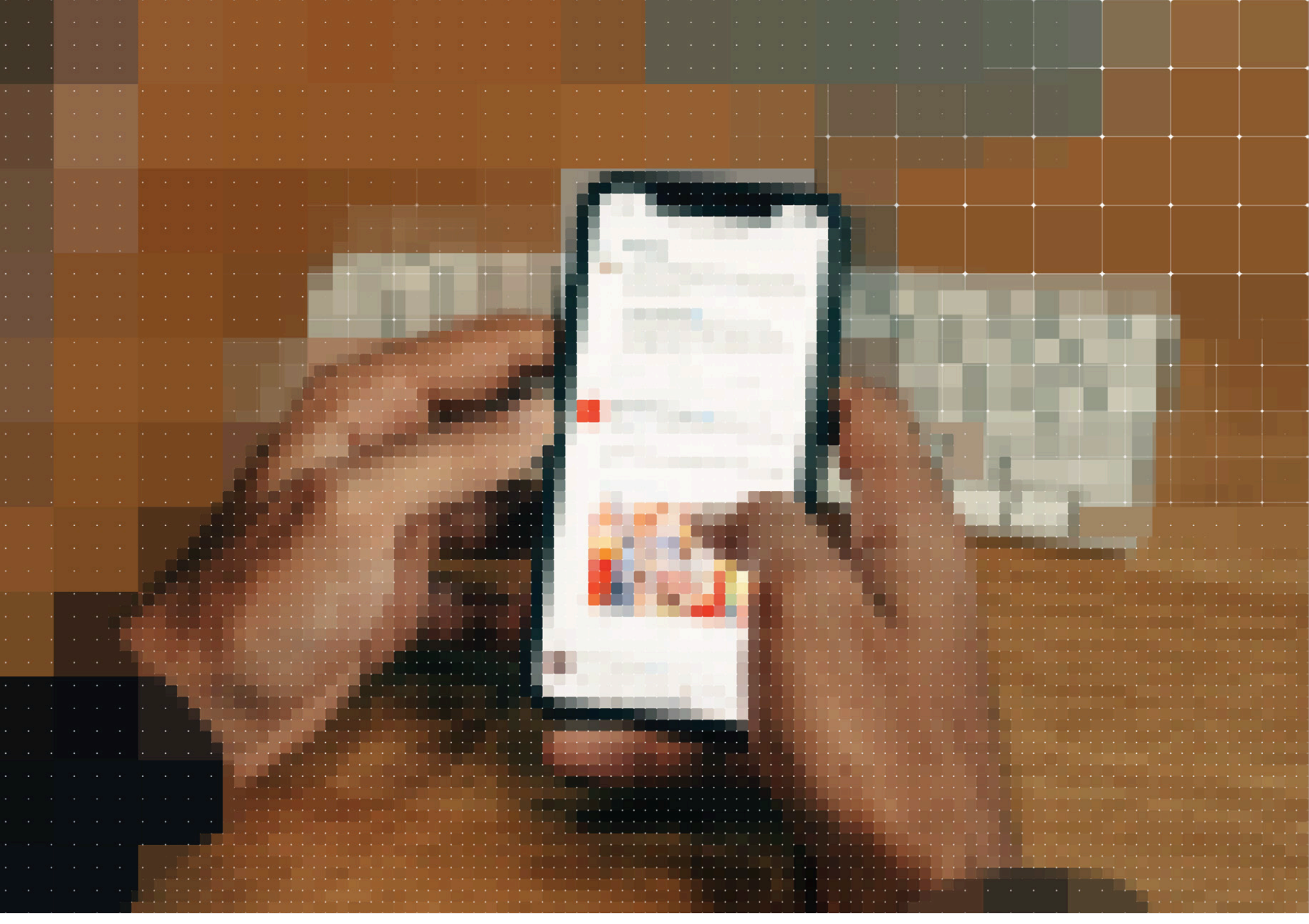


Next Generation Digital Identity

Future-proof technologies for secure digital societies

CYBERNETICA

Convenient and cost-efficient

SplitKey turns smartphones into secure authentication devices, equipping online service providers with a reliable and secure access management tool.

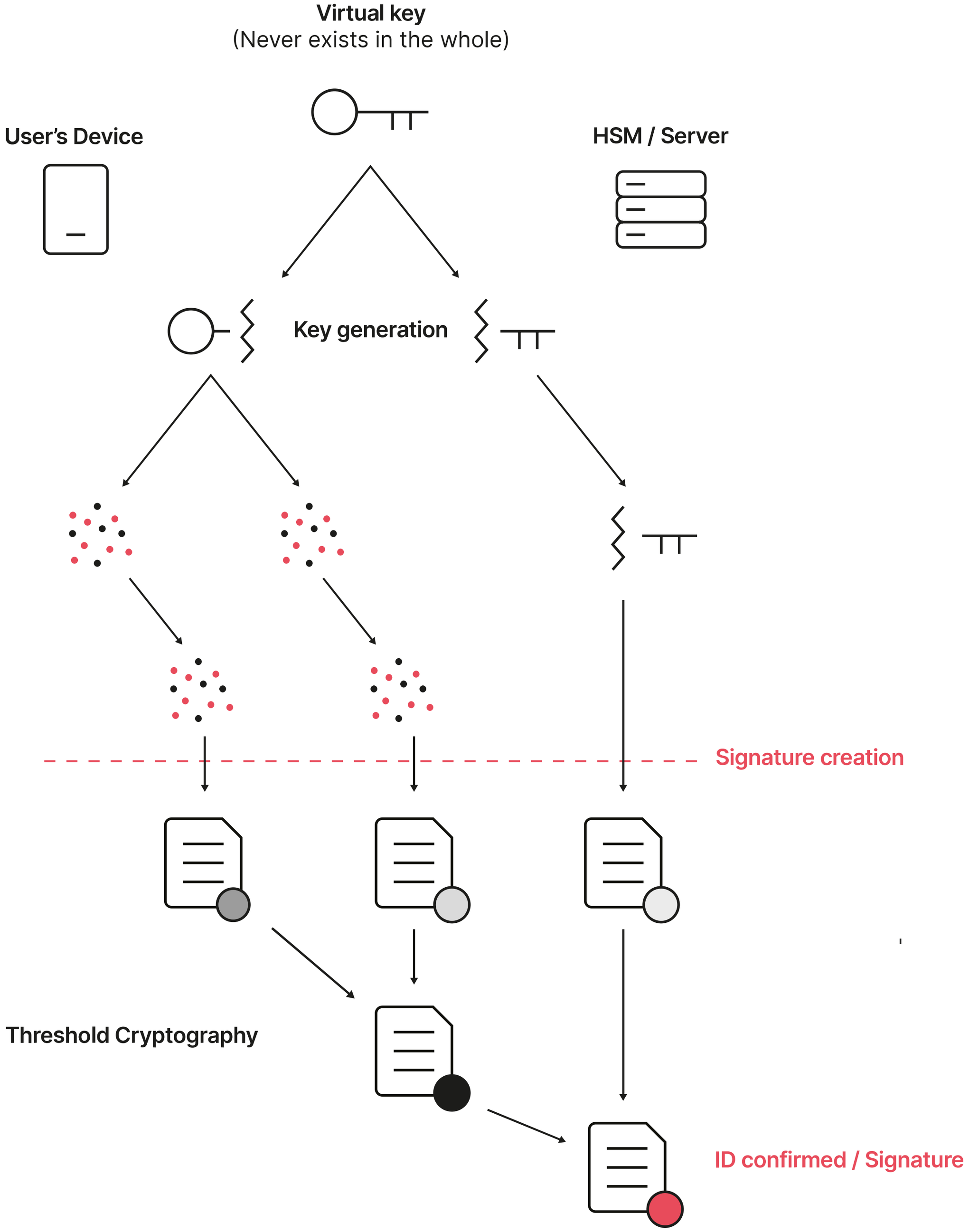
Tokenless mobile digital identity that can turn any smart device into secure authentication and qualified signature device. No need for a special smartcard, PIN-calculator or the like.

Secure PKI cryptography with full user control over their private key.

Regulatory compliant with the EU PSD 2 and the eIDAS (electronic Identification, Authentication and Trust Services) regulations.

Turnkey solution with full infrastructure, service design and advisory for implementing digital identity.

Unique technology



Cryptographic Solution

SplitKey technology is based on proven principles of public key cryptography, digital signature schemes, and PKI. Public key cryptography works on the concept of key pairs:

- the public key is bound with the verified identity of the user
- the private key is confidential and protected, e.g. inside a smart-card, which is under sole control of the user

Access authentication

SplitKey provides secure but simple authentication for accounts that require superior online security. Banking sites, trading platforms, government department sites, or any online portal can protect its users' accounts by ensuring that only the user has control of their private key.

Digital signing

SplitKey ensures that only the user can sign or approve a transaction, due to the user retaining one piece of their private key which never leaves their device. SplitKey complies with the European QSCD (Qualified Signature Creation Device) requirements and PSD2 (Payment Services Directive).

Patented technology

The technology applied in the SplitKey product is patented as a European patent no. 3529948.

Unbreakable security

Common Criteria certified to EAL4+ (Evaluation Assurance Level 4+) as a qualified signature creation device (compliant with current eIDAS regulation).

Assessed to correspond to assurance level “high” eID authentication scheme (compliant with the current eIDAS regulation).

Evaluated internally within a MS, an un-notified eID scheme.

Used on daily basis for eIDAS high level authentication and qualified digital signing by more than 2 million customers in Estonia, Latvia and Lithuania (both in public and private sector services, including widely in financial services).

Developed by scientists and cryptographers, research published in a peer-reviewed journal.

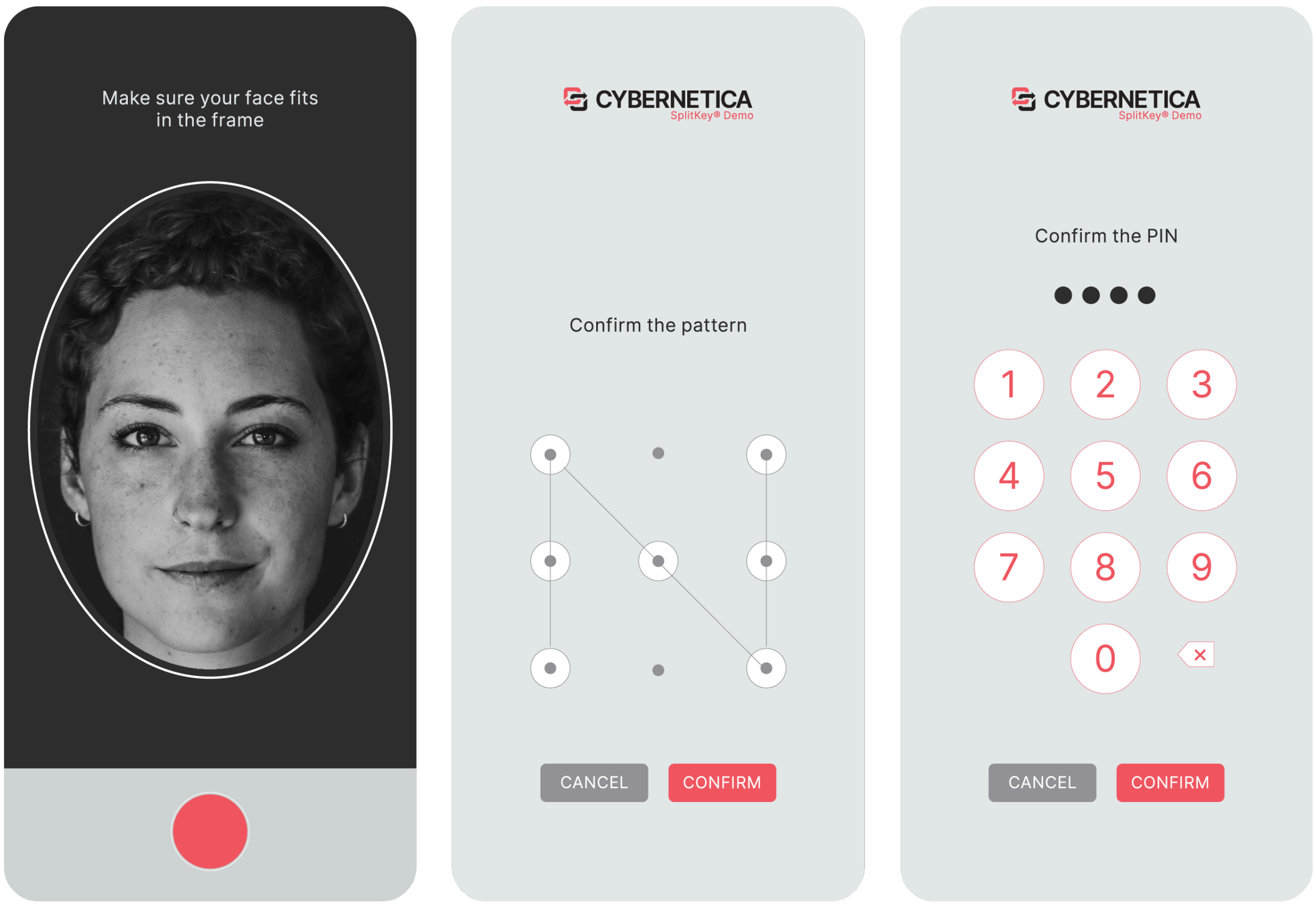
No security breaches or other privacy compromising security incidents during past 5 years.

SplitKey+

Knowledge and biometrics based authentication and signing solution.

SplitKey+ builds on Cybernetica's 4 and 5-digit PIN knowledge-based solution for authentication and signing. By combining threshold cryptography and liveness testing with face recognition, SplitKey+ adds a level of security that gives confidence and reduces risk.

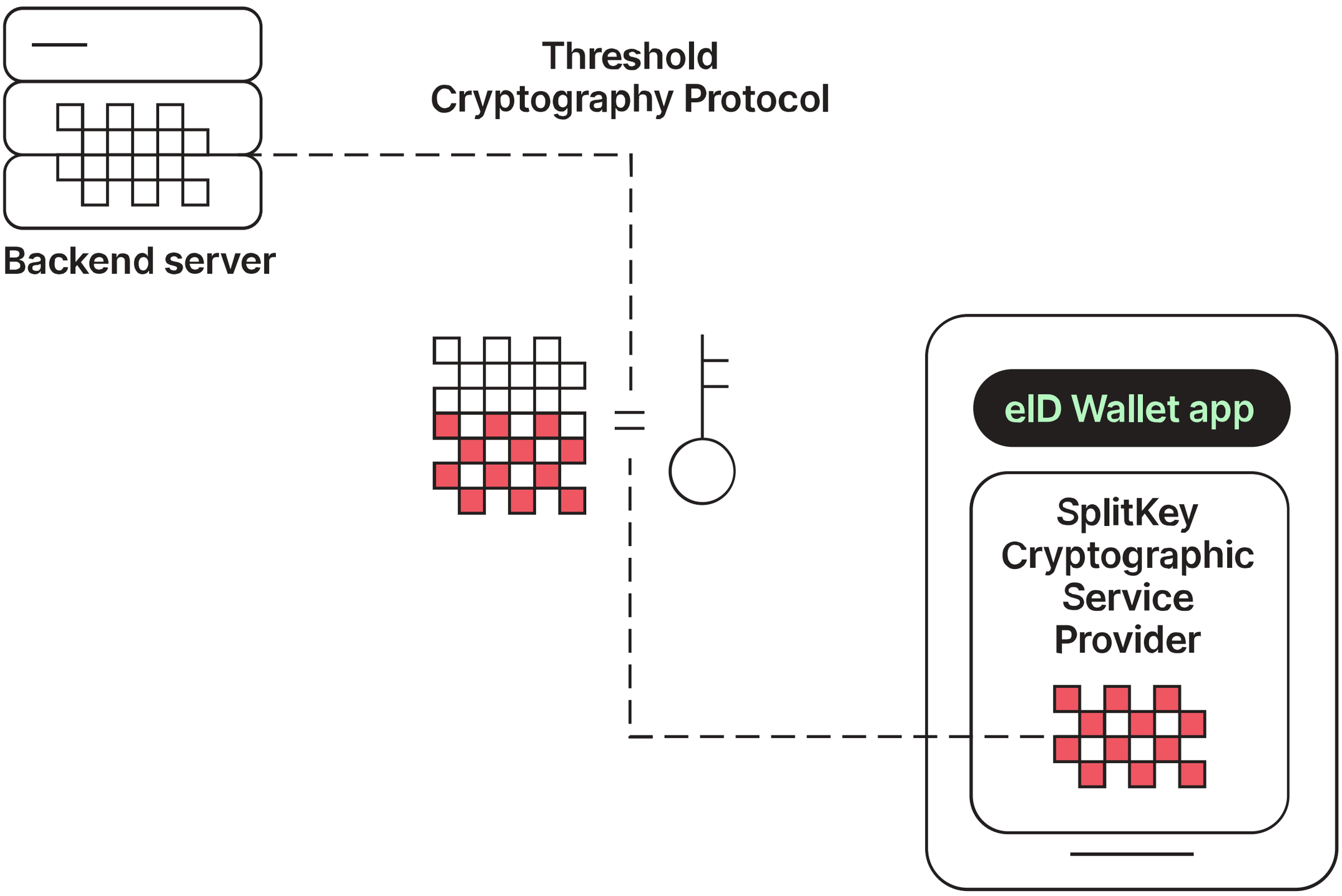
Working with our liveness testing partners, we can offer a LoA High for both PIN and biometrics, with the additional option of pattern. Service providers can select which combination and when these methods are used.



> Authenticate with PIN and sign with biometrics, or prompt PIN and biometrics for authentication and PIN2 for signing. Any combination of PIN, pattern and biometric based liveness testing can be utilised.

SplitKey CSP

Cybernetica is expanding its SplitKey product line to complement the emerging European Union Digital Identity Wallet (EUDIW) ecosystem.



Cryptographic service provider based on SplitKey

Hardware agnostic

For mobile platforms that do not have a suitable hardware-based Trusted Execution Environment or Secure Enclave chip

Advanced cryptographic services for digital identity wallet applications

SplitKey was designed in 2016 for the needs of software-based eID means, providing eIDAS1-compliant “high” level authentication and QSCD-level electronic signatures. We used threshold-cryptography-based algorithms and achieved unique security properties for a software-based solution.

Now, we have taken same idea and developed an advanced, ready-to-integrate software module for wallets, which provides following security features:

- Private key generation and signature creation
- User’s sole control of cryptographic material, PIN verification and clone detection
- RSA algorithm support, ECDSA/EdDSA and PQC on the roadmap
- Common Criteria EAL4+ certification ready, aligned with EN 419 241-2 (rQSCD PP)
- Integration with identity proofing (RA) and X.509 certification (CA)

Security requirements of wallet apps

Digital identity wallets, EUDI wallets and mDL wallets have great potential to provide security critical services to citizens, governments and commercial organisations. In order to gain trust, they must be secure against attacks.

eIDAS2 has recognised this by mandating that components and processes in the EUDI wallet ecosystem should be at a Level of Assurance “High”.

There are following options for ensuring safety and security of private key protection technology:

Embedded SE/TEE of modern mobile phone

It is unknown, how such security elements may be certified and if phone vendors will undergo the certification efforts by themselves.

External hardware: certified smart-card or SIM-card, via NFC interface

This is the easiest route from certification viewpoint, as it relies on existing QSCD security practices, but most inconvenient for users.

Remote HSM for security and signature creation, similar to rQSCD solutions

- Convenience of users
- High-level security
- Wallet providers gain independence from phone vendors and certification roadmaps of chipset manufacturers
- Quick route to market and flexibility

Consultancy

Cybernetica offers a consulting service for digital identity to advise and analyse the current landscape and provide meaningful input for the journey ahead.

Harnessing the strength of our PhD’s, Research Institute and being one of the original architects of e-Estonia, we have a strong pedigree to assist and guide your digital identity transformation.

The list of services contains but is not limited to:

- Mapping the initial scope of activities and assessing the status quo in the Client Organisation(s).
- Advisory on legal aspects, existing legislation in the area of electronic identification, authentication, digital signing, drafting recommendations to regulatory requirements.
- Advisory on the project management.
- Advisory on the change management and communication of adopted changes.
- Support of orientation and transition for the employees, guidelines, trainings, workshops, knowledge bases.

Evaluation of current eco-system

The mapping of initial scope begins with a number of objectives that build a foundation for the adoption of digital identity.

- Identifying the key stakeholders in the government ecosystem.
- Communicating the goal and intention of the incoming innovation.
- Assigning a leading management role to a specific authority that will act as a steering authority responsible for achieving the strategic and organisational goals and roadmap for the Pilot implementation.
- Assigning a leading technical role to a specific authority and/or unit that will be responsible for the integration and maintenance of the technical solution on the Client’s end.
- Collaboration of leading management and technical authorities, resource building and continuous communication with the Contractor during the pilot duration.
- Identifying legislation on (digital) identity, digital identity management, e-transaction law and other regulations which are relevant to the technical solution usage scale.
- Analysing legal acts that regulate and/or are related to data protection and access policies.

As a further step of scoping, a deeper overview of lower-level processes that are taking place within entities and departments can be created. In this case, such techniques as surveying and interviewing can be utilised for data collection.

Depending on the research goal that comes from the initial scoping activities, surveying of staff and conducting interviews with the unit overheads and management teams may help with the following:

- Assessing general awareness on (digital) identity management, specifically, authentication and digital signing.
- Acquiring an understanding of the current technology acceptance level within the organisation(s).
- Identifying the level of cybersecurity awareness.
- Identifying gaps in the usage of authentication solutions in the current processes and workflows, and bottlenecks these gaps are causing.
- Collecting feedback and insights from personnel.

The outcomes obtained from the analysis of the collected data may be of relevance for further integration and adoption activities.

References

Smart-ID / Baltics and Iceland

Cybernetica’s digital identity technology is used all over the Baltics and Iceland in collaboration with the Smart-ID service operator.

- 3 million users and 75 million transactions per month.
- Used in services provided by top Nordic banks, leading telcos and e-commerce providers.

Partnership with PwC / Middle East

Digital identity strategy for the Digital Government Agency.

- Elevating the Saudi digital identity with new technological opportunities.
- Work on Technical Architecture, eID and Trust Services, Standards, and Legal chapters.

ENISA framework / European Commission

Consultancy services regarding digital wallets and electronic identification related to the eIDAS regulation in the EU.

Partnership with EY / European Commission

The first EU-wide market study on digital wallets to explore the various digital wallets and their providers, with the ultimate goal of increasing the uptake of digital identity wallets throughout Europe.

- Consultancy services to support, advise, and validate the research analysis.

- Sharing expert opinions and experience regarding existing regulatory frameworks.

Partnership with the Estonian Information System Authority

Estonia’s cyber security is born out of and constantly improved by daily cooperation between government and private entities. Cybernetica has a long history in leading and participating in applied research projects with the Estonian Information System Authority, hence contributing to sustainable and secure development of digital identity tools and services.

Hear from our customers

“Cybernetica AS has been a trusted partner in the development of the Estonian Digital Identity ecosystem and has been a long-standing strategic partner of the Estonian government. They have been involved in projects, both with the Estonian Ministry of Economic Affairs and Communications and other agencies.”

Luukas Ilves
Government Chief Information Officer

“Using Smart-ID for customer authentication doubled the number of monthly new users in our mobile bank. We are very satisfied with Smart-ID regarding both the ease of technical integration, as well as convenient user experience of the application. This mindset is supported by our internet and mobile banking clients from whom already 25% are using the possibilities of Smart-ID.”

Margus Holland
LHV Bank - Head of Digital Banking

“Cybernetica has been a valuable partner of PricewaterhouseCoopers in the Middle-East in advising our customers on designing digital governance and identity frameworks and solutions.”

Fadi Komati
PwC Middle East - Digital Consulting Partner

Why Cybernetica

Cybernetica has over 25 years of experience in building future-proof products that rely on research & development. Currently our technologies are used in more than 35 countries globally.

> “We are extremely proud of our decades-long journey. We are certain that with our values, our people, and our capabilities, we will continue to be the driving force in emerging technologies.”

Oliver Väärtnõu
CEO

Essential facts

Established in **1997**

Roots in academia **since 1960**

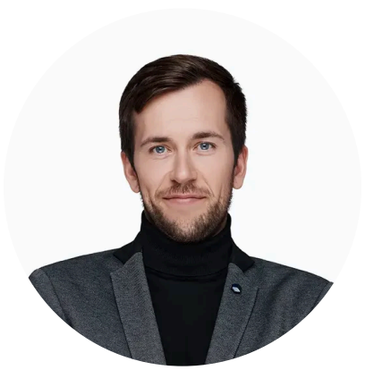
Strong focus on **R&D**

Architects of **e-Estonia ecosystem**

Technologies exported to 30 countries, incl. **USA, Japan, UAE, Ukraine**

12% of employees **have a PhD**

Contact our team:



Florian Marcus
Head of Sales and Partnerships (Digital Identity)
florian.marcus@cyber.ee

cyber.ee/solutions/digital-identity