ComTRUST

ComTRUST CyberSecurity, LLC
US, 90013, California, Los Angeles, S. Hill Street, 448, office 235
+13232325390
WEB: comtrust.by

ComTRUST

ООО «КомТРАСТ КиберСекьюрити»
США, 90013, Калифорния, Лос Анджелес, С. Хилл Стрит, офис 235
+13232325390
WEB: comtrust.by

Single Standards for Payment Systems (SSPS)

Version: **1.0**

Effective date: **08/11/2024**

1. Contents

2. Basic concepts

Service is a web program or platform hosted on the Internet to which these SSPS security standards apply.
Website is an Internet resource that may include one or more Services.
User - a person who visited the Service and registered in it (if such an opportunity exists).
Developer is an individual or legal entity responsible for the technical implementation and operation of the Service.
Service Owner is an individual or legal entity that has ownership rights to the Service and is responsible for its operation and compliance with SSPS standards.
Service administration is a group of people involved in managing and supervising the operation of the service.
Service technical support is a group of people who provide the User with support on all issues that arise while working with the Service.
A legal entity is the same as a Developer.
Hosting provider is an individual or legal entity that provides the Developer with services for hosting the Service on servers.
Personal data - any information relating to a directly or indirectly identified or identified User.
Payment information - data related to the User's financial transactions, including, but not limited to, bank card numbers, account data and payment history.
Accreditation is the process of reviewing the Service by an Accredited Reviewer or Authorized Organizations for compliance with SSPS security standards.
Accredited inspector is a person providing Accreditation services to the Service.
Authorized organizations (Accredited inspector) - persons authorized by the Accredited Inspector to provide Accreditation Services.
The de-accreditation process is the process of resetting the Service’s Accreditation for compliance with these security standards due to their non-compliance by the Developer. This process is carried out by an Accredited Inspector.

Additional technical concepts are available in the Glossary of The Technical Terms (see Application).

3. Preface

The rapid development of digital technologies and e-commerce has led to a significant increase in online payments. At the same time, the risks associated with cybersecurity and user data protection have increased. In response to these challenges, ComTRUST developed **the Single Standards for Payment Systems (SSPS)**.

SSPS is a comprehensive set of requirements and recommendations aimed at ensuring a high level of security and reliability of payment systems. These standards take into account the best global practices and correspond to current threats in the field of cybersecurity.

The purpose of **the SSPS** is to provide clear and measurable criteria for assessing the security of payment systems and to help increase user confidence in online transactions. **SSPS** compliance verifies that a website or payment system meets high standards for protecting data and financial information.

This document is intended for payment system developers, information security specialists, auditors and all interested parties in the field of electronic payments. We encourage the active implementation of these standards to create a safer and more reliable online payment environment.

ComTRUST is committed to regularly updating **the SSPS** to ensure the standards remain current and effective in addressing emerging cybersecurity threats.

4. Introduction

4.1. Purpose of the document

The purpose of this document is to establish uniform security standards for payment systems (SSPS), ensuring a high level of protection for users and their data when making online payments.

4.2. Scope of application

These standards apply to all Accredited Services.

4.3. Normative references

When developing these standards, the requirements of the following regulatory legal acts of the Republic of Belarus were taken into account:

- Law of the Republic of Belarus of November 10, 2008 No. 455-Z “On information, informatization and information protection”
- Law of the Republic of Belarus of May 7, 2021 No. 99-Z “On the protection of personal data”
- Law of the Republic of Belarus of July 28, 2003 No. 231-Z “On Trade”
- Resolution of the Council of Ministers of the Republic of Belarus dated May 18, 2019 No. 311 “On approval of the Information Security Concept of the Republic of Belarus”
- Decree of the President of the Republic of Belarus dated February 1, 2010 No. 60 “On measures to improve the use of the national segment of the Internet”
- Resolution of the Board of the National Bank of the Republic of Belarus dated May 18, 2020 No. 155 “On approval of the Instructions on the procedure for functioning of the unified settlement and information space of the Republic of Belarus”

SSPS standards are developed in accordance with these regulations and complement their requirements for ensuring the security of online payments and the protection of user data.

5. General provisions

5.1. SSPS Security Principles

The SSPS standards are based on the following key principles:

1. **Confidentiality**: Ensuring the protection of personal data and payment information of users from unauthorized access.

2. **Integrity**: Guarantee that data remains unchanged during storage and transmission.

3. **Availability**: Ensuring the uninterrupted functioning of payment systems and user access to their data.

4. **Authenticity**: Confirming the authenticity of users and transactions.

5. **Transparency**: Providing users with full information about security measures and the processing of their data.

6. **Scalability**: The ability to apply standards to payment systems of varying scale and complexity.

7. **Relevance**: Regular updating of standards in accordance with the development of technology and the emergence of new threats.

5.2. Standards structure

The SSPS standards include the following main sections:

1. Protection of user personal data
   - Data collection and storage methods
   - Rules for processing and transmitting information
   - Mechanisms for deleting data upon user request

2. Security of financial transactions
   - Protocols for secure transmission of financial information
   - Transaction verification methods
   - Fraud prevention systems

3. User Authentication and Authorization
   - Requirements for passwords and other authentication methods
   - Multi-factor authentication
   - User session management

4. Data encryption

- Encryption standards for data transmission
- Requirements for storing encrypted data
- Encryption key management

5. Fraud monitoring and prevention
   - Anomaly detection systems
   - Incident response procedures
   - Security analysis and reporting

6. Ensuring system integrity and availability
   - Requirements for infrastructure fault tolerance
   - Disaster recovery plans
   - Regular data backup

7. Accreditation and audit procedures
   - Methodology for accreditation
   - Frequency of inspections
   - Requirements for accredited inspectors
   - Official registration of the payment service

Each section contains specific requirements, implementation guidelines, and compliance assessment criteria. Compliance with all sections of the SSPS standards ensures comprehensive protection of payment systems and user data.

6. Security requirements

6.1. Information Security Management

- Development and implementation of information security policy
• Creation of a comprehensive document covering all aspects of information security
• Policy coordination with management and legal department
• Regular updates (at least once a year)

- Appointment of persons responsible for information security
  • Creation CISO (Chief Information Security Officer) positions
  • Formation of an information security department
• Clear definition of roles and responsibilities in the field of information security

- Regular review and update of security policies
• Quarterly analysis of the effectiveness of existing policies
• Taking into account new threats and changes in legislation
• Making adjustments based on the results of audits and incidents

- Training of personnel in the basics of information security
• Development of a training program for different categories of employees
• Conducting regular trainings (at least once every six months)
• Testing employee knowledge and conducting training phishing campaigns

6.2. Network Infrastructure Security

- Use of new generation firewalls
• Implementation of NGFW with IPS, antivirus, antispam functions
• Configure filtering rules based on applications and users
• Regular updates of signatures and rules

- Network segmentation to isolate critical systems
• Dividing the network into VLANs based on functionality
• Isolation of payment processing systems into a separate segment
• Using microsegmentation technologies for containers and virtual machines

- Protection against DDoS attacks
• Use of specialized solutions for DDoS protection
• Configuring traffic filtering at the provider level
• Development of a plan to respond to DDoS attacks

- Regular network scanning for vulnerabilities
• Weekly scanning of the external perimeter
• Monthly full scan of the internal network
• Prompt elimination of detected vulnerabilities

- Secure configuration of network equipment
• Using secure configuration templates
• Disabling unused ports and services
• Regular audit of configurations

6.3. Access Control

- Implementation of the principle of least privilege
• Providing users with only the rights necessary for work
• Regular review and adjustment of access rights
• Using Role-Based Access (RBAC)

- Use of multi-factor authentication for critical systems
• Mandatory use of MFA for administrative access
• Implementation of MFA for users when working with sensitive data
• Support for various second factor methods (SMS, tokens , biometrics)

- Regular audit of access rights
• Quarterly review of access rights for all users
• Automation of the audit process using specialized solutions
• Immediate removal of access rights upon dismissal of an employee

- Automatic blocking of inactive accounts
• Setting up auto-locking of accounts after 30 days of inactivity
• Notifying administrators about blocked accounts
• Procedure for verification and reactivation or deletion of inactive accounts

- Complex requirements for passwords and their regular change
• Minimum password length - 12 characters
• Using a combination of letters, numbers and special characters
• Forced password change every 90 days
• Prohibition on reusing the last 10 passwords

6.4. Data encryption

- Use of modern encryption algorithms
• Use of AES-256 for symmetric encryption
• Use RSA-4096 or ECC for asymmetric encryption
• Regular review of the algorithms used (at least once a year)

- Data encryption during transmission
• Mandatory use of TLS 1.3 for all external connections
• Disabling support for legacy protocols (SSL, TLS 1.0/1.1)
• Configuring HSTS to force HTTPS

- Data encryption at rest
• Encryption of all storage media containing sensitive data

• Use of hardware encryption for mobile devices
• Column-level encryption of databases with sensitive information

- Secure encryption key management
• Use of specialized key management systems (KMS)
• Regular rotation of encryption keys (at least once a year)
• Strict access control to encryption keys

- Regular updates of cryptographic protocols
• Monitoring news and recommendations in the field of cryptography
• Timely updating of libraries and components responsible for encryption
• Planning the transition to post-quantum cryptography

6.5. Application Security

- Conducting code security analysis
• Using automated static code analysis tools
• Conducting manual code analysis for critical components
• Integration of security checks into the CI/CD process

- Protection against OWASP TOP -10 vulnerabilities
• Development and implementation of checklists to protect against each vulnerability from OWASP TOP -10
• Regular training of developers on secure development issues
• Use WAF for additional protection against common attacks

- Regular updating and patching of applications
• Install critical security updates within 24 hours
• Monthly updates of all system components
• Automation of the process of tracking and installing updates

- Using secure development methods (SDL)
• Implementation of secure development practices at all stages of the software life cycle
• Conducting threat analysis at the design stage
• Mandatory penetration testing before release

- Conducting regular pentesting
• Annual full pentest of the external perimeter
• Quarterly pentesting of critical applications
• Involvement of external experts to conduct pentests

6.6. Monitoring and audit

- Implementation of a SIEM system for collecting and analyzing logs
• Centralized collection of logs from all critical systems
• Setting up correlation rules to identify incidents
• Log storage for at least 1 year

- Monitoring of abnormal activity in real time
• Use of intrusion detection and prevention systems (IDS/IPS)
• Implementation of behavioral analysis systems (UEBA)
• Setting up alerts for suspicious activity

- Regular internal and external security audits
• Conducting an internal security audit once a quarter
• Annual external audit for compliance with standards (PCI DSS, ISO 27001)
• Development and implementation of a plan to eliminate identified deficiencies

- Maintaining logs of access and changes in critical systems
• Logging of all actions of privileged users
• Tracking changes in critical system configurations
• Ensuring the integrity and immutability of audit trails

- Analysis and response to security incidents
• Create procedures for different types of incidents
• Defining metrics and KPIs to evaluate response effectiveness
• Regular incident analysis to improve security processes

6.7. Incident Management

- Development of an incident response plan
• Creation of a detailed document describing response procedures
• Defining roles and responsibilities in the response process
• Regular update of the plan (at least once a year)

- Creation of an incident response team (CERT)
• Formation of an interdisciplinary team of specialists
• Ensuring 24/7 availability of the team
• Conducting regular trainings for team members

- Regular incident response training
• Conducting simulations of various types of incidents
• Practicing interaction between different departments
• Analyzing training results and making improvements to processes

- Incident analysis and lessons learned
• Conducting post-mortems after each serious incident
• Documenting lessons learned and recommendations
• Implementation of improvements based on incident analysis

- Timely informing users about serious incidents
• Development of notification templates for various types of incidents
• Definition of criteria for mandatory informing of users
• Ensuring transparency and honesty in communication with users

6.8. Business continuity

- Development and testing of a business continuity plan
• Conducting Business Impact Analysis (BIA)
• Identification of critical business processes and systems
• Annual full testing of the business continuity plan

- Creating and maintaining data backups
• Implementation of a 3-2-1 backup strategy
• Daily incremental and weekly full backups
• Regular testing of recovery from backups

- Ensuring fault tolerance of critical systems
• Implementation of cluster solutions for key services
• Use of load balancers and geographically distributed data centers
• Automatic switching to backup systems in case of failures

- Regular testing of recovery procedures
• Quarterly testing of individual system recovery
• Annual full disaster recovery testing
• Documentation and analysis of test results

- Availability of alternative communication channels and payment processing
• Providing backup communication channels (satellite communications, backup providers)
• Availability of agreements with alternative payment providers
• Developing procedures for switching to alternative channels in case of failures

These requirements may be supplemented or improved at the discretion of the Website Developer or Owner.

7. Conformity assessment procedure

7.1. Assessment methodology

- Comprehensive website analysis:
• Safety check of Frontend and Backend components
• Analysis of processing and storage of user data
• Assessing API security and integrations with external services

- Technical testing:
• Automated vulnerability scanning
• Manual testing of critical functions
• Checking the security of mobile versions (if applicable)

- Process assessment:
• Analysis of update procedures and patch management
• Review of incident response processes
• Evaluating development and testing practices

- Frequency of assessment:
• Initial full assessment
• Annual revaluation
• Unscheduled inspections in case of significant changes to the site

7.2. Eligibility Criteria

- Key areas of website assessment:
• Protection against common web vulnerabilities (OWASP TOP -10)
• Authentication and session management security
• Data encryption in transit and at rest
• Security of payment information processing
• Protection against DDoS attacks and other external threats

- Quantitative metrics:
• Number of critical, high and medium vulnerabilities
• Time to eliminate identified vulnerabilities
• Percentage of successfully repelled test attacks

- Qualitative criteria:
• Availability and quality of safety documentation
• Regularity of security system updates
• Transparency in communication with users about security issues

7.3. Certification process

- Website certification stages:

1. Submission of an application by the site owner
2. Preliminary self-assessment using the provided tools
3. Remote website audit by an accredited auditor
4. Elimination of identified inconsistencies (if necessary)
5. Final inspection and decision on certification
6. Issuance of a digital SSPS badge for placement on the website

- Requirements for website owners:
• Providing full access to the test version of the site
• Timely elimination of identified vulnerabilities
• Informing about significant changes in the structure or functionality of the site

- Certification validity period:
• 1 year with possibility of extension

- Maintaining certification:
• Quarterly automated scanning
• Mandatory reporting of serious security incidents

- Revocation of certification:
• Criteria: serious security breaches, failure to address critical vulnerabilities
• Appeal procedure for website owners
• Public notice of revocation of certification

Application

Application A: Self-Assessment Checklist

This checklist is intended to assist organizations in self-assessing compliance with SSPS standards. Using this list, companies can ensure that their systems and processes meet established security requirements.

1. Protection of personal data of users:

- Methods for secure collection and storage of personal data have been determined.
- Rules for processing and transmitting information have been implemented in accordance with SSPS requirements.
- Mechanisms have been put in place to allow a user to request the deletion of their data.

2. Security of financial transactions:

- Protocols are in place for the secure transmission of financial information.
- Reliable transaction verification methods have been introduced.
- Systems for preventing and detecting fraudulent activities are in place.

3. Authentication and authorization of users:

- Requirements have been established for passwords and other authentication methods.
- Multi-factor authentication methods (MFA) are used.
- User sessions are managed with security in mind.

4. Data encryption:

- Encryption standards are applied for data transmission.
- Encrypted data storage requirements are met.
- Encryption keys are managed in accordance with established rules.

5. Monitoring and fraud prevention:

- Systems for detecting anomalies in the operation of services have been implemented.
- Security incident response procedures are described and documented.
- Regular analysis and reporting on safety issues is carried out.

6. Ensuring the integrity and availability of systems:

- The system meets the requirements for infrastructure fault tolerance.
- Developed and tested disaster recovery plans.
- Regular data backup procedures have been implemented.

7. Accreditation and audit procedures:

- The methodology for accreditation has been determined.
- The frequency of inspections for compliance with SSPS standards has been established.
- Requirements for accredited inspectors are met and payment services are registered.

Application B: Glossary of Technical Terms

This glossary provides definitions of key technical terms used in the SSPS standards to provide a common understanding of their meanings.

- **Authentication** is the process of verifying the identity of a user or system. Includes identity verification using a password, biometrics, tokens or other methods.
- **Multi-factor authentication (MFA)** is a security method that requires the user to provide two or more verification factors to gain access to a system. MFA improves security over password authentication alone.
- **Authorization** is the process of granting a user or system the rights to perform certain actions or access certain resources after successful authentication.
- **Encryption** is the process of converting data into an encrypted format that is inaccessible to unauthorized users. Encryption can be used both when transmitting data (for example, over the Internet) and when storing it.
- **A protocol** is a set of rules and standards that define the exchange of data between systems or devices. In the context of SSPS, secure data transfer protocols protect financial information.
- **An encryption key** is secret information used in cryptographic algorithms to encrypt and decrypt data. Without the correct key, access to the encrypted data is impossible.
- **Data backup** is the process of creating copies of data that can be used to restore information in the event of loss or damage.
- **Fault tolerance** is the ability of a system to continue operating in the event of failure or malfunction of its components. Fault tolerance is achieved by duplicating key elements of the system.
- **Disaster recovery** is the process of restoring system operation after a serious failure or disaster. Includes data and infrastructure recovery plans.
- **Security monitoring** is the process of continuously monitoring system activity to identify suspicious activity or attempted unauthorized access.

- **Security incident management** is a set of procedures and actions that are performed when a security incident is detected in order to minimize damage and restore normal system operation.
- **Anomaly detection** - Processes and technologies that detect deviations from normal system behavior that may indicate hacking or fraud attempts.
- **Payment information** - data related to financial transactions, such as bank card numbers, accounts, payment history. This data is subject to encryption and protection in accordance with SSPS requirements.
- **Accreditation** is the process of formally confirming that a system or service meets SSPS security requirements. Accreditation is carried out by authorized inspectors.
- **Certification** is documentary confirmation of the service's compliance with established standards and safety requirements.
- **Phishing** is a type of cyber attack in which attackers try to obtain confidential information by posing as trusted sources.
- **Financial transaction fraud** is any action aimed at deceiving a payment system in order to obtain financial gain, such as using stolen bank card data.
- **Cryptography** is the science and practice of protecting information using encryption methods to ensure the confidentiality, integrity and authenticity of data.
- **Personal data** is information that allows you to directly or indirectly identify an individual. Includes name, address, contact details, and unique identifiers.
- **Server** is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network.

Application C: Examples of Successful SSPS Implementations

This section may contain cases and examples of successful implementation of SSPS standards in various companies. Descriptions of specific solutions and results achieved will help new users better understand the value of these standards.

Example content:

1. **Case 1: Implementation of SSPS in a large online store**
    - Problem Description: Frequent fraudulent transactions
    - Implemented solutions: integration of multi-factor authentication and monitoring system
    - Results: Fraud rate reduced by 80%
2. **Case 2: Ensuring security in the banking system**
    - Description of the problem: leakage of personal data of clients
    - Implemented solutions: strengthening data encryption and developing new data storage rules

- Results: complete elimination of data leakage incidents within a year

3. **Case 3: Implementation of security standards in a startup**
    - Problem Description: Lack of a structured security system
    - Implemented solutions: creation of a comprehensive security system based on SSPS
    - Results: successful accreditation and increased customer confidence

Document change history

- Version 1.0 (from 08/11/2024)

The latest version of this document is available on the official SSPS website (https://spss.comtrust.by).

Copyright information