Contactless payment systems based on RFID Technology

Izabela Lacmanović[1], Biljana Radulović[2], Dejan Lacmanović[2]
[1]Vojvodjanska banka a.d. Novi Sad, branch Zrenjanin, member of NBG Group
Trg Republike bb, 23000 Zrenjanin, Serbia
Phone: (381) 23-562 925 E-mail: izabela.lacmanovic@gmail.com
[2]Technical Faculty "Mihajlo Pupin" – Zrenjanin
Djure Djakovica bb, 23000 Zrenjanin, Serbia
Phone: (381) 23-550 543 Fax (381) 23 550 520 E-mail: {bradulov,dlacman}@tfzr.uns.ac.rs

Abstract - Contactless payment systems represent cashless payments that do not require physical contact between the devices used in consumer payment and POS terminals by the merchant. Radio frequency identification (RFID) devices can be embedded in the most different forms, as the form of cards, key rings, built into a watch, mobile phones. This type of payment supports the three largest payment system cards: Visa (Visa Contactless), MasterCard (MasterCard PayPass) and American Express (ExpressPay). All these products are compliant with international ISO 14443 standard, which provides a unique system for payment globally. Implementation of contactless payment systems are based on same infrastructure that exists for the payment cards with magnetic strips and does not require additional investments by the firm and financial institutions, other than upgrading the existing POS terminals. Technological solutions used for the implementation are solutions based on ISO 14443 standard, Sony FeliCa technology, RFID tokens and NFC (Near Field Communication) systems. This paper describes the advantages of introducing contactless payment system based on RF technology through pilot projects conducted by VISA, MasterCard and American Express Company in order to confirm in practice the applicability of this technology.

I. INTRODUCTION

Definition that describes RFID and smart cards are used interchangeably, resulting in confusion between the differences. Confusion is especially strong between contactless smart cards and RFID. Both contactless smart cards and RFID use radio frequencies for communicating between the card and reader. The applications for which radio frequency (RF) is used can be different for RFID and smartcards.

RFID is mainly meant for applications within the supply chain, for track and trace. Contactless smart cards on the other hand are mainly meant for payments, banking, mass transit, government and ID, and access control.

This paper aims at clearing the confusion between the two technology definitions and presents the way of using contactless cards with the business benefits of these technologies.

II. TECHNOLOGY

Fig. 1 depicts the various applications of contactless smart cards and RFID, along with their level of information security.

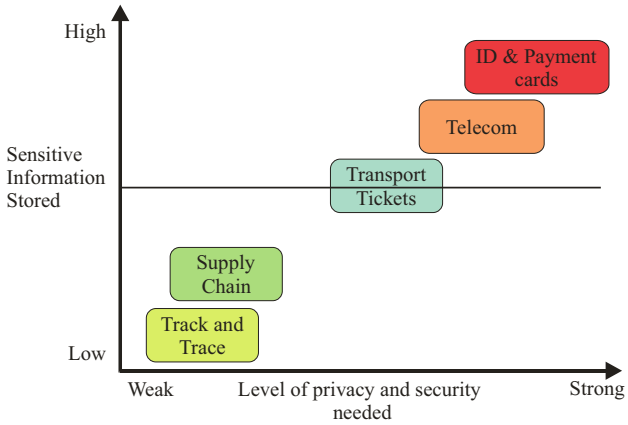

Fig. 1. Level of privacy and information security on various application [1]

RFID and smart cards both can be used in transit payment applications and most of the time they are used together to provide increased convenience to end users. An example of this would be the "Touch n Go" cards used on toll ways. The "Touch n Go" card is a contactless smart card, but this card can be purchased with an additional RFID transponder (where the smart card will be inserted) so that the toll booth reader can read the cards from a greater distance than the 10 cm limit restricted by smart card standards. Without the additional RFID transponder, the contactless smart cards can still be used, which means that the driver need to screen down their windshield to tap the card on the reader, instead of just driving through while the RFID transponder will be detected by the reader above the toll booths at a greater distance [1].

RFID is a wireless automatic identification and data capture (AIDC) technology. It includes tags, Antenna or coil Electronics programmed with unique information, reader and software. The Integrated circuits group comprises of IC designers, antenna and IC manufacturers. These ICs are used in the development of RFID hardware equipments which comprises of tags (that can be active or passive), in addition to readers and printers.

The software and middleware in the equipment is integrated with the back-end systems by the system integrators who also act as the distributors and value added resellers. In addition, several companies provide training and consulting services. Some companies focus on one key aspect while others provide services across the value chain. The Table I lists the various RF technology features.

TABLE I
RF TECHNOLOGY FEATURES

Frequency Range	Low frequency RF	High frequency RF ISO/IEC 15693	High frequency RF ISO/IEC 14443	Ultra High frequency RF
	125/135 KHz	13,56 MHz	13,56 MHz	902 – 928 MHz
Technology name	RFID	RF enabled contactless smart card	RF enabled contactless smart card	RFID
Standard (for communications link)	Proprietary for access control. ISO/IEC 11784 and ISO/IEC 11785	ISO/IEC 15693	ISO/IEC 14443 and ISO/IEC 7816, parts 4 & above for application/security standards	ISO 18000-6 for inventory control tags
Operational Range	Medium: < 20 - 60 cm	Medium: < 70 cm	Short: < 10 cm	Long: 3,5 - 10 m
Data transfer rates	< 10 Kbps	26 Kbps	106 – 848 Kbps	20 – 100 Kbps
Chip types supported	Memory only	Memory, Fixed Logic	Memory, Fixed Logic, Microcontroller, Crypto processors	Memory only
Memory capacity range	Hundreds to low kilobytes	256 bytes and 2K bytes	64 Kbytes and more	Hundreds of bits today
Read/write ability	Read/write	Read/write	Read/write	Read/write
Factory affecting security	Longer range, Fixed logic chip, Limited flexibility in communications protocols	Longer range, Fixed logic chip, Limited flexibility in communications protocols	Short range, Programmable microcontroller, Counterfeiting and tamper resistance features, More Flexibility in communications protocols	Longer range, Fixed logic chip, Limited flexibility in communications protocols
Available form factors	Tags, Plastic card, Key fob, Watch	Tags, Plastic card, Key fob, Watch	Plastic card, Key fob, Watch, Mobile phone	Tags, Plastic card
Applications	Security, Access control, Asset tracking, Animal tracking, Automobile immobilizer	Inventory tracking, Physical access control systems	Secure ID cards and documents (ePassport), Credit and debit card payment, Transit payment, Physical access control systems	Transportation vehicle Inventory tracking, Supply chain

ISO 15693 is making an important impact in the contactless market with its tracking function capability within a contactless application and its convenience through increased proximity distance and hands-free operation. It expands the communication range for vicinity operations to around 1.5 m. In proximity operations, ISO 15693 doubles the communication distance of ISO 14443 [1].

ISO 18000 was developed, originally, for electronic identification applications. There are now many variations within the ISO 8000 standard, from 125 KHz to several GHz, including ISO 15693 for 13.56 MHz.

Contactless Smart Cards are cards that contain an IC (integrated chip) that complies with ISO 14443 (mostly type A) or better known as MiFare. ISO 14443 sets communication standards and transmission protocols between card and reader to create interoperability for contactless smart card products. Read/write range of devices is usually up to 10 cm. (Note: this is generally accepted but it is not stated in the standard). End users these days often require full compatibility in both the readers and in the cards. Cards are intended to communicate with the reader antenna at a frequency of 13.56 MHz. The main communication protocols are supported under the ISO 14443 standard series - Type A (MiFare), Type B and Type C (Sony - FeliCa IC - mostly in Japan). ISO 14443A is the most widely used contactless smart card standard in the world, mainly for transport applications.

Contactless smart cards have been particularly popular in recent years because of its security and multi-application aspect. This means that one card can be utilized across transit, payment and access (combined into one card). Transit (sometimes combined with payment) is currently the most popular application using contactless smart cards. The key applications aside from transit and door access are currently the growth areas such as government ID, payment/banking, logical access control and e-passport (which are technically not a card, but use the same contactless IC chip). Contactless smart cards are generally used for applications like these, where a higher level of security and privacy is necessary to protect the information stored by the card. Some of the key differences between RFID and smart cards are that where RFID can read up to longer

read distances; contactless smart cards have the capability to read up to 10 cm only. RFID can operate at 125/135 KHz, 13.56 MHz, 902-928 MHz.

Contactless smart cards on the other hand operate at a frequency of 13.56 MHz, with higher memory capacity. The higher security capabilities and memory capacity of smart cards renders them suitable for applications such as e-passports, payment cards, and identification. Such applications are also better positioned to absorb the higher cost of smartcards as compared to passive RFID tags. Passive RFID is primarily touted for track and trace applications especially within supply chains. Generally, while RFID is used in applications that identify and track objects, contactless smart cards are used in applications that identify objects/persons as well store financial/personal information [2].

There are certain limitations of the RFID technology, due to which smart cards are considered more secure. Firstly, in case of RFID there are certain privacy issues. Since it is an identification technology and that too contactless, there are chances that a nearby reader can read the tag and hence come to know the details of the products, without the holder's knowledge. Whereas in the case of smart cards the information can be encrypted, so only an authorized reader can access the information.

One of the sources of confusion arising between the two technologies occur because proximity cards (which are RFID cards using 13.56 MHz) and contactless smart cards are both applicable in physical access control. Both cards uses 13.56 MHz and can be used for door access to buildings and restricted areas, but proximity cards can allow a read distance of up to 1.5 meters, while contactless smart cards have a read limit of 10 centimetres [1].

Given that both technologies uses contactless interface, RFIDs and smart cards are expected to compete on security grounds. However, this possibility is unlikely for a long time, because the current market potential for both the technologies in their respective application segments is immense.

III. CONTACTLESS CARD ISSUERS

EMV is an acronym derived from the names of the three companies that developed it: EuroPay, MasterCard and Visa. American Express was joined in February 2009. It was developed to improve security and enable offline payment transactions. The EMV protocol heightens security by using encryption algorithms to authenticate the card's legitimacy.

EMV cards contain an embedded integrated circuit that stores encrypted information about the account and can process the authentication protocols with the payment terminal [3]. EMV transactions can be done either in online mode, where the payment-processing terminal links with a payment-processing centre, or offline, with authentication taking place only between the payment card and the payment terminal. The offline mode is used largely in remote areas by merchants lacking a means of linking their payment systems with payment processors in real time. The issuing bank sometimes requires a cardholder to key in a personal identification number (PIN) to provide a secondary means of identification. Visa Europe does not require the use of a PIN for purchases fewer than €15, though the bank that issues a given Visa EMV card may require one.

The big credit card companies each have their own system – PayPass for MasterCard, payWave for Visa and PayExpress for AmericanExpress.

The introduction of EMV chip technology across Europe brings added security to traditional card transactions and is enabling the payments industry to introduce new, faster and more convenient ways to pay. Contactless payments are the process where payment instructions are securely exchanged between a contactless chip card and acceptance terminal using wireless communication technologies. The same type of payment instructions could also be exchanged between an acceptance terminal and a contactless EMV standard application in a mobile phone or an item such as a key fob. Irrespective of which method is used, contactless payments can be processed securely and cost-effectively in seconds. They are therefore an ideal payment method in situations where merchants need to process a large number of low value transactions, such as in fast food restaurants, convenience stores and transport terminals. They are also ideal for remote or unattended payment situations, such as vending machines, road tolls or parking meters.

Alternative for low cash value transactions is contactless payments. Cash continues to dominate lower value payments although payment cards have successfully displaced cash and cheques in favour of higher value transactions. In the UK, it is estimated that consumers make 27 billion cash transactions a year, worth a total of £250 billion [4]. However, over 80 percent are for purchases of less than £10.00. Retailers and consumers have traditionally resisted using payment cards for low value transactions. Consumers think cards are slower than cash and do not associate them with buying routine day-to-day items. Retailers see the cost of processing a traditional card transaction, often needing online authorization by the card issuer, as unattractive and too costly for low value payments. At the same time, everyone recognizes that cash does present its own problems. As well as being inherently insecure, it is expensive to handle, and errors are commonplace. There is therefore a real and sizeable market for a true cash replacement product that is faster, more convenient and more secure than notes and coins. Visa believes that the combination of the EMV standards and wireless technologies offers just such a solution. EMV is the global payment standard for chip cards – providing banks, vendors and merchants with a single, interoperable set of specifications for chip-enabled payment cards and acceptance devices. Across Europe, more than 4,600 European banks are in the process of issuing a quarter of a billion Visa EMV chip cards and upgrading millions of card acceptance devices [4]. Although Europe is leading the way, the migration is truly international. EMV programs are running worldwide and, in some countries, the number of EMV acceptance terminals is beginning to outnumber traditional magnetic stripe terminals. These EMV specifications give card issuers far greater control over how different transaction types should be processed. In the case of low value payments, for example, card issuers can program certain security parameters onto an individual card, for instance freezing the PIN verification requirement for transactions below a certain limit so that they can be authorized offline. This means that transactions can be completed much more quickly. It also means that these lower risk low value

transactions can be processed more cost-effectively than higher-value transactions. EMV chip technology could potentially address many barriers that have traditionally prevented payment cards from being used for lower value transactions. By going one-step further – and combining EMV standards/concepts with today's wireless technologies – Visa offers entirely viable cash replacement solution. The solution uses a standard Visa Smart Debit and Credit (VSDC) application on a dual interface EMV chip card (a chip that enables both contact and contactless payments). Using the existing ISO 14443 Radio Frequency specification, the card communicates with a Point of Sale terminal connected to a 'plug-in', contactless reader. Faster and more secure than cash, the solution is ideal for busy sectors such as fast food, convenience stores and public transportation – which process large numbers of low value transactions. The solution allows the card issuer to maintain a high degree of control over the way that transactions are processed. For example, the issuer could personalize a card to enable 'wave and pay' offline transactions where each transaction amount is below a threshold of about £10 in the UK (c.€20), and the total of these offline transactions does not exceed for example £50 (c.€70). Once this limit is reached, the card will only operate in contact chip and PIN mode, at which point the issuer can authenticate the cardholder and reset the contactless counters. This means that if a card is lost or stolen or the cardholder exceeds their personal pre-authorized offline limit, the card issuer's financial exposure is kept to an acceptable level. Costs are expected to come down significantly, as contactless technology is rolled out in volume.

Although contactless card payments represent the most immediate opportunity, there are a variety of ways that contactless payments can be processed. A wireless technology called Near Field Communication (NFC) is set to be integrated into mobile devices such as phones, PDAs, cameras and music players. Originally developed by Philips, the technology is endorsed by Sony and Nokia. It operates at 13.56 MHz across distances of up to 20 cm, and is designed to be easy and intuitive to use.

To illustrate the potential, Visa Europe has demonstrated a contactless payment solution using a mobile phone. This project enabled the creation of payment solutions via mobile phones using Visa payWave.

MasterCard's survey suggests that cash transactions will become less frequent in the future. In a survey by MasterCard, 38% of people thought they would use cash less in five years' time, while 16% said they often did not make everyday purchases such as newspapers, sweets or cigarettes because they did not have change or didn't want to pay with a note [5].

Merchant adoption is at the heart of the technology's success, and according to MasterCard, there are now 51 million merchant locations worldwide that accept PayPass payments.

There are concerns about cards being 'hacked' while still in the user's wallet. There is also a concern that contactless payment cards could be potentially much more expensive for retailers to handle than cash. Not really a concern for retailers, but something for consumers to watch out for is the observation that users spend more when they are not limited to coins or cash. In some cases the theft of a card could be worse than having cash stolen. MasterCard admits that a card could be used up to five times without a PIN being requested, giving the would-be fraudster the chance to get away with up to £50 [5].

Contactless payment can be done at any retailer that displays the symbol as shown in Fig. 2.

Fig. 2. International symbol for contactless payments [5]

It's expected that the contactless payment will save time at the checkout. Known as 'wave and pay' or 'tap and go' cashless and contactless cards are a method of paying for everyday items, such as coffee or newspapers, simply by swiping a credit or debit card across a reader. Contactless payments are expected to revolutionize the way low-value purchases are made. This particular method of payment is designed to save time for customers, reduce the risks of handling cash and mean less time dealing with purchases for retailers. It is expected to be used most often in transactions where speed is essential, such as at cinemas, fast-food outlets, petrol stations, supermarkets and theatres.

The future success of contactless depends on broader awareness and a more robust value proposition for the consumer.

IV. SECURITY CAPABILITIES

Despite the ease of payments, card issuers have insisted that the security risks are fairly low. They assure that a retailer will not be able to accidentally take consumer payment twice from same account as the reader can only perform a single transaction at a time.

They also claim that purchases cannot be made without consumer knowledge (for example, if consumer walk past the card reader it will not automatically activate) as the card must be within 10 centimetres of the reader and the retailer must have first entered the amount to approve [6].

Significantly, there are no limits to the number of contactless transactions that consumer can make in a day (payments will be limited only by consumer maximum withdrawal limit). This has its advantages, but it also means that if the card falls into the wrong hands, it would be very easy for someone to make a lot of transactions very easily as they don't need to know owner PIN.

Most credit cards are protected by a 100% fraud protection guarantee which should cover for any loss, theft and misuse.

Contactless smart cards and readers conform to international standards, ISO/IEC 14443 and ISO/IEC 7816, and can implement a variety of industry-standard cryptographic protocols (e.g., AES, 3DES, RSA, ECC). Contactless smart cards that implement security features are referred to as RF-enabled smart cards.

The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes RFID tags lack–i.e., the ability to securely manage, store and provide access to data on the card, perform complex functions (for example, encryption and mutual authentication) and interact intelligently via RF with a contactless reader. Applications using contactless smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following [7]:

-Mutual authentication. For applications requiring secure card access, the contactless smart card-based device can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.

-Strong information security. For applications requiring complete data protection, information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card-based device and the reader can be encrypted to prevent eavesdropping. Hashes and/or digital signatures can be used to ensure data integrity and to authenticate the card and the credentials it contains. Cryptographically strong random number generators can be used to enable dynamic cryptographic keys, preventing replay attacks.

-Strong contactless device security. Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

-Authenticated and authorized information access. The contactless smart card's ability to process information and react to its environment allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.

-Protection against transaction replay. For applications where it is critical that contactless transaction data not be able to be replayed in a fraudulent transaction, contactless smart cards can generate dynamic data every time they are read. Dynamic data generation per read provides logical security and inhibits fraudulent replay of contactless card data that may have been previously read. For example, contactless credit, debit and prepaid payment card data includes a dynamic card verification number (CVC or CVV) or transaction certificate (for an EMV card) that is unique for every transaction. This dynamic data is generated by the contactless card based on a secret key that was stored in its secured memory by the card issuer. This key, along with a random number, transaction counter and a specific algorithm, is used to generate dynamic data every time a contactless payment card is read for a transaction. The same capability exists regardless of the form factor for the contactless smart chip (e.g., card, fob, mobile phone).

-Support for biometric authentication. For human identification systems that require the highest degree of security and privacy, smart cards can be implemented in combination with biometric technology. Biometrics is measurable physical characteristics or personal behavioural traits that can be used to recognize the identity or verify the claimed identity of an individual. Smart cards and biometrics are a natural fit to provide two- or multi-factor authentication. A smart card is the logical secure storage medium for biometric information. During the enrolment process, the biometric template can be stored on the smart card chip for later verification. Only the authorized user with a biometric matching the stored enrolment template receives access and privileges.

-Strong support for information privacy. The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required. The ability to support authenticated and authorized information access and the strong contactless device and data security make contactless smart cards excellent guardians of personal information and individual privacy.

It is important to note that information privacy and security must be designed into an application at the system level by the organization issuing the contactless device, card or document. It is critical that issuing organizations have the appropriate policies in place to support the security and privacy requirements of the application being deployed and then implement the appropriate technology that delivers those features. The ability of contactless smart card technology to support a wide array of security features provides organizations with the flexibility to implement the level of security that is commensurate with the risk expected in the application.

V. THE BUSINESS BENEFITS OF CONTACTLESS SMART CHIP TECHNOLOGY

Governments, corporations, financial service providers, and transit agencies are selecting contactless smart chip technology to implement new, secure identification and payment applications.

RF-enabled technology can deliver a number of benefits to an identity verification application. For example:

-Speed and convenience. RF-enabled technology can improve the speed and convenience of the identity verification process. A user can simply hold an RF-enabled identity credential in close proximity to a reader and have the required identity information quickly communicated to the identity verification system. This can improve throughput vs. processes that require the user to insert or swipe an identity credential.

-Durability and reliability. RF-enabled technology is well suited to identity verification systems that are exposed to the elements and have high usage. RF-enabled smart cards are durable and reliable. RF-enabled smart cards and sealed RF readers prevent damage when identity credentials and readers are exposed to dirt, water, cold, and other harsh environmental conditions.

-Security. RF-enabled smart card technology can improve the security of the identity verification process and credential–providing secure storage and communication of

identity information and making it much more difficult for identity credentials to be forged or modified.

-Privacy. RF-enabled smart card technology implements and enforces the issuer's privacy policies to protect an individual's privacy.

-Contactless financial payment devices. Consumers tap their contactless payment devices on (or wave them at) specially equipped merchant terminals, transmitting payment information wirelessly from the consumer to the merchant. The benefits of contactless payment for the consumer and the merchant have been proven in numerous implementations. Increased convenience for the consumer results in increased sales and faster transaction times for the merchant. Merchants also enjoy lower costs, due to fewer requirements to handle cash, improved operational efficiencies, and lower maintenance costs, resulting from improved reliability of contactless readers. By issuing secure, contactless smart chip-based payment devices, financial service providers are providing consumers with a more convenient payment mechanism and increasing transaction volumes by replacing cash.

-Corporate and government employee identification. Both government agencies and corporate enterprises are increasingly implementing smart card-based employee identification badges. These ID badges typically include both a contactless smart chip for secure physical access to buildings and facilities and a contact smart chip for secure logical access to networks and computers.

-Transit payment. Today, virtually all new transit fare payment systems either in delivery or procurement use contactless smart chip-based cards as the primary ticket medium. Contactless fare payment cards offer increased customer convenience, which helps to generate ridership growth and improve the transit operator's bottom line. Such cards provide an efficient and convenient substitute for cash, increasing security, reducing fraud, and reducing handling costs for transit operators. Contactless fare payment implementations also lower operating costs, due to increased reader reliability and longer card lives.

Credit card companies are claiming the following advantages for contactless credit cards:

-The card is faster to use. To make a purchase, the card owner just waves his card over the RFID reader, waits for the acceptance indicator - and goes on his way. American Express, Visa and MasterCard have all agreed to waive the signature requirement for contactless credit card transactions under $25. Contactless smart card transaction takes 15 seconds, magnetic strip card transaction 25 seconds, cash transaction 34 seconds [8].

-The contactless cards use highly secure data transmission standards. Contactless cards make use of the most secure encryption standards practical with current technology. 128-bit and triple DES encryption makes it nearly impossible for thieves to steal any data.

-The contactless card never transmits a card number. Instead, the RFID chip within the card creates a unique number for the transaction; if a criminal intercepted the number, it would be useless even if successfully decrypted.

The following disadvantages have been noted with contactless credit cards:

-Contactless credit cards are more exposed than regular credit cards.

Privacy advocates are particularly concerned about this technology; it is feared that having this much information available "in the open air" will lead inevitably to problems.

The "Relay attack" causes the reader to identify a remote card, which is not the device that is presented. This fact breaks the hidden assumption that the physical medium is secure and that the identified card must be very close to the reader device [9].

-It is easier to spend. Studies have demonstrated that consumers will be more likely to spend, and will spend more frequently, with contactless credit cards.

VI. CONCLUSION

Financial corporations worldwide are placing a high priority on implementing new technologies that improve the security and convenience of identity verification and payment transactions.

Contactless smart cards are the largest RFID sector by far and the business is booming. Contactless chip technology enables strong security features along with convenience, durability, flexibility and reliability. It provides the features and performance needed to meet the different business requirements that drive a diverse set of applications. There will be rapid growth in sales of next ten years with contactless smart cards, tickets and RFID enabled phones. Consumers prefer the fast transactions and reliability that come with contactless approaches.

REFERENCES

[1] Parul Oswal, Michelle Foong, *RFID Vs Contactless Smart cards – An unending debate*, Frost & Sullivan, Asia Pacific, 2006.

[2] Klaus Finkenzeller, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification", John Wiley & Sons, New York, 2003

[3] Terry Bradford, "Contactless: the next payment wave?" Payments System Research Briefing, Federal Reserve Bank of Kansas City, December 2005.

[4] Visa International Service Association, Multinational financial corporation, http://www.visaeurope.com, 2009

[5] MasterCard Worldwide, Multinational financial corporation, http://www.mastercard.com, 2009

[6] Dan White, "NCR: RFID in retail", S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 381–395, Addison Wesley, 2005

[7] Ari Juels, "RFID Security and Privacy: A Research Survey", RSA Laboratories, September 2005

[8] Thomas J. P. Wiechert, Frédéric Thiesse, Elgar Fleisch, "A quantitative evaluation of NFC based contactless payment systems in retail", Research Paper, 17th European Conference on Information Systems, Verona, 2009

[9] Ziv Kfir and Avishai Wool, Picking virtual pockets using relay attacks on contactless smartcard systems. IEEE CreateNet SecureComm, IEEE, 2005