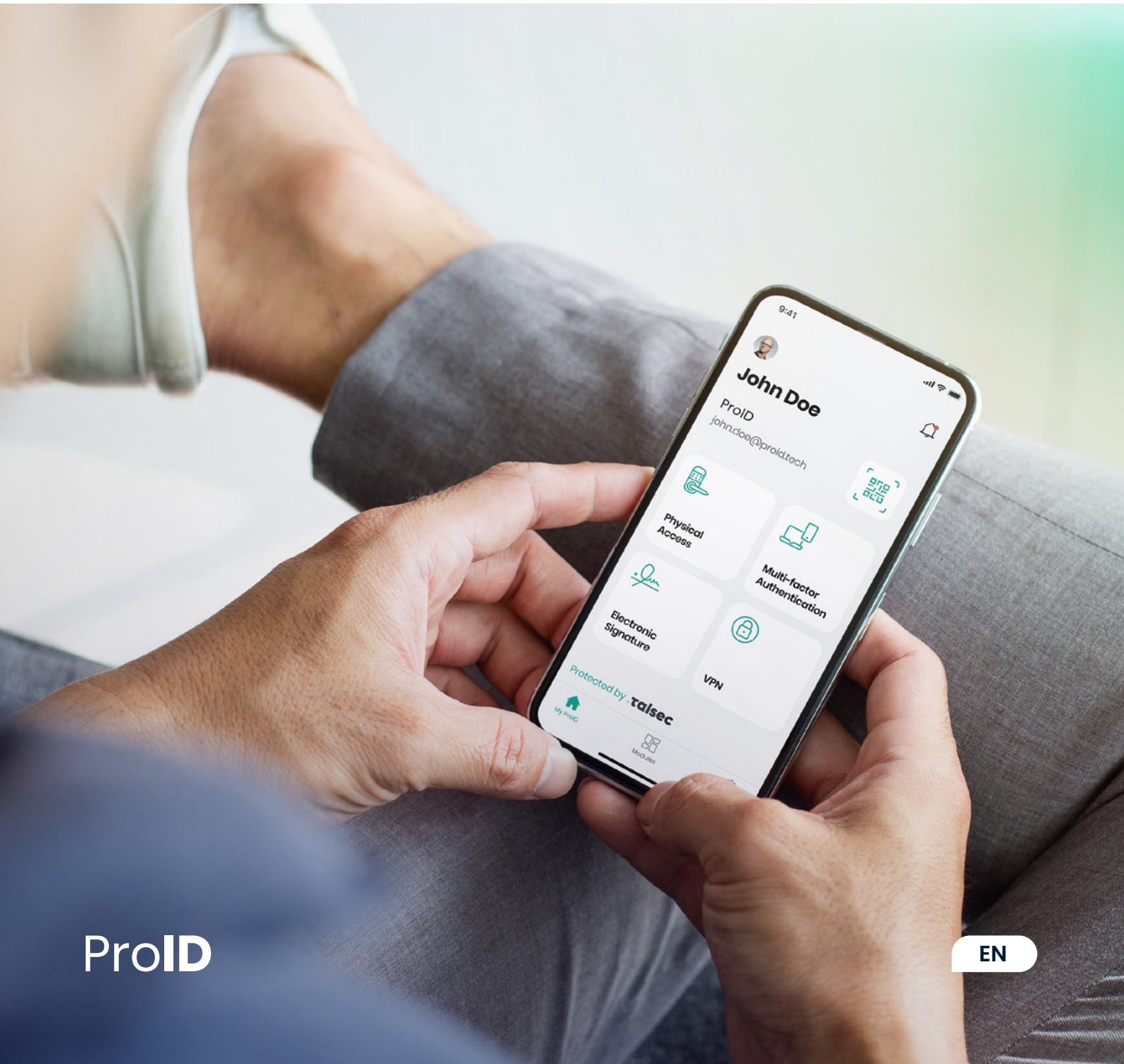
ProID

Workforce Identity White Paper



ProID

EN

ProID

Secure Digital Identity for Employees and Organisations

Today, digital identity is everywhere, making our everyday public and professional lives easier. But how do we ensure that it is truly secure while remaining user-friendly?

Over the past few years, the number of cyberattacks on organisations of all types and sizes has increased dramatically. These attacks cause long-term service outages and massive financial damage. With the advancing digitization of business processes and the development of the international situation, it can be expected that **cyber threats will continue to grow**.

It is a sad truth that **80% of successful cyberattacks** are caused by the breach or **theft of the login credentials** of **the employees** themselves or **the privileged accounts of** administrators who have access to all systems and interfaces. However, the same danger applies to access to the interfaces of technical elements (servers, OT infrastructure, smart metres, etc.).

But a secure digital identity doesn't have to be a scarecrow anymore. The solution is not to use even longer, more complex and virtually unmemorable passwords. There is another way. Convenient, user-friendly and yet as absolutely secure as possible.

ProID Enterprise Security Platform

ProID is a modular platform for securing organizations **focused on work and technical identity**, completely developed by MONET+.

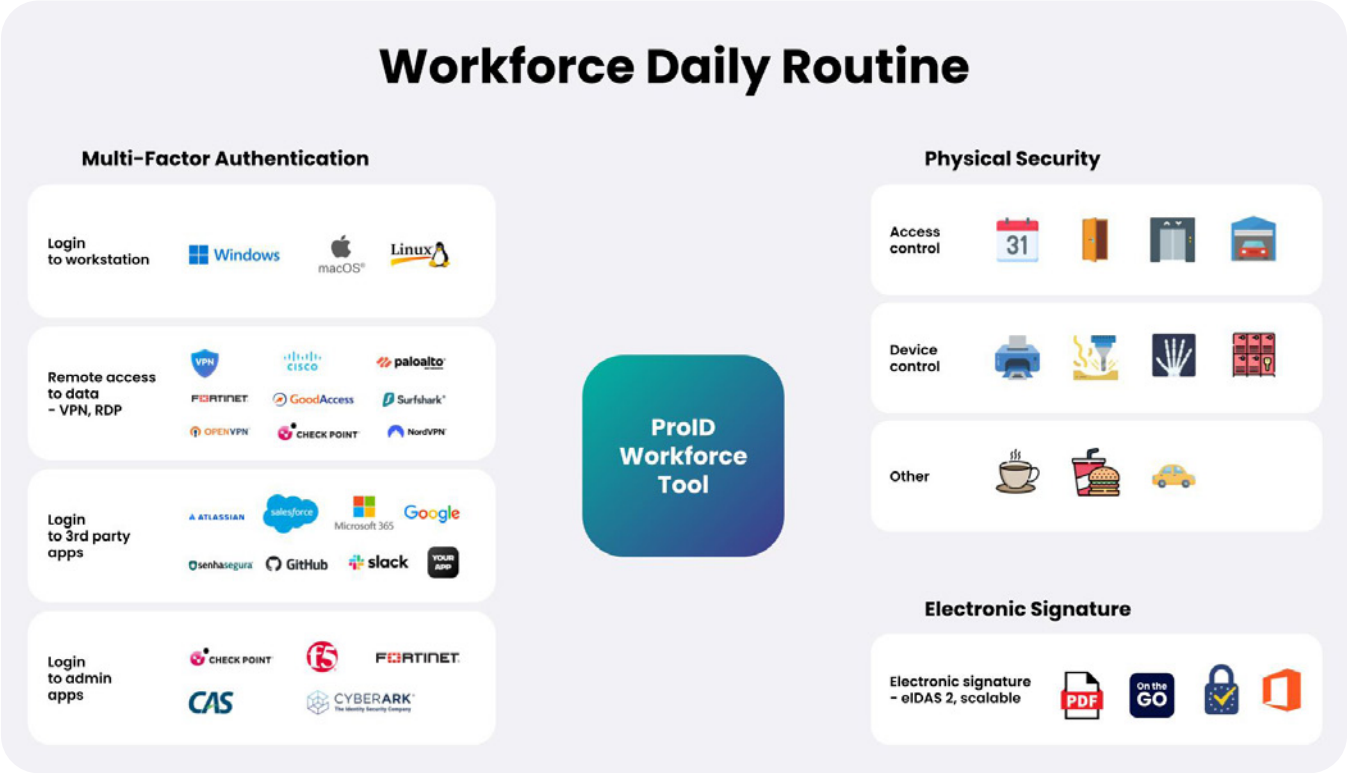
It provides protection for **more than 170,000 users** in more than **180 organizations across a wide range of verticals** – fintech, telcom, healthcare, utilities, manufacturing, public sector, and more.

EIDAS 2 | NIS 2 | ISO 27001 | TISAX | DORA

info@proid.tech | +420 577 110 411 | www.proid.tech

ProID Workforce
Secure Employee Identity

ProID offers methods and tools that do not look at the issue of security only from the point of view of solving a certain part. On the contrary, it strives to provide a comprehensive solution that brings together all the needs of the employee during their daily work routine.



ProID Workforce covers all 3 basic areas of an employee's digital identity:

1. **Multi-factor authentication** - Secure and user-friendly login to various systems and applications.
2. **Electronic signing and sealing** of digital documents up to the highest qualified level.
3. **Physical identification** of employees using a contactless chip (printing solutions, attendance, access and catering systems, etc.).

ProID Workforce tools and management

ProID Workforce offers validated employee identity tools that are able to meet even the most demanding customer requirements and scenarios:

1. Multifunctional ProID **smart card** and its various variants.
2. **ProID Mobile App.**
3. Bittron **HW Token with Mobile Authentication App.**

The ProID Workforce includes modular management for process automation and simple management of ProID tools.

All the tools can be combined within one organisation according to the needs of individual users, and at the same time each user can have multiple tools for the most suitable combination.

The entire ProID platform can be delivered on-premise to the customer's environment or used as a service (SaaS).

Multifunctional ProID Smart Card

Smart cards are a proven and time-tested means of securing the identity of an employee. Historically, they were mainly used to secure access to protected areas. We have added additional features to our portfolio that make them a tool for ensuring both physical and logical security.

Key features:

- FIDO2 compliant – passwordless authentication, also contactless.
- Bestseller, a proven tool for ensuring an employee's digital identity.
- Secure storage of digital keys and certificates.
- Works even in offline mode.
- Certified tool listed on the EU Trusted List.

Possible uses:

- **Employee ID card**
  It fulfils the function of personal cards thanks to the possibility of graphic personalization of cards.
- **Multi-factor authentication**
  A tool for MFA verification to systems and applications (MS, Linux, MacOS), VPN, RDP, and third-party applications.
- **Contactless function**
  The cards support most contactless technologies/manufacturers (Mifare DESfire, HID, Legic, etc.) and can be connected to attendance systems, payment records (e.g. lunches) and external devices (printers, turnstiles, elevators...).
- **Electronic signature**
  The Chip cards are equipped with a certified QSCD chip and allow the creation of qualified electronic signatures according to applicable legislation and EU regulations.
- **Offline mode**
  It does not depend on online certificate authentication.

We also supply related products (card readers, printers for printing, etc.) and a wide range of modules for administrators and administrators.

ProID Mobile App

The mobile phone has become an integral part of the work routine of most employees. It is a device that they have with them always and everywhere and they are used to solving more and more work tasks on it. We have made it a new tool for corporate security.

Our ProID Mobile app is available for both Android and iOS and supports **passwordless access** using biometrics.

Key features:

- A very user-friendly method with a high level of security.
- Elimination of passwords (biometrics support).

- Integration of multiple methods (push notifications, OTP generation, SMS).
- "Island mode" (offline scenarios) in case of crisis situations.
- Possibility of full on-premise deployment.
- Supports contactless user identification (Legic, HID, NXP, etc.).

Possibilities of using the ProID Mobile application:

- **Multi-factor authentication**

  A tool for MFA verification to systems and applications, VPNs, RDP and third-party applications, or custom applications.

- **Contactless functions**

  Enables contactless functions such as control of turnstiles and lifts, unlocking locks or controlling external devices (for SDK Legic Connect, HID and Mifare 2Go).

- **Electronic signature**

  It allows you to create advanced and qualified electronic signatures directly from your mobile phone.

Bittron HW Token with Mobile Authentication App

The tool combines the unique features of a USB HW token and a mobile authentication application. It is completely developed by our company and meets the highest safety requirements. It contains a qualified chip integrated with the reader into the USB token. Individual actions (confirmation, electronic signature...) then take place in the connected mobile application.

Key features:

- The most secure method due to an additional factor (application using biometrics).
- Supports FIDO 2.
- Works even in offline mode.

Possibilities of using the Bittron HW token:

- **Multi-factor authentication**
  A tool for MFA authentication to systems and applications (MS, Linux, MacOS), VPN, RDP and third--party applications conveniently using biometrics (Touch ID, Face ID) or PIN.
- **FIDO 2 support**
  Signing in to web applications that support this protocol.
- **Automatic logout when moving away from the PC**
  If the USB stick detects that the mobile phone has moved away from the computer, it will automatically log the user out and lock the computer (optional).
- **Qualified electronic signature**

  Our USB Key Is a certified means of identification according to the European eIDAS Regulation with a high level of trust, so you can sign even the most important documents with it.

- **Offline mode**

  It is not dependent on online verification of certificates, because you carry them all on a chip with you. It communicates with the mobile phone via an encrypted Bluetooth channel.

ProID tool management modules

To simplify the management of ProID Workforce tools, we offer modular management for users and administrators of the organisation. **It centralises and automates** complex operations associated with tool management. It simply **implements the required processes** and allows for **easy configuration** of ProID tool lifecycle management requirements.

Key features:

- Significant acceleration and automation of all processes.
- Elimination of errors.
- Ensuring the system security of the organisation.
- Cost and time savings.
- Intuitive control.

Possibilities of using ProID modules:

- **Organisations under control**

  The modules offer a perfect overview of all tools, users and certificates within the organisation, regardless of its size.
- **Coverage of important scenarios**

  User onboarding, assignment of user tools and their management, or key and certificate management, card printing, etc. All this in real time and without complicated steps.
- **Part of internal security**

  The modules are a central database and a backup of certificates and keys in case of crisis scenarios, including the possibility of searching and logging.
- **User roles**

  The modules are designed for admins and administrators, as well as for HR departments (issuing or printing smart cards) and end users (automatic renewal of expiring certificates, QPIN storage, etc.).
- **Cloud or On-premise**

  The modules can be installed both at the customer‘s premises on their servers and workstations and operated as a service (SaaS).

Use case overviews

Visual ID	✓	✗	✗
Login to computer	✓	✓	✓
Login to VPN	✓	✓	✓
Login to RDP	✓	✓	✓
Login to various applications (M365, Gsouite, ...)	✓	✓	✓
Electronic signature	✓	✓	✓
Access control	✓	✓	✗
Device control	✓	✓	✗
FIDO2	✓	✗	✓

ProID eSign - System for Remote Qualified Electronic Signature

With the digitization of documents and the idea of „paperless“, it is necessary to ensure that such documents have the same legal weight as printed ones. This is made possible by means such as a qualified electronic signature, seal or time stamp. One of the most effective ways for organisations to create them is remotely. This eliminates the use of resources with a stored certificate, the signature is available from anywhere, it also works on a mobile phone and allows central management of all certificates.

Our Remote Sign system combines the convenience of remote signing with maximum security. It is installed directly inside the organisation as ''on-premise'', including all necessary components.

Part of the solution is our own certified SAM module, which is listed on the EU Trusted List. It is used to authorise the signature process.

Why choose this solution?

- It provides user convenience, is easy to use and eliminates the need to be physically present in the branch.
- Intuitive control, passwordless.
- Digital document management and creation with full legal force easily and from anywhere.
- Device-specific independence, can be used on laptop, tablet and mobile phones.
- Certified solution according to eIDAS 2.

Possibilities of using the eSign system:

- **Signature, seal, stamp**
  Qualified electronic signature, qualified electronic seal and time stamp from anywhere and from any device, including smartphones and tablets.
- **Integration into organisational systems**
  The possibility of connection with records management or existing applications (CRM, ERP, invoicing and ordering systems, etc.).
- **Business Opportunity**
  The organisation itself can be an electronic signature provider for its customers, suppliers, or subsidiaries.

Systems for the management of technology certificates

Not only humans, but also various devices and technical equipment already have a digital identity. Moreover, the number of such technological elements is growing exponentially and so are the associated security risks.

OT infrastructures, servers, sensors, measurement systems, sophisticated production machines, hospital equipment and a host of other devices communicate with corporate networks and receive or send sensitive data on a daily basis. An attack can cause the collapse of an entire organisation and disrupt operations for days. That is why we have extended our identity solution with a part that protects vulnerable technical elements.

Why choose this solution?

- Universal use to manage the identities of technical elements across the entire organisation.
- Ability to link to employee identity.
- Use of state-of-the-art cryptographic algorithms.
- Based on Public Key Infrastructure technology.

Possibilities of using the systems:

- **Central Management Point**
  The Systems provide a central location for securely storing cryptographic material, performing cryptographic operations, and controlling access based on user roles.
- **All-in-one solution**
  Systems are integrated with certificate management modules, domain PKI and certificate authority.
- **KMS (Key Management System)**
  Enables encrypted communication between devices, servers and applications, import and distribution of cryptographic keys.
- **Certificate Lifecycle Management (CLM)**
  Effectively manages the lifecycle of technology certificates. Ensures critical scenarios (automated issuance, ID checking, and certificate requests...) as well as supporting processes for central certificate management.
- **Support for global protocols**
  The systems work with widely used protocols and ensure their integration into a single interface (ACME, SCEP, EST, Proprietary protocol...).
- **Supporting HW**
  The solutions also include the supply of the necessary HW resources (HMS servers, tokens, smart cards...).