MONET +

Product brief

IDport platform: **Customer digital identity**

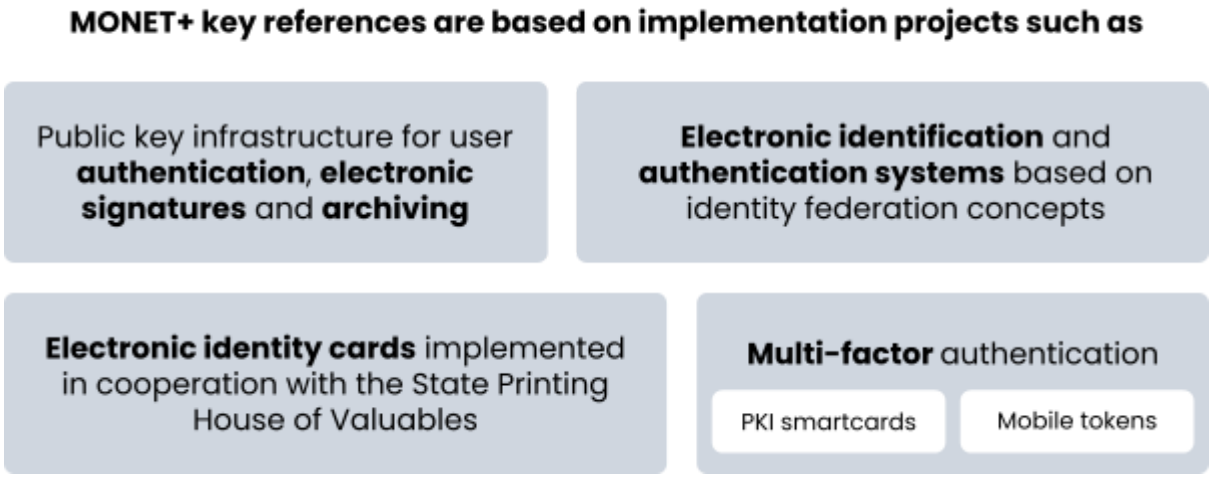
Rev no.: 2024-011

1. Table of contents

2. Management summary

MONET+, a.s. has long been recognized for its specialization in deliveries related to the processing of financial transactions, securing users' access to online electronic services such as: eGovernment solutions, Internet banking, mobile banking and other online applications, and securing access to corporate networks.

We develop solutions related to electronic user identification and strong authentication - we rely on applied cryptography technologies for smart cards, mobile and web applications and help our clients integrate heterogeneous application environments using identity federation principles.



Based on our understanding of Jonson Country requirements, this response to the RFI is aiming to propose a modern multi-factor authentication solution that is mainly based on

- Mobile key solution
- Central authentication service and identity management based on federative approach

Despite the fact that we are not directly present on the US market, we believe that we can help Jonson Country to build a modern and robust identity and access management solution that is based on our long-term experience in implementing systems for government, banking as well as commercial institutions.

3. Business solution description

3.1. Mobile key

As mobile devices are with us everyday, this makes them a perfect choice to be our key to the online world. We have created a mobile key implementation that is not only a single-purpose key but rather supports multiple use-cases and scenarios.

We are targeting especially the following scenarios

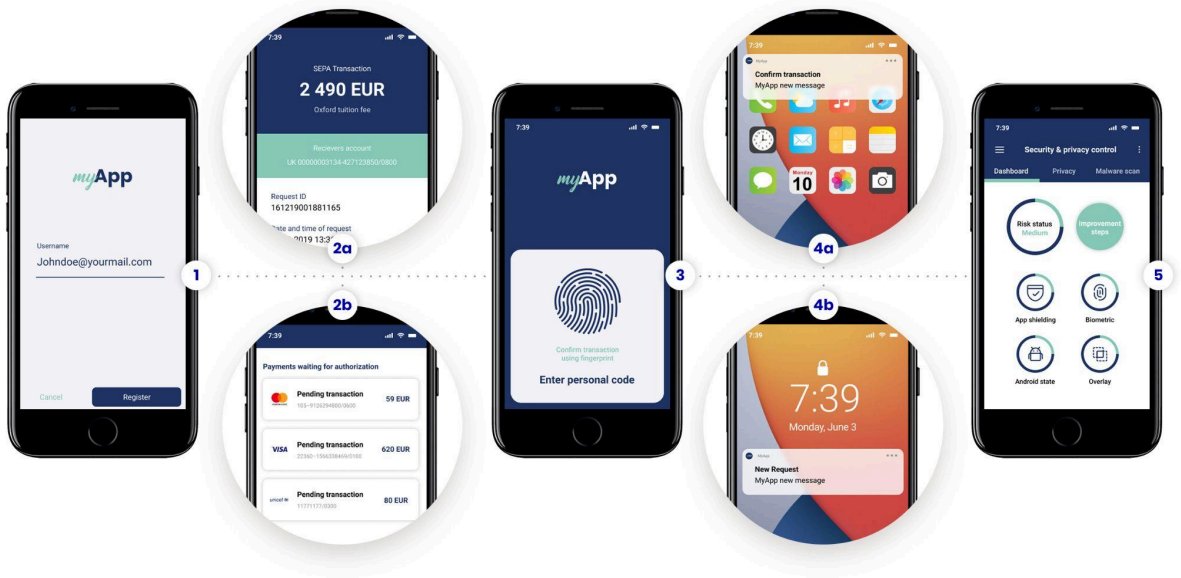
Strong authentication (2FA) without additional HW

Simple integration

Flexible onboarding

Convenient and secure access to online services - no more forgotten password

Multiple transaction types - one app approach



3.1.1. Strong authentication (2FA) without additional HW

Mobile key was created to be able to fully replace HW tokens - maintain necessary level of security, improve overall user experience and reduce costs of HW distribution.

Thus high-level security concept was created to able to cover all requirements on using a mobile app as an replacement for HW authentication tokens

- Utilizing maximum security features of mobile platforms (key store features)
- Cryptographic integrity with the mobile token back-end
- Data encryption for data on fly and data in rest
- Facilitating biometric capabilities

To improve user comfort, the mobile key performs maximum operations in online mode. Only for backup scenarios offline features are also available (OTP code generation, QR mode etc.)

3.1.2. Convenient and secure access to online services - no more forgotten password

Multiple usage scenarios are supported including

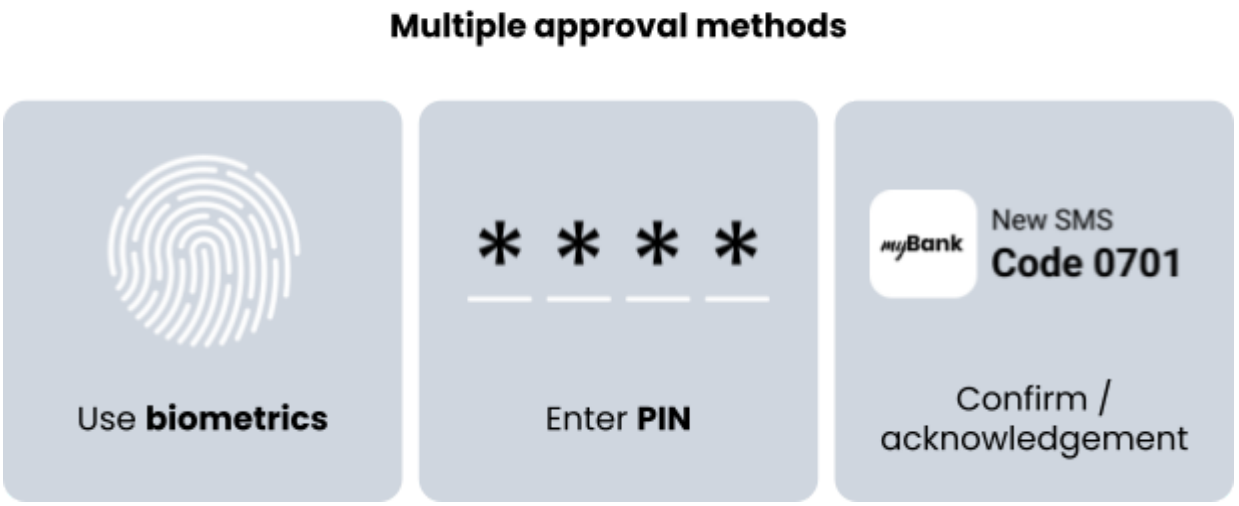
In-app scenarios	designed for applications that require in-build identity verification or transaction authorization features (e.g. mobile banking, shopping app, in-app purchases etc.)
On-device use	mobile key features are in standalone application; other applications installed on the device can its functionality directly to enable smooth customer journeys and reduce friction where advanced security is required
Mobile-to-web use	identity verification and transaction authorizations for web applications (e.g. internet banking log-in, payment approvals etc.)

Push notifications can even improve the user experience by informing the customer about news, updates and required actions.

3.1.3. Multiple transaction types - one app approach

Mobile key is not a single purpose application and needs to support multiple transaction types - logging-in to different types of applications, variety of transaction, workflow approvals and even electronic signature of documents.

We have therefore created a flexible WYSIWYS concept (What You See Is What You Sign) that is able to handle all different types of transactions.



There are multiple types of transactions that can be approved with help of IDport token SDK. The user can authenticate him-/herself or authorize financial transactions. Multiple approval methods are available, depending on business flow of the transaction:

- enter PIN
- use biometrics
- confirm/acknowledgement (online transactions only)

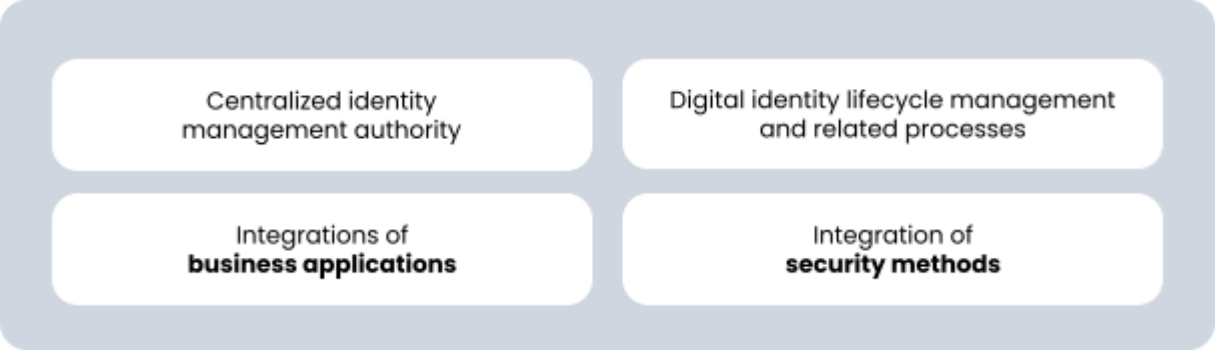
3.1.4. Flexible onboarding

As different usage scenarios are supported, IDport app supports saving the PKI X.509 certificates in the secure repository of the mobile device. The secret is also based on the PIN code number that is only known to the user. The PIN code is required to generate an OTP or to sign a transaction.

3.1.5. Simple integration

Available as SDK for existing mobile apps or standalone application for portals
Easy integration for mobile and web scenarios.

3.2. Central authentication services / Identity management



Our approach on Central authentication services is based on federalization of online applications and services (web based and mobile applications as well API services).

Monet+ is developing its own technical solutions - IDport - to cover specific requirements of identity management and authentication in controlled environments; esp. banking and government.

The main concepts is to split roles of the system to:

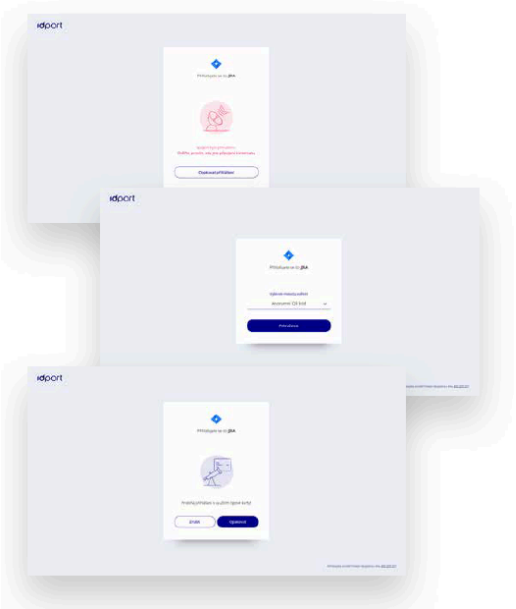
- Business oriented services, and
- Identification, authentication and authorization services.

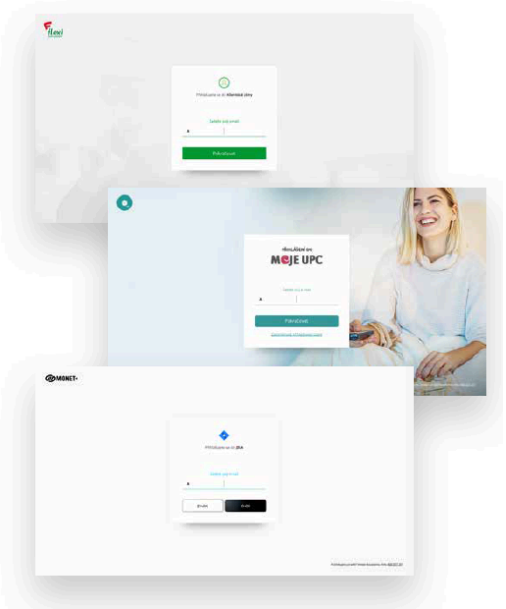
Primary responsibility of (i) Business oriented services is to provide and handle all business functionalities to the client while responsibility of the (ii) Identification, authentication and authorization services is to provide mainly:

- Centralized identity management authority

- Support digital identity lifecycle management and related processes
- Simplify integration of new online channels and applications
- Provide integration layer for security methods

Login page customization example:





3.2.1. Centralized identity management authority

The main purpose of the centralized identity management is to enable **One ID concept** across channels, multiple online applications regardless whether they are web, mobile or API based.

Centralized identity management simplifies integration of new online channels and day-to-day changes - new product implementation, new security methods, legal / regulation compliance.

3.2.2. Digital identity lifecycle management and related processes

Authentication processes covered by the solution

- Customer onboarding
- Login services - single sign-on features (incl. single sign-off and session management)
- Consent services
- Authorizations and signing services
- Fall-back and backup scenarios

3.2.3. Integrations of business applications

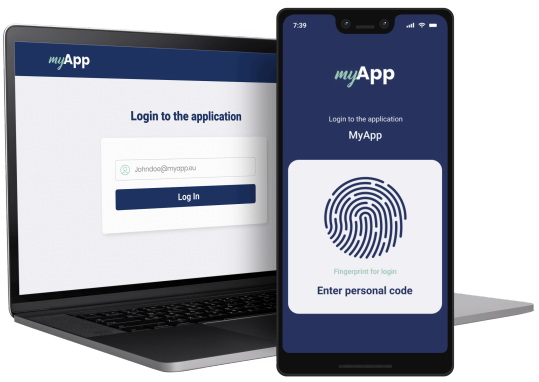
Connecting online services using widely recognized open-standards for services and identity integrations like SAML, OAuth and OpenID Connect.

3.2.4. Integration of security methods

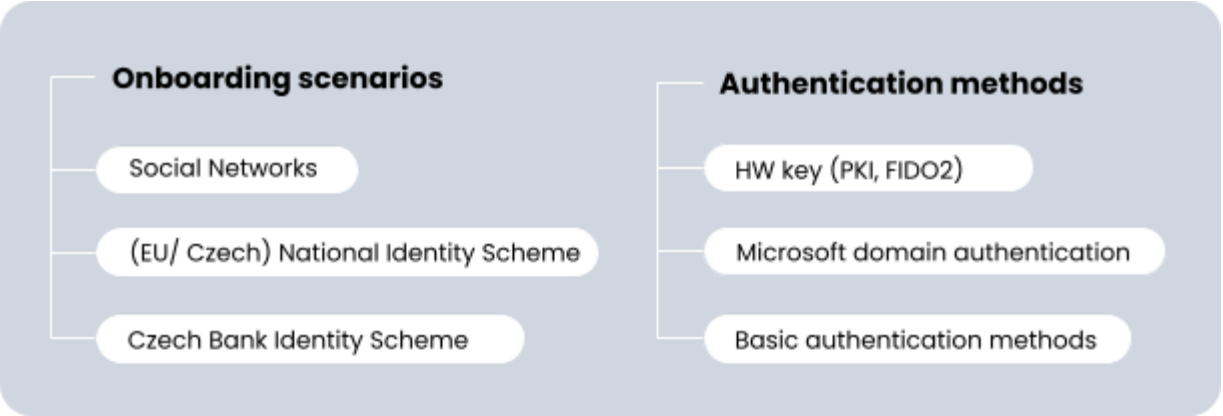
M+ is delivering a platform to enable smooth implementation of new authentication methods with minimum costs and risks.

We provide number of pre-defined (technological as well as process integration) authentication methods, including

- Static PIN and passwords
- One-time codes
- SMS codes
- Mobile token - online, offline, push notifications, deep linking
- PKI / X.509 certificate
- External identity - using SAML, OAuth, OpenID Connect
- Microsoft domain



3.3. Extensions and add-ons



3.3.1. Onboarding scenarios

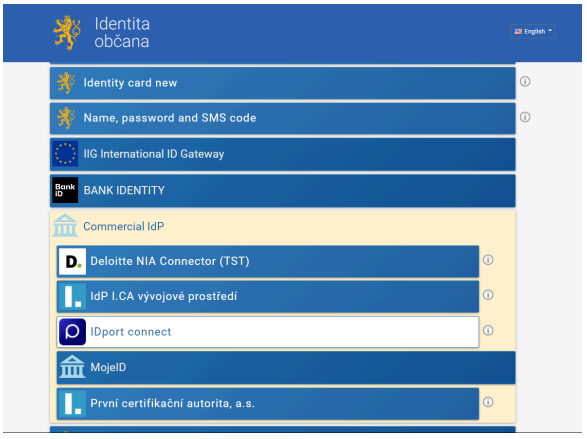
3.3.1.1. Social Networks

Use third party social network providers like Apple, Google, Facebook, Microsoft and others to enable quick user enrollment where no extra data verifications are required.

This scenario may be useful when no additional data verifications are required and only basic non-validated user data are sufficient.

3.3.1.2. (EU/ Czech) National Identity Scheme

Using the National Identity Scheme to get verified user data. Depending on the country implementation and client consent, this can provide from basic verified user data (name, address, age information etc.) to a number of additional information (ID card / passport information, additional registry information etc.)



List of integrated National Identity Schemes

- Czech republic - National Identity and Authentication service

3.3.1.3. Czech Bank iD Scheme

Czech Bank ID (https://bankid.cz/) service provides a variety of options for client onboarding, similarly as the Czech National Identity Scheme, from basic client data to full AML data sets.

List of integrated Czech BankID services

- connect - login to business services or client zone via bank identity
- sign - electronic signature of a contract or document in PDF, which makes it possible to verify who signed it
- identity - set of information for client verification or contract closing over the internet

Using this service assumes that the end-user has a bank account opened with one of Czech banks and is entitled to use this service.

3.3.2. Authentication methods

3.3.2.1. Basic authentication methods

Authentication server CASE supports a number of additional authentication and security methods. For example, we assume that the following security codes will be user:

- Activation (and validation) codes - one time numeric password used in activation processes
- PIN codes and static passwords - apart those implemented in mobile key, numeric or alphanumeric password could be implemented to support web-based authentication processes
- SMS OTP - for mobile key activation and in some other use cases we suggest that SMS OTP functionality will be implemented; SMS OTP can be also used as simple back-up mechanism for user authentication processes

3.3.2.2. Microsoft domain authentication

The Windows operating system implements a default set of authentication protocols, including Kerberos and Transport Layer Security/Secure Sockets Layer (TLS/SSL).

These protocols and packages enable authentication of users, computers, and services; the authentication process, in turn, enables authorized users and services to access resources in a secure manner.

3.3.2.3. HW key (PKI, FIDO2)

For specific web-based authentication scenarios, we have designed and are currently developing a solution IDport key and desktop client that can be widely adopted by users who are not willing to or cannot use mobile app and its security features.

This security method is very suitable for corporate clients, retail clients without mobile app and user / clients with some disabilities.

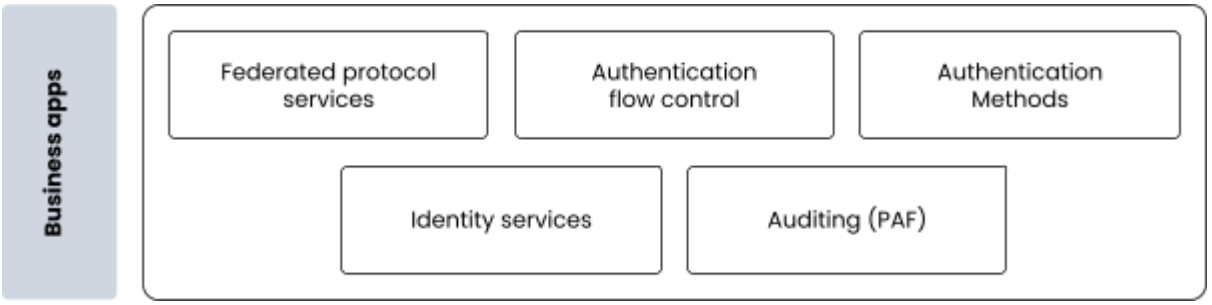
As mentioned above, the solution is based on two main components

- **IDport key** - HW key in a form of a smartcard optimized for strong and quick authentication scenarios; HW key security concept is based on PKI and ECC keys / certificates that are tied with particular HW key issued (there is no need to manage robust PKI systems and bother the user with regular certificate / key renewal process). Once expired (issued usually for 3 years validity), the client will simply get a new HW key as he or she gets his / her new payment card.
  The IDport key could be also used in contactless use-cases and therefore also suitable to combine with mobile scenarios (SDK will be available in late 2020).

- **IDport desktop** client is a native app for PC (Windows and macOS) that enables strong customer authentication scenarios for users without mobile token; it has the following key functions:
  - transaction visualization and transaction authorization
  - easy to use and simple user interface and overall usability concept
  - HW key integration (card drivers)
  - smartcard readers integration

4. Technical solution description

4.1. Architecture big picture



4.1.1. Business applications

Represents any business application that has been made available to the client in a form of native app (mobile, PC), web application or API service.

Business application is consuming client identification, authentication and related services using integration rather than direct implementation.

4.1.2. Federated protocol services

Federated protocol services (FPS) enable standards based multi-application and multi-channel identity services. Implement integrations with various identity providers.

FPS is a crucial pillar in enabling one identity concept.

Essential FPS features include

- Standards based DI integration services
  - OAuth, OpenID Connect
  - SAML
- Single login & logout, Session management with inactivity detection & resolution, Electronic identification
  - Full auth method abstraction
- Access tokens for REST API call authorizations
- Web, mobile, API friendly
- Existing custom extensions

- Social network
- NIA connector
- Bankovní identita, a.s. bank IdP services

4.1.3. Authentication flow control

Authentication flow control (AFC) enables easy implementation of multiple authentication scenarios. Especially in scenarios where multiple security methods are supported and where multi-level or multi-step scenarios are required.

AFC provides integration services to both front-end and back-end.

Essential AFC features include

- Flow control and REST API access enforcement
  - Multilevel & Multi-step authentication flow protection with session elevation
  - Authenticated session protection
- I.e. controls who can access what REST APIs
  - From anonymous to fully authenticated sessions
  - Based on level of authentication
- Supported by authentication workflow engine that turns complex authentication flows into simplicity of single transaction
- Web and native app friendly
- High performance

4.1.4. Authentication method provider(s)

Authentication methods providers (AMPs) enable integration of multiple security methods under one umbrella. This helps to significantly reduce costs on changes, improving time to market for new methods or applications. Consolidating auth* scenarios improves user experience while using security methods and as a result improves the trust of services provided.

We provided out-of-the box support for basic and strong authentication methods included in this document, however third party methods can be also integrated.

Essential AMP features include

- Components responsible for authentication means

    - Lifecycle
    - Usage
    - Identity binding
- What I see is what I sign (WYSIWYS) principle
- Highest level of security
    - eIDAS substantial level
    - PSD2 SCA compliance

4.1.5. Identity Services

Identity Services (IDS) provide an integration layer that manages actual client data. This is either done through the integration to the current IDS / IAM scheme (e.g. LDAP, CRM system etc.) or provide project implementation based on our reference API.

Essential IDS features include

- Identity lifecycle and state management
- Controls identity onboarding / offboarding
- Stores identity state, aliases, attributes, roles, consents

4.1.6. Auditing

Auditing services (PAF) are based on post-quantum algorithms to provide indisputable proofs of actions with long-term archiving functionality. Event driven architecture makes them ideal for a large number of use-cases and deployment scenarios.

Essential PAF features include:

- Audit events gathering and storage
    - Kafka / WLS JMS / REST event streaming
- Long term audit log retention with integrity protection
    - Traditional and post-quantum algorithms
    - Reliable data for dispute resolution
- IDport architecture works with “Event extracting” and “Event enrichment” principles
    - Project specific event data collection and data mining

4.2. Security concept

IDport and all its components are designed and developed according to OWASP methodologies. For the purpose of validating the methodologies we use the OWASP Application Security Verification Standard, currently implemented in version 4 of 2019.

During implementation of the project, a risk assessment and security requirements of the customer are performed to confirm target solution compliance with all requirements set.

The target solution is implemented so that used technology fulfils maximum security requirements. More specifically:

- Solution uses at least 2FA authentication and authorization methods.
- Security credentials and resulting digital signature are uniquely linked to the user who is in the role of signatory.
- Strong emphasis is placed on the use of WYSIWYS (What You See Is What You Sign) principle in all authentication, transaction authorization and document signature operations.
- System allows cooperation with a FDS system and weakens or strengthens authorization mechanisms so it maintains usability for low risk transactions and security for higher risk transactions.
- System provides real time data that can be used for further analysis of the overall security state of the environment.
- All authorization operations are electronically sealed regardless of the method used by the user for the authorization. Electronic seal contains all important data and can be used as a proof of user intention to carry out the operation.
- Handling of all credentials and sensitive data is thoroughly designed to follow best known security practice.
- Implementation emphasizes use of the most secure interfaces the given platform offer.

Resource security & client authentication

Access to all resources is secured by means of mutual TLS. Client certificate is dedicated for every instance, which means it is specific per user per app installation, and it is enrolled during the activation process.

User needs to authorize every authentication or signing request. Authorization can be done via:

- PIN (shared across all instances, verifiable only at BE, knowledge + possession)
- biometrics (device-specific, unlocks keying material verified at BE, inherence + possession)
- confirm/acknowledgement - tap / swipe (only possession factor verified)

Authorization modality is specified during request initialization. PIN or biometrics data are never cached to maximize security of the whole solution.
From a technical perspective - user is always authenticated prior to access transaction details.

4.3. System requirements

The minimal infrastructure and runtime environments requirements are

- Containerized microservices
  - Java, native core crypto, Angular based FE apps
  - Run in Docker compose, Kubernetes, OpenShift
  - "Traditional" deployment possible (JBoss, Apache/Nginx, Linux x86-64 native apps)
  - Minimal HW reqs: 4 vCPUs, 32GB RAM, 75GB HDD
- Databases
  - Oracle, PostgreSQL
- In memory caches
  - Hazelcast, most of components support also Redis
- PKCS#11 based HSMs for HW crypto and key protection

5. Implementation

Solution implementation would usually consist of the following phases and activities:

Phase	Activities of M+	Activities of Customer
Preliminary analysis	• Solution architecture. • Infrastructure requirements. • Project phases, activities and responsibilities.	• Define solution requirements with focus on business, process, security, technology, deployment and other required qualities. • Formal approval of the solution architecture.
Analysis	• Impact analysis for M+ components performed. • Integration architecture and API calls.	• Technical requirements for solution integration. • Impact analysis for Customer systems. • End2End use cases incorporating M+ technical use cases, wireframes. • Integration architecture and API calls. • Formal approval of the solution design.
Implementation	• Solution parametrization performed. • Project-based implementation (if required). • Internal testing environment setup. • Factory tests performed. • Installation instructions.	• Environments setup (DEV, TEST, INT/UAT, PROD). • Changes to impacted systems. • Integration and acceptance testing. • Resolution of design gaps during the implementation phase.
Testing	• Oncall support for integration and user acceptance testing.	• Integration testing performed. • User acceptance testing performed.
Production deployment	• Oncall support for production release.	• Go-live procedures.
Babysitting	• 2-weeks solution babysitting after go-live.	• 2-weeks solution babysitting after go-live.

6. Operation, support and maintenance

All software modules covered by this document are developed and maintained by Monet+. As part of available software support and maintenance services, the following 3rd level support services are provided

- service desk and hotline services
    - hotline and incident management system 24/7
    - Technological support 8/5
- software patches and security hotfix delivery

6.1. Hotline services

We provide global hotline services; English and Czech are supported by default.

Standard business hours to Monet+ is 9:00 - 17:00 CET; the holiday season follows the Czech calendar. We also provide 24/7 services for the hotline and incident management system.

Incident management is based on JIRA platform that enables transparent issue tracking and management

6.2. SLA and 2nd level support

All supported services will be performed from Monet+ headquarters and we are currently not planning onsite presence. This may be subject to further discussion based on respective team / bank requirements.

The following incident categories and SLA to production environments will apply

Incident category	**Reaction time**	**Resolution (work-around or fix)**
Critical	30 min.	4 hours
Medium	4 hours	48 hours
Minor	5 business days	Next release

We assume to provide basic second level services (working days, 8:00 - 18:00 CET). Premium support services 24/7 can be also discussed and agreed.

6.3. SW maintenance

Maintenance fee includes upgrades of new releases of the solution; maintenance fee cover upgrades to major releases only providing the same functionality. New features may be subject to additional license fees. Customers are notified in advance and can decide whether or not to use these new features.

7. Business model and licensing

MONET+ provides non-exclusive rights to use the software for a designated geographical location, business unit and / or designated tenant. Licensing of the solution is based on the on-premise or cloud licensing models.

The following licensing terms and conditions apply to the Program provided under this License agreement:

- Licensee is not authorized to use any part of the Program or its components without acquiring the appropriate production entitlements.
- Licensee will be required to obtain the following licenses
    - Setup license - covering solution setup and delivery to the target environment (delivery of the out-of-the functionality and preparing it for the customer environment setup; this however does not cover integration services that might be required like integrating the solution with a specific application, testing the end-to-end integration)
    - Annual license - starting after go-live; based on number of components and number of users (monthly peak) in respective geographical location, business unit and / or designated tenant.

Setup license is covering the standard implementation and from the MONET+ perspective is supported by

- project manager - to coordinate planned activities with your team
- solution architect / IT analyst - review and design the target architecture concept with you
- infrastructructure specialist - provide technical integration guide for your setup as well as installation, administration and configuration assistance

Additional professional services may included (upon mutual agreement and definition of the requirements / scope of involvement):

- Overall architecture design
- Business impact analysis
- Software development services
- End-to-end testing services
- Infrastructure management
- Security project
- Hotline services
- 2nd level technical support

8. About MONET+

8.1. Company profile

Trading name	MONET+, a. s.
legal form, registration	Joint-stock company, Registered in the Commercial Register maintained by Regional Court in Brno, section B, entry 3351
registered office	Za Dvorem 505, 763 14 Zlín-Štípa
company id number	26217783
company vat number	CZ26217783
statutory body	Ing. Břetislav Endrys – Chairman of Board of Directors Ing. Zdeněk Janda – Member of Board Ing. Jan Vavrys – Member of Board

Core competencies of Monet+

- **Transaction systems** - complex solutions for the acceptance of bank payment cards; applications for payment terminals, authorization central systems, secure solutions for the operation of all sorts of types of payment and loyalty systems.
- **Electronic identification and authentication** – systems of secure identification and authentication in electronic communication channels; technology strengthening the security of electronic banking.
- **eGovernment solution** - solutions for the area of public administration, systems for the personalization of identity documents.
- **Personalization systems & Special applications** – solutions enabling the issuance of cards and the modern identification documents; services of in-house personalization centre.

Monet+ is certified according to the ISO 9001 and ISO 14001 standards. In the area of personalization services for EMV payment schemes, Monet+ is a certified provider of MasterCard and Visa technologies.

8.2. Vendor profile MONET+

MONET+ is an expert provider of smart card and mobile technology for secure identity and payment solutions. Since 1996 we have been pioneering the business use of smart cards technology. We brought an electronic wallet and chip-based payment cards to the Czech market.

Today, we are delivering card acceptance and issuing services to major banks, retailers, transport and fleet solutions. In the area of strong authentication and authorization, we trust the smart cards and PKI. Following recent trends we are also making use of mobile platforms and alternative authentication methods, delivering authentication solutions in banking, telco, healthcare etc..

Our personalization and authentication technology protects the digital identity in electronic id documents and other applications of e-government.

We are a fully Czech joint stock company with exclusively Czech capital. It was founded in 1996 and is headquartered in Zlín, Czech Republic.

„I believe in the uniqueness of Monet+ and my colleagues. In our ability to co-create a digital world that doesn't just follow the trend of simplicity but also bears responsibility for the future.
That requires developing new ideas, innovative approaches, and above all convincing ourselves and others of the right path. This is what we strive for every day at Monet+."

Břetislav Endrys
Chairman of the board

For more than 25 years of hard work we have grown into an industry-leading software house specializing in applied cryptography for client authentication, electronic payments, enterprise ID, e-government identity, and smart ticketing in cities.

We have been engineering for over 25 years unique solutions for electronic payments and digital identity to meet the needs of large corporations, banks, and other organizations in the public sector. Monet+ powers large scale digital services used by millions of people every day in Europe, Africa, and the Americas.

Digital identity and authentication

In the area of client authentication, we develop and implement a modular system for securing user access to web and mobile services. Our open system developed a highly experienced team of over 250 professionals which set a trend in digital identity protection, allows modern third-party applications to securely access highly sensitive client data via defined API services, and in accordance with applicable legislative standards (including PSD2, eIDAS, GDPR,...).

We develop unique solutions based on continuous innovation of solutions, services and tools, reflecting the growth and development of the customer, covering all life situations of their clients.

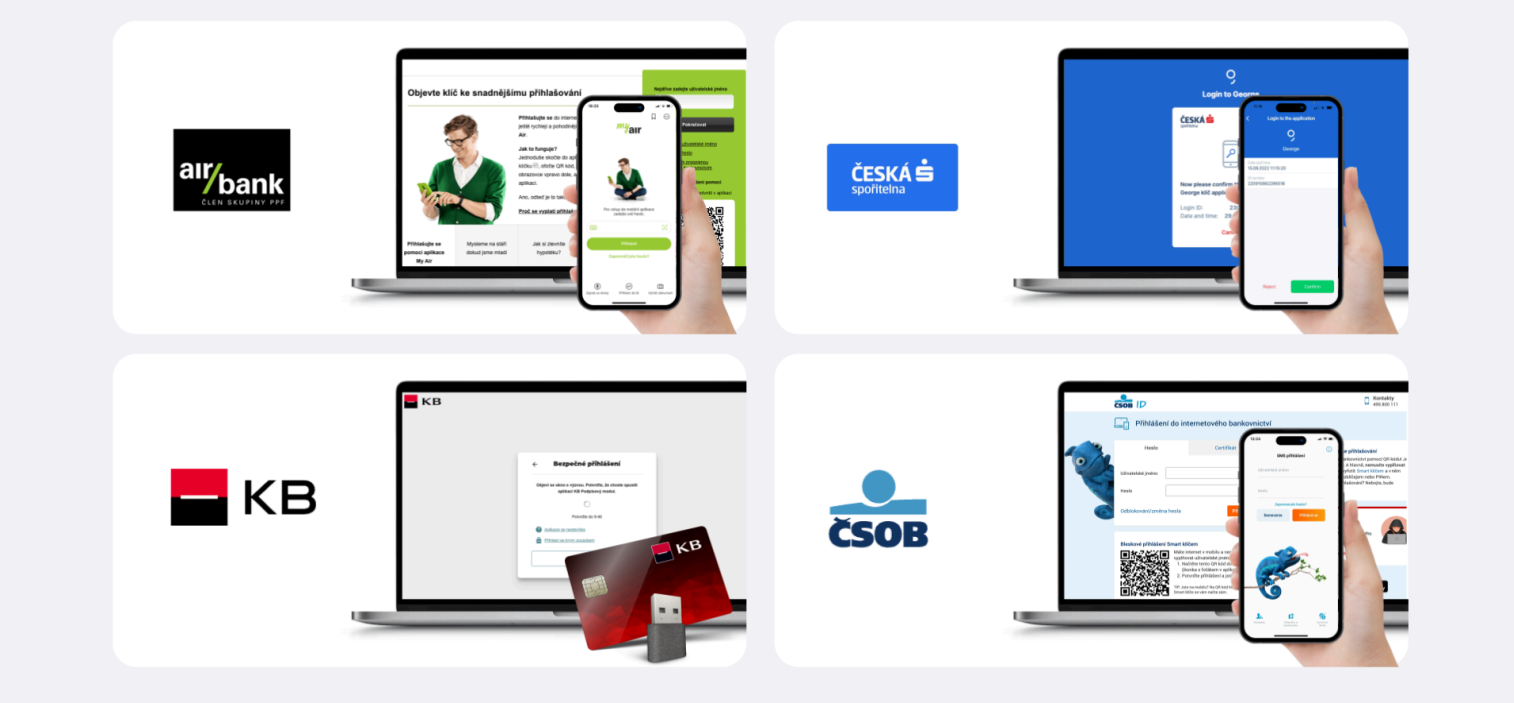
We are the market leader in authentication solutions for client security, digital identity and authentication in the electronic world. Our online solutions are used by banks, technology providers, corporations as well as government and public sector institutions within the EU.

In the Czech and Slovak market, Monet+ is the authority and natural choice for new authentication methods and ways of integrating them.

For over 5 years we have been a main partner in the delivery of uncompromising security for the largest CZ banks and we are the dominant supplier of digital identity on the Czech market. We secure hundreds of thousands of online transactions every day and our modular solution for two-factor authentication is relied on by over 5.5 million Czech citizens of leading Czech banks, including Česká spořitelna a.s., ČSOB a.s. and Air Bank a.s.. We protect as well the billions CZK of the financial assets of our clients' customers.
We help our customers manage and protect their clients' digital identities. Our solutions covers the entire lifecycle, from onboarding, through routine operations to dealing with non-standard situations. It is built on longtime experience and investment in digital identity and its security, robustness and scalability.

Our customers appreciate the high professionalism of our team, the robustness of the solution, its high level of security, modularity and user comfort. Thanks to its high penetration among users, security and simplicity, the mobile key developed by us has become an integral part of electronic customer service and an important accelerator of digitization of services.

8.3. Selected references



6 Banks

- authentication solution with mobile key authentication
- authentication methods based on OTP technology
- authentication solution based on mobile token to secure retail online channels
- mobile key as comfortable method for secure logon and validation of transaction
- the solution simplified authentication and payment authorization
- electronic identification and user authentication
- the central administration of security methods
- the solution consolidated the processes of electronic identification and authorization, including UX / UI principles
- interoperability with third parties, employing federated identity principles/services

2 Insurance

- mobile key as comfortable method for secure logon
- the solution simplified authentication and authorization
- electronic identification and user authentication
- interoperability with third parties, employing federated identity principles/services

	• the solution consolidated the processes of electronic identification and authorization
32 Municipalities	• building of PKI including documentation • HSM supply • applications for cards and certificates • cards and readers supply
58 Hospitals	• smart card delivery (USB Token, Hybrid Cards) • smart card management applications
National Security Authority	• Czech Republic security authority • smart card delivery (USB Token, Hybrid Cards) • smart card management applications
Czech Social Security Administration	• social insurance • building of PKI including documentation • smart cards, usb, readers • applications for cards and certificates • 9.000 active users
13 Regional authorities	• smart card delivery (USB Token, Hybrid Cards) • smart card management applications • Public key infrastructure
Center for Regional Development	• administration and control of the use of EU funds • building of PKI including documentation • smart cards, usb, readers • applications for cards and certificates
3 Ministries	• public key infrastructure • smart card delivery (USB Token, Hybrid Cards) • middleware for smart cards • approx 25.000 active users • system applet for protection against chip misuse • middleware for authentication and electronic signature • mobile and desktop application for authentication with electronic ID card for Windows, Linux, macOS, Android and iOS platforms