Protecting digital identities: secure, simple and cost efficient

The Motivation: Protecting digital identities for any industry. From Automotive to Banking, from Smart Energy to Medical, from Connected Home to Health Monitoring

As banking, payment, and financial services shift massively to web and mobile, fraud opportunities multiply. Cars get connected and in-car & cloud services sprout. Cybersecurity issues raise safety & privacy concerns.

inWebo realized the imperative importance of providing for multi-factor authentication, and built an easy to implement, manage and use solution with a low total cost of ownership. Since the foundation of the company in 2008, this solution has been deployed to millions of users.

The Challenge: Solving the authentication dilemma

Historically, multi-factor authentication required that users be equipped with hardware tokens. This is often complex and costly to deploy, but there were only a few situations where the risk was great enough to justify the impacts of deploying these solutions.

inWebo is one of a few companies to offer a solution that combines certified hardware-grade security with extreme ease of use, deployment, and operations.

The Solution: hardware-grade security in dual-authentication

inWebo provides user authentication solutions built to secure customer, member, and employee access to VPN, IAM, web, Cloud, and IoT applications. inWebo seamlessly adds a layer of security by turning user devices including laptops, cell and smartphones, tablets, and wearables into strong authentication methods. It uniquely combines certified hardware-grade security with extreme ease of use, deployment, and operations. The inWebo solution relies on the Utimaco Hardware Security Module as its "Root of Trust".

Utimaco's FIPS-certified hardware security module generates and stores the secure cryptographic keys that are required for authenticating one person via one or several devices, for example their car or their phone. The trusted device uses dynamic keys to generate a "One-Time-Password", in online or offline mode. Those dynamic keys protect the trusted device from any relevant reverse engineering, not because you cannot access the keys, but because the keys are no longer valid when stolen. On the server side, inWebo authentication validation is not processed on the front-end servers but within the Utimaco HSM using a specific firmware developed by inWebo. This provides a unique trust in the authentication platform, especially against the administrators who do not have any mean to access customers' keys.

About inWebo

inWebo Technologies is an independent security software company founded in 2008, with R&D in Paris and operations in EMEA and North America. Our mission is to make online, mobile, and remote services more secure. For end users obviously, but also for businesses and organizations providing these services, since good practices of security can hardly be required from most end users: cybersecurity is a B2B market…Our objective has been to significantly improve security by designing multi-factor authentication solutions that are easy to implement, manage, and use, with lower ownership costs, therefore attractive on the market. Universal, open, implemented in a matter of hours, suited for deployments of any size, without upfront investment… Discover how inWebo solutions make your online business more secure. Easily. Visit www.inwebo.com for further information.

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep your cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Utimaco delivers a general purpose HSM as a customizable platform to easily integrate into existing software solutions or enable the development of new ones. With professional services, we also support our partners in the implementation of their solutions. Put your trust in Utimaco – today and in the future. For more information, visit hsm.utimaco.com