Identity Proofing Service Provider Practice Statement

This document is public

Version	Author	Modification type	Date
V1.0	Fintech OS	Initial version	19-09-2022 | 17:03:04 EEDT

	Name	Title	Signature	Date
Prepared By	Andrei Poll	Product Owner	DocuSigned by: Andrei Poll EE79D9A14A3A4EB...	19-09-2022 | 17:04:14 EEDT
Reviewed by	Alin Nichifor	Legal Counsel	DocuSigned by: 1D393BAB4DFA4CA...	19-09-2022 | 17:03:04 EEDT
Approved by	Marcio Spinola	SVP Product Management	DocuSigned by: Marcio Spinola FD315D8F3697494...	19-09-2022 | 17:25:03 EEDT

Contents

1 Introduction

1.1 Overview

Fintech OS SRL (**“FintechOS”**) is a high-tech company delivering a technology-as-a-service platform for banks, insurance companies and enterprise financial services organizations.

The digital solution described in this document is meant for various business processes including Know Your Customer, and online subscription to commercial services. FintechOS integrated in its solution remote video identification of end-users in partnership with AriadNext.

The present document is the Identity Proofing Service Provider Practice Statement according to Standard ETSI TS 119 461 - Requirements for TSP components providing identity proofing of trust service subjects. This Statement is public. The confidential information of the Identity Proofing Service Provider Practice Statement is present in the internal documentation of FintechOS.

1.2 Approval & Review

This statement is reviewed (whichever event occurs first):

- at least once a year; or
- whenever an evolution in technology, or in the security context of remote video identification services will impose it; or
- in case of significant changes to ensure this statement’s continuing suitability, adequacy, and effectiveness.

The Product Owner for the remote video identification services is responsible for the review of this Identity Proofing Service Provider Practice Statement.

The overall management and implementation of this Identity Proofing Service Provider Practice Statement within the organization will be the responsibility of SVP Product Management.

Any changes to the Identity Proofing Service Provider Practice Statement must be approved by SVP Product Management.

Changes are indicated by a new version number in the respective updated document and are promptly republished in FintechOS’s repository after the current version has been released.

1.3 Parties

1.3.1 Client

A financial institution to which Fintech OS provides remote identity proofing services.

1.3.2 Identity Proofing Service Provider (IPSP)

FintechOS positions itself as a third party in identity proofing with a functional remote video identification of person service, by hybrid – automated and manual means. The product is integrated within more complex digital processes via which users can access services and products from financial institutions. The identification journey configured in FintechOS has the following components:

- OCR, Selfie, Guided Liveness, Human verification done in Back Office - Ariadnext

The journey starts in the client's local network on FintechOS web page that contains the AriadNext SDK. The solution implementation can be performed on premise or SaaS, in FintechOS Cloud. All critical infrastructure not related to the identity proofing process is hosted in Microsoft Azure. All systems that are critical to the identity proofing process is kept by AriadNext in one or more secured zone(s).

1.3.3 End-users

The end-users of the solution are FintechOS clients' end-customers (i.e., natural persons) that will be remotely identified and be able to sign their documents electronically.

2 Facility, Management, and Operational Controls

2.1 General requirements

In the field of security management, FintechOS guides itself by the generally recognized standards, e.g. ISO/IEC 27001, and other standards required by regulations and law.

The FintechOS's security management policy documents include the security controls and operating procedures for the FintechOS facilities, systems and information assets providing the services. FintechOS carries out and revises risk assessment regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures.

The FintechOS's management establishes the IT Security Policy, which forms a basis for consistency and completeness of information security and management support.

The FintechOS Chief Technology Officer approves policies and practices related to information security for the overall FintechOS services. The FintechOS management communicates information security policies and procedures to employees and relevant external parties who are impacted by it. FintechOS has implemented and maintains an Information Security Management System (ISMS) which is certified against ISO27001:2013 and subject to annual audit by an accredited external auditor.

2.2 Physical security controls

2.2.1 Site location and construction

The FintechOS services are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of Sensitive Information and systems whether covert or overt.

The protection provided is commensurate with the identified risks. The FintechOS ensures that physical access to critical services is controlled and that physical risks to its assets are minimized.
All critical infrastructure elements are held in Microsoft Azure, certified with ISO 27001 and ISO 22301, ensuring security and redundancy of the overall system.

2.2.2 Physical access

Physical access to FintechOS premises is controlled according a physical access policy.

Access to ICT facilities shall be strictly limited to authorized persons. The owner of the ICT facility, or his authorized designee (custodian), shall approve all requests for permanent access to it, including vendors under contract.

All persons with approved permanent or temporary access shall be documented in an ICT facility access list. This list shall also be used as the source for setup access authorizations in the electronic access control system, where applicable.

All visitors or other third-parties, as well as employees with a temporary need for access shall only enter into ICT facilities if authorized by the appropriate owner or authorized designee (custodian). Visitors to ICT facilities shall be authorized, verified and accompanied into ICT facilities by authorized personnel.

ICT facility access lists shall be reviewed at least annually by the owner of the ICT facility or his authorized designee (custodian) for continued business needs of individuals.

ICT facility access control reports of an electronically controlled access system shall be reviewed at least quarterly to ensure that unwanted physical access is revoked (e.g., temporary access).

ICT system equipment shall be located in an appropriate ICT facility or locked cabinet secured from unauthorized access or physical damage.

Within our offices we have a clean desk policy. No laptops or mobile devices are allowed in the office when the office is closed, unless locked away.

Since all data is stored in the cloud, physical access to the data center of the public cloud provider is relevant.

This cloud provider ensures that physical components are housed in nondescript facilities and physical barrier controls are in place to prevent unauthorized entrance to the facilities. Access to the facilities is only provided to employees and contractors who have a legitimate business need. Access points to the facilities are monitored by video surveillance cameras designed to record all individuals accessing the facilities. Intrusion detection systems are also in place to detect unauthorized access. All physical access is logged and routinely audited. The public cloud provider has CSA STAR Certification, SOC 1, SOC 2, SOC 3, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001 certifications.

2.2.3 Power and Air Conditioning

FintechOS has proper heating, ventilation, air conditioning systems to control the temperature and relative humidity. The public cloud provider offers even better facilities in this regard.

2.2.4 Water Exposures

FintechOS has taken reasonable precautions to minimize the impact of water exposure to the information systems.

2.2.5 Fire Prevention and Protection

FintechOS has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The fire prevention and protection measures of the FintechOS have been designed to comply with local fire safety regulations.

2.2.6 Media Storage

Security procedures define the handling conditions for the different media in order to avoid damage, loss and theft.

2.2.7 Waste Disposal

Media containing classified information that are no longer required shall be physically destroyed by authorized disposal services for media or the applicable on-site appliances, such as shredders.

Disposal of media shall be done according to the classification of the contained material as provisioned by the Data Classification Policy (IS_DCLAS_PO).

Information within the Azure ecosystem is destroyed according with NIST SP 800-88. https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

2.2.8 Off-Site Backup

Information backup is planned and performed in accordance with the established Backup Policy (IS_BACKUP_PO in place) and Backup Procedure (IS_BACKUP_PR in place), ensuring all business requirements of customers are met.

2.3 Procedural Controls

2.3.1 Trusted Roles

The employees of FintechOS have job descriptions that specify the following Trusted Roles critical for security:

- System Administrators: how to install, configure and maintain the IPSP's trustworthy systems for service management. This includes recovery of the system.
- System Operators: how to operate the IPSP's trustworthy systems on a day-to-day basis. This includes system backup.
- System Auditors: how to view archives and audit logs of the IPSP's trustworthy systems System Administrators: how to install, configure and maintain the IPSP's trustworthy systems for service management. This includes recovery of the system.
- Security Officer: responsible for the administration of and the implementation of the security practices.

2.4 Personnel controls

2.4.1 Qualifications, experience, and clearance requirements

The employees of the FintechOS have received adequate training and have all the necessary competence for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

All the employees of the FintechOS have signed a non-disclosure agreement (NDA) to maintain the secrecy of confidential information that has come to their knowledge in the course of their performance.

Any person in a Trusted Role is informed of his responsibility through its job description and/or procedures related to system security and personnel control.

All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding Fintech OS operations.

2.4.2 Onboarding procedures

This process consists of all the necessary steps taken before the onboarding of new personnel in the process including employee screening, according to applicable laws, and any other requirements, such as passing through a mandatory security awareness training before the start of daily activities.

2.4.3 Training requirements

All employees are evaluated for their job performance activities and passed through continuous training which are also openly available to them or performed on demand.

2.4.4 Sanctions for unauthorized actions

Internally defined organizational framework has identified measures or punitive actions taken against parties which have been found to be in nonconformity with organizational measures and controls.

2.4.5 Independent contractor requirements

All personnel involved throughout identity proofing process in scope, regardless of being internal or external, need to comply with internal controls and need to guarantee confidentiality through NDAs.

2.4.6 Documentation supplied to personnel

All internal procedures are communicated and available to all personnel on internal platforms dedicated for this purpose.

2.5 Audit Logging Procedures

A Log Management Policy and Procedure are defined and maintained by FintechOS.

Security events are gathered at multiple levels of the infrastructure, including applications, systems, network devices, and Microsoft Azure resources.

The Log Management Framework lists the information to be recorded for each type of logged event. This includes, in particular, the event type, the trigger, the date and time, the event outcome.

Logged events are recorded throughout the process.

The logging system is automatic from system start-up and is uninterrupted until the system is interrupted.

In the case of legal proceedings, FintechOS has defined procedures for sharing relevant logs and ensuring that they are not tampered with.

Logs are required to be synchronized on the same time. The time synchronization is ensured by using Microsoft Azure mechanisms.

Access to logs is based on least-privilege principle and need-to-know and facilitated through a RBAC Matrix.

All the records regarding the identity proofing process are stored for two months active use and archived for another 2 years.

2.6 Records Archival

2.6.1 Data types to be archived

Archival periods for FintechOS information are done according to requirements set out in Data Classification Policy (IS_DCLAS_PO) according to the business needs identified by the information owner. All other information held on behalf of clients within FintechOS managed infrastructure is done according to the clients' business needs and any other requirements.

2.6.2 Protection of the archives

All archiving activities rely on Microsoft Azure infrastructure.

2.6.3 Archive backup procedure

Archives are backed up so as to ensure their availability over time, enhanced by Microsoft Azure.

2.6.4 Data timestamping requirements

Archives requiring a date (event logs) comply with the requirements of paragraph 3.4.

2.6.5 Archive collection system

The archive collection system is based on Microsoft Azure principles.

2.6.6 Archive retrieval and verification procedure

All access to archives held in Microsoft Azure is done by authorized personnel through internal IAM process ensuring authorization and accountability for all actions.

2.7 Compromise and Disaster Recovery

2.7.1 Incident management

FintechOS has defined an internal security incident management framework comprising of the following stages: incident management, reporting, assessing, responding, learning, testing, and escalation.

Incidents are detected through a monitoring and alerting system and on the basis of event log analysis.

Based on predetermined event types, FintechOS monitors all activities involved in the process.

Throughout regular security incident management training, any possible improvement, be it supervision improvement or operational enhancement are raised and proposed for future implementation.

A vulnerability management process is defined internally in order to be able to identify and manage vulnerabilities on the information systems in scope. Multiple sources are taken into account, including threat intelligence and regular penetration tests of the solution. Critical underlying infrastructure relies on Microsoft Azure, which is constantly patched and kept up-to-date.

Vulnerabilities are addressed based on their severity, critical vulnerabilities are addressed 48 hours after their discovery. All vulnerability treatment actions rely on a risk management approach, leading either to a vulnerability patch or to a risk acceptation, depending on the patch availability or the possibility of applying a temporary fix.

Major incidents are processed as soon as they are detected, in accordance with the security incidents management procedure and including all relevant personnel in this process.

2.7.2 Business continuity management

FintechOS has a Business Continuity Policy (BCP) and Disaster Recovery Plan.

This plan is based on FintechOS study of business continuity needs and the risks of damage to continuity, to define the suitable measures. It serves two purposes: managing incidents damaging the continuity of the establishment and preventing these incidents. All critical infrastructure is provisioned in Microsoft Azure, compliant with several international standards on business continuity including ISO 22301.

The BCP in particular addresses the problem of the resumption of activity following corruption of computer resources.

The entire BCP is tested regularly, at least yearly. During given scenarios, business continuity events can be further escalated into crises, triggering specific crisis management procedures and relevant personnel involvement, including top management.

2.7.3 IPSP systems data backup and recovery

A backup policy is defined on the perimeter of the systems in scope. The ground principle is that all data are backed up. Backups are performed in Microsoft Azure according to schedules that best satisfy the client's business needs.

2.8 IPS Termination

One or more components of the identity proofing service may be terminated or transferred to another entity for a variety of reasons.

FintechOS makes the necessary arrangements to cover the costs of meeting a number of minimum requirements in the event that it enters bankruptcy or for other reasons is unable to cover these costs on its own, as far as possible, in accordance with the constraints of applicable bankruptcy legislation.

FintechOS supports reversibility services that will be triggered based on specific events contractually agreed with its clients.

3 Technical Security Controls

3.1 Computer Security Controls

FintechOS has defined the following security objectives:

- Identification and strong authentication of users for system access (two-factor authentication, physical and / or logical)
- User rights management
- User sessions management (logout after a period of inactivity, file access controlled by role and user name)
- Protection against computer viruses and all forms of compromising or unauthorized software, and software updates
- User accounts management, including quick change and deletion of access rights
- Protection against intrusion by unauthorized persons
- Network protection to ensure the confidentiality and integrity of data moving around the network
- Audit functions

3.2 Operation security

All IT operations are made according to procedures, including the provision of services.

3.2.1 Security measures related to system development

FintechOS ensures that the security objectives are defined during the specification and design phases. FintechOS uses reliable systems and products that are protected against modification. FintechOS has defined an internal SDLC process, clearly stating the necessary security controls for the system development and involvement of the Security Department throughout its stages.

Several tools also aid this process, ensuring the final product and its dependencies to not have security vulnerabilities. This is further enhanced by periodic independent tests performed by an external party.

3.2.2 Security management measures

Measures are implemented in the information system of the FintechOS, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread. Only approved software is used in the information system, according to internal defined mechanisms.

FintechOS has environment separation in place, ensured by deploying each environment in separate resource group in the Microsoft Azure infrastructure.

FintechOS uses Azure Key Vault to store all secrets. All access to this tool is only granted to authorized personnel according to their job descriptions.

FintechOS physically and logically implemented security elements for the standard flow for the purpose of filtering external and inbound / outbound connections and services through Application Gateway and local firewall at Azure resources level, encryption of communication channels, authentication of the portal exposed on the internet with digital certificate.

3.2.3 Life cycle security controls

FintechOS policies and assets for information security are reviewed at planned intervals, or, should significant changes occur, they are reviewed to ensure their continuing suitability, adequacy and effectiveness.

The configurations of the FintechOS systems are regularly checked for changes that violate the FintechOS security policies.

The Security Department approves changes that have an impact on the level security provided. FintechOS has procedures for ensuring that security vulnerability are treated according to a risk management approach and patches are applied to the system within a reasonable time frame and according to their vulnerability severity, ensuring all modifications are successfully tested and deployed within 48 hours after detecting a critical vulnerability. Any exception to security policies passes a risk evaluation and is documented as an exception.

FintechOS manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment.

3.3 Network Security Controls

FintechOS has a number of security controls applied both physically and logically for the standard flow in scope:

- Filtering external and inbound / outbound connections and services through Application Gateway and local firewall at Azure resources level
- Application-level firewall protection
- Encryption of all communication channels
- Traceability of actions using a centralized SIEM solution
- Authentication of the portal exposed on the internet with digital certificate
- Authentication through IDP solution that allows integration with customers' internal solutions.
- Systems in high availability dual configurations.
- DDOS protection

All of these elements are safeguarded using Azure mechanisms, which take into account several security principles, such as:

- Web Application Firewall – protect the front-end services
  - IP Whitelisting
  - OWASP rules
- Enforce HTTPS communication Data in transit (TLS min. v1.2)
- Site 2 Site VPN for connectivity from local network
- Isolation design for data and application layer
- Reverse proxy in front of the exposed services

3.4 Timestamping

FintechOS implements a dating system ensuring all timestamps are adequately synchronized both for internal resources as well critical Microsoft Azure infrastructure.

4 Compliance Audit and Other Assessment

FintechOS has a continuous improvement approach and thus conducts internal audits to inspect the compliance of the implementation in relation to the legal requirements.

FintechOS has an audit plan covering IT security tests (e.g., penetration testing, social engineering tests, application security testing) performed regularly by independent external security specialists. The frequency of the tests is based on the IT risk the system is exposed to, but not exceeding 12 months.

A management summary of all reports from IT security tests/audits (e.g., internal or external audits, penetration testing) are sent to the FintechOS Security Department and are communicated regularly to top management according to the severity of findings.

4.1 Subjects covered by internal audit

Internal audit is performed at least once a year:

- quarterly access logs and Firewall rules
- monthly cloud infrastructure audit through benchmarks such as Azure Security Benchmark and Azure CIS 1.3.0
- yearly – governance and documented information audit
- yearly – process audit, e.g. incident management
- yearly – internal audit ISO 27001
- weekly – DLP events analysis

4.2 External audit

External audit is performed once a year according to certification obligations (e.g. ISO 27001).

4.2.1 Conformity Assessment

Conformity audits with regard to eIDAS are performed by the Conformity Assessment Body (CAB).
The CAB must be a certified Conformity Assessment Body with regard to ETSI EN 319 403 standard.

5 Other Business and Legal Matters

5.1 Financial Responsibility

FintechOS maintains sufficient financial resources and possesses appropriate liability insurance, in accordance with national law, to cover liabilities arising from its operations and/or activities, including cyber activities.

FintechOS has the financial stability and resources required to operate in conformity with this statement.

5.2 Confidentiality of Business Information

5.2.1 Scope of confidential information

Information considered confidential is as follows:

- The personal data required by the identity proofing process
- Infrastructure
- Client information
- Event logs

5.2.2 Responsibilities in terms of protection of confidential information

FintechOS undertakes to apply security procedures in order to ensure the confidentiality of the information identified above and its integrity in the event of data exchange.

FintechOS undertakes to comply with the laws and regulations in force. In particular, it may have to make data from the remote identification process available to third parties as part of legal proceedings.

5.3 Privacy of Personal Information

5.3.1 Personal data protection policy

FintechOS complies with the European regulation 2016/679 (General Data Protection Regulation).

The right of access, rectification or opposition to personal data in accordance with the GDPR regulation may be exercised by the individuals in question by contacting FintechOS.

5.3.2 Personal information

Information considered personal is as follows: images and video with identity card, biometrics, images and videos of the end-user.

5.3.3 Personal data protection responsibility

FintechOS acknowledges that it has completed the formalities for reporting any processing of personal data, for which it is responsible.

5.3.4 Notification and consent to use personal data

In accordance with the laws and regulations in force, personal information resulting from the identity proofing process will not be disclosed or transferred to a third party except where (i) prior consent of the end-user has been give or (ii) it is necessary to fulfil any statutory requirement (e.g., court decision or other legal authorization).

5.3.5 Conditions on the disclosure of personal information to courts or administrative authorities

Any disclosure of personal information to courts or administrative authorities shall be done in compliance with the laws and regulations in force.

5.4 Intellectual Property Rights

Software shall be acquired only through known and reputable sources, to ensure that copyright is not violated.
Controls shall be implemented to ensure that any maximum number of users permitted within the license is not exceeded.
Reviews shall be carried out that only authorized software and licensed products are installed.

5.5 Term and Termination

5.5.1 Validity period

This document is applicable until further notice.

5.5.2 Early end of validity

The release of a new version of the eIDAS norms applying to TSPs, depending on the changes made, may require the need for FintechOS to change the corresponding Practice Statement.
Depending on the nature and importance of the changes to the eIDAS norm, the period within which the Statement must be made compliant will be decided according to the arrangements provided for by the regulations in force.

5.6 Amendments

5.6.1 Amendment procedures

FintechOS will ensure that any proposed modifications to its Statement still comply with the requirements eIDAS applicable norms. In the event of a significant change, FintechOS may rely on a technical inspection to monitor its impact.

5.7 Dispute Resolution Procedures

FintechOS has policies and procedures for the management and resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

5.8 Governing Law

All contractual documents are subject to the laws and regulations in force in Romania.

5.9 Compliance with Applicable Law

This document complies with the requirements set out in the laws and applicable regulations.

In particular, FintechOS complies with the regulation regarding the protection of personal data: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. In this respect, appropriate measures are taken to protect personal data.

Also, FintechOS observes the ADR (the Authority for Digitalization of Romania) Norm regarding the regulation, recognition, approval or acceptance of the remote person identification procedure using video means from 2021 and ETSI Standards: ETSI TS 119 461 - Requirements for TSP components providing identity proofing of trust service subjects and ETSI EN 319 401 General Policy Requirements for TSP.

5.10 Miscellaneous Provisions

Cases of force majeure are those considered usually accepted by the Romanian courts, in particular the case of an irresistible, insurmountable and unforeseeable event.

FintechOS should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the terms and conditions.

Identity proofing practices under which FintechOS operates shall be non-discriminatory.

Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities.