophisticated modern designs. Through this evolution, wallets have remained a necessity and are used daily by most people. With the advent of computers, mobile phones, and the internet, a new type of wallet has begun to change what we think of as a wallet. Digital wallets are now being used to hold everything from bank and credit card details to airplane tickets, hotel reservations, and security credentials for authentication.

A major challenge for these payment and identity systems is user adoption, largely because consumers want something that is as easy to use as cash and traditional wallets, but with all the advantages of the new systems. When someone takes out a credit card to pay for something, that process is very quick and easy, compared to fumbling to remove an NFC-enabled mobile phone from inside a purse, activating the phone, waiting for the app to load, and then holding it to a terminal for the payment to clear. If mobile wallets are easier to use than credit cards, people will adopt them. Digital wallet proponents think that smartphones will become the wallets of the future, allowing holders to store money, tickets, boarding passes, and coupons.

6.2.1. Traditional Wallets vs. Digital Wallets

Webster defines a wallet as "a folding case for holding paper money, credit cards, and other flat objects" and cites its origins in Medieval English, probably from Old Norse valdi, meaning "to rule," but the word wallet was first used in English in 1377 as "a bag or pouch." Other claims suggest the historic baggage roots of a wallet, originally a bag for carrying injured soldiers' personal effects. Over the centuries the design of wallets changed very little, the materials used to make wallets changing from leather in the earliest days to cloth, synthetic, and leather components today. Wallets also evolved from being used primarily as money carriers, to carrying not only money, but pictures, cards, keepsakes, receipts, and offers.

In contrast, digital wallets are a relatively recent phenomenon and the digital wallet landscape is quickly changing, with a heavier emphasis on the term digital wallet being applied to mobile payment applications. Today many definitions exist on what constitutes a digital wallet, few wallet vendors agree on a consistent definition, and many define their product with a narrow focus on a single payment feature. At a high level, a digital wallet is an application that allows consumers to conveniently store and access their payment methods, loyalty cards, coupons, gift cards, tickets, ID cards, boarding passes, transit passes or other forms of digital credentials. Few wallet definitions specify who the target user or users are for digital wallets with a few focusing on providing a secure interface accessing bank payment accounts, while others focus solely on supporting mobile payments. Digital wallets permit consumers to conduct transactions via websites, mobile devices, POS terminals, or automated kiosks without entering payment, transaction, or customer account information, or downloading a mobile application for a transaction or purchase.

6.2.2. User Adoption Trends

The largest mobile wallet providers only recently began seeing revenue growth. The slow early uptake of mobile wallets mirrors the experience of online banking, which took more than ten years to cross the 50% adoption threshold, and that of remote mobile payments, which took six years to cross that same bar. Like these other technologies, mobile wallets began life in a small niche. Consumers are generally not big spenders, so their use has not attracted merchant interest. Even among those who believe in early adoption, the timing of mobile wallets' emergence onto the mainstream stage is a matter for further discussion.

Smart card-enabled contactless payments in general have seen rapid adoption, especially in the United States, where the presence of third-party payment service providers has fueled merchant interest. Physical card contactless payments have come into their home turf. Banks in the United States have successfully persuaded thousands of retailers to add contactless acceptance to their marketing pitch. But, as we will discuss, the merchants have faltered more than altitude so far. Card contactless payments are currently lagging. Adoption is also being helped in Europe, where there is a vibrant ecosystem of industry players eager to design and deploy tokenization. Tokenization disguises cardholder data by masking it with randomized tokens to make mobile payments more secure and put consumer minds at ease. Five European countries are seeing merchant contactless trials, as are individual banks operating in other European states. Successful outcomes from these trials are leading participants to retrofit lessons learned back to the contactless infrastructures they had previously designed for their banks, in advance of going live with their interoperability projects.

6.3. Smart Cards: A Comprehensive Overview

Although the term smart card is often used to denote any plastic card with an embedded chip, the term actually refers to a specific configuration, which differs from contactless and proximity credentials. To explain, smart cards can be housed in a plastic casing containing either a memory chip or a microprocessor with a basic operating system. Both contain digital data that facilitate communication with card readers, usually through hardened contact pads. In this section, we will provide an overview of smart card types and smart card security. While all smart cards need to be securely mounted inside a plastic casing, there are three types of designs for doing so. These are called contact cards, contactless cards, and dual interface cards. In contact cards, the contact pads are embedded flush with the surface of the card. These cards are normally less expensive than contactless and dual interface cards and are capable of storing more data. However, they are less convenient than contactless credentials, which do not require any physical contact with a reader. The only requirement is that the card be brought sufficiently close to the reader to establish communication over radio waves. But unlike proximity cards, which communicate exclusively through radio frequency signals, contactless smart cards have contact pads embedded inside the plastic casing, enclosing the chip. This allows users to obtain the higher level of security offered by direct access through hardwired contacts when required. Normally, contactless smart cards serve to securely authenticate users and permit access to systems and locations. These functions require rapid identification and verification at many different physical locations, without the need for establishing physical contact with a reader.

6.3.1. Types of Smart Cards

Smart cards are categorized based on a variety of criteria. The three main types are identification cards, memory cards and microprocessor cards. Identification cards, also referred to as ID cards, have a type of integrated circuit chip whose circuits are wired inside and bonded to the chip, and the only function is to store an authentication key for a host system. This one-key-only system has a low capacity and is ineligible for use in sensitive applications. Memory cards are chips that hold data and their memory can be easily accessed, but they do not have a microprocessor chip to compute information. Therefore, they are only used for secure storage and transfer of applications between the two communicating entities. Microprocessor cards, referred to as smart cards based on their unique functions, have their own built-in microprocessor which is loaded with an operating system and multiple applications. These microprocessors are dependable, low-power and small devices. Most of the general purpose smart cards fall under this category.

Of the three different types of smart cards, the microprocessor card has a compact design, larger capacity and advanced security functions that allows smart card systems to utilize diverse applications. Besides these three categories, there are different ways of classifying smart cards as contact, contactless or dual-interface types based on the way of connecting to a host system, or based on the mode of operation that connects either a single pad or both pads. The reason for the types mentioned above is primarily because of the electrical and physical connections for intelligent communications between the smart card and the host. The physical connection between the chip inside a smart card and the outside world is accomplished using PINs. In this case the smart card is known as a contact smart card. Contacts are located on the smart card surface which may be made of several kinds of materials. Most smart cards are plug-in modules that fit inside the reader.

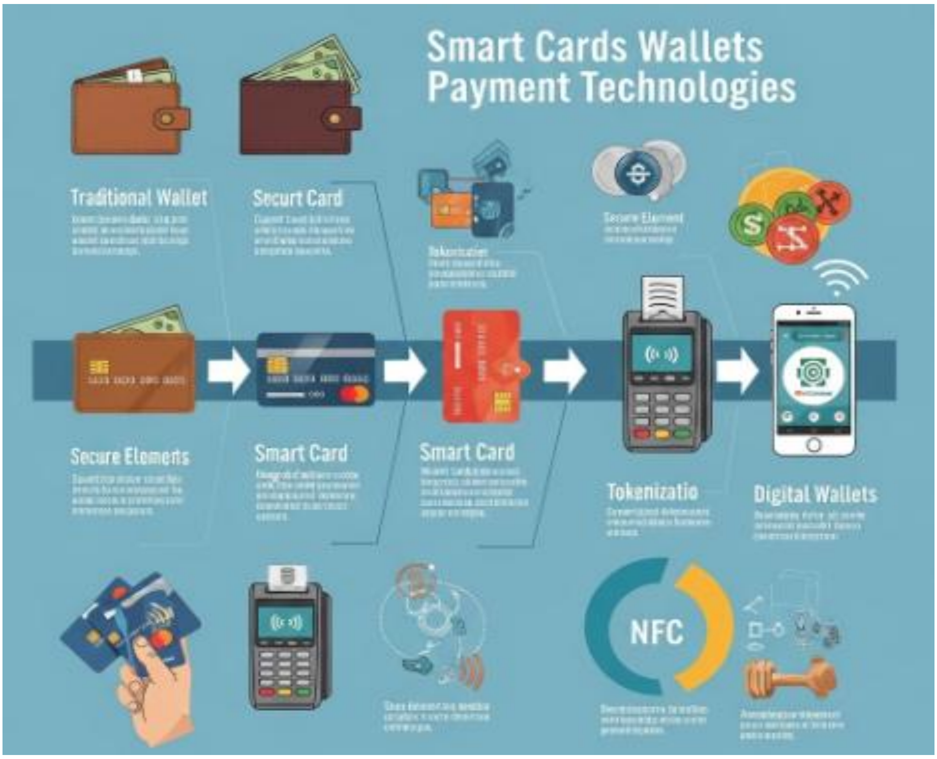

Fig 6.2: Types of Smart Cards of Modernization of Wallets

6.3.2. Security Features of Smart Cards

More and more applications are using smart card technology. Payment, healthcare, driving licenses, identity verification, banking, and numerous other systems now use smart cards for secure identification. The increase in demand has motivated lots of research work in the area of smart card security. Work has been done in the area of physical attacks, software attacks, access control, secure channel, and so on. In this paper, we will classify attacks on smart cards, which have been proposed recently and had a reasonable impact on card security.

Smart cards are small electronic devices that can be carried in wallets, purses, or as key fobs. Smart cards allow users to easily perform such tasks as: making payments for goods and services; providing tokenized access to events, buildings, and secured technology; providing network, desktop, and application-level authentication; controlling access to both stored and encrypted information; verifying identity for on premise and remote transactions; storing health records for use in emergencies; providing transportation access; and much more.

The smart card market can be segmented into contact smart cards, contactless smart cards, and dual-interface smart cards that have both contact and contactless capabilities. Smart cards are available in a variety of form factors, and the primary function of both the chip and the smart card is security. Smart cards are designed with basic physical hardware security, access control, internal data encryption and decryption, support for secure communications protocols, secure on-card data storage, internal storage cipher, and banking key support. Additional advanced smart card security features include anti-cloning services, extended key management options, and real hardware true random number generators.

6.4. Contactless Payment Technology

Despite the concerns about security associated with contactless payment technology, mobile payment is growing rapidly. Contactless payment is a way to pay for goods or services through a wireless, electronic transaction that requires little or no electronic contact between the sales clerk's and the customer's terminals. Contactless smart cards or smart phones and terminals are equipped with short-range radio frequency identification technology or other contactless technologies that allow fast electronic payments using a wireless connection. The consumer simply holds the near field communication-enabled card or smartphone very close to the terminal to complete the process. Some consumer contactless devices require biometrics, such as a fingerprint scan, before enabling the payment; others do not.

Contactless payments can occur only over short distances (typically 2–10 cm), which reduces the risk of fraud; capture of account information is not likely by a thief at a distance. The maximum amount for a contactless transaction is generally limited to some amount below the amount mandated for a signature. Users need no cash, no coins and no signature. In addition to transport, ticketing and vending applications, other types of merchant and banking terminals are being equipped with contactless payment technology. Contactless payment technology is part of many vision-based unified personal mobility systems under development. The technology is already used in systems for automobiles and trucks to pay highway tolls or railway tickets; use of equipped toll or ticket booths permits thousands of vehicles to travel through a specialized electronic throughway lane without stopping or slowing down.

6.4.1. How Contactless Payments Work

The primary and requisite functionality of a payment card is to transmit financial and identity data from the consumer to the payment processor via contactless or card-present transactions. Contactless transactions require specific underlying technology, because certain technologies are not suited to this application. This technology is passive, wherein a card contains no power supply or battery, and chips cannot perform any computation until powered by an external field from a reader or transponder. While passive technology can operate protocols employed in some contactless payments, it cannot perform the security checks, challenges, and data enciphering in an encrypted channel that secure closed systems create to assure the payment transaction's integrity.

On the other hand, this technology is active where the transponder and reader can both power and communicate with each other to perform secured closed communications. Furthermore, everybody has a reader in their phone and its communications link can authenticate users with other tags or chips using asymmetric keys. Thirdly, we tried to convince that biometric security and privacy requirements can also be satisfied to allow one-to-one communications or transactions between a reader for a smartphone and a tag or chip in whatever personal device that identifies the wearer. It follows that, under proper assumptions and management of asymmetric keys in the authentication phase, supports secure and privacy-preserving contactless payments. During any one of these pay transactions that admittedly use this technology, the consumer in question, payments can be enabled by implementing locally the various supported features of secure closed payments as part of a card emulation mode.

6.4.2. Benefits of Contactless Payments

Contactless payment technology speeds up payment transactions and improves the checkout experience with more convenience for customers. Customers only need to wave or hold their contactless-enabled card or mobile device near a secure contactless reader instead of inserting a card or swiping it on the terminal. As a result, transactions usually take less than a second to complete. This technology eliminates many time-consuming and often painful steps in the check-out process. It also offers a faster, more user-friendly experience than cash, and is less likely to spread germs than touching a keypad or handling paper currency and coins. A contactless payment is especially beneficial in quick-serve environments with many small, frequent transactions, such as fast-food restaurants or retail outlets. These merchants account for nearly 75% of payment transactions. Contactless payments will be equally important at venues that will experience a huge surge in traffic volume when they re-open after closure due to a pandemic or other crisis. Such merchants need solutions to safely and quickly process transactions.

This technology enables a merchant to deliver safer, faster, digital interactions throughout the payment transaction process. Customers can check out from anywhere with a contactless payment, for example, right at their seat in a restaurant or any location on the premises. They have several payment options available via their mobile device and can make transactions in a safe and private manner while retaining their social distance.

6.5. Integration of Wallets with Smart Cards

The substrate on which contactless wallets are built is essentially the same as for smart cards. There are many possible reasons why users who have a contactless smart card may wish to add that smart card to their mobile payment application. One of the most frequently stated purposes for a mobile wallet is personalization. A mobile wallet allows users to store all their accounts in one place and to easily select which one to use for various dealings. Direct support for smart cards within mobile wallets provides an easy way for banks and other financial institutions to expose smart card functionality or their functionality with existing smart cards to mobile devices. Another reason may be usage statistics. Banks and other financial institutions are very interested in obtaining usage information about the accounts that their customers are using.

While integration of contactless wallets with contactless smart cards is likely to be accomplished primarily via the virtual card concept – a smart card in your phone rather than in your pocket – there are other reasons that smart card support should go beyond just virtual cards stored in the mobile wallet. Each method of making payment has positives and negatives regarding its security and ease of use. So there will be some cases in which the user will prefer that a contactless smart card be used instead of the mobile wallet, particularly for higher-value transactions. One specific reason a user may choose to use a smart card for a transaction rather than a payment app may be reduced application launch time. Depending on the payment app, it may add an additional delay when eventually selecting the payment app from all those located on the mobile device.

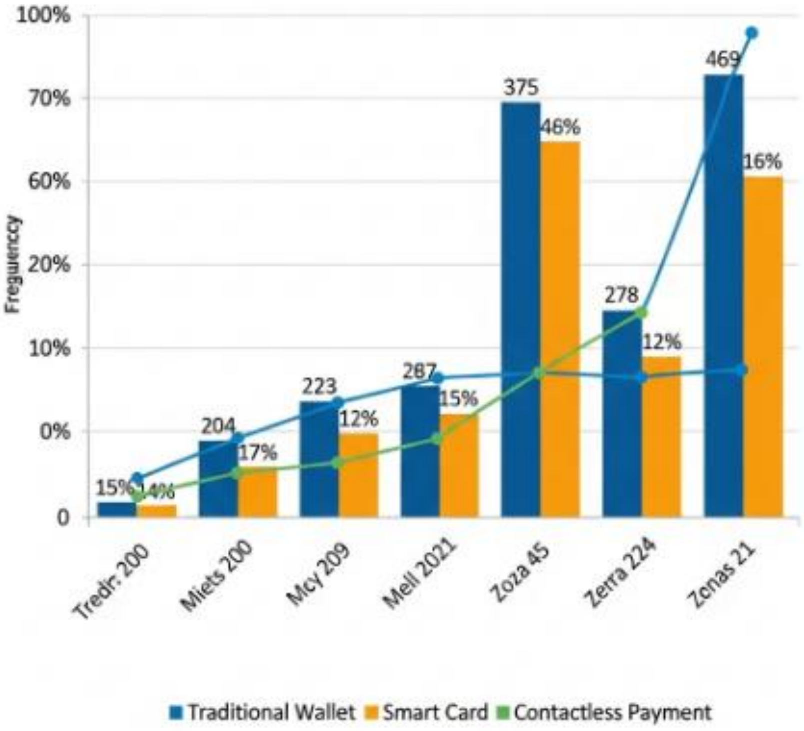

Fig : Bar graph of Modernization of Wallets

6.5.1. Interoperability Issues

The integration of wallets with smart cards opens up new markets for wallet vendors and extends the range of functions to which the wallet interface may be applied. Any chip card with a contact or contactless interface may act as a wallet, a payment token, or other types of smart cards, but interoperability poses several challenges. First, wallets resemble applications stored in the memory of contactless cards, where the card user may be contractually associated with one financial institution that provides payment and prepaid services and with another institution that offers services related to loyalty, couponing, etc. In addition, a wallet does not have an issuer, but the applications and service providers that it manages do, so no single entity can impose 'rules of engagement' that apply to all installed applications.

This has important consequences. Wallets offer an entry point between the user and a wide range of service providers; these may change regularly over time. Service providers may thus want to place their applications in wallets, but they cannot predict how many users will install them; nor can wallet vendors guarantee them that their applications will be included in the list of 'technically or analytics recommended' applications that go through the preemptive or predictive ordering process. Because the wallet is not a single service provider, it is also not guaranteed that a wallet should be chosen prior to interaction. As a result, lifecycle management of apps in the wallet and app resource allocation modalities are multiple, complex, and asynchronous. This complexity is encapsulated in rules of engagement of instantaneous smart card omnibuses and other specification-driven bottom-up approaches. One result is the occasional failure of contactless transactions, which tend to annoy users.

6.5.2. User Experience Considerations

One of the main mechanisms used by mobile wallet applications to interact with users is notifications. These notifications can indicate transactions, remind users to take specific actions, or provide users with updates regarding their accounts. Payment applications and financial services rely significantly on notifications to communicate with users. In order to effectively serve as a wallet replacement these applications need to support a variety of payment types. Currently this support is very limited, and often only one payment mechanism is used. A user looking to take advantage of mobile wallets for a variety of payment types has to juggle multiple notification channels and mechanisms, which clog their notification center, greatly affect the user experience, and make it difficult to maintain transaction history. Consolidating all wallet-based transactions into a single application can reduce the number of notifications that users receive and provide a better user experience. Unifying the mobile wallet experience across multiple payment mechanisms relies on service application vendors opening communication protocols that allow all applications and services to interact with a single wallet application. This requires a large mobile wallet service ecosystem to justify the investment needed to develop a unified communication model. Tap-to-pay experiences, on the other hand, require the mobile wallet user experience to be very seamless. There are two types of tap-to-pay transactions: (1) the ones that the user has to first tap in their mobile wallet and then tap to pay (2) the ones that happen automatically when the mobile wallet is in the background. In both situations, the user has to interface with the mobile wallet application on their smartphone in order to execute the payment action. Ideally the user experience should allow tap-to-pay actions to happen without requiring the user to unlock, launch, or actively use the smartphone, which makes mobile wallets more convenient than traditional methods of payment.

6.6. Regulatory Framework and Compliance

The modernization initiative aims to position itself toward becoming a global country with regards to Economy, Technology, Social Infrastructure, Health, Environment, Trade, Peace, and Governance. The initiation of the modernization initiative is primarily driven by the digital transformation of payment systems that is observed globally. The implemented processes and techniques must comply with the regulatory framework as well as the consumer sentiments specific to such systems. The transactions should be secure, payment initiation processes seamless, data protection measures implicit, no adverse actions taken toward the consumer, and high consumer trust established in the system. This section examines existing international and regional regulatory frameworks and provides an overview of their compliance to the proposed modernization initiative. First, it will discuss global regulations impacting the payment system, post which consumer sentiment in terms of data protection and privacy concerns is discussed. In addition, this section provides an overview of the existing regulatory frameworks related to modernizing digital payment wallets and proposes a path toward achieving regulatory compliance. Ever since the introduction of various payment services regulations, there has been a focus on the improvement of authorization, authentication, data protection, and permission management involved in payment handling systems. Recently, a proposed data act has put further emphasis on data sharing, access, and usability across payment ecosystem players. Multiple regulatory frameworks have been put in place for protecting consumer data and privacy. These frameworks address, for example, consumer protection, liability, consumer data disclosure, retention, access, erasure, protection from misuse, and more. There are a variety of policies that focus on achieving data protection principles.

6.6.1. Global Regulations Impacting Payment Systems

Payment systems are subject to a multi-faceted and evolving global and regional regulatory framework. The process of modernization and liberalization of the payment system underwent significant transitions with the birth of the digital economy and commerce, which urged WMTs and their associated payment systems to develop further at a fast pace. That was made possible by the proliferation of smartphones and the adapted interfaces, security features, and standards intended to integrate payment systems into multiple services based on the use of mobile devices to generate value for each user.

However, the convergence of telecommunications, digitalization, and finance raised numerous concerns since cross-border services often involve several jurisdictions, the applicability of regulations is not transparent, and oversight mechanisms are often fragmented and weak. This Section presents a review of the international and regional regulations intending to provide oversight rules for the financial elements of mobile wallets and mobile payment transactions, examining key aspects of payment transactions in privacy and consumer protection terms. The primary objective of this regulatory framework is consumer protection, covering issues such as privacy, data protection, or liabilities in case of unauthorized transactions. The regulatory landscape includes global or self-regulatory initiatives, as well as regimes designed to ensure user protection in cross-border services, implemented by banks and financial institutions, and regional, bilateral, and national financial regulations.

6.6.2. Data Protection and Privacy Concerns

The use of payment systems can expose consumers and merchants to various kinds of risk. An important commercial and legal framework exists to manage such risks at local and international levels. Specifically, given the globalization of commerce, many payment transactions cross borders and may be subject to different regulations. However, despite these regulations, there are still some issues that may have a negative impact on consumers and merchants.

Privacy is usually defined as the right to keep to oneself and control access to personal information. This definition may be interpreted broadly or narrowly. For example, a broad interpretation allows a person to force an online service provider to keep no record of the person's transaction with the service provider. Accordingly, this service provider has privacy obligations as a custodial service provider for the person. A narrow interpretation may assume that the service provider is not a custodial party at all and therefore does not have privacy obligations. The narrow interpretation is based on the service provider's business model, but this interpretation is controversial.

Depending on the interpretation, various parties involved in an online payment transaction may have privacy obligations to each other. In broad terms, a payment service provider or a merchant may have privacy obligations to a consumer, but the parties may also have these obligations acting as service providers. At the same time, the commercial and contractual relationships of the parties may not create any privacy obligations.

6.7. Conclusion

The conclusion of this paper presented an overview of ongoing and potential future developments in contactless smart card product and infrastructure capability and usage. As demand has grown for increased performance smart card functional capability and the recognition that contactless smart cards can effectively play a practical role in the infrastructure of a contactless payment system, there has been a drive to develop more sophisticated multi-application contactless smart cards. As sophisticated contactless cards become widely available, the number of potential applications that smart cards and the associated contactless reader infrastructure system can support on the card will expand over the next few years. We believe that there will be increased focus on, and demand for, contactless smart cards providing an increased level of security and reliability in the areas of financial payment and related connection with mobile payment mode applications. Additional standardization efforts aimed at producing a generic and affordable platform for various contactless applications will further stimulate market growth and decrease time-to-market for new contactless applications such as those pertaining to ticketing and access control.

Contactless smart cards allow a contactless reader to obtain power from the RF signal that it generates, and then to communicate via near field magnetic coupling. This contactless transactional procedure does not require any physical contact between the card and the reader, and they can only effectively operate over very short ranges. Over the last five years, the systems used to develop and deploy contactless smart card applications have become increasingly efficient and capable of supporting a diverse range of product configurations, performance characteristics, and pricing models. Contactless smart cards, proprietary tokens, wristbands, and key fobs will generate more than 1.7 billion transactions. The majority of that total transaction volume will consist of contactless transportation fare payment; use of contactless smart cards and tokens for non-based transportation fare payment will drive about 32% or approximately 548 million transactions.

6.7.1. Emerging Trends

Wallets have evolved and are increasingly being integrated into mobile phones and mobile platforms. More than 13 million users used mobile wallets for retail payments in 2010, a number that is forecasted to rise to 50 million by 2013. Banks, software developers, device manufacturers, payment networks, mobile operators, merchants, and solution providers are all playing critical roles in mobile commerce. The United States has lagged behind Asia and Europe in the adoption of mobile payment technology. While the technology has already cascaded through markets such as Japan and South Korea, whose credit card penetration and traditional payments overhead are only a fraction of what exists in the United States, the diffusion of mobile payment innovation in the United States has been constrained by a lack of merchant adoption. Now, ironically, it is the United States' strong credit card infrastructure that is inhibiting mobile payment competition. Visa, MasterCard, American Express, and Discover all profit handsomely from transaction fees.

To attain the benefits of mobile payments, all the players and drivers need to recognize that some protectionist interests may interfere within their work. The card associations must revise their rulebooks and allow phone vendors to receive the same quality of service offered to merchants, instead of routing the transaction to the card networks before asking the merchants to pay the charges of that routing. Only then can the advantage of mobile phones as the contactless payment interface be realized. The players must recognize that cooperation, and not competition, is the key to bringing mobile payments to market. In this way, everybody wins, and finally includes the consumer who will truly choose his online wallet.

References

Moon, I. T., Shamsuzzaman, M., Mridha, M. M. R., & Rahaman, A. S. M. M. (2022). Towards the advancement of cashless transaction: A security analysis of electronic payment systems. Journal of Computer and Communications, 10(7), 103-129.

Patel, Y., Chovatia, N., & Kaur, H. (2024, February). Securing Payment Transactions: A Comprehensive Review of Smart Cards and Contactless Payments with Cryptographic Methods. In 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 785-790). IEEE.

Mogaji, E., & Nguyen, N. P. (2024). Evaluating the emergence of contactless digital payment technology for transportation. Technological Forecasting and Social Change, 203, 123378.

Shah, G. S. (2025). Bridging the Digital Divide: The Technical Evolution of Omnichannel Payment Systems in Modern Commerce. Journal of Computer Science and Technology Studies, 7(4), 923-932.

Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: a systematic literature review. Future Internet, 15(1), 21.