PolishAPI

Recommendations regarding the security area for entities using the standard

Document developed by the PolishAPI Project Group

4 September 2019
Version 1.0

1 Table of contents

2 Introduction 4
2.1 Context 4
2.2 Document structure 4
2.3 Document application 5
2.4 Assumptions 5
3 Definitions 6
3.1 Terms used to prioritize requirements: 7
4 Area 1: Organizational and procedural requirements 8
4.1 Information security policy 8
4.2 Organization of information security 8
4.3 Management of services provided by external suppliers 9
4.4 Asset management (from an information security perspective) 9
4.5 Physical and environmental security 10
4.6 Safe operation and change management 10
4.7 Access control 11
4.8 Ensuring security throughout the entire life cycle of the information systems 12
4.9 Handling of operational events and security incidents, including those of ICT nature 13
4.10 Business continuity management 14
4.11 Policies for safe use by employees 14
4.12 Security of human resources 15
4.13 Risk management and security tests 15
4.14 Prevention of money laundering 16
4.15 Informing Users about safety principles 16
5 Area 2: Requirements for the system infrastructure 18
5.1 Network configuration 18
5.2 Configuration of servers, devices and software 18
5.3 Logical access control 20
5.4 Processing of the Protected Data on the server side 20
5.5 Management of cryptographic keys 20
5.6 Ensuring high availability of services 21
6 Area 3: Requirements for the PolishAPI interface 22
6.1 Authentication and authorization under the PolishAPI 22
6.2 Cryptographic data security mechanisms 23
6.3 Data validation 24
6.4 Accountability of events 25

7 Area 4: Prevention of abuse and attacks..... 25
7.1 Event monitoring..... 25
7.2 Fraud Detection Principles 26
7.3 Protection of the system against access denied attacks..... 26

2 Introduction

2.1 Context

The new Directive on payment services in the internal market (PSD2) introduces a legal framework for offering new payment services - account information access services, payment initiation services and services confirming the availability on the payer's payment account of the amount necessary to perform a payment transaction. Both banks and cooperative savings and credit unions or branches of credit institutions, as well as the so-called third party providers (TPP) will be able to provide new services based on PSD2 regulations by gaining access to payment accounts maintained on-line by authorized entities (Account Servicing Payment Service Providers, ASPSP).

The provision of new payment services and providing their providers with access to payment accounts, however, requires the use of the highest security measures that will allow to the maximum extent possible the risk of disclosure of confidential data to unauthorized persons or other security incidents to be limited.

To this end, a common, universal API standard has been developed (for which the name PolishAPI is used) for all entities involved in communication as part of the provision of new services, i.e. TPPs and ASPSPs. Pursuant to the provisions of chapter 6 of the PolishAPI (Information Security) standard documentation, the PolishAPI Project Group has been required to develop an additional detailed document, including security issues of implementation, operations and maintenance of PolishAPI-based systems. This document fulfils this obligation.

The document includes the following regulations and guidelines:

1) Directive 2007/64/EC of the European Parliament and of the Council 2015/2366 of 25 November 2015 on payment services in the internal market (amended Directive on payment services, PSD2),
2) Delegated Regulation with regard to regulatory technical standards regarding strong customer authentication and common and secure open communication regulatory technical standards (RTS), published in the Official Journal of the European Union on 13 March 2018,
3) Guidelines on the requirements for reporting fraud under Article 96 Section 6 of the Second Payment Services Directive (PSD2),
4) Guidelines for reporting serious incidents in accordance with Directive (EU) 2015/2366 (PSD2),
5) Guidelines on security measures regarding operational risks and risks for the security of payment services under Directive (EU) 2015/2366 (PSD2),
6) Opinion of the European Banking Supervision on the use of eIDAS certificates as part of RTS for SCA and CSC.

2.2 Document structure

The document consists of four parts concerning the following areas:

1) Area 1: Organizational and procedural requirements
2) Area 2: Requirements for the system infrastructure
3) Area 3: Requirements for the PolishAPI interface
4) Area 4: Prevention of abuse and attacks.

2.3 Document application

All the requirements set out in this document apply only to elements related to the functionality of the PolishAPI interface unless the detailed provisions hereof provide otherwise.

This document applies to payment service providers using the PolishAPI standard, i.e. both TPPs and ASPSPs (together as “PSPs").

2.4 Assumptions

1) PSPs may, at their own discretion and following their risk assessment and on their own responsibility, decide to comply with the recommendations and requirements presented herein, in whole or in part.
2) This document is also not a legal opinion.

3 Definitions

Access token - a string of characters that is a technical representation of a communication session, with a set validity period, established between the TPP and the ASPSP in the context of a strictly defined PSU and for a specific scope of services and resources on the ASPSP's part, which TPP has gained access to.

Assets - everything that has value for the organization [ISO / IEC 13335-1: 2004]. There are two types of assets:

- Basic assets:
  - Business processes and activities
  - Information
- Supporting assets (of all types):
  - Equipment
  - Software
  - Network
  - Staff
  - Seat
  - Organizational structure

Secure Communication Channel - a communication mechanism ensuring confidentiality, integrity and data availability.

Protected Data - sets of sensitive information that may constitute sensitive information including:

- credentials and authorization data,
- transaction data (information on financial transactions carried out as part of the PolishAPI interface: amounts, descriptions and names of transaction parties),
- bank details (information on bank accounts and their balances),
- personal data (data identifying persons in accordance with the Personal Data Protection Act),
- cryptographic keys (e.g. all private keys present in the environment and the public key to the TLS certificate in the case of mutual authentication in this protocol - in terms of its integrity)
- information about the internal structure of the system (architecture of internal databases on the server side, format of messages sent between internal systems and names of internal objects).

EAT (External Authorization Tool) - an external authorization tool that is a system that provides the SCA procedure, i.e. strong PSU authentication.

Security Incident - a single event or series of events unplanned by the payment service provider that has/have or is/are likely to have an adverse effect on the integrity, availability, confidentiality, authenticity, authentication and/or continuity of payment services [ISO / IEC TR 18044: 2004].

Protected Media - physical information media containing Protected Data.

OAuth2 - open authorization standard. It allows one to share resources stored in one application with another application without having to delve into handling their credentials. As a result of authorization in the OAuth2 standard, access to resources between applications is provided.

Frontend Servers - part of the PolishAPI infrastructure available on the public network.

Backend Servers - part of the PolishAPI infrastructure unavailable on the public network.

SCA (Strong Customer Authentication) - authentication based on the use of at least two elements (components) belonging to at least two different categories: knowledge (something that only the user

knows), possession (something that only the user has) and customer characteristics (something that the user is) independent in the sense that the violation of one of them does not weaken the credibility of the other, which authentication is designed in a way that protects the confidentiality of the credentials.

Standard - PolishAPI standard.

Data Environment - an environment containing Protected Data.

TS 119 495 - technical specification of the standard relating to the profile of qualified certificates for the purposes of the Payment Services Directive *(Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU*).

User - the user of the payment account whom transactions carried out via PolishAPI relate to (the so-called PSU - Payment Service User).

Sensitive Areas - areas containing Protected Data, sensitive or critical information, and information processing means, e.g. a data centre.

XS2A (Access to Account) - interface between TPP and ASPSP enabling access to payment accounts and used to perform services provided as part of the PolishAPI.

Operational Event - is a specific change in the state of a system, service or network that indicates a possible breach of information security policy, security error, or an unknown situation that may be related to security [ISO / IEC TR 18044: 2004]

3.1 Terms used to prioritize requirements:

The capitalized keywords "MUST", “MAY", "SHOULD" and their variants, conjugated forms and negated forms are to be interpreted as described below:

- MUST, IS REQUIRED, MUST NOT, MAY NOT: These keywords mean an absolute requirement. This requirement must be implemented on all systems covered by the standard.
- SHOULD, IS RECOMMENDED, SHOULD NOT, IS NOT RECOMMEND: These words mean a strong recommendation. Failure to meet the requirement bearing the phrase "SHOULD" is permissible only in explicitly described and justified cases. It is necessary to conduct an analysis of the effects of failure to comply with the recommendation and the related risks.
- MAY, IS OPTIONAL, DOES NOT HAVE TO, IS NOT REQUIRED: These keywords mean the optional implementation of the recommendation. Furthermore, failure to implement such recommendations need not be justified or documented.

4 Area 1: Organizational and procedural requirements

4.1 Information security policy

Objective: An entity using PolishAPI MUST have an implemented and regularly updated information security policy approved by the top executives of the organization, which defines all obligations in the field of information security and clearly assigns these obligations to designated cells/units.

An entity using the PolishAPI MUST:

1. Have defined, published to their employees and associates as well as cooperating external companies, approved by top executives, maintained and disseminated security policies.
2. Ensure compliance with the procedures in the organization and cooperating entities in the area of management of operational risk and risk of breach of security including IT security, as well as effective implementation of control mechanisms and ongoing assessment of measures limiting operational risk and security breach risk in the provision of payment services.
3. Regularly review the security procedures and policies and update them in connection with changes that are significant from the organization's point of view.

4.2 Organization of information security

Objective: *An entity using PolishAPI MUST have implemented policies regarding information security management within the organization and exchange of information with external entities.*

An entity using the PolishAPI MUST:

1. Assign the duties and roles of information security management to designated cells/units of the organization, in particular:
   - Defining, documenting, approving and disseminating security policies and procedures;
   - Monitoring and analysis of security and information alerts and dissemination to appropriate cells/units of the organization;
   - Defining, documenting and disseminating the procedure for responding to operational incidents and security incidents to ensure prompt and effective management;
   - Managing user account, including adding, modifying and deleting;
   - Monitoring and controlling access to data;
   - Maintaining due contact with relevant authorities, including in particular the Polish Financial Supervision Authority.
2. Define and implement the authorization process for new means of processing information entered into use, in particular information systems and IT network elements.
3. Define the requirements for confidentiality agreements and regularly review them in terms of ensuring protection of information adequate to the current needs of the organization.
4. Define security requirements for contracts with third parties (including IT system providers), in particular regarding access, processing or management of organization information in networks and information systems.
5. Perform regular independent reviews of the security system.

4.3 Management of services provided by external suppliers

Objective: An entity using PolishAPI MUST have implemented policies and procedures for managing service providers that will allow the risk associated with the use of services of external companies to be assessed and reduced.

An entity using the PolishAPI MUST:

1. **Maintain and implement policies and procedures for managing service providers (including in particular as part of outsourcing) that have an impact on the security of Protected Data, in accordance with the following requirements:**
   - Creating and updating a list of service providers;
   - Verifying before establishing cooperation with service providers that they meet the requirements of the Standard;
   - Ensuring in contracts with third parties the commitment that those entities meet the requirements of the Standard adequately to the scope of services rendered.
   - Implementing the programme of at least annual monitoring of compliance of the service provider with the requirements of the Standard, adequate to the scope of the service provided.

4.4 Asset management (from an information security perspective)

Objective: ***An entity using PolishAPI MUST have implemented processes related to asset management (from the point of view of information security) including: inventory of assets, determination of their ownership and determination of the principles of acceptable use, as well as the principles of information classification, system components and data storage management.***

Accessing the PolishAPI interface, ASPSP MUST, and TPP SHOULD ensure:

1. Periodic inventory of assets and its documentation.
2. Assignment and documentation of ownership of assets dedicated to employees of the organization or authorized persons from external companies.
3. Definition and documentation of the principle of acceptable use of assets.
4. Implementation and update of documentation of activities related to inventory, assignment of ownership and determination of the principles of acceptable use of assets in accordance with the internal regulations of the organization.
5. Physical protection of all Protected Media (including mass storage devices, data carriers, printed documents, etc.). Storage of backup copies of Protected Media in secure locations, preferably in a location outside the organization's seat where the Protected Media is physically located.
6. Maintenance of strict control over the use and distribution of the Protected Media both inside and outside the organization in accordance with the regulations implemented in the organization, including:
   - Sending the Protected Media by means of a secure method, in particular allowing accurate tracking of the shipment;
7. Destruction of the Protected Media that is no longer needed for business purposes or for legal reasons. Destruction of physical information media (prints, CDs, etc.) using a shredder, combustion methods or other mechanical/hardware methods to prevent the restoration of the Protected Data. Protection of containers for storing materials for destruction.
8. Documentation and use policies and procedures for restricting physical access to Protected Data.

4.5 Physical and environmental security

Objective: An entity using the PolishAPI MUST have implemented effective safeguards against unauthorized physical access to the rooms where Protected Data is processed. Environmental security measures MUST be provided for the system.

An entity using the PolishAPI MUST ensure:

1. The use of appropriate access control measures to limit and monitor physical access to systems in the Data Environment:
   - Use of video cameras and/or access control mechanisms to monitor physical access to Sensitive areas. It is required to store recordings for at least 3 months, unless otherwise required by law.
   - Collection of logs from the access control system and their storage for a minimum of 1 year.
   - Implementation of physical and/or logical control mechanisms to limit access to publicly available sockets.
   - Limitation of physical access to wireless access points, network gateways, mobile devices, network equipment and communications, telecommunications lines.
2. Establishment of procedures to facilitate distinguishing guests from staff:
   - Identification of guests (e.g. badges, badges).
   - Revocation of access for former employees or for invalid guest IDs.
   - Provisions governing changes in guest access requirements.
3. Control of employees' physical access to sensitive locations by means of:
   - Authorization for access in accordance with the duties performed by the employee.
   - Immediate cancellation of access to employees upon termination of employment and immediate return of devices / items used for access control (e.g. keys, magnetic cards, identifiers, etc.).
4. Implementation of guest identification procedures and authorization for their access:
   - Authorization to provide guests with access prior to admission, escorting guests while in areas where Protected Data is processed or stored.
   - Identification of guests based on badges or other identifiers that expire over time and allow visual distinction from staff.
   - Return of badges or other identifiers before leaving the facility or on the day of expiry.
   - Using the guest book or electronic register to record guests gaining access to the facility where the Protected Data is stored. It is necessary to document, among others: the name and surname of the guest, the company represented and the name of the person authorizing access. Maintenance of the book for a minimum of three months, unless the law provides otherwise.
5. Implementation of procedures for protection against threats such as flood, flooding, fire, overheating and other forms of natural or man-made disasters.

4.6 Safe operation and change management

Objective: An entity using PolishAPI MUST have implemented procedures for the safe operation of its PolishAPI interface components and the principles of management of changes in these components.

An entity using the PolishAPI MUST ensure:

1. Separation of environments used to develop/test software from the production environment and the use of user access control and other systems of the organization to these environments.
2. Separation of the duties of the persons involved in software development/testing and managing the production environment, adequately to the information security policies currently applicable in the organization.
3. Limitation of the use of production data for testing or in the development of software, and with a justified necessity for such use, development and application of a procedure for preparing production data for testing applications (e.g. data anonymization, data selection, access to data only for authorized persons).
4. Deletion of data and test accounts prior to the launch of production.
5. Removal or disabling of unnecessary services, processes, routing, network connections (so-called hardening) on all system components.
6. Change management procedures for implementation of security patches and software modifications that, when applied, will result in:
   - Production of a documented change accepted by authorized personnel;
   - Performance and documentation of tests to verify that the change does not adversely affect system security;
   - Creation of a procedure to undo the changes made.

4.7 Access control

Objective: An entity using the PolishAPI MUST have procedures implemented to ensure that access to protected data is limited to the minimum required by business processes.

An entity using the PolishAPI MUST ensure:

1. Restriction of access to system components and the Protected Data to a group of people whose business tasks require such access:
   - Defining access needs for each role:
     a) Identification of system components and data sources to which access for a given role is necessary,
     b) The level of authority required to access sources (e.g. user, administrator, etc.).
   - Restricting users' rights to the minimum necessary to perform their official duties in accordance with the least privileges principle.
   - Granting access based on individual classification of tasks and functions of personnel
   - Requirement of documented (written or electronic) consent of the authorized entity to grant permissions. Assigning credentials to employees:
     a) by applying a formally established and documented security procedure.
     b) with confidentiality, upon prior identification of employees.
   - Employees' use of credentials in a way that limits the possibility of unauthorized access to them.
   - Defining, documenting, applying and periodically reviewing the minimum requirements for authentication methods and credentials that the organization can use in the system (in particular the so-called password policy).
2. Use of an access control system to the system components that limits access on a “need to know” basis with the default setting of “deny all”. The access control system MUST ensure:
   - Coverage of all system components, including IT network and network devices.
   - Granting of access to individuals or groups of people based on tasks and functions.
3. Documentation, use and provision of users with security policies and procedures regarding the restriction of access to Protected Data.

4. Periodical review of security policies and procedures regarding the restriction of access to Protected Data.
5. Establishment, documentation and implementation of a process of regular review of users' access rights to all components of the PolishAPI interface under direct management of the organization.
6. Establishment, documentation and implementation of the “clean desk policy” and the “clean screen policy” taking into account:
   - The need to keep paper documents, data carriers, and electronic documents confidential for unauthorized parties (including unauthorized employees of the organization).
   - The need to immediately destroy paper documents, data carriers, electronic documents that do not require further processing within the system and which are not subject to the obligation to be stored under applicable state law or internal regulations of the organization.

4.8 Ensuring security throughout the entire life cycle of the information systems

Objective: **An entity using PolishAPI MUST have procedures implemented to ensure information security throughout the entire life cycle of the information systems that constitute components of the PolishAPI interface, i.e. at the stages of acquiring, developing, maintaining and decommissioning these systems.**

An entity using the PolishAPI MUST ensure:

1. That business requirements for new IT systems included in the PolishAPI interface or its extensions should include requirements for information security and IT security.
2. Protection of the PolishAPI interface against abuse related to errors in the components of this system, loss and unauthorized modification of the input and output data processed in it, in particular through multi-stage tests and formal acceptance of individual system functionalities.
3. Protection against unauthorized access and versioning of the source code of the system components.
4. Protection of confidentiality and integrity of the Protected Data at the start of the productive use of new system components or developed components.
5. Supervision over the development works of the PolishAPI interface entrusted to a third-party company.
6. Establishment, documentation and implementation of the vulnerability management process of the PolishAPI interface components in order to immediately eliminate these vulnerabilities and protection against system exposure to loss of data availability, confidentiality or integrity.
7. Secure application development (including administrative access to applications over the network):
   - In compliance with the Standard (e.g. secure authentication and authorization),
   - Based on industry standards and best practices,
   - Using information security techniques throughout the entire software development cycle.
8. Evaluate code modifications before production installation or before being handed over to the user to identify potential vulnerabilities (using a manual or automated process) at least taking into account whether:
   - The evaluations of code modifications are carried out by persons other than those who are their creators, having appropriate knowledge of code evaluation techniques and safe programming practices,
   - The evaluators ensure that the code is written in accordance with the guidelines of safe programming, in particular with regard to item 4,

- The required corrections are applied prior to making the application available,
- The results of the code evaluation are subject to verification and acceptance of authorized persons prior to making the application available.

9. Removal of common programming errors in accordance with the current, publicly available "OWASP TOP 10" list, including:
   - Lack of validation of application input and output data, in particular vulnerability to injection attacks, e.g. SQL injection, code injection, OS injection.
   - Buffer overflow.
   - Data encryption errors.
   - Unsecured data communication.
   - Inappropriate error management.
   - Vulnerability to Cross-site scripting attack (XSS, cross-site scripts)
   - Inadequate access control (e.g. unsecured direct object references, unrestricted URL access, unrestricted user access to functions).
   - Vulnerability to Cross-site request forgery.
   - Incorrect authentication and session support.
10. Removal of all critical and high risk vulnerabilities identified in the vulnerability identification process.
11. Removal of accounts of developers, testers and other user IDs and passwords prior to the system's start in the production environment.
12. Minimization of errors by providing developers with training in:
    a. the security of the developed software,
    b. avoidance of common security holes,
    c. understanding how sensitive data is processed in memory.
13. Continuous protection and identification of application security holes:
    - Application security assessment using manual reviews or automatic security assessment tools, at least once a year,
    - Errors deemed critical according to the classification used in the organization MUST be removed immediately.
14. The PolishAPI software MUST only use libraries that do not contain publicly published material security vulnerabilities. The publisher of PolishAPI software MUST monitor the published information about vulnerabilities in the libraries used by its software. The time between the publication of the information about a significant security vulnerability in such a library and the implementation of the amendment in the PolishAPI software MUST result from a risk analysis and may not exceed 3 months for high vulnerabilities.

4.9 Handling of operational events and security incidents, including those of ICT nature

Objective: **An entity using PolishAPI MUST have appropriate procedures in place to ensure a quick, effective and orderly response to information security incidents to minimize financial and reputational damage.**

An entity using the PolishAPI MUST ensure:

1. Creation and effective implementation of a response plan to an Operational Event and Security Incident regarding services related to the PolishAPI interface - ensuring immediate actions to minimize the scope and effects of an Operational Event or Security Incident, gathering evidence and drawing relevant conclusions and implementing adequate safeguards. The plan SHOULD at least:
   - Describe the roles, responsibilities and strategy of communication and contact in the event of an Operational Event and Security Incident or even its suspicion,

- Provide details and response times for each type of an Operational Event and Security Incident,
- Include procedures for restoring / ensuring business continuity,
- Define how to report actions taken during the handling of an Operational Event and Security Incident, including external reporting of major Security Incidents,
- Cover all system components,

2. Cyclic testing, verification and/or update of the response plan.
3. Assignment of personnel to respond and handle Operational Events and Security Incidents and ensuring their availability at a level adequate to the scale and severity of an Operational Event or Security Incident recorded.
4. Provision of appropriate training to those responsible for responding to an Operational Event or Security Incident.
5. Definition of the process of modifying and improving the security incident response plan aimed at taking into account the organization's experience and industry progress.
6. Collection, storage and making available of evidence in accordance with the rules of evidence in force in the relevant legislation (s).

4.10 Business continuity management

Objective: An entity using PolishAPI MUST have implemented and regularly tested plans for maintaining business continuity and restoring activity in the scope of functioning of the PolishAPI interface

An entity using the PolishAPI MUST ensure:

1. Development and implementation of continuity plans based on the results of Business Impact Analysis and risk assessment.
2. Maintenance of a uniform structure of plans so that the plans are consistent with each other.
3. Periodic verification of the effectiveness of the business continuity plan.
4. Maintenance and testing of the business continuity plan and, if necessary, its correction and reassessment.
5. Maintenance and update of a list of processes critical to the organization.
6. Inclusion in the business continuity plan of at least:
   - Lists of critical processes with assigned priorities and RTO/RPO times,
   - The mode of operation of the organization during and after the crisis,
   - Crisis management structures with defining roles and responsibilities,
   - Communication and cooperation with third parties,
   - Return to normal operations.

4.11 Policies for safe use by employees

Objective: An entity using the PolishAPI MUST have implemented safe use policies for security-relevant technologies by its employees (e.g. remote access, use of mobile devices, use of wireless networks, etc.). The introduction of new technologies in an organization MUST require a formal process (in particular through the change management process).

An entity using the PolishAPI MUST ensure:

1. Development and implementation of policies for introducing new technologies together with definitions for the correct use of these technologies, e.g. remote and wireless access technologies, laptops, tablets, other portable electronic devices (e.g. flash drives), e-mail and Internet use. Policies for introducing new technologies MUST describe the following areas:

- Authorized entity consent
- Ensuring authentication when using new technologies where it is justified
- Providing mechanisms to control access to organizational infrastructure resources
- A method of quick identification of a user using organizational infrastructure elements
- Permissible uses of technology
- A list of technologies approved for use

2. Prohibition of copying, transferring and storing the Protected Data on mobile devices without mechanisms ensuring confidentiality.

4.12 Security of human resources

Objective: **The entity using PolishAPI MUST have implemented policies related to the security of human resources to minimize risks to information security arising from the recruitment of new employees, their performance of the official duties and the risks related to the termination of their employment or to a change of position.**

An entity using the PolishAPI MUST ensure:

1. Implementation of a formal personnel awareness building program on information security to raise awareness of the significance of the security of the Protected Data. This process MUST include:
    a. Performance of thorough verification of candidates for employees of the organization, with due diligence prior to their employment, in accordance with applicable law to minimize risk.
    b. Training of personnel after employment and at least once a year, depending on the official duties and level of access rights.
    c. Confirmation by personnel that they have read and understood the organization's security procedures and policies.

4.13 Risk management and security tests

Objective: An entity using the PolishAPI MUST have a process of regular analysis, risk reduction and acceptance as well as safety testing of the PolishAPI interface components belonging to it.

An entity using the PolishAPI MUST ensure:

1. Implementation of the process of identifying security holes using reliable sources of information and creating a risk level classification to describe newly discovered vulnerabilities.
2. Protection of all system components against known security threats by installing appropriate vendor patches within the time limit resulting from the classification of the application in terms of business risk level and the identified vulnerability.
3. Implementation of a cyclical process of checking the presence of unauthorized devices in the internal network, including wireless access points (802.11).
4. Launch of internal and external (from the Internet) scans of the organization's infrastructure ("vulnerability scan") at least once a year and after all significant changes in the network (e.g. installation of new system components, changes in network topology, product updates), together with corrections and necessary repetitions until all high and critical risk issues are resolved.
5. Implementation of penetration tests of the PolishAPI interface components based on OWASP recommendations (or developed own test approach) and/or industry security testing methodologies at least once a year and after each significant modification or upgrade of the infrastructure or application.

6. Performance of penetration tests at least once a year and each time after a significant change in the PolishAPI infrastructure affecting the mechanisms of segmentation or separation at the network level to verify that the Data Environment is effectively isolated from other networks.
7. Use of intrusion detection techniques and/or intrusion prevention techniques (IDS/IPS systems). Monitoring of all traffic on the edge of the Data Environment and alerting staff in case of suspected compromise. Update of all intrusion detection and prevention engines shortly after the update is released.
8. Documentation, use, update of security monitoring policies and procedures.

4.14 Prevention of money laundering

Objective: An entity using the PolishAPI MUST have implemented anti-money laundering policies.

An entity using the PolishAPI MUST comply with the provisions of the Act on Counteracting Money Laundering and Terrorism Financing of 2018.03.01 (Journal of Laws of 2018, item 723, as amended), to the extent required by this Act.

4.15 Informing Users about safety principles

Objective: An entity using PolishAPI MUST inform its clients about the principles of safe use of the PolishAPI interface and make clients aware of existing threats in this respect.

An entity using the PolishAPI MUST ensure:

1. Provision of at least one Secure communication channel (e.g. dedicated website) to clients for the purposes of communication related to the correct and safe use of the PolishAPI interface, and in this channel the Client SHOULD be notified of the following:
   - That any other way of communication may involve a fraud attempt,
   - The process of reporting suspicious transactions (frauds), suspicious events or anomalies during a payment service session or suspicion of using social engineering methods by the client,
   - The course of the response to the client's notification,
   - The process of notifying the client about potential frauds and warning about attacks.
2. Informing the client about updates to security procedures through the Secure communication channel, as well as notifications about new threats (e.g. information about phishing attempts).
3. Provision of support to clients in the event of questions, claims and complaints, reports of unauthorized payment transactions, the need to obtain technical assistance, notifications of unusual situations, the need to report incidents related to payment services and related services.
4. Provision of the following payment-related information to the client:
   - Requirements for software and other necessary tools (e.g. anti-virus software, firewall),
   - Tips for the correct and secure use of authentication credentials,
   - A detailed description of subsequent steps in the procedure of executing and authorizing the payment transaction and obtaining information, including the consequences of each action,
   - Tips on the correct and safe use of the hardware and software provided to the customer,
   - The procedure to be followed in the event of theft or loss of authentication credentials, hardware or software used to log in and perform transactions,

- The procedure to be followed when a client detects or suspects a security incident or operational incident,
- Description of the parties' responsibility in the context of using the services provided through the PolishAPI interface.
- In the case of TPP - a description of the steps to be taken to initiate the process of disabling services by the client themselves.
- Description of the terms of the client's transaction blocking, notification of this fact and the mode of disabling it.

5. Informing the User that in the event of a threat to transaction security, individual transactions or the payment service may be blocked. At the same time, the method and conditions for notifying the client about the blockade and the mode of disabling it MUST be specified.
6. Conducting an education programme and improving Users' awareness of security, aimed at helping to understand the needs of:
   - Securing credentials and all confidential data,
   - Software security management by installing and updating security components (e.g. anti-viruses, security patches, etc.),
   - Avoiding threats involved in downloading and installing software from untrusted sources.

5 Area 2: Requirements for the system infrastructure

5.1 Network configuration

Objective: An entity using PolishAPI MUST isolate the Backend Servers of the system from public networks, and MUST ensure the use of network intrusion detection or prevention systems.

An entity using the PolishAPI MUST ensure:

1. The use of a network configuration that limits connections between non-trusted networks (beyond the organization's control) and the Data Environment
   - Limiting inbound and outbound traffic necessary for the Data Environment, in particular blocking any unreasonable business needs of network traffic.
   - Securing the configuration files of network devices.
2. Protection against unauthorized access to the Data Environment from wireless networks, e.g. by
   - blocking network traffic from wireless networks to the Data Environment, except the one that is necessary from the point of view of business requirements
   - strong (two-factor) authentication of access to wireless networks
   - physical limitation of signal distribution of wireless networks
   - use of the Network Access Control system
3. Prevention of a direct connection between the Internet and each system component in the Data Environment, excluding boundary infrastructure facilities (at the interface with the Internet), dedicated for this purpose:
   - Use of demilitarized zones (DMZ), in particular to limit incoming traffic only to those necessary components and services of the system that have been approved for release.
   - Prevention of direct incoming and outgoing connections for traffic between the Internet and the Data Environment.
   - Use of anti-spoofing techniques to detect and block spoofed source IP addresses.
   - Blockade of unauthorized traffic from the Data Environment to the Internet.
   - Use of dynamic packet filtering (SPI - Stateful Packet Inspection: only "established" connections are allowed into the network).
   - Placement of system components storing Protected Data (such as databases) in an internal network zone separated from untrusted networks, in particular networks from which and from which Internet traffic comes directly.
   - In addition, system components SHOULD be separated within the network on the basis of minimum access required to meet business needs.
   - Keeping private IP addresses and routing information confidential from unauthorized persons.

5.2 Configuration of servers, devices and software

Objective: An entity using PolishAPI MUST ensure that software is up-to-date, minimize the risk involved in malware and unauthorized access, ensure event monitoring, and take into account the separation of production and test environments.

An entity using the PolishAPI MUST ensure:

1. Change of the default access settings contained in the provider’s configuration and remove or deactivate unnecessary default accounts before installing the system on the network. This applies to all default passwords, including for operating systems, software providing

security services, applications and system accounts, POS terminals, SNMP community strings, etc.

2. For wireless environments connected to the Data Environment or sending Authorization Data, change of all default settings at installation, including default cryptographic keys, passwords, SNMP passwords (community strings).
3. Determination of a configuration standard for all system components, taking into account known security holes and compliance with industry-recognized system hardening standards, e.g. Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS) Institute , National Institute of Standards Technology (NIST).
    - Implementation of only one main function at a single instance of the operating system to prevent the coexistence of functions requiring the use of different levels of security (e.g. database, web services, DNS implemented on separate servers)
    - Launch of only services, protocols, daemons etc. necessary for the system to operate.
    - Separation of the PolishAPI interface components into data layer, controller layer and presentation layer.
    - Implementation of additional security for all necessary services, protocols and daemons considered unsecured, e.g. using technologies that guarantee confidentiality and integrity, such as SSH, SFTP, TLS or IPSec to protect unsecured services such as NetBIOS, Telnet, FTP etc.
    - Configuration of system security parameters to prevent misuse.
    - Removal or blockade of all unnecessary functionalities such as scripts, drivers, add-ons, subsystems, file servers, and unnecessary web servers.
4. Encryption of all remote administrative access using strong cryptography. Use of technologies such as SSH, VPN or TLS to manage from the web level or other type of remote access.
5. Maintenance of up-to-date documentation of the architecture of components and system connections subject to the PolishAPI interface.
6. Documentation, use and provision of policies and procedures, security parameters for management and implementing IT solutions to the parties concerned.
7. Antivirus software installed on all systems exposed to malware, in particular personal computers and servers.
    - The antivirus software MUST be able to detect, remove malware.
    - For systems where the use of anti-virus systems is for objective reasons impossible or unreasonable, conducting a cyclical assessment to identify and assess the risk in terms of confirmation whether these systems still do not require the use of anti-virus software
8. Antivirus mechanisms that:
    - Are up-to-date,
    - Perform periodic scans for malware,
    - Generate logs for audit purposes.
9. Antivirus mechanisms work continuously and cannot be deactivated by users.
10. Documentation, use and provision of security policies and procedures for protecting systems against malware to the parties concerned.

5.3 Logical access control

Objective: The system MUST ensure user identification and accountability of activities as well as user and authorization management in accordance with the minimum access rules.

An entity using the PolishAPI MUST:

1. Ensure that access to the PolishAPI interface components and Authorization Data is restricted to the group of persons whose business tasks require such access.
2. Define access requirements for each role:
   - Specify the system components and data sources to which access for the role is necessary.
   - Specify the permission level required to access the data sources (e.g. user, administrator, etc.).
   - Limit users' rights to the minimum scope necessary to perform official duties.
   - Grant access based on individual task classification and personnel functions.
   - Require documented (written or electronic) consent of the authorized entity to grant permissions.
   - Apply the "Segregation Of Duties" principle.
3. Use the access control system to the system components that limits access on a “need to know” basis with the default setting of “deny all”.
   The access control system MUST:
   - Cover all system components
   - Grant access to individuals based on tasks and functions.
   - Include the "deny all" default setting
4. Document, use and provide the parties concerned with security policies and procedures regarding the restriction of access to Authorization Data.

5.4 Processing of the Protected Data on the server side

Objective: Protected data MUST be secured in accordance with accepted criticality in the area of integrity and confidentiality during storage, transport, modification, deletion.

An entity using the PolishAPI MUST ensure:

1. Integrity and confidentiality of the Protected Data throughout its transmission.
2. That access to Protected Data is logged in a way that ensures an audit trail, at least to the extent enabling identification of the accessing personnel or element of the IT infrastructure.
3. That modification of Protected Data is only possible by previously authenticated and authorized personnel.
4. Data removal from media carried out in a way that prevents its restoration.
5. That Authorization Data is stored by the Entity using the PolishAPI only for the time strictly required to handle the payment process and complaints.

An entity using PolishAPI MUST make every effort to guarantee the integrity and confidentiality of Protected Data processed in the infrastructure.

5.5 Management of cryptographic keys

Objective: The system MUST ensure the security of cryptographic keys throughout their life cycle.

An entity using the PolishAPI MUST:

1. Implement the principles for using cryptographic security.

2. Implement key management policies that enable the use of cryptographic techniques, including at least:
    - Key generation.
    - Storage and backup of keys.
    - Purpose of using the key.
    - Key length.
    - Key lifetime.
    - Key distribution.
    - Key exchange.
    - Key deletion and archiving.

5.6 Ensuring high availability of services

Objective: The system MUST ensure high availability of services in accordance with the adopted classification of criticality, in particular through redundancy of components, backing up data and software as well as automatic maintenance of system continuity.

An entity using the PolishAPI MUST:

1. Ensure the availability of system services in accordance with the accepted SLA conditions contained in the agreements and the results of the risk analysis carried out by the Entity using PolishAPI.

6 Area 3: Requirements for the PolishAPI interface

6.1 Authentication and authorization under the PolishAPI

Objective: Access to PolishAPI interface services MUST be possible only for the authorized Entity using the PolishAPI and the User. The method of authenticating the Entity using the PolishAPI and the User and authorizing their actions MUST ensure that the risk of unauthorized access is minimized.

1. Entities using the PolishAPI MUST be properly authenticated before they are granted access to the XS2A interface. Authentication errors MUST result in access to the XS2A interface being denied.
2. Authentication MUST be based on public key certificates in the mutual authentication process using the TLS 1.2+ protocol.
3. Entities using the PolishAPI MUST have a valid certificate for mutual identification in the XS2A interface, obtained from a qualified trust service provider that meets regulatory requirements in the area of trust services and electronic identification. This certificate MUST meet the requirements defined in the RTS and the ETSI technical specification (TS 119 495). Entities using the PolishAPI MUST, as part of the authentication process, verify the validity (using the OCSP protocol or CRL) of all certificates on the certification path each time.
4. TPP MUST be registered in at least one register in a European Union member state in the role in which it wants to act during the implementation of communication based on the PolishAPI standard. The ASPSP SHOULD verify the TPP registration status as part of the authentication procedure.
5. TPP authorization MUST be based on the Role Based Access Control (RBAC) model, in which the level and scope of access to individual API resources depends on the role of the Entity using the PolishAPI.
6. The use of individual methods within the PolishAPI interface MUST be authorized in such a way that the rights depend on the role of the Entity using PolishAPI and the scope of consents granted to it by the User. In particular, the level and scope of authorization SHOULD be different for TPP depending on the scope of their rights.
7. The user (PSU) MUST be authenticated on the ASPSP's side or in an external authorization tool (EAT).
8. User Authentication (PSU) MUST be carried out using the SCA procedure in all cases required by the PSD2 Directive. If the transaction can be released from the obligation to implement the SCA procedure, such decision remains the responsibility of the ASPSP.
9. Authentication on the ASPSP's side MUST take place after redirection to the ASPSP's side, whereby the PSU's authentication and authorization data MUST be transferred only to the ASPSP.
10. In the case of mobile applications, redirection to the ASPSP website and back to the TPP website MUST be done in the system browser (browsers other than system browsers are not allowed, the use of WebView is not allowed), and not in the mobile application itself. The TPP can register the appropriate URL in the device's operating system to automatically resume the mobile application after being redirected to the TPP.
11. PSU's authentication in an external authorization tool (EAT) MUST meet the following conditions:
    - EAT MUST provide the functionality of strong PSU-SCA authentication as defined in the technical requirements of the PSD2 Directive;
    - PSU MUST first successfully activate access to the EAT tool in accordance with the procedure developed and required by each ASPSP;

- ASPSP prepares a message containing basic information about the transaction displayed in the EAT before confirming it;
- The result of the SCA procedure carried out in the EAT tool MUST be securely notified to the appropriate ASPSP.

12. User credentials and sessions, as well as tokens for authorizing operations MAY NOT be transferred in the form of URI parameters.
13. Regardless of the PSU's authentication mechanism used, the successful authentication process MUST end with the issuing of a token by the ASPSP Access. Operations via TPP MUST be ordered using a valid Access token. The access token can be used once or repeatedly before it is invalidated by the ASPSP, which will require the SCA procedure for the PSU to be repeated.
14. The authorization code and the Access Token MUST ensure compliance with the provisions of up-to-date, publicly available OWASP recommendations for session management, in particular regarding the length, entropy and validity.
15. After a maximum of 5 consecutive unsuccessful attempts to authenticate the user (when logging in or during transaction authorization), its account MUST be blocked by the ASPSP. Account MUST be unlocked in accordance with ASPSP procedures.
16. After exceeding the User's inactivity limit, the Access token MUST be invalidated by the ASPSP.
17. After exceeding the active user's session limit, the Access Token MUST be invalidated by the ASPSP. The active session length limit is set individually by each Entity using the PolishAPI.
18. Transactions with a higher level of risk (e.g. with higher amounts or to persons with whom such transactions have not been previously performed) SHOULD be additionally authorized by the ASPSP.
19. The payment system MUST allow limiting the number or value of transaction amounts carried out by a specific System User in set time intervals (e.g. 1 hour, 1 day, 1 month). Default restrictions MUST also be set (applicable to the System User as soon as the services are activated).

6.2 Cryptographic data security mechanisms

Objective: All Protected Data sent between an Entity using PolishAPI and between the User and an Entity using PolishAPI MUST be protected against disclosure, modification and impersonation of one of the parties to communication.

1. Communication via the PolishAPI MUST be cryptographically secured at two levels:
   - The TLS protocol MUST be used at the transport level. TLS connection parameters MUST be renegotiated securely in accordance with the RFC 5746 standard.
   - At the message level, to ensure non-repudiation, a JSON Web Signature MUST be used in accordance with the RFC 7515 standard. The signature MUST be placed in each request in the header called X-JWS-SIGNATURE.
2. PolishAPI participants SHOULD use the most secure versions of cryptographic data protection solutions. The minimum requirements for algorithms and encryption key parameters MUST be no worse than those recommended by recognized institutions, e.g. NIST.
3. Each of the communication parties (TPP, ASPSP) MUST have its own unique two pairs of keys (for transmission and signature).
4. Separate certificates MUST be used to secure the HTTPS level transmission and JWS-SIGNATURE signature. For HTTPS, the certificate MUST have extended key (Client Authentication) use for the signature (Digital signature).
5. The certificates used to set up the transmission and signature MUST be validated in terms of:
   - Validity (certificate validity dates from and to)
   - No cancellation (CRL or OCSP)
   - Path Verification (RFC 4158)

6. Certificates MUST be issued taking into account ETSI TS 119 495 specifications.
7. All requests and responses MUST be signed in accordance with the JWS SIGNATURE standard, as part of the XS2A interface (on the ASPSP side) and the callback interface (on the TPP side).
8. The following conditions MUST be met as part of the JWS-SIGNATURE signature header:
    - the use of the "kid" header parameter is required (extension of section 4.1.4 RFC 7515),
    - the use of the "x5t # S256" header parameter is required (extension of section 4.1.8 RFC 7515),

    Thanks to this, it is possible to uniquely identify the certificate on the reading side, find it in the internal cryptographic infrastructure and use the signature content to read it, and bypassing the need to reconcile the certificate with every message sent and received via XS2A interfaces and callbacks.
9. Communication participants MUST agree the certificate on a one-off basis, e.g. by:
    - using the JWS-SIGNATURE signature header parameter named "x5u" (section 4.1.5 RFC 7515); which allows one to pass the URL to the resource that is the public X.509 certificate key in the same message in which the JWS-SIGNATURE signature was first built using that certificate;
    - applying the procedure based on the "OAuth 2.0 Dynamic Client Registration" (RFC 7591) protocol, allowing for prior (in relation to actual communication using the XS2A interface or callback) certificate agreement between the parties.

6.3 Data validation

Objective: Input data from untrusted sources MAY NOT be processed by the PolishAPI interface software in such a way as to enable attacks on the system or its users (e.g. by invoking Cross-Site Scripting, SQL Injection, XML Injection, Directory Traversal attacks).

1. PolishAPI software MUST check the correctness of data obtained from untrusted data sources before it is used by positive validation - that is, for each type of input data there MUST be rules of their correctness, which will be as restrictive as possible. If the input data can contain special characters, they MUST be encoded correctly using dedicated functions.
2. If data obtained from untrusted sources is displayed on the screen, then any special characters in this context (i.e. HTML tags if the component used for displaying them) MUST be removed from the input data or properly encoded using a dedicated mechanism.
3. If PolishAPI software uses embedded components of the web browser, it MUST block the active elements of this browser (e.g. Javascript support and loading of external plugins) or enable the use of these components by downloading active elements from trusted sources or ensuring proper validation of data from untrusted sources.
4. If data obtained from untrusted sources is used by PolishAPI software, the verification requirements for handling malicious input data MUST be met in accordance with the current OWASP Application Security Verification Standard.
5. Structured JSON data MUST be verified in accordance with formal validation procedures using an approach based on white lists. Content-type and Accept (application / json) headers MUST also be validated for compliance of the header value with the actual content of the HTTP message.
6. During validation, the digital signature MUST be verified in the header (X-JWS-SIGNATURE) in the context of data transmitted in both HTTP requests and responses exchanged in communication on the ASPSP-TPP line (also in the case of communication initiated by ASPSP).
7. Input validation errors MUST be logged.

8. Validation errors MUST be signalled with HTTP 400 (Bad Request) and data MUST be rejected. This also applies to the negative validation of the JWS-SIGNATURE signature.
9. In case of Content-type and Accept content validation errors, HTTP message number 406 (Not Acceptable) SHOULD be returned.

6.4 Accountability of events

***Objective: The system MUST ensure the accountability and non-repudiation of system users' activities, while ensuring the confidentiality of Protected Data and the privacy of users*.**

1. The PolishAPI software MUST register all key operations as well as successful and unsuccessful authentication and authorization attempts.
2. Log retention time MUST comply with applicable law and SHOULD be as long as possible.
3. The time sources of all entities using the PolishAPI SHOULD be synchronized with a trusted time source (maximum stratum 3) to ensure that log entries have the correct time.
4. Logging in of key business operations MUST ensure non-repudiation and integrity of entries, which SHOULD be done by using data from the JWS Signature.
5. The log SHOULD contain the necessary information that will allow for precise time analysis in the event of an event that allows individual entries to be joined into one transaction. E.g. an abbreviation from the authorization token can be the element connecting individual entries.
6. Particularly sensitive information, including identity credentials and authorization keys MAY NOT be buffered or saved in logs.
7. Each request sent by the TPP to the XS2A interface on the ASPSP side MUST contain a unique identifier (a parameter named requestId in the header structure transmitted in the body of each request and in the header named X-REQUEST-ID). The uniqueness of this identifier MUST be maintained in the scale of all requests sent by all TPPs to the selected ASPSP. The format of the request identifier MUST be UUID (Universally Unique Identifier), which is the standard described in document RFC 4122. The request identifier MUST be generated in option number 1 (see section 4.1.1 RFC 4122) and version 1 (see section 4.1. 3 RFC 4122), which ensures that the value of the identifier of the monotonic component based on the time of sending the request and information identifying the requesting entity (TPP) is included.
8. Because of the timeout events that may occur during the processing of the HTTP request, the ASPSP MUST provide uniqueness verification at the requestId level. After determining the non-uniqueness of the request, ASPSP MUST return error 400.1 (Repeat request).
9. The timeout of request processing MUST be specified and not longer than 5 minutes, and when the limit is exceeded, the request MUST be cancelled.

7 Area 4: Prevention of abuse and attacks.

7.1 Event monitoring

Objective: The system MUST record user activities and information necessary to detect attempts to attack the system, while ensuring the confidentiality of Protected Data and the privacy of users.

1. An entity using PolishAPI MUST ensure that a risk analysis is carried out and a decision is made on the basis thereof to implement and use a risk-adequate fraud detection and prevention system to identify suspicious transactions, prefers authorization prior to authorization, and to monitor payers and merchants.
2. An entity using PolishAPI SHOULD ensure:

- The ability to perform a comprehensive transaction control and assessment procedure within an acceptable time;
- Rejection of potentially fraudulent payment transactions.

7.2 Fraud Detection Principles

Objective: **The monitoring system SHOULD analyse the operation of the payment system using all sources of information available under this system - including anomalies and errors in the operation of various components. The effect of the monitoring system SHOULD be information about the attacks carried out against the system, their scale and methods used by the attackers. This SHOULD lead to the blocking of attacking activities at the earliest possible stage of the attack (e.g. during reconnaissance) and minimize the risk of fraud leading to financial or reputation losses.**

1. Within the PolishAPI interface, mechanisms should be implemented to detect and block suspicious transactions.
2. An entity using the PolishAPI SHOULD exchange information on suspected unauthorized transactions/compromised IPs, etc.

7.3 Protection of the system against access denied attacks

Objective: **The PolishAPI interface MUST be protected against the possibility of a Denial Of Service attack aimed at one or more of the entities involved in the payment process.**

1. Publicly available PolishAPI interface components MUST be protected in a manner that allows the risk of denial of service attacks to be minimized. In particular, operations available to unlogged users (e.g. new user registration) MUST be protected against this type of attack.
2. As part of the PolishAPI interface, protection mechanisms against denial of service attacks MUST be implemented by counting the number of transactions and enforcing maximum limits, exceeding of which will cause blockades, e.g.
   - the number of transactions initiated by TPP, taking into account who they are addressed to and what amounts they are for
   - the number of transactions initiated by the selected user
   - the total number of transactions with the option of manual or automatic isolation.
   - the number of queries for each mechanism (function, service) available to the TPP in a specified time period.
3. Limit values SHOULD be established on the basis of recognition of specific operational conditions. Limits of this type SHOULD be subject to parameterization. Measuring the number of resource access requests SHOULD be based on the use of a key that uniquely identifies the TPP and counters implemented per TPP on the server side. Exceeding limits MUST be signalled by HTTP message number 429 (Too Many Requests).