Please activate slideshow

In-Webo Technologies

IN-WEBO Mobile & Web Strong Authentication

InWebo Service Model

Free soft-tokens

Multi-device, multi-environment

Universal

Self-service oriented

Security-as-a-service

Certified product

CSPN

Easy, transparent

- Comprehensive Security-as-a-service solutions for Businesses and Service Providers
  - Easy, universal, scalable, « web-minded »
  - Security core : data protection, users remain anonymous, trusted services provider

self-service management of strong authentication **soft-tokens** integrated into **consumer & business** handsets, devices and applications

InWebo free soft-tokens

In-App Token
Strong authentication library (SDK)

Based on certified library

Cloud Token
No-install, full-web 2-factor authentication from any device

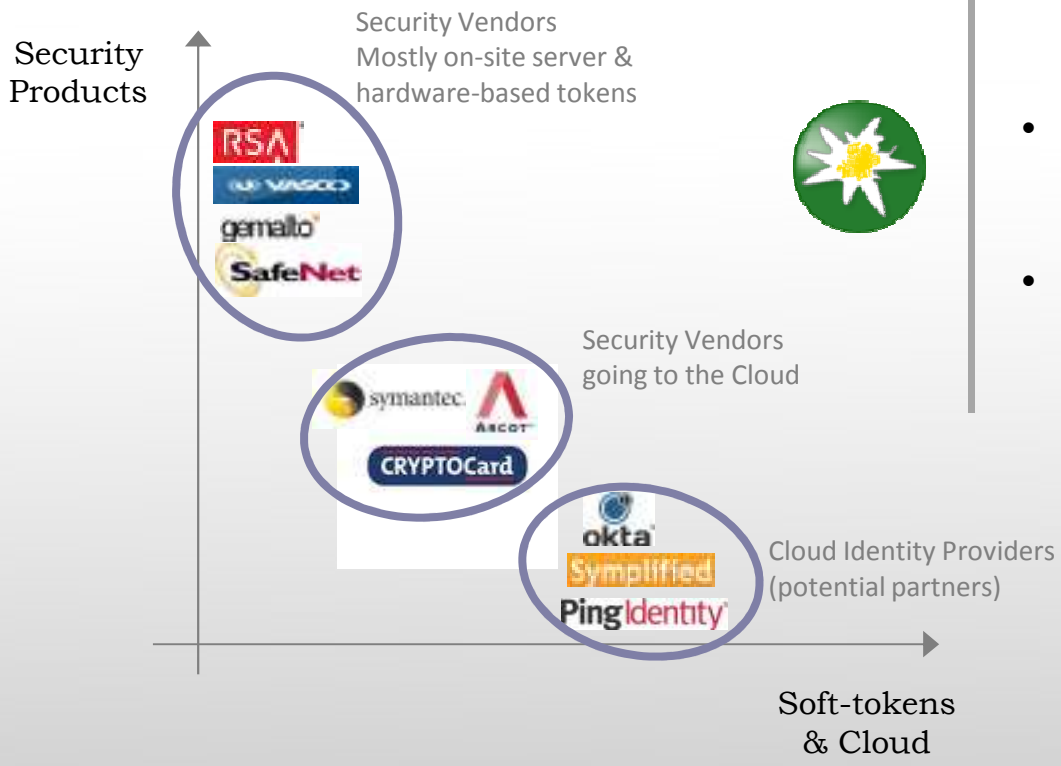
Mobile Token
Universal OTP-generator on any cell-/smartphone

CSPN

Certified product

Desktop Token
Authentication client and browser extension

Competitive Landscape: a Security vs. Flexibility Tradeoff



- The only security-proven & certified software OTP technology
- The only trusted authentication platform
- Unique set of soft-tokens (mobile, desktop, In-App, Cloud)

Proven Security

OTP = Function (Main Secret Key , PIN , Counters)



Token SW

OTP = Function (Main Secret Key , PIN , Counters)



Once the soft-token has been reverse-engineered, knowledge of a unique OTP (*even if no longer valid*) gives the PIN with a **local** and straight calculation; OTP must therefore be considered as sensitive information *over the complete token lifetime* and such soft-tokens are no genuine 2-factor tokens

IN-WEBO

OTP = Function (Main Secret Key , PIN , Counters,



Service Key, Random Dynamic Keys)


Calculation of the PIN involves a systematic search over 512 bits, that is not feasible in practice and would anyway provide unusable results (due to under defined equation systems). InWebo application is not sensitive to reverse-engineering

Proven Security explained – 1

OTP = One_Way_Function (Main Secret Key , Counter , PIN)

Typ. 20 bits

Typ. 13-17 bits if digital
(more if alphanumeric)

Traditional soft-token (proprietary such as RSA, Vasco, Arcot, or public such as HTOP/TOTP)
*without random dynamic keys**

The « Counter » has no entropy (it is deterministic), so calculating the PIN is equivalent to solving a system of ~20 equations and 13-17 unknown variables. As the functions are « one-way », the best possibility is a systematic search involving (worst case) 2^{17} local calculations. Current workstations require less than a second to perform these calculations.

Consequence is that with such a soft-token, every OTP must be kept confidential over the complete lifecycle of the token (several years). **Said differently: a simple password has the same security level**.

*keys = shared secrets

Proven Security explained – 2

OTP = One_Way_Function (Main Secret Key , Counter , PIN , Random Dynamic Keys)

Typ. 20 bits

Typ. 13-17 bits if digital (more if alphanumeric)

Typ. 512 bits

InWebo soft-token involving random dynamic keys

Calculating the PIN is equivalent in theory to solving a system of ~20 equations and 525 unknown variables. The best possibility is a systematic search involving (worst case) 2^{525} local calculations. Such computing power is definitively out of reach. Even if it were, all PIN possible values would be found as valid candidates, as the equation system is hugely under-defined.

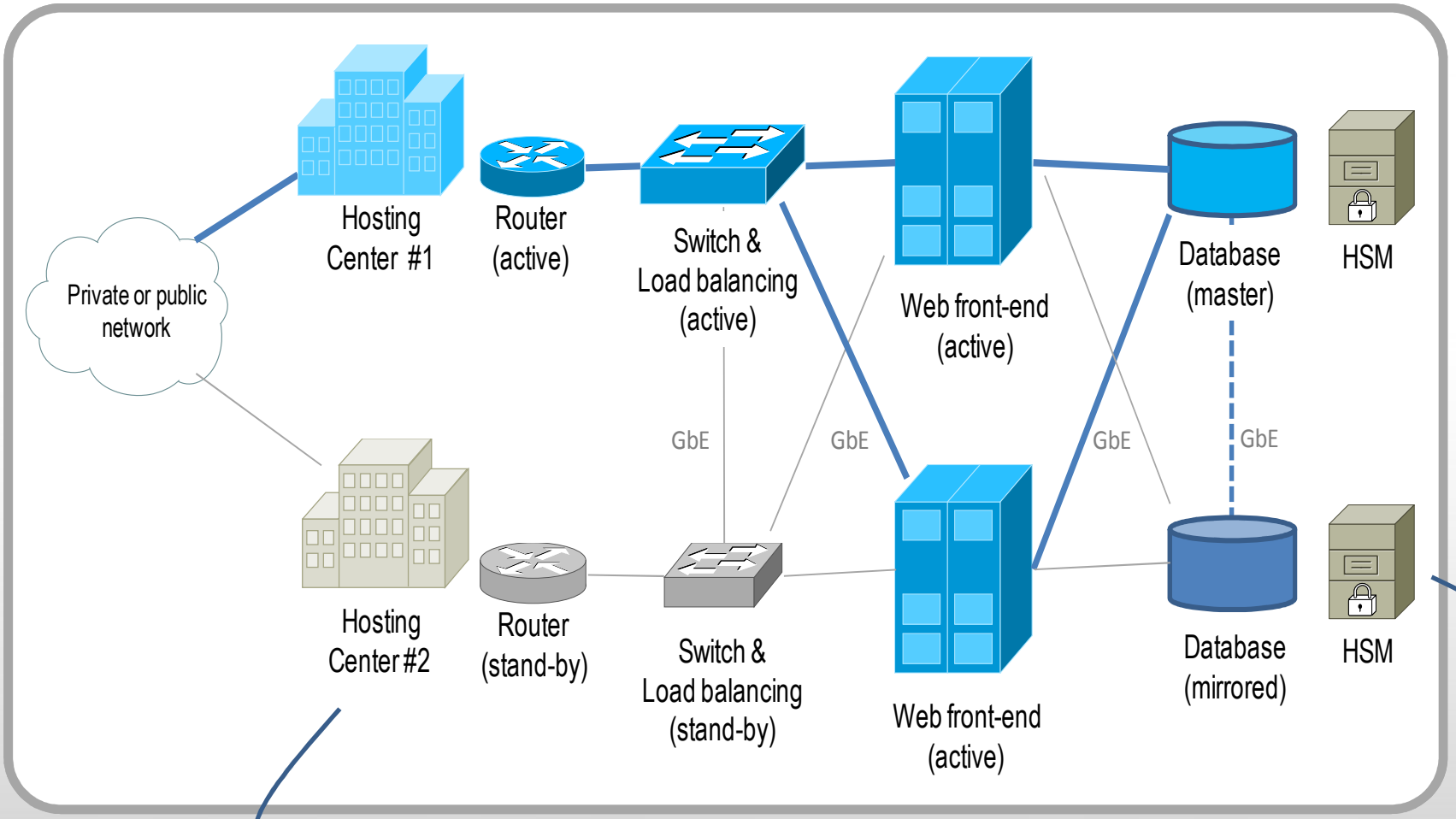
Consequence is that In-Webo OTP are not sensitive information (once they have been used or have become invalid, e.g. after max. 2 minutes). Said differently: In-Webo soft-tokens are not sensitive to reverse engineering. **Said differently: In-Webo soft-tokens have a security level similar to that of hardware tokens.**

This technology has been analyzed by independent academic research in 2009, and evaluated/certified by ANSSI in 2012 (both reports available in French). ANSSI certification also relates to the correct cryptographic implementation in InWebo products.

The first and only Trusted Platform

- In-Webo customers (Banks, Businesses, etc.) keep under their exclusive and cryptographic control their users' tokens' « service keys »
- This is achieved thanks to an initial key ceremony with the customer
- InWebo HSM perform all security related operations
- InWebo HSM do NOT trust
  - InWebo webservers
  - InWebo sysadmins
  - and of course 'anonymous'

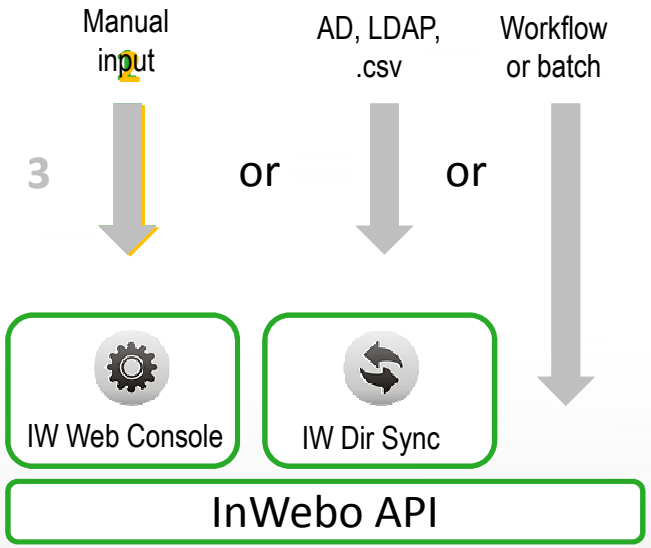
High Availability Architecture



2 distinct data centers « Tier 3 » or « Tier 4 »
(Telecity / Equinix)

Hardware Security Modules

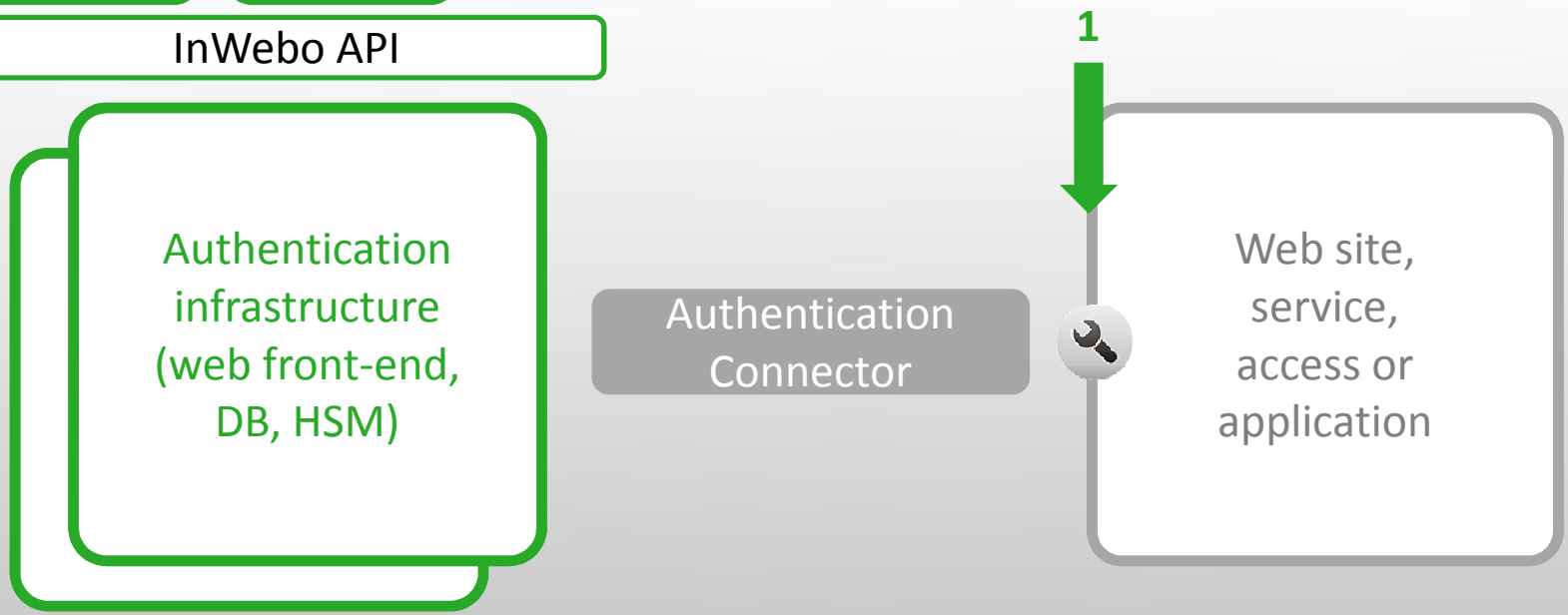
« No IT » Setup



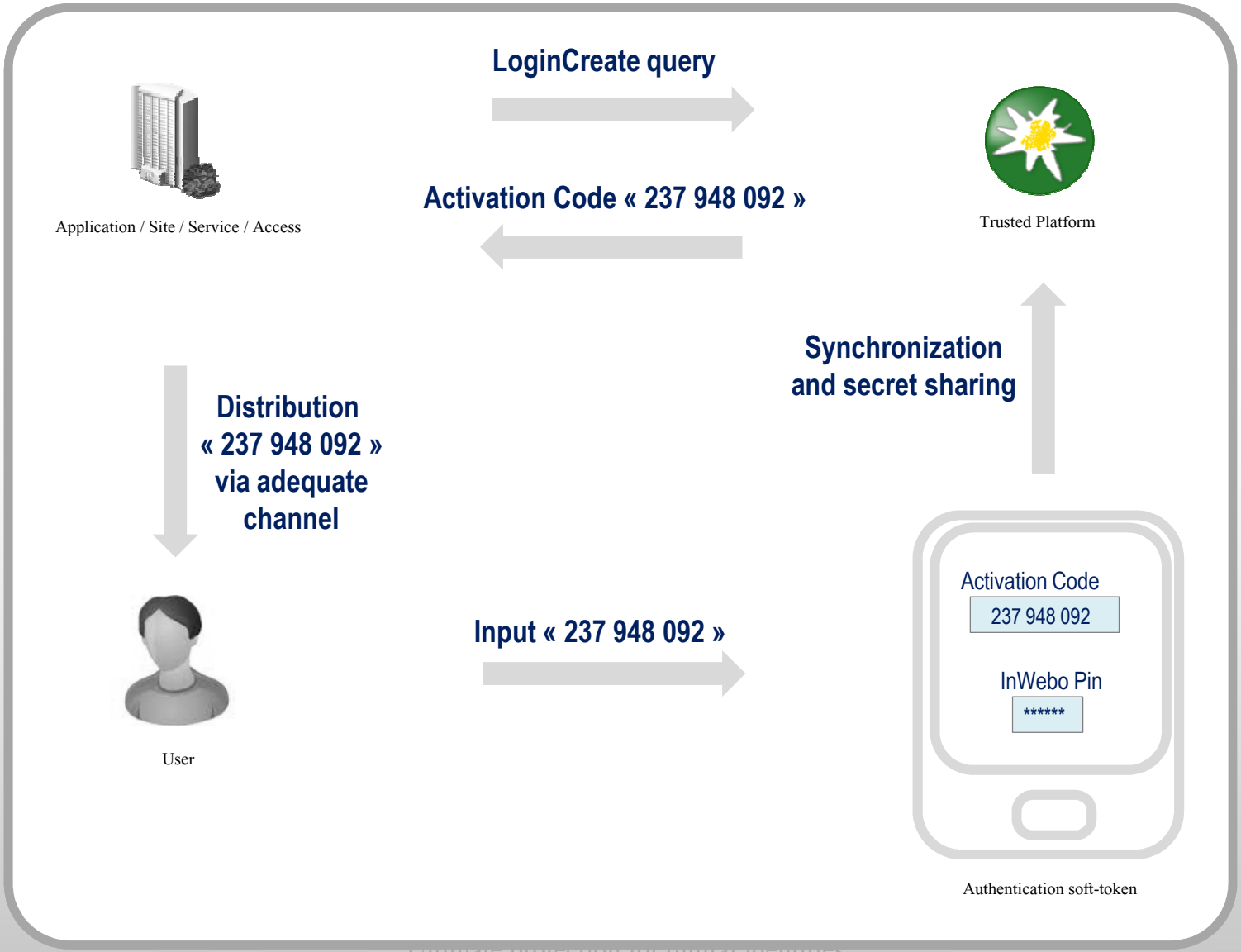
1- Configuration of an authentication "connector" (radius, SAML 2.0, WebService)

2- Selection of a security policy for authentication: supported InWebo tokens, OTP format, trust model, etc.

3- User provisioning or synchronization



Enrollment


LoginCreate query
Application / Site / Service / Access
Activation Code « 237 948 092 »
Trusted Platform
Synchronization
and secret sharing
Distribution
« 237 948 092 »
via adequate
channel
Activation Code
237 948 092
InWebo Pin
******
Input « 237 948 092 »
User
Authentication soft-token

IN-WEBO
Mobile & Web Strong Authentication

Thank you

More information on www.in-webo.com