SMART PAYMENT ASSOCIATION

THE CYBER RESILIENCE ACT (CRA) IN THE LIGHT OF EXISTING PAYMENT CARD CERTIFICATIONS

November 2024

1. INTRODUCTION

Introducing cybersecurity by design and by default principles into digital products, the Cyber Resilience Act (CRA) which was recently approved by the EU Council[1] and has been published in the Official Journal of the European Union[2] marks a clear commitment from the European Union (EU) to protect millions of businesses and consumers in an increasingly connected world across all vertical segments.

The Regulation will enter into force on 10 December 2024, and its main obligations will apply from 11 December 2027.

As the trade body of the cards and mobile payments industry – a vertical sector that, for over the last three decades, has delivered the highest levels of protection for its payment instruments – the Smart Payment Association (SPA) welcomes all initiatives seeking to eliminate security flaws, address fraud and tackle new risks.

The introduction of the CRA has raised concerns among the payments industry stakeholders because of its potential impact on the Payment Smart Cards industry and its consumers[3]. The SPA considers that while the CRA aims to enhance cybersecurity, its implementation may impose substantial costs without corresponding improvements in end-user security. The current payments industry security practices have proved successful in effectively minimizing fraud rates over the past three decades.

The SPA addresses the challenges of a fast-evolving payment ecosystem, promoting innovation, security, and interoperability of retail payment instruments. The SPA works closely with regulators and standardization bodies, offering leadership and expert guidance to help its members and their

[1] (Cyber resilience act: Council adopts new law on security requirements for digital products - Consilium
[2] Regulation - 2024/2847 - EN - EUR-Lex
[3] Cyber Resilience Act (CRA) - SPA's Response to the EC Consultation - January 2023

customers adopt new payment technologies. SPA members, all based in Europe, account for the shipment of more than 80% of Payment Cards worldwide, with 13 billion Payment Cards in circulation globally reported in 2023, including 1.5 billion in Europe[4]. These cards are integral to the functioning of the finance and retail sectors in Europe.

The following sections of this paper explore current security practices, regulatory compliance mechanisms, and the operational realities of Payment Smart Cards. They also assess regulatory alignment and applicability, aiming to substantiate the arguments presented.

2. PROBLEM STATEMENT

1. Regulatory Concerns and Industry Impact: The SPA is worried that new regulations, like the Cyber Resilience Act (CRA), will impose high costs on the EU Payment Smart Cards industry and consumers without improving end-user security. The industry has operated under strict regulations for over 25 years, maintaining low fraud rates through stringent security processes.
2. Risk of Duplication and Complexity: Current international payment industry standards, based on international standards (ISO), already ensure high levels of security at least equivalent to CRA requirements. These practices have successfully reduced fraud rates to 0.031% of the total value of card payments in the EU[5]. Introducing new processes alongside the existing ones could lead to certification duplication, complicate planning, and potentially cause delays in the delivery of new Payment Cards. This redundancy may increase complexity, contradicting the goal of simplifying security measures for the end-users.
3. Technical Constraints of Smart Cards: Payment Smart Cards are passive unpowered devices with no direct or indirect internet connection, only communicating with payment readers using ISO 7816-4 commands to facilitate secure payment transactions only at the time of payment.
4. Security Evaluation Compliance: The security evaluation of Payment Card products already meets CRA requirements through rigorous conformity assessments, site audits, and security testing equivalent to Common Criteria (CC) EAL4+. Surveillance rules and mitigation plans ensure ongoing security and very low fraud rates.
5. Emerging Threats and Continuous Improvement: Security standards are continuously updated to address new threats, including those posed by quantum computers. EMVCo, along with European National Agencies and the EU Payments Industry, monitors emerging threats and updates security certifications and rules accordingly.

[4] Source: Worldwide EMV® Deployment Statistics | EMVCo
[5] ECB and EBA publish joint report on payment fraud

3. SUITABILITY OF CRA FOR PAYMENT SMART CARDS.

The current processes and specifications already address the key requirements outlined in the regulation, rendering additional processes unnecessary and inappropriate. In this context, the CRA should provide a mechanism to confirm compliance with the rules using the existing evidence. Compliance through Module H of the CRA could also be a viable solution.

How does it work currently? Conformity Through Letters of approval (LOA)

How does the industry comply to obtain an LOA, renew an LOA, and manage vulnerabilities?

Security certification today is maintained through a system of Letters Of Approval (LOAs). Industry stakeholders collaborate to manage vulnerabilities, conduct risk analysis, and develop mitigation plans to protect end-users.

A Letter Of Approval (LOA) is an official document issued by EMVCo and the Payment Schemes. It certifies that a Payment Card product complies with the defined specifications and industry standards, assuring that the product meets security, functional, and interoperability requirements.

The approval process consists of three main steps: Registration, Testing, and Approval.

1. Registration: The vendor submits product details in a registration form, including technical specifications. The product then receives a unique identification number.
2. Testing: The card product undergoes rigorous standardized testing by an approved laboratory to ensure it meets security, functional, and interoperability standards. The most complex part of the testing is Security Testing, which includes:
    - Code Review: Identifying potential product vulnerabilities.
    - Vulnerability Analysis: Informing the test plan.
    - Testing: Conducting the tests based on the plan.
    - Reporting: Summarizing the results and findings.
3. Approval: The test reports are reviewed by the payment scheme. If the product passes the tests, the vendor is issued a certificate with a defined validity period, allowing them to produce and sell the product. The EMVCo process is detailed at: Chip & Platform Approval Process | EMVCo

The security evaluation of Payment Card products complies with CRA requirements, specifically in the following areas:

- Technical Documentation: Registration of the product, which includes all relevant data and product details such as production and development sites, hardware characteristics, software version, and security guidance documents.
- Site Audits: Periodic on-site audits of development, production, and delivery infrastructures conducted by third-party recognized security evaluation laboratories.
- Scope of Security Evaluation: Based on clearly identified assets and threats, updated according to the latest advancements. Products must be developed with new security countermeasures to address various attack categories, including physical attacks, side-channel analysis, and fault injection attacks as defined by JHAS: JIL Attack Methods for Smart Cards and Similar Devices (JIL AM).
- Security Testing: Conducted at a level equivalent to Common Criteria (CC) EAL4+. A minimum evaluation workload is established based on input from laboratories and the JHAS subgroup.
- Approved Security Laboratories: Testing is performed by security laboratories accredited by the scheme, meeting specific and clear requirements regarding skills, equipment, and both logical and physical security. Service Providers Archive | EMVCo
- Knowledge of Security Laboratories (Explained in more depth in the next chapter).
    - They are active participants in the JHAS group, sharing the latest advancements in attack paths, methods for evaluating attacks, and contributing to the evolution of the field.
    - These same security laboratories are also accredited to perform CC evaluations - Licensed Laboratories: CC Portal (commoncriteriaportal.org).
- Surveillance Rules: they are in place, with renewal testing required on a predefined timing (mostly more frequent than the 5 years listed in the CRA)
- In case of potential vulnerability identified a process is defined to manage this case with the scheme and the customers
- In case of exploited vulnerability, mitigation plans are put in place, including but not limited to communication to the scheme and to the concerned customer, reinforcing additional checks on the transaction and potentially up to the replacement of the cards having this vulnerability.

According to the ECB and EBA joint report on payment fraud[6] , the current set-up effectively keeps the level of fraud very low, even as the volume of products in the field increases. This indicates that the framework is already meeting the necessary requirements well.

Building on the evolving processes implemented by the schemes in response to advancing security standards (as detailed above), the next section delves into dedicated security measures and their implications.

[6] ECB and EBA publish joint report on payment fraud

4. THE SECURITY IS CONTINUOUSLY IMPROVED

The Payment Card products are designed, manufactured, and used according to proper security rules and certified to significantly reduce the risks of potential attacks related to hardware, software, and operational processes.

To address potential threats to DES and RSA, Advanced Encryption Standard (AES) and Elliptic Curves Cryptography (ECC) have been specified and are ready to be deployed. AES as defined in the new specification, when used in online-only transactions, could also serve as protection against Post Quantum Cryptography (PQC) attacks.

These security rules are defined according to the state of the art and are updated to address new threats, such as the use of quantum computers to perform attacks. This is highlighted as the 19th priority of ENISA in its "Foresight Cybersecurity Threats For 2030 - Update 2024)".

Emerging threats are constantly monitored by EMVCo to update its security certifications and rules for developers and schemes. EMVCo, along with European National Agencies, follows the work, recommendations, and classifications of the JIL Hardware-related Attacks Subgroup (JHAS).

The JHAS is focused on investigating and mitigating hardware-related security threats and is monitored by the JIWG (Joint Interpretations Working Group) of the SOG-IS (Senior Officials Group - Information Systems Security) which oversees information systems security across European countries. The JIWG interprets and provides guidance on security standards, policies, and best practices (for details, see SOG-IS - Details of operation (sogis.eu)) references of the latest JIL attack path methods).

Laboratories conducting security tests are also constantly improving their test methodologies with the knowledge of payment product codes, existing countermeasures, and new test equipment. This challenges hardware manufacturers and payment application developers to continuously enhance their security countermeasures to successfully pass the security certifications.

5. HOW SMART PAYMENT CARDS COMPLY TO THE CRA?

After explaining how security is effectively managed in the Payment Card sector, demonstrating that the industry fully understands the importance of this issue and addresses all components (both the cards and their environment), it is crucial for SPA to ensure that, while complying with this regulation, payment smart cards do not experience any duplication of existing processes. As previously noted, the payment smart cards are relying on specifications build on ISO standards (like ISO 7816-1 to 4, ISO 14443-3:2018 and ISO 14443-4:2018 (ISO - Standards)), which are recognized through the Vienna Agreement by the CEN/CENELEC. Therefore, the specifications used for those products could be considered as partially recognized by the European commission.

Additionally, the laboratories conducting the testing are ISO 17025 certified, demonstrating their competence and compliance in carrying out the required testing for these products.

It is interesting to note that the EMVCo security certification process has been accredited by ANSI National Accreditation Body (ANAB) according to ISO 17065[7].

The European Payment Stakeholder Group (EPSG) outlines in Book 5 of the Volume Book of Requirements (current version v10) how the EU payments industry certifies components of Card Payment systems, and how this certification process could be recognized within the context of SEPA. Additionally, Book 5 details the EPSG's "Labelling Process". Any organization that provides implementation specifications for EU Card Payment systems is eligible for an EPSG Label, provided its implementation specification complies with the functional and security requirements set out in the Volume.

EPSG Volume Book 5 does not mandate Common Criteria (CC) evaluations for Payment Cards and terminals. Instead, it acknowledges the existing certification processes used by the card payments industry as reliable and efficient. Moreover, Book 4 of the EPSG Volume sets out security objectives and requirements for individual components of card payment systems. For example, Book 4 specifies that the security objectives for chip cards must be equivalent to the assurance package defined as EAL4 in the Common Criteria methodology, along with additional security requirements agreed upon by the payments industry.

In conclusion, the EU payments industry operates within a framework based on EU-recognized standards. Since there is currently no EUCC certification process available and mandated for payment smart cards, compliance through Module H and the quality management process should be carefully evaluated.

6. EVALUATING REGULATORY ALIGNMENT AND APPLICABILITY FOR SMART PAYMENT CARDS

Additionally, if we examine the essential requirements outlined in the regulation, most are already addressed by existing processes and specifications. An ISO-certified quality management system should further strengthen compliance with these essential requirements.

Tables 1 and 2 below are illustrating the compliance of the current model with the regulatory requirements. Table 1 outlines the essential requirements, while Table 2 focuses on vulnerability handling requirements.

Table 1: Essential requirements

Requirement	SPA Comment	SPA Proposal
(a) be made available on the market without known exploitable vulnerabilities;	Evaluation and certification practices adopted by the Payment Card Industry ensure that Payment Cards that are marketed and issued to the customer don't feature any known vulnerability that could be exploited by a fraudster.	Already covered by existing process.

[7] https://anabpd.ansi.org/Accreditation/product-certification/AllDirectoryDetails?&prgID=1&OrgId=202616&statusID=4

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	Only a secure by default configuration could be put on the market: the configuration review during the security and functional certification, the one referenced in the LOA. This is the only state allowed in the field. In addition, before putting the product on the field, the personalization has to go through a review in a laboratory (Level 3 certification) to ensure it is compliant with the banking scheme and issuer security rules.	Not applicable
(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	The Payment Cards industry solves the card security issue either: • by the update of parameters through a script command, if sufficient • or by the replacement of all the cards in the field by new ones for which the vulnerability has been fixed. In between, the Payment Card issuers can put in place additional control in their backend systems to push transactions online, to add controls and be able to reject transactions in case of doubt.	Mitigation plan: • Issuers may fix an issue using the Issuer Script processing if linked to the parameters of the payment application • Issuers may block the card temporally in case of problem • Issuer may request to force online only transaction • Issuer may decline a transaction if there is any doubt vs their risk management
(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	Unauthorized access to a card, lost or stolen, is prevented by the use of personal authenticators (PIN or Biometrics). In addition, Payment Cards feature tamper resistant security controls that make economically infeasible to break the card to extract keys and other confidential data that could be exploited for fraud purposes. Finally, when the payment is authorised online, access to the	Already covered by existing process.

	card is only possible upon the verification of the PIN online and the authentication by the card of its issuer using the Secure Messaging standard mechanism.	
(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means	Payment Cards provide tamper proof storage of user and payment account identifiers as well as cryptographic keys for encryption purposes of data in transit. Thus transaction data that could be used for fraud purposes are encrypted by the card (in integrity and data origin) for contact transaction (e.g., online authorization authenticator, transaction certificate). For contactless transactions, confidentiality is also provided. Both asymmetric and symmetric robust state-of-the art cryptography is used by Payment Cards. Moreover, the Payment Card industry is migrating to AES symmetric cryptography and ECC asymmetric cryptography to improve security and still keeping the best user experience; done through specifications.	Already covered by existing specifications
(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions	The essential property of the Payment Card is that it provides a secure environment for data and software (External Commands acting on the Card Operating System, Application Data, Cryptographic Libraries, Cryptographic keys, Configuration and Transaction Log Data, Personal Authentication Data). Security certification is there to ensure the sensitive data stored in memory is not manipulated or modified (restoration/blocking of the card).	Already covered by existing process.

	Moreover the card is only powered when used to pay (typical transaction time of less than 500 msec). If a card is on average used twice/day, it means that only for one second/day the card is powered. Meaning the time could be compromised (if not lost or stolen) represents 1/86400! More powerful means could be to steal the card or modify the terminal in order to get more time to attack. For the first case there is a process to declare stolen cards rapidly before fraudulent use. In the second case the target of the attack is the terminal not the cards. In contactless, there is no personal data accessible through the communication, and data could not be modified without an authentication or the knowledge of the keys.	
(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements ('minimisation of data');	The Payment Card stores securely the references of personal data (PIN code and/or biometrics) used to authenticate the cardholder. These data once personalized never leave the card. In addition, the card only provides the data required by the terminal to switch the transaction messages to the Issuer Bank (the Payment account identifier named the PAN). Moreover, the new generation of contactless card protects the confidentiality of personal data in transit. Data that could be exchanged are limited and predefined to what is listed in the specifications.	Already covered by existing specifications
(h) protect the availability of	The Payment Card features offline functionalities, meaning that even	Already covered by existing specifications

essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	in case of an incident in the card payment system or a Denial-of-Service attack, the Payment Card may continue to execute transactions offline. It's noted that Denial-of-Service Attacks don't have any detrimental impact on the security of the Payment Card itself.	
(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	The card is exclusively connected to the network through the payment terminal or an ATM (Cash Dispenser) at the time of a transaction. Yet this network is dedicated exclusively to process card payment transactions. Because the Payment Card is not accessible to store **any new or changed functionality and by this unable to store any malware** malware it cannot infect other devices used in the processing of the payment. In addition, upon card presentation, the terminal proceeds to an immediate card authentication. Fake cards would require the compromise of a legitimate card to steal the card unique cryptographic keys and then to personalize them in another card made or stolen by the attacker. Moreover, Payment Cards don't transmit data susceptible to redirect any component of the processing chain to a fake server. The only routing information provided by the card is the PAN. Yet this PAN is authenticated through a card certificate signed by the Bank, that must be validated before being used by the terminal. A fake certificate would require for the attacker to be able to break the	Not applicable

	RSA algorithm. This has not been observed, nor documented so far.	
(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	There are four levels of countermeasures implemented in the Payment Card: • Security features of the Card Body itself was intended to prevent any trial to produce a fake card indistinguishable from a legitimate one. • Then three other security components to protect data and software in the card microcontroller are designed to minimize the risk of physical (access to memory sensitive data using e.g., a microprobe) or logical attacks (e.g. assessment of a cryptographic key analysing data card responses to challenges chosen by the fraudster or by fault injection to perturb the code execution): 1. Chip Hardware 2. Operating System 3. Application The countermeasures present in those components are evaluated during security evaluation at a level of CC EAL5+ for Chip Hardware and an equivalent level of CC EAL4+ for the two others. The fact that the Payment Cards are not general small computing devices but can only be used to execute a reduced number of commands designed and programmed to initiate and confirm a payment reduces dramatically the external surface of attack. In addition, the Payment Cards have the possibility to	Already covered by the current process and evaluation

	decline the transaction if anything is incorrect. Notice that all SPA members participate and apply the recommendations of the JHAS to identify and fix new vulnerabilities created by more sophisticated attackers.	
(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	Because Payment Cards are not powered at rest, they are by definition invulnerable against any compromise, attack or unintended disfunction of the payment system to whom they're indirectly connected by the terminal during 1/86400 of the time (on average). If a terminal is compromised, it can eventually exploit the Payment Card data for fraud purposes (for instance unduly capturing and storing the PIN codes). But this information is not sufficient to make a fake twin card.	Already covered by the process
(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;	The Payment Card operating system may record some card activity-related data (transaction logs) as evidence to solve exclusively disputed transactions. However, the card operating system is designed in a way that the user even with the complicity of another party cannot modify the log files. Opt-out mechanisms doesn't apply to Payment Cards which are non-connected devices and cannot receive nor display advertising information.	Not applicable
(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such	Requirement not applicable to Payment Cards. The Payment Card generates transaction data that are to be temporary stored by the Issuer Bank to produce the card expenses	Not applicable

data can be transferred to other products or systems, ensure this is done in a secure manner.	report that Banks regularly send to their customers. But the Payment Card is not a networked product. It cannot be used to connect to the Issuer Bank and generate any request of the kind. Removing on a permanent basis is equivalent to destroy the chip embedded in the Payment Card.	

Table 2: Vulnerability Handling requirements

Requirement	SPA Comment	SPA Proposal
(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products	Payment Cards are going through security evaluation processes that covers the full scope of the product and ensure that no exploitable vulnerabilities are present on the product when delivered to customers. During those evaluations a full code review is done to identify the potential vulnerabilities to test them. So the identification and description of potential vulnerabilities are done, listing also why the exploitation is not possible.	Already covered by existing process.
(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	When a vulnerability is identified and the associated risks evaluated, communication to the customers/schemes is done to manage in coordination the remediation plan. As stated, to answer to essential requirement (c): The Payment Cards industry solves the card security issue either: • by the update of parameters through a script command, if sufficient • or by the replacement of all the cards in the field by new ones for which the vulnerability has been fixed.	Already covered by existing process.

	In between, the Payment Card issuers can put in place additional control in their backend systems to push transactions online, to add controls and be able to reject transactions in case of doubt.	
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	Payment schemes are defining the rules of survey of the security of their products during the issuance period. Security testing is requested after a fix period of time (less than 5 years) but could also be requested at any time during this period by the scheme or also rely on the evaluation of the subpart (chip, Operating System). The lifespan of the product on the field is also limited by the rules of renewal or validity of the testing.	Already covered by existing process.
(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	In the context of payment smart cards, as no direct update is possible, the security risks of publication outweigh the security benefits. The mitigation plan is done with the banks/schemes concerned by the vulnerability. Up to the banks to communicate in detail or not to their end user about the reason of the additional control put in place on the payment, or the anticipated change of payment smart card. As a vendor we give all the necessary support to our customer.	Not applicable
(5) put in place and enforce a policy on	This is done on a case by case basis, potentially enforced by the	Already defined in the process

coordinated vulnerability disclosure;	contracts. But this vulnerability disclosure is limited to the persons that needs to know in bank and scheme to avoid any counter-productive effect before the mitigation plan is defined and run	
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	Several means are available for the sharing of information about a potential vulnerability, from whoever this sharing comes from: • for external: a Computer Emergency Response Team (CERT) per vendor with an identified address, • for laboratories: the contact details of the person in charge of the certification • for scheme: the contact details of the person in charge of interfacing with the scheme • for banks/customer: the salespeople they are in contact with All those entities revert internally to the person in charge of the product to perform the risk analysis.	Already in place
(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner	Payment smart cards are stand-alone, not connected products. The update of the product (for example by loading a corrective patch) could not be done without a request to the end user and its active participation to get the update loaded. In addition, the current infrastructure in the banking area is not defined to address such update on non-connected device.	Not applicable
(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in	It is part of our information mitigation plan, as already mentioned	Already part of the process

relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken		

7. CONCLUSION

In conclusion, the existing industry standards, relying on international standards (ISO), European standard (EPSG) and rigorous security practices continuously improved have maintained a robust defence against fraud, with fraud rates as low as 0.031% of total card payments in the EU.

The implementation of additional regulatory processes alongside existing ones will introduce redundancy and complexity, which could hinder operational efficiency without proportionate gains in the security and protection of the end-users.

Furthermore, the security evaluation framework for Payment Card products already aligns with CRA requirements through comprehensive conformity assessments, site audits, and security testing equivalent to CC EAL4+. Continuous surveillance and mitigation strategies ensure sustained security against emerging threats.

Given these considerations, the Smart Payment Association (SPA) advocates for the recognition of current payment schemes or conformity to the CRA based on Module H, along with a self-assessment that consolidates all relevant information and statements derived from the existing certification process.

The SPA remains committed to advancing security measures that protect both consumers and industry interests, ensuring that payment smart cards continue to provide secure and reliable payment solutions in compliance with established EU and international standards.