SMART PAYMENT ASSOCIATION

EBA GUIDELINES ON OUTSOURCING AND PCI CPP

An SPA Analysis

October 2021

1. INTRODUCTION

In February 2019, the European Banking Authority (EBA) published the revised EBA Guidelines on outsourcing arrangements. The goal of the document is to provide financial institutions recommendations and guidance to properly manage the risk of outsourcing services and activities to third parties.

The document clearly targets IT outsourcing activities in the context of a growing digitalisation of financial services and an increased use of cloud-based infrastructures and services.

Nevertheless, while the EBA Guidelines clearly exclude industrial activities such as the production of payment cards, the broad definition of an outsourced arrangement[1], has led some financial institutions to consider payment card personalization as an outsourced service falling in the scope of the EBA Guidelines.

Indeed a few banks in Europe use their own facilities, equipment and personnel to personalise the payment cards that they issue.

The Smart Payment Association (SPA) was surprised of this interpretation of the EBA Guidelines because card personalization is more of an industrial activity. Many banks actually procure readily personalised cards which makes the separation of the personalization service from card production difficult. And, most importantly, the activity of card personalization is already subject to very stringent security requirements defined in the Payment Card Industry Card Production and Provisioning (PCI CPP) standard.

The purpose of this SPA paper is to explain what the PCI CPP standard is and how the evaluation and audits performed to obtain the PCI CPP certification may directly be used by financial institutions to comply with the EBA Guidelines. SPA is confident that this proposed approach will help all parties in scope of the EBA Guidelines to avoid unnecessary cost, time and efforts by reusing recognized and neutral 3rd party audit results while still complying with the Guidelines.

[1] Per the EBA Guidelines, 'outsourcing' means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.

2. PCI CPP – CARD PRODUCTION & PROVISIONING STANDARD: SCOPE & MAIN OBLIGATIONS

The Payment Card Industry Security Standards Council (PCI SCC) is a global organization which publishes, maintains and promotes payment card industry standards for the safety of cardholder data across the globe. PCI SSC security standards cover all aspects of producing, issuing, accepting payment cards and processing payment card transactions. They apply to merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

PCI SSC was founded in 2006 by American Express (Amex), Discover, JCB International, Mastercard and Visa. They share equally in ownership, governance, and execution of the Council's work.

Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. Such standards help to ensure trustworthy payment card transactions for the hundreds of millions of people worldwide that use their cards every day.

One of these PCI security standards is “PCI Card Production and Provisioning” (PCI CPP). This standard consists of both physical and logical security requirements that address card production and personalization activities including card body manufacturing, chip embedding, card and chip personalization, fulfilment, PIN printing and mailing, and electronic PIN distribution.

Provisioning is the process of adding cardholder account information to a device, typically a mobile phone or wearable, via an over-the-air or over-the-internet communication channel, to enable that device for payment.

All vendors who handle payment cards and/or personalization or provisioning data for such cards in the context of a Visa, Mastercard, Amex, JCB, Discover etc. product offering must be PCI CPP certified.

Only companies that meet certain financial requirements may be approved by card organizations as a suitable manufacturer and personalizer of payment cards. Appropriate evidence must be provided during the registration process.

2.1. Structure of PCI CPP

2.1.1. Logical Controls

The PCI CPP standard contains a set of sensitive controls applicable to the IT environment, including servers, computers and each electronic device inside the HSA (High Security Area) perimeter. Its requirements are more restrictive and specifically related to the personalization process than those of PCI DSS (Payment Card Industry Data Security Standard) which has a different scope.

There are a total of 453 requirements which are described in the following chapters:

- Roles and responsibilities (11 requirements)
- Security Policy and Procedures (14 requirements)
- Data Security (42 requirements)
- Network Security (120 requirements)
- System Security (68 requirements)
- User Management and System Access Control (42 requirements)
- Key Management: Secret Data (118 requirements)
- Key Management: Confidential Data (20 requirements)
- PIN Distribution via Electronic Methods (18 requirements)

Some examples:

Staff is not allowed to take or use any private devices into the HSA (mobile phone, smartwatches, tablets, USB storage devices etc.). Production staff cannot be alone in the HSA. There must be a minimum of two individuals present at all times.

For the card personalization network different requirements are in place which ensure a secure and confidential handling of personalization data. Several firewalls must protect the specific segment of the physical isolated network.

There must be no communication with external and/or public networks from inside the HSA. Only the transfer of personalization data is able to reach the HSA IT systems and/or networks.

The appropriate controls require that only "pulled" information can get into the De-Militarized Zone (DMZ). All documents that enter the DMZ, containing sensitive information or not, should have a legitimized justification being in the DMZ.

A card personalization vendor has to patch and update any IT system / device as soon as the relevant supplier provided an update for such system and/or application.

Encryption controls are a core component of the logical security requirements of PCI CPP. All encryption activities must be executed by a FIPS 140-2 Level 3 certified Hardware Security Module (HSM) to encrypt and protect personalization data accordingly.

2.1.2. Physical Controls

The HSA is the physical perimeter that characterizes the card production or personalization environment. Everything outside of the HSA is “external”. PCI CPP requires a particular kind of security technique and the implementation of an appropriate security concept.

There are a total of 483 requirements which are described in the following chapters:

- Personnel (83 requirements)
- Premises (229 requirements)
- Production procedures and Audit trails (90 requirements)
- Packaging and Delivery Requirements (70 requirements)
- PIN Printing and Packaging of Non-Personalized Prepaid Cards (11 requirements)

Some examples:

HSA rooms and offices must be secured and not easily accessible (e.g. access to HSA only by using man traps for person by person access). Furthermore, server rooms must always be accessible only under dual access control under full CCTV coverage. There should be at any time a minimum of two individuals present in the HSA. Otherwise an electronic and acoustic alarm will be activated to inform the guards in the security control room.

All the HSA rooms and perimeters must be CCTV covered. There should be no blind spots. The perimeter must be sufficiently able to resist attacks and have alerts in the event of attempted break-ins.

For a secure storage of cards, the HSA should provide a dedicated vault room which has stronger walls and higher security controls.

Each production site has a staffed security control room when production is performed. The guards are checking the Identification of each person who want to visit the production site. The HSA can only be accessed by visitors when an employee of the production site is escorting him. The guards have to ensure that the related PCI CPP requirements are fully followed and documented.

2.2. Organization

PCI CPP requires a corresponding security organization with specific roles assigned. In this context a CISO and an appropriate Security Manager must be designated which have the responsibility for the security issues and the PCI CPP certification process. Dedicated security staff is needed to ensure a strict segregation of duties between operations and security. Only visitors approved by the Production Manager are allowed to access the HSA.

2.3. Documentation

Full documentation is mandatory and shown to the auditors on demand. A corresponding documentation (e.g. Policies, Standards, Procedures) must be in place for every PCI CPP requirement.

To be PCI CPP compliant the vendor needs to have a corresponding documentation existing for all processes which are operated at the vendor site. That can add up to several hundred pages. During the audit all these documents will be reviewed by the auditor in detail to check if they are suitable and cover the related security requirement.

2.4. Audit

A vendor has to undergo an annual certification audit when all components and controls are in place. An authorised auditor reviews the implementation of controls in the environment, ensuring that the organization meets the logical and physical controls in detail.

The annual audit takes multiple days and evaluates all requirements described in the PCI CPP standard. In addition to interviews with the relevant employees, the auditors check the IT systems, user management, security technology etc. in detail (settings, patch level, user access and role concept etc.). Furthermore, some processes are checked by executing a simulation to see whether all process steps are carried out properly and in accordance with the written procedure (e.g. electronic key management).

Deviations from the standard identified in the audit are summarized in an audit report. The vendor must report suitable measures / solutions to the auditor within 30 days and only receives its certification from the Vendor Program Administrator (VPA) when all non-compliances have been resolved.

All auditors are accredited by PCI SSC.

2.5. Summary

The PCI CPP certification is a complex and time-consuming process. A certified vendor must ensure compliance with the PCI CPP requirements and has to demonstrate this by the corresponding documentation within the annual audits. Deviations can be expensive if, for example, a non-compliant equipment such as HSMs or firewalls have been purchased. In the case of serious deviations, a decertification by Visa, Mastercard, Amex, JCB, Discover etc. could be possible.

The PCI CPP standard is targeted exactly to the needs and processes of a high secure and privacy protecting card production and personalization facility. While other security standards only check the basic compliance with IT security-relevant requirements, the PCI CPP standard provides a detailed set of rules which takes into account all possible risks of processing payment cards and ensures traceability for each individual card. No other security standard covers card and cardholder data handling in such a thorough way.

3. HOW DOES PCI CPP HELP COMPLY WITH THE EBA GUIDELINES

This chapter provides a comparative analysis of the EBA Guidelines on outsourcing arrangements with the PCI CPP standards, with a focus on clauses 87, 91, 93, 94 and 96 of the EBA Guidelines

The SPA has focused its analysis on the five clauses listed above as they are the ones for which the PCI CPP standard already provides a detailed set of rules for card personalization services.

3.1. Clause 87

[Extract of Clause 87 of the EBA Guidelines]: "With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:

a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights');"

Card personalizers will cooperate to facilitate issuer audits at locations where services are rendered. Card personalizers and issuers will mutually agree upon the audit plan respecting Clause 96. The issuer may choose to leverage the results of the audit performed by the PCI auditors. An attestation of compliance may be shared with the issuer. The scope of the PCI audit is comprehensive and targeted to cover all pertinent areas and therefore is sufficient to comply with this clause 87. The audit covers annually, all physical sites and computer systems where the services are provided.

[Extract of Clause 96 of the EBA Guidelines]: "When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.

b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements."

Card personalizers will cooperate to facilitate issuer audits at locations where services are rendered. Access to inspection to be agreed upon with card personalizer as part of the audit plan in order to respect Clause 96. Card personalizer systems are highly specialized and serve multiple clients. Issuers are recommended to leverage the PCI audits as the auditors are highly trained and represent the payment brands (Visa, Mastercard, Amex, …). The PCI auditors audit against the PCI CPP standards to ensure all card personalizers adhere to the most stringent controls. SPA has

reviewed the EBA Guidelines and the PCI CPP standard. It is of the opinion of SPA that the PCI CPP standards will satisfy the EBA Guidelines.

3.2. Clause 91

[Extract of Clause 91 of the EBA Guidelines]: "Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use:

a. pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;"

SPA recommends to leverage the PCI CPP audits. These are independent certification audits recognized and managed by the payment schemes (Visa, Mastercard, Amex, JCB, …). This is a mandatory annual audit overseen by the payment brands.

"b. third-party certifications and third-party or internal audit reports, made available by the service provider."

PCI CPP proof of certification and attestation of compliance may be shared at the request of the card issuer to assist in the compliance with the EBA Guidelines.

The scope of the PCI CPP audit is comprehensive and targeted to cover all pertinent areas and therefore is sufficient to comply with this Clause 91.

3.3. Clause 93

[Extract of Clause 93 of the EBA Guidelines]: "Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:

a. are satisfied with the audit plan for the outsourced function;"

PCI CPP audit plans cover the entire payment service scope dependent on the product. The audit reviews physical security, personnel security, data security, network security, operational security, access and identity management, and cryptographic key management as examples of primary control areas. The PCI CPP audit plan will satisfy the EBA Guidelines.

"b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements;"

The PCI CPP standards are under continual governance by the PCI Council. The standards are reviewed and updated on a consistent basis with feedback from the card issuers, payment brands, vendors, and interested parties.

"c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;"

As noted above, the PCI CPP standards are continuously reviewed for effectiveness and applicability. Audits occur on an annual basis. The latest version is v2.0 Jan 2017. A new version v3.0 is currently under review. The PCI CPP standards are the de facto industry best practices for card personalizer industrial activities. All card personalizers must abide by the PCI CPP standards.

"d. ensure that key systems and controls are covered in future versions of the certification or audit report;"

As the PCI CPP certification has been specifically made for card personalizer Industrial activities, it will always cover key systems and controls. As the card personalizer activities evolve, so will the standard to ensure evolution is secure. Audits occur annually, therefore any new additions to the industrial activity, will be reviewed by the auditor. Card personalizers must make any changes or improvements while respecting the PCI CPP standard.

"e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);"

Audit companies are independent of the card personalizer and the payment brands. PCI SSC vet the audit companies and have strict requirements to ensure audit delivery is optimum. Audits are reviewed for quality by the payment brands. Visa in particular maintains a requirement where the same audit company may not audit a facility more than 2 times in a 3-year period. This ensures impartiality and audit controls are reviewed consistently across card personalizers.

"f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;"

PCI CPP audits are rigorous and thorough. Certification is required in order to provide card personalizer industrial services. Without certification, a vendor may not handle payment brand materials or issuer data. PCI CPP tests physical and logical security controls on card personalizer premises reviewing operational effectiveness of controls identified within the standard. The payment brands govern the certification and may at their discretion, revoke certification at any time, where there are legitimate grounds (e.g. significant compliance issues, poor financial situation, non-payment of VPA fees).

"g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective;"

The PCI CPP audit is very comprehensive, and the PCI CPP auditors are empowered by the payment brands to review controls as necessary to validate compliance. Card personalizers fully cooperate to ensure a complete audit annually.

"h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions."

SPA recommends card issuers leverage the PCI CPP audit to meet the EBA Guidelines. SPA does not object to card issuers reserving the right to perform their own individual audits.

3.4. Clause 94

[Extract of Clause 94 of the EBA Guidelines]: "In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures."

The PCI CPP audit reviews penetration tests performed by the card personalizer. These tests consist of external Internet facing systems and internal segregated production systems. Card personalizers are required to obtain periodic PCI ASV (Approved Scanning Vendor) certificates for all external systems. Due to the highly complex and multi-client card personalizer environments, SPA recommends the card issuer to leverage the PCI CPP certification to meet the requirements of Clause 94.

3.5. Clause 96

[Extract of Clause 96 of the EBA Guidelines]: "When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated."

Card personalizer environments are highly specialized and multi-client. The PCI CPP certification has been leveraged by many financial institutions to assist in their own due diligence programs. The PCI CPP standard addresses all aspects of card personalizer industrial activities as its core purpose. PCI CPP auditors are highly qualified and familiar with card personalizer industrial activities ensuring audits are performed with confidence and quality.

4. WHAT IS NOT IN THE SCOPE OF PCI CPP BUT IN THE SCOPE OF THE EBA GUIDELINES (BCP/DRP, SLA, ETC.)

Risk assessment and business continuity are aspects that are prominent within the EBA Guidelines directed to the institutions. The EBA Guidelines mandate that institutions assess risks of outsourcing functions they deem falling under the definition of critical or important functions, monitor service provider's performance, and establish a business continuity plan for these functions that can be effectively implemented.

4.1. Risk Assessment Approach and Performance Monitoring

[Extract of Clause 11 of the EBA Guidelines]: "Institutions and payment institutions should be able to effectively control and challenge the quality and performance of outsourced functions and be able to carry out their own risk assessment and ongoing monitoring. It is not sufficient for institutions and payment institutions to undertake only formal assessments of whether or not outsourced functions meet regulatory requirements."

The EBA Guidelines highlight in Clause 11 that it is not sufficient for institutions and payment institutions to undertake only formal assessments of whether or not outsourced functions meet regulatory requirements. The EBA Guidelines add in Clause 48 that the institutions should monitor and manage their risk on an ongoing basis, i.e. risk assessments are not a one-off requirement but are part of the continuous management of institutions' risks.

SPA members individually apply for industry-widely recognized certifications for their respective sites that institutions can use as assisting evidence for compliance with the EBA Guidelines. They cover a large scope of risks, possibly including yet not limited to the management of non-quality through ISO 9000 certification, environmental risks with ISO 14000, occupational health and safety with OHSAS 18001 or the management of IT systems security with ISO 27001, as well as applicable local regulatory certifications depending on site location. They all enforce thorough assessment of risks within respective area and intense monitoring through internal and independent external audits of compliance making them the foundation of SPA Members' operational strategy.

[Extract of Clause 49 of the EBA Guidelines]: "Business continuity plans should take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. […]"

Mastercard Card Quality Management (CQM) is a certification strongly recommended by Mastercard for all personalizers[2]. It ensures that card process capability is stabilized within acceptable process windows over time (within controlled min/max variance) and at all steps of the manufacturing process for each site. The program is based on CQM requirements self-assessment made by service providers to institutions. These assessments are reviewed and checked during on-site audits by independent auditors. Audit frequency is adaptive and a function of site maturity.

Institutions can use CQM certifications as assisting evidence for compliance with the EBA Guidelines.

4.2. Establish a Business Continuity Plan

[Extract of Clause 112 of the EBA Guidelines]: "Further to the information recorded within the register, as referred to in Section 11, competent authorities may ask institutions and payment institutions for additional information, in particular for critical or important outsourcing arrangements, such as: […]

b. whether the service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution or payment institution; […]"

In line with the EBA Guidelines, SPA has been promoting business continuity management principles and best practices for the card payments industry to recover from catastrophic or significant events with the objective to resume business as usual. In its white paper *Business Continuity Management in the Payment Card Industry*[3], published already in December 2011, SPA provides an understanding of the value proposition associated with business continuity plan, and establishes a set of guiding principles and best practices for developing and managing business continuity programs.

In line with the EBA Guidelines, SPA advocates proportionality for business continuity management. Independently of an incident happening, a business continuity plan has indeed an attached cost for initial set-up, scheduled maintenances, regular testing so that it can be effectively implemented. Its cost of implementation must therefore be proportionate to the impacts estimated by the institution. As an illustration and in line with EBA Guidelines refraining from providing an exact time frame for recovery, SPA agree that this greatly depends on the impact of a potential disruption and the complexity of the outsourcing arrangement, thus tailored to the agreement between the institution and the service provider.

[2] Mastercard CQM certification is mandated for all card vendors and is strongly recommended for card personalizers.
[3] White paper: https://smartpaymentassociation.com/index.php/publications-smart-payment-association/position-papers-smart-payment-association/entry/business-continuity-management-in-the-payment-card-industry-a-white-paper-by-spa-december-2011
Video: https://smartpaymentassociation.com/index.php/publications-smart-payment-association/videos-smart-payment-association/entry/business-continuity-management-in-the-payment-card-industry

5. CONCLUSIONS AND RECOMMENDATIONS

The PCI CPP standard establishes stringent physical and logical controls for card personalization activities. The compliance of card personalizers with PCI CPP physical and logical security requirements is assessed at least annually, according to strict compliance programs, associated with the relevant requirements, as defined by the individual payment brands.

The comparative analysis done in this paper between the EBA Guidelines and the PCI CPP standard shows that card personalizer's compliance with PCI CPP fulfils all the security-related requirements of the EBA Guidelines.

The PCI CPP certification proof and attestation of compliance may be shared with issuers upon request, as assisting evidence for compliance with the EBA Guidelines.

Card personalizers will naturally cooperate with issuers for the performance of their audits at relevant business premises. However, taking into consideration the time and effort issuers could put in such audits and the fact that card personalizer systems are serving multiple clients, SPA recommends that card issuers take advantage of the PCI CPP audits and certification to ensure security compliance with the EBA Guidelines on outsourcing arrangements.

6. REFERENCES

6.1. EBA Guidelines on outsourcing arrangements

Guidelines on outsourcing arrangements | European Banking Authority (europa.eu)

6.2. PCI Card Production and Personalization (CPP) standard

https://www.pcisecuritystandards.org/

Set filter to "Card Production" in "Document Library" menu bar of the PCI web site to view and download the PCI CPP physical and logical security requirements version 2.0 from January 2017 or follow the two links below:

PCI Card Production_Physical Security Requirements v2.pdf (pcisecuritystandards.org)

PCI Card Production_Logical Security Requirements v2.pdf (pcisecuritystandards.org)

Comment: PCI CPP version 3 is currently under revision. SPA will revisit its recommendations when the new version is published by PCI.

6.3. Mastercard Card Quality Management (CQM) requirements

Mastercard CQM certification is mandated for all card vendors and is strongly recommended for card personalizers.

Card Quality Management - Smart Consulting (smart-consulting.com)

6.4. SPA Business Continuity Paper and Video

White paper: https://smartpaymentassociation.com/index.php/publications-smart-payment-association/position-papers-smart-payment-association/entry/business-continuity-management-in-the-payment-card-industry-a-white-paper-by-spa-december-2011

Video: https://smartpaymentassociation.com/index.php/publications-smart-payment-association/videos-smart-payment-association/entry/business-continuity-management-in-the-payment-card-industry

7. ABOUT THE SPA

The Smart Payment Association (SPA) is the trade body of the cards and mobile payments industry. SPA addresses the challenges of a fast-evolving payment ecosystem, promoting innovation, security and interoperability of payment instruments. SPA works closely with regulators and standardization bodies, offering leadership and expert guidance to help its members and their customers adopt new payment technologies of today and tomorrow.

www.smartpaymentassociation.com