

CryptoSignServer TECHNICAL INFORMATION

CryptoSignServer consist of a hardware/software platform, which ensures security on the processes of electronic signature and validation in computer systems-oriented services.

Technical Specifications

HSM System

This consists of integrating a storage cryptographic module and a key administration platform, which allows multiple operations and configuration management, related to key generation and electronic certificates importation. The cryptographic device is certified by the FIPS 140-2 Level 3 standard.

Features:

HSM compiles with the certification standard FIPS 140-2 level 3.

The firmware module prevents the output of confidential data.

It prevents access to various parts of the HSM with sensors that detect intrusions or anomalies, erasing the information..

The HSM is covered by an opaque epoxy resin, a metal cover protects the whole.

Server System

Processor with Intel architecture.

ETHERNET 10/100/1000 Mbps.

Rack System.

Functional Features

Setting up through secure HTTPS protocol, which provides the ability to perform:

- a) Generation of RSA private keys, from 1024 to 2048 bits.
- b) Generation of certificate requests from a safely accredited device.
- c) Import certificates towards the cryptographic device.
- d) Set up the network addresses, re-initialize system services and cryptographic functions embedded in the device.

System Access

At the level of administration, it is presented an authentication model base on a Certification Authority embedded in the device itself. In this CA, it generates electronic certificates that verify the identity of the system administrators.

At the level of custom component, an API is provided, developed in Java technology, which can be integrated in TI platforms, monitoring tasks tools or components embedded in custom applications using simple sentences. This API is independent regardless the platform used.

Included Features

Available Functionalities

- a) Electronic Signature in XAdES format, with capabilities to customize and integrate non-compulsory attributes within its structure.
- b) Electronic Signature in PKCS#7 RSA format.
- c) Electronic Signature in native PDF format.
- d) Electronic Signature(s) verification in native PDF format.
- e) Electronic Signature verification in PKCS#7 RSA format.
- f) Electronic Signature with support for timestamp PKCS7 RSA format.
- g) Electronic Signature with support for timestamp native PDF format, supporting native validation.

Performance

Electronic signature processes executed per hour	1024	2048
Native PDF (a)	189.473,00	132.410,00
Native PDF with timestamp (b)	105.882,00	90.000,00
PKCS#7 RSA	302.740,00	276.000,00
PKCS#7 RSA with timestamp (b)	190.217,00	165.120,00
XAdEs	246.780,00	211.457,00

Electronic Signature Verification

Native PDF(a)	210.631,00
PKCS7	190.974,00

- a. Depends on the number of electronic signatures that has the document
- b. Timestamp is 2048 bits length