Corporate information systems (IT) are enlarging their environment: remote access and VPN, new users (customers, partners), business applications delivered from the Cloud, new devices for mobility (tablets and smartphones)...

The proliferation of these new types of access is a challenge for IT organizations, in terms both of security and ease of use. Traditional 2-factor authentication, as well as single-sign-on solutions (SSO) do not meet these challenges.

In-Webo offers strong, multi-factor authentication solutions, combining ease-of-use and security for traditional use cases (remote access, VPN), as well as for innovative types of access, such as SaaS/Cloud, new handsets and devices, extranets, B2B portals, « bring your own device ».

Customer Benefits

Security made easy. Whether to implement, to manage, or to use, secure 2-factor authentication has never been so easy.

Solutions and tools well suited for complex and heterogeneous environments, for deployments of any size, for B2B as well as B2C contexts.

Affordable security. Management and support costs dramatically reduced, so that you do not have to compromise on security.

Use Cases for Enterprise® Solution

- Business applications on tablets and smartphones
- SSL or IPSec VPN
- Remote access, webmail
- SaaS applications (Google Apps, Salesforce, Office 365, CRM, Dynamics, ...)
- Site developed with popular CMS®
- Partner Extranet

In-Webo Technologies

In-Webo is an independent security software company promoting strong authentication adoption thanks to innovative solutions that are easy to implement, manage and use.

In-Webo allows companies of all kinds and sizes to secure transactions with their employees, partners and customers by protecting and simplifying access to their business-critical information.

In-Webo operates trusted authentication platforms and owns the only security certification for a software authentication product from France Government Security Agency (ANSSI).
Out-of-the-box strong Authentication

Unmatched security
Execution environments - computers, smartphones, tablets - cannot guarantee the confidentiality of stored secret keys. In-Webo R&D has therefore introduced authentication technologies based on random dynamic keys. This worldwide patented and exclusive innovation allows In-Webo to propose authentication soft-tokens with unmatched security.

Flexibility and ease-of-use
- Activation and initial tokens customization done by entering a disposable key delivered to a user by their service provider or system administrator.
- 2-factor authentication triggered by entering the user secret code (PIN) defined at token customization stage.

Compatible environments

Security API* – « Strong authentication as a Service »
Thanks to connectors integrated in In-Webo solutions, you may configure in a few clicks a strong authentication service matching your architecture, your security policy, as well as your identity management (IAM).

Generic applications connectors are available (webservices, radius, SAML), as well as dedicated ones (Google Apps, Salesforce, Office 365, CRM Dynamics …).

Provisioning and management can be done either through APIs, through web tools (In-Webo WebConsole), or with a directory synchronization utility tool (In-Webo Directory Sync).

Implementation options enable you to match the authentication service security and availability to your own requirements (dedicated server, local back-up, keys under your exclusive control...).

Soft-tokens
Strong authentication soft-tokens designed by In-Webo R&D are available for free, and allow for immediate access protection for IT and online services, whether by users, customers of partners.

Mobile Token: nCode & Authenticator
mobile application, universal generator of secure OTP®
Standalone (no connexion, no SMS) and multipurpose (web access, interactive voice responder, desktop clients…).

Desktop Token: InWebo Application
2-factor authentication soft-token for Mac & PC
Security and user experience at their best.

Cloud Token: Helium
no-install token for any Internet browser
Full-web strong authentication on tablets, smartphones and desktops.

In-App Token: mAccess
SDK* for in-App strong authentication
Securing access from desktop clients, embedded and mobile applications.

* One-Time Passwords
* Software development kit
* Open application programming interface

Strong Cloud SSO
In-Webo Enterprise solution integrates the main systems and standards for identity federation. You may therefore allow the users to access their external applications both in an easy (SSO) and secure way (strong authentication), wherever they work from, on site or remote. You also avoid collecting and concentrating remote and mobile users traffic on your private network, which is a typical cause for bad performances.
Last but not least, no additional equipment (appliance, SSO, ...) is needed in your architecture.

Identity Hub
The play evolves from closed security to open identity, where online users and service providers will exchange « attributes » (user data), self-claimed or certified by trusted 3rd parties.

InWebo Identity Hub is an attribute and identity broker where you can exchange - and possibly monetize - user attributes. The purpose is to allow service providers to engage in trusted relations or transactions with online prospects, without requesting heavy form filling or paperwork, while prospects keep a full control of who gets access to their data.

In-Webo Technologies - 11 Marty Drive - Merrimack - NH 03054 - USA contact@in-webo.com www.in-webo.com