PkJBox as simple and secure cloud electronic signature creation and validation solution

Giuseppe Damiano
CTO B.U. Products Intesi Group | gdamiamo@intesigroup.com

Andrea Caccia
Consultant | andrea.caccia@studiocaccia.com
Intesi Group at a glance

Intesi Group is an Italian private company that operates in the ICT industry offering specialized professional services, products with high technological content and advanced cloud solutions.

Entirely self-funded, Intesi Group has been since 1998, when it was established, in steady and rapid growth.

With 2014 revenues of EUR 10 million and more than 100 highly skilled professionals, Intesi Group is the ideal partner for those who want to integrate advanced technologies in a fast and reliable way.

Specialized skills, established references and adherence to organizational models are the elements that distinguish Intesi Group.
CONFIRMATION PURSUANT TO § 18 PARA. 5 SIGG

Secure Signature Creation Device
PkBox, Version 3.0.3

Applicant:
Intesi Group SpA
Via Torino 48
I-20123 Milano, Italy

Confirmation Issued on: 2015-02-03
Reference number: A-SIT-1.111

Preliminary Remarks
Zentrum für sichere Informationstechnologie - Austria (A-SIT) is declared by the Federal Chancellor’s Ordinance BGBl II 31/2000 as a confirmation body pursuant to § 19 of the Austrian Signature Act (Signaturgesetz - SigG), BGBl I 190/1999 as amended by BGBl I 75/2010.

A-SIT is notified as a designated body under the European Signature Directive (1999/93/EC) article 3 para. 4.

A-SIT is thus made responsible for confirming the compliance of secure signature creation devices with the security requirements laid down in the Austrian Signature Act as transposition of the Annex III requirements of Directive 1999/93/EC into Austrian legislation.

1. Product Description
PkBox is a product for electronic signatures intended to be used as a Secure Signature Creation Device (SSCD) in a secure operational environment. It implements a Trustworthy System Supporting Server Signing (TW4S) in accordance with CEN/TS 419241:2014. When used in combination with qualified certificates PkBox generates qualified electronic signatures as defined in Directive 1999/93/EC with the legal effects of article 5 para. 1.
PkBox 3.0.3 – Architecture

#SecurityFirst

Security of sensitive information ensured by Thales HSM

Two Factor Authentication – HSM password and OTP validation

Signature Keys and OTP Seeds are protected by the HSM
PkBox: main features

- Millions of signature credentials and OTPs managed
- Performances: several hundreds of signatures/sec
- Scalability: load balancing and multi tier architectures
- High reliability: one central DB for all PkBox (SSCD)
- Easy to use: high level API
- Signature formats: CAdES, PAdES, XAdES, S/MIME, ...
- Complete Validation Authority Functionalities
- Authentication OATH OTP (Time & Event based): Mobile App, Mobile SDK and SMS
- Multivendor OTP: Vasco, RSA, Safenet, Gemalto, McAfee
Use cases

- Strong Authentication and Qualified Signature
- Remote Banking
- Strong Authentication and Qualified Signature
- Mobile Banking
- Strong Authentication
- Mobile Wallet
- Internet
- Cloud Apps
  - PkBox COD
  - PkBox COD
- Remote Signature
  - eCommerce
  - Contracts signature
  - Strong Authentication
Industries

The first 3 most important Italian Banks (contracts signature, eInvoicing, ...)

3 Italian Certification Authorities (Remote Signature Services)

2 Public Body Providers (eInvoicing)

Several small and medium banks

Universities

Outsourcing services for banks

Insurances
Strengths

- Paperless
- Acceleration of all processes – above all new clients acquisition
- Costs saving
- Security
- Up to date platform
PkBox in numbers

2 million active users, distributed as follow:

10 Banks

20 Universities

3 Certification Authorities

2 Outsourcing Services Companies

4 Insurances

10 Public Bodies

10 Manufacturing Enterprises
PkBox was confirmed as SSCD and can be used to implement Remote Qualified Electronic Signature solutions

PkBox has been confirmed as a **Secure Signature Creation Device (SSCD)** by **A-SIT** (Austria - Secure Information Technology Center) the body designated by Austria according to the Article 3(4) of the **Directive 1999/93/EC** to comply with the requirements set out in Annex III of the Directive and can therefore be used for the realization of **Remote Qualified Electronic Signature** solutions with full legal validity.

The confirmation certificate is valid in all the member States of the European Union according to Article 3(4): "The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. [...] A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States".

The **eIDAS Regulation** extends the validity of Article 3(4) of the Directive 93/1999/93/EC after the its repeal. Article 51(1) reads: "Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation".
The eIDAS Regulation recognizes the benefits of remote electronic signatures

Recital (52): The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.
Requirements for Qualified remote electronic signature solutions from the eIDAS Regulation

Recital 55 states that "**IT security certification based on international standards such as ISO 15408** and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted"

It should be read in combination with recital 52: "remote electronic signature service providers should apply **specific management and administrative security procedures and use trustworthy systems and products**, including secure electronic communication channels, **in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory**"

According to article 30, the Certification of qualified electronic signature creation devices shall be based on a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products present in a list to be established by the Commission.
Qualified remote electronic signature solutions under the eIDAS Regulation: a proposal

A remote signature solution is in general the combination of software and an HSM hosted by a TSP.

Our proposal is that the certification of the SSCD is a combination of:

ISO 15408 certification of the HSM for Signatory key pair generation, storage and signature creation

Define a specific qualification path for TSPs offering the service by developing a specific policy and security requirement standard, based on TS 419 241 (Security Requirements for Trustworthy Systems Supporting Server Signing) or its evolution, to be assessed by a Conformity Assessment Body accredited with EN 319 403 and under supervision.
Security Pill of the day

At the end of the day, the goals are simple: safety and security.

Jodi Rell

Security is an attitude: learn it with a game!
www.catchergame.com