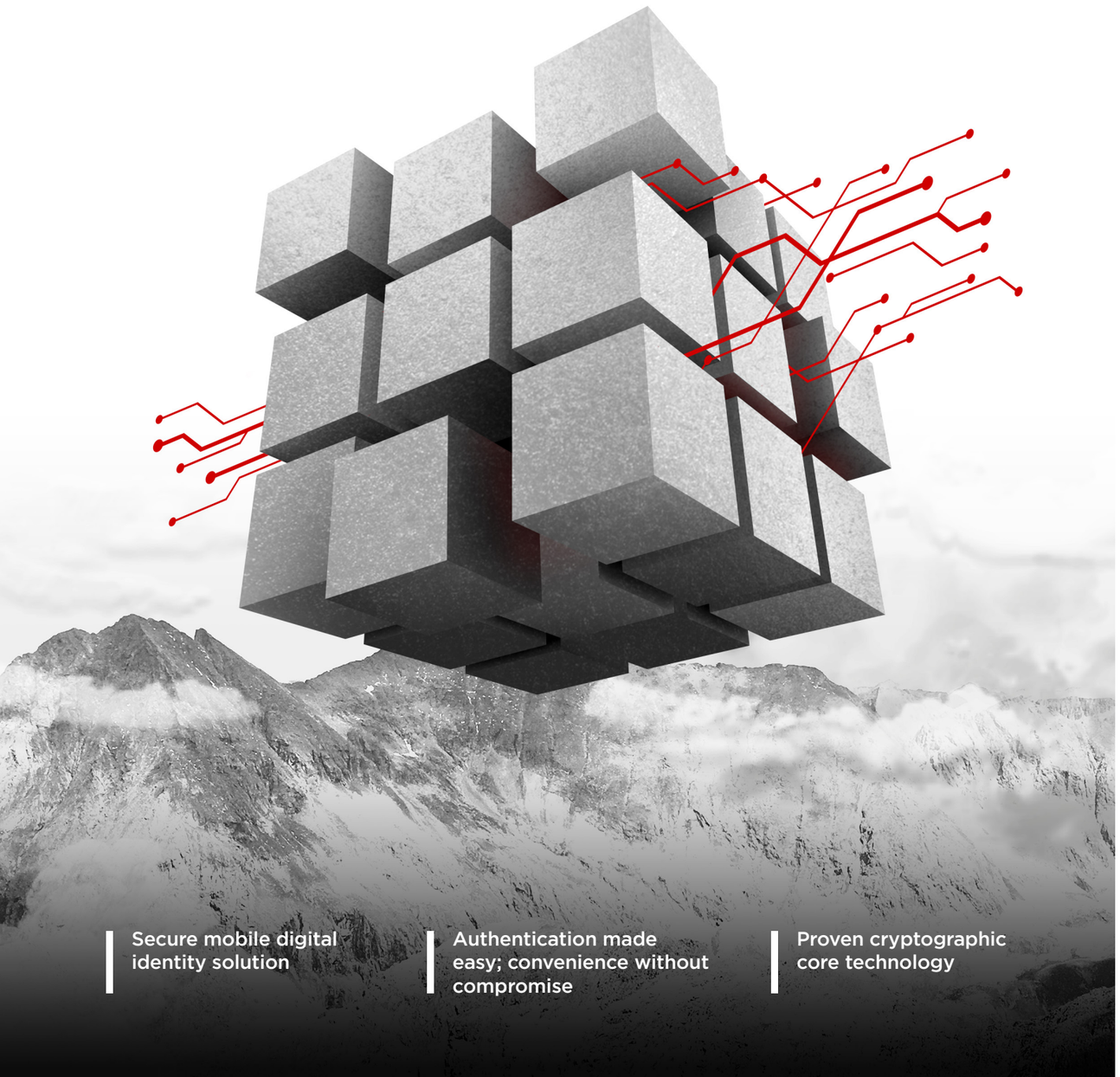
CYBERNETICA

# SplitKey Mobile Authentication and Digital Signature Platform



Secure mobile digital identity solution

Authentication made easy; convenience without compromise

Proven cryptographic core technology

## Cybernetica

**OUR STORY**

Founded in 1997, Cybernetica grew from the Estonian Institute of Cybernetics (est. 1960); our focus and history making us the founders of the Estonian cyber industry.

**BUSINESS**

Cybernetica is an ICT company focusing on secure digital solutions. We create and provide mission-critical software for the public and private sector in more than 35 countries.

We develop advanced maritime surveillance technologies, deployed at the external borders of the EU and NATO, as well as to observe and protect the waters of the Black Sea, and the Adriatic Sea. Our radio communication solutions are, among others, implemented in the largest port in the world, Jebel Ali in Dubai, and in the Grand Canal System in Venice. For the aviation industry, we offer the Remote Tower solution to remotely control air traffic.

Our innovative technologies are the foundation of critical e-Government systems, such as the Estonian X-Road, i-Voting, e-Customs, and more. With successful implementations from the US to Japan, we offer the Unified eXchange Platform for secure data exchange, SplitKey for mobile authentication and qualified signing, and Sharemind for confidential data analysis.

CYBERNETICA

**CUSTOMERS**

We have a wide range of customers, both public and private, such as governmental authorities (border guard, ICT infrastructure agencies, maritime authorities, police administrations, security agencies, tax & customs authorities, etc), financial institutions, telecom operators, port authorities, medical institutions and research labs, and critical infrastructure operators.

## SplitKey Applications

SplitKey technology powers the Smart-ID authentication and digital signature service that has over 2 million end-users in the Baltics and is used by top Nordic banks, leading telcos, and e-commerce providers. The service is offered by SK ID Solutions, with technology support and maintenance provided by Cybernetica. See more: smart-id.com

## Contact us

Email us to see how our technology could improve your service, or simply visit our website to learn more.
**splitkey-sales@cyber.ee | cyber.ee**

**CYBERNETICA AS**
Mäealuse 2/1, 12618 Tallinn, Estonia
+372 639 7991
info@cyber.ee

# Secure Authentication Made Easy

SplitKey Mobile Authentication and Digital Signature Platform is a **next generation electronic ID technology.** The platform turns end-user's **smartphones and tablets into secure authentication devices,** equipping online service providers with a reliable and secure end-user access management tool. The platform also enables end-users to **digitally sign documents** in accordance with the highest European Union (EU) regulation for authentication and trust services – eIDAS.

# SplitKey - Hardware Level Security Without the Hardware

Secure authentication typically requires special hardware; physical tokens like smartcards, pin-calculators, USB keys, etc., to protect against phishing and malware attacks. These devices are expensive, inconvenient to use, and issuing them is time-consuming. SplitKey protects private keys using threshold cryptography, so the user can simply use their smart device to authenticate and sign at the same assurance level as traditional hardware tokens.

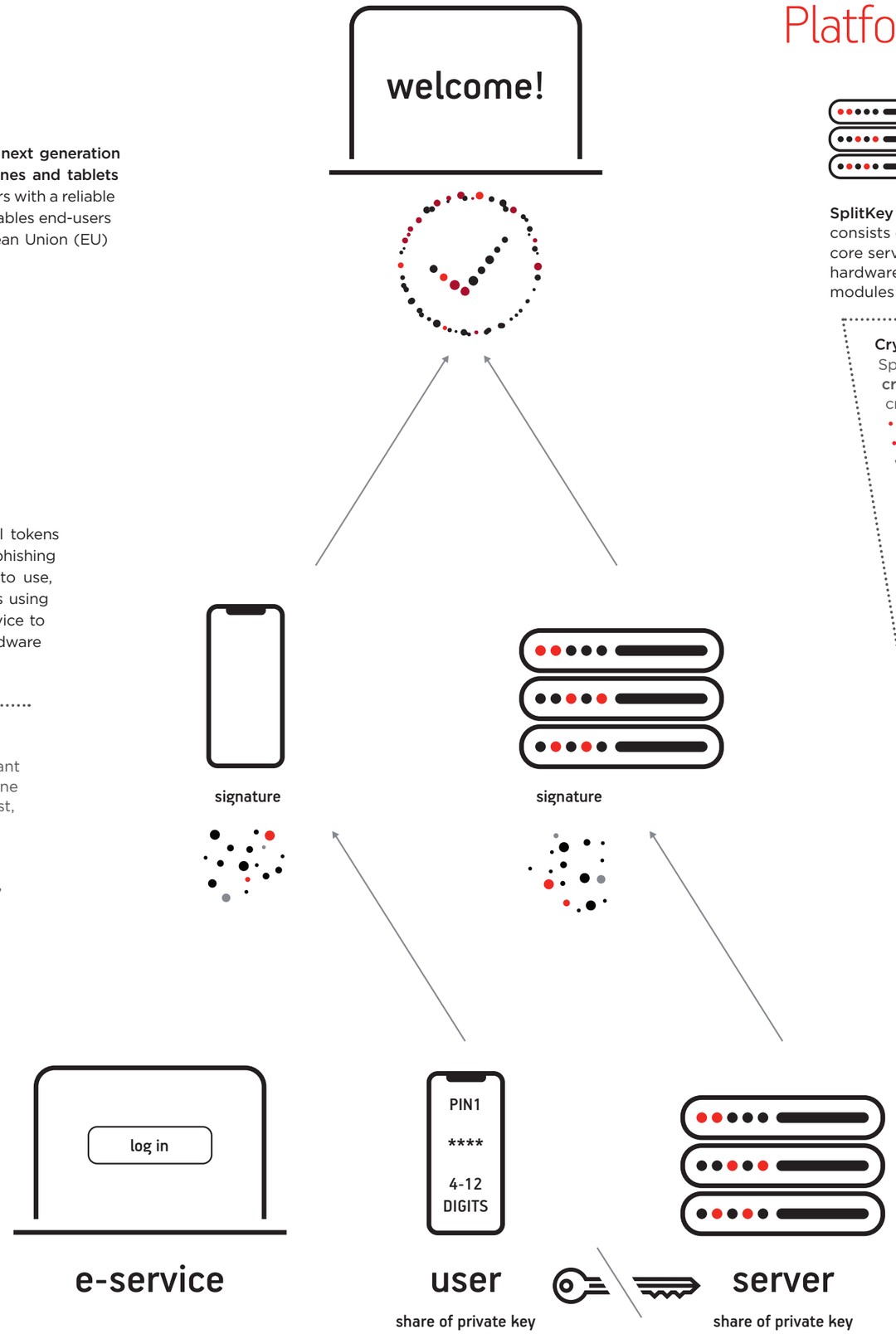
**FAST AND SCALABLE**
SplitKey can be deployed in a high-availability and fault-tolerant setup, aimed for use in scalable systems, like e-government, online banking, and large-scale commercial platforms. SplitKey is fast, enabling user authentication and digital signing in just 4 seconds.

**RELIABLE AND SECURE**
SplitKey is based on proven principles of public key cryptography, digital signature schemes, and Public Key Infrastructure (PKI). User's private key protection is based on a threshold cryptosystem.

**COST EFFICIENT**
SplitKey does not use physical cryptographic tokens nor rely on mobile operators, making it far more cost efficient and simple to deploy than token-based solutions.

**REGULATORY COMPLIANT**
SplitKey's authentication and signing function is compliant with the EU's second Payment Services Directive (PSD2) and the European Central Bank's recommendations for internet payments' security. SplitKey has also been evaluated against Common Criteria, achieving EAL4+ certification, meaning that electronic signatures given using SplitKey are legally binding, equal to handwritten signatures.

**EASY TO USE AND INTEGRATE**
SplitKey uses common interfaces (JSON/REST and OpenID Connect) to enable seamless integration with online service providers' existing systems (e.g. internet banking, e-commerce etc.) and ensures a smooth user experience.




# Platform Components

**SplitKey Core System**
consists of SplitKey core servers and hardware security modules

**SplitKey Portal**
web interface for accounts management, user registration, and end-user support

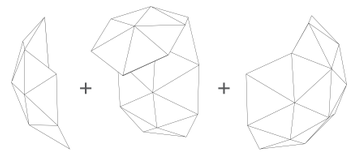
**End-user App**
application on the end-user's smart device for authentication and digital signing

**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.

But SplitKey utilises a **threshold cryptosystem,** which does not require any dedicated devices for key storage. The **private key is generated and stored in shares,** thus, protecting the key never relies on a single device. The different key shares are held separately in the user's smart device and SplitKey core system, each unusable and illegible on their own.

The signature is created with the cooperation of both the end-user app and core system. The cryptographic protocol ensures the protection of key shares and detection of key part cloning, etc., providing hardware level benefits and additional protection. SplitKey generates and uses 3096-bit RSA key pairs.

**SPLIT KEYS**
The private key exists in 3 individually unusable shares which are never combined. Each share signs a portion of the hash, the three signatures coming together on the server side, verifying the user.



**TRY SPLITKEY**
With SDKs, APIs, a demo app, and test hosting environment, we can work with you to quickly set up demos or pilots to help you experience how fast the technology works and how simple it is for end-users to securely access your online services, verify transactions remotely, and sign confidently.

**OPTIONAL COMPONENTS:**

**SplitKey CA (Certification Authority)** » Issues certificates necessary for user authentication and digital signing.

**Single Sign-On** » An authentication platform that allows users to access multiple applications with one login.

**Timestamping** » Ensures additional non-repudiation and reliable timing of user operations.

**White Label App** » End-user application with your branding.