IDENTITY AND ACCESS MANAGEMENT

Synera is a leading provider of high-tech cybersecurity solutions, with more than 30 years of experience in the industry. Our expertise in cryptography allows us to offer a full range of products and solutions to meet a variety of security requirements, from the most stringent requirements to everyday corporate needs. We specialize in authentication, digital signatures, data and information systems protection.

Our solutions are trusted by governments, vendors and corporations worldwide. We help our customers meet e-government requirements, secure remote offices and teams, protect communication channels between organizations, protect sensitive data, and authenticate professionals who work with sensitive information, such as doctors and lawyers. We also offer secure document management and banking security solutions in line with international standards.

We understand the complexity and ever-changing nature of cybersecurity risks, and our goal is to provide cutting-edge solutions that keep our clients one step ahead. Best practices from different countries are now available worldwide thanks to Synera solutions.

Multi-factor-authentication

In the world of cyber threats, Multi-factor-authentication (MFA) is becoming a grand challenge. Attackers not only need to compromise credentials, but also gain access to the device with a second factor. This robust defense strategy significantly increases the effort and time required to capture credentials, preventing mass hacks.

Identity Provider (IDP) allows businesses to issue certificates to employees and devices to ensure that the credentials presented are always authentic. Single-Sign-On (SSO) provides ease of access with maximum security. Remote-Access VPN and Remote-Access TLS allow employees to work r emotely while maintaining data confidentiality and integrity, eliminating the possibility of data interception during remote communications. Privileged Access Management (PAM) regulates elevated user privileges, minimizing security threats and helping to segregate access according to the needs of a particular organization.

» Combining MFA solutions provides a balanced defense against cyber threats, enabling organizations to effectively manage access, secure data and improve the user experience. Integrated Synera solution is designed to provide secure and convenient authentication and to build a customized identity and access system.

Our solution:

- Multi-factor-Authentication (MFA)
- Identity Provider (IDP)
- Single-Sign-On (SSO)
- Remote-Access VPN
- Remote-Access TLS
- Privileged Access Management (PAM)

The Power of PKI for Any Scale and Purpose

A PKI is a system used to secure data transmission over a network, based on public key cryptography. A PKI integration solution can help organizations configure and manage their certificates, digital signatures and data encryption.

One of the main benefits of a PKI is the ability to transmit data securely over an open network such as the Internet. However, setting up and managing a PKI can be a complex process that requires a high degree of expertise and knowledge.

A PKI integration solution can help organizations automate the process of managing and using certificates and digital signatures, reducing the time and resources required to support data security. Such a solution can also provide additional features, such as certificate usage auditing and automatic certificate updates, which can significantly improve an organization's security.

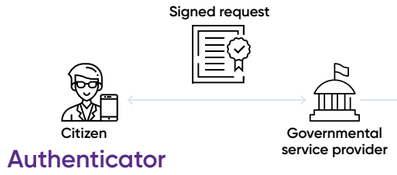
- Some PKI integration solutions can also provide out-of-the-box integrations with other security systems, such as access control and identity management systems, to create more comprehensive security systems.
- The main feature of PKI is scalability. Once properly implemented, the infrastructure allows digital services to grow. A PKI can be deployed within a private organization as well as within an entire country or across multiple countries for secure international interaction.

Protection of interaction with state information services

Today, many organizations and individuals use various digital services almost daily to provide access to government services. Among them there are submissions of tax returns and tax statements receiving, registration of goods by manufacturers, participation in electronic auctions, and etc.

- Synera authenticators help protect access to personal accounts from intruders using two-factor authentication, and also allow to generate a digital signature for signing legally significant documents.
- Synera authenticators act in this case as a reliable alternative to login-password authentication using in governmental information systems.

Our solution:



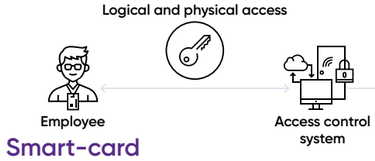
- State PKI
- Digital Signature Server
- Authentication Server
- Hardware Security Modules (HSM's)

Access control to premises and information systems

As a rule, modern organizations use contactless employee cards exclusively to control access to office and industrial premises (ACS systems). At the same time, access to information systems is carried out using a login-password combination, which leads to vulnerabilities in the security of enterprise data.

- Synera smart card combines the functions of a pass and a token for accessing the company's internal information systems and participating in EDM.
  Strengthening the protection of access to corporate information systems is achieved through strong two-factor authentication, where the first factor is the possession of a physical device – a token or a smart card, and the second is the knowledge of a PIN code to access the device.
- The implementation of cryptographic encryption algorithms is carried out "on board" Synera smart cards, without transferring keys to the memory of a computer or smartphone.

Our solution:



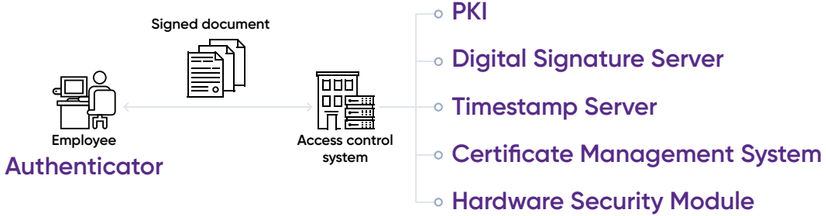
- PKI
- Authentication Server
- Certificate Management System
- Privileged Access Management
- Hardware Security Module

Protection of internal corporate document flow

The ability to certify and transfer electronic documents within the organization significantly speeds up business processes and eliminates the need to store significant volumes of paper documents. At the same time, the use of EDM systems implies compliance with certain information protection rules – organizing secure registration and authentication of users, preventing unauthorized access to documents during transmission, and ensuring the legal significance of electronic documents.

» Synera authenticators are using cryptographic algorithms for data encryption, strong two-factor user authentication and digital signature, including mobile devices, are capable of solving the tasks set effectively. Storing user authentication allows to ensure their reliable protection.

Our solution:



Secure remote banking and mobile banking protection

The development of remote banking systems (RBS) has accelerated significantly during the pandemic and remote work, finding new growth points for such systems. At the same time, fraudster attacks on RBS systems have intensified, and through these systems intruder can attack the infrastructure of financial organizations and their clients.

- One of the elements of protection against the actions of cyber fraudsters is the use of multi-factor authentication technologies. Synera authenticators devices help financial institutions to identify users of the Internet Bank, thereby strengthening both information security and customer loyalty.
- Synera hardware and software authenticators working on mobile devices provide strong two-factor authentication and confirmation of transactions using a digital signature.

Our solution:

Authenticator

- PKI
- Digital Signature Server
- Authentication Server
- Timestamp Server
- Certificate Management System
- Hardware Security Module

Support for mobile teams

The need to search for and fill out paper documents, as a rule, creates a lot of difficulties for specialists of mobile teams (oil workers, miners, power engineers, forwarding drivers) performing work in difficult conditions in remote areas. Use of electronic document management (EDM) on mobile devices greatly simplifies the receipt and confirmation of orders, filling in the necessary forms and reports, execution of many other documents.

- Synera certified cryptographic devices in EDM ensures the security and convenience of a mobile digital signature. With a minimum of effort and maintaining the continuous business processes, the user gets the opportunity to sign the necessary documents with a digital signature via an NFC wireless channel.
- In this case, the digital signature key is stored separately from untrusted mobile devices and applications for document management.

Our solution:

Smart-card

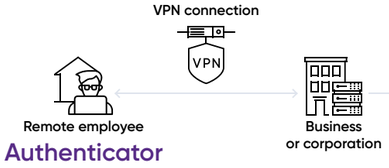
- PKI
- Digital Signature Server
- Authentication Server
- Timestamp Server
- Certificate Management System

Organization of secure remote work

The remote work has become a modern reality for business. An initially forced measure has become an integral element of the organizational and corporate culture, which requires close attention to the security of corporate data and infrastructure. There are risks of financial and reputational losses, and in some cases — the threat of termination of the organization's business processes.

- Setting up two-factor authentication using hardware or software authenticators in integrated solutions for organizing remote work will help prevent the theft of logins and passwords and unauthorized access to the corporate network.
- Two-Factor Authentication is the most secure authentication method. Two types of factors are used: Possession of authenticator — and knowing the PIN. Even having compromised the PIN code, an attacker needs to have to authenticator, the theft of which is always detected promptly. More advanced authentication can be added to improve security, for example — biometrics.

Our solution:



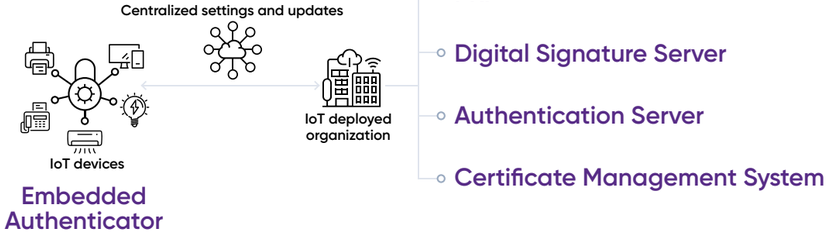
- PKI
- Digital Signature Server
- Authentication Server
- Privileged Access Management
- Certificate Management System

Protection of machine-to-machine interaction in IoT

Over the past years, IoT devices have become an absolute reality in business, industry and everyday life. Autonomous sensors, energy consumption meters, smart household appliances, smart cameras, all this works without the direct participation of a person, generating and processing data arrays. This data needs to be protected, as the machine-to-machine environment is extremely vulnerable to attacks by intruders. After all, IoT devices are often located in a public space or on the territory of a potential attacker. Such an intrusion can result in confidential data leaks, reputational and material losses, production process shutdowns, and even industrial disasters.

- Integration of cryptographic protection Synera tools into IoT devices can provide control over the integrity and ownership of data through a cryptographic digital signature. Thus, the interaction of the user's IoT devices only with legal devices or operators will be conditioned.
- Reliable storage of cryptographic keys that never leave their carrier will negate the likelihood of disclosure and forgery of important information.

Our solution:

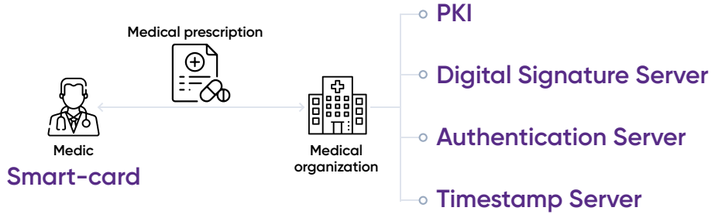


Organization of remote work of emergency services

Ambulance crews, firefighters , environmentalists, law enforcement officers and other services working on the road are actively using mobile devices for electronic document management today. This allows to reduce time and avoid difficulties when processing paper documents, preventing risk of their loss.

» The use of Synera authenticators by field teams allows them to participate in electronic document management by signing legally significant documents with a digital signature on a mobile device with one touch.

Our solution:

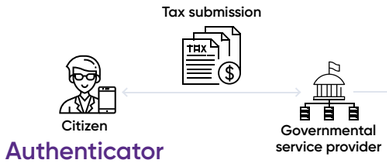


Issuance of digital signature certificates at the CA of the tax service

The work of organizations, entrepreneurs and notaries today cannot be imagined without so important in business processes tool as a digital signature. The norms of the legislation prescribe the use of digital signature for reporting, participation in auctions, conducting electronic document management with the state, confirming the purchase and sale of dairy products in a single state automated information system for recording the volume of production and turnover of diary products, registering online cash desks and many other applications. Issuance of digital signature certificates carries out the certification center of the tax service, trusted certification centers, as well as accredited CAs.

» Synera authenticators and are protected with built-in cryptographic algorithms to generate a digital signature safety with no intrusion possible. That allows to be sure that only authorized access is possible.

Our solution:



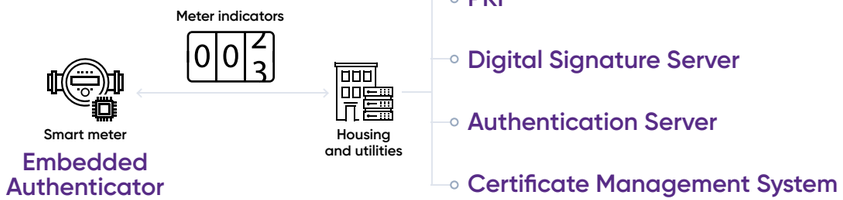
- PKI
- Digital Signature Server
- Authentication Server
- Timestamp Server
- Certificate Management System
- Hardware Security Module

Protection of "smart" meters in the GIS housing and communal services system

The use of "smart meters" in the state information system of housing and communal services helps to automate the taking of readings, transmission and accounting of data on consumed resources. However, the fact that metering devices are located outside the perimeter of the information system (in fact, on the territory of a potential intruder) makes them unprotected from various kinds of physical and information influences, casting doubt on the reliability of the data transmitted to the management company.

» Synera IoT protection devices built into smart meters, through the use of strong cryptographic authentication, guarantee the reliability and integrity of the information transmitted to the management campaign and, as a result, the formation of a correct single payment document.

Our solution:



Product catalog Synera

Identity and Access Management

Workforce:

- Multi-factor-Authentication (MFA)
- Identity Provider (IDP)
- Single-Sign-On (SSO)
- Remote-Access VPN
- Remote-Access TLS
- Privileged Access Management (PAM)

Customers:

- Mobile Authentication
- Cloud Authentication

Data Protection

- Digital Signature
- Timestamping
- Data Encryption
- Hardware Security Module (HSM)
- Tokenization
  - OTP Authentication
  - USB-Token Based Authentication
  - Software Authentication
  - Smart-Card Based Authentication
  - Smart-Card Readers
  - FIDO 2 Authentication
  - Biometric Athentication

Public Key Infrastructire (PKI)

- Certification Authority (CA)
- Key Management
- Certificate Management

IoT Security

- Embedded Protection
- Software Protection

Software Monetization

- Software Licensing and Protection
- Reverse Engineering Protection
- Embedded Protection
- Software Sales Management

synera

Innovations that shape future

synera.global