HU

NETLOCK.HU/SIGNASSIST

NETLOCK CRYPTOSERVER - SIGNASSIST

Vállalati rendszerekhez illeszthető, automatizált hitelesítőmegoldás

A NETLOCK CryptoServer **SIGNASSIST** egy **új generációs, moduláris felépítésű, univerzális és vállalati IT-rendszerekhez is illeszthető szerveroldali hitelesítő és folyamatvezérlő alkalmazás**, amely komplex és nagyszámú kriptográfiai művelet végrehajtására képes. A **NETLOCK SIGNASSIST CryptoServerrel** nagy megbízhatóságú, illetve nagy biztonsági igényű központosított aláírási környezet alakítható ki, **amely mind szoftveres, mind hardveres (HSM), mind távoli NETLOCK SIGN alapú kulcskezelés támogatására képes**.

TÁMOGATOTT PLATFORMOK, ALÁÍRÁSTÍPUSOK ÉS JOGSZABÁLYI MEGFELELÉS

A NETLOCK CryptoServer SIGNASSIST modul, **Microsoft Windows vagy LINUX** operációs rendszeren is futtatható. A modul **ETSI Baseline XAdES, PAdES, CAdES, ASIC és E-AKTA** aláírás- és időbélyegző formátumokat támogat. A NETLOCK SIGNASSIST alkalmas arra, hogy az átadott dokumentumokat a **910/2014/EU eIDAS rendeletnek és a 2015. évi CCXXII. törvény előírásainak megfelelően kiadott tanúsítványok használatával elektronikus aláírással, elektronikus bélyegzővel, valamint minősített időbélyeggel és visszavonási információval lássa el.**

TÁMOGATOTT FORMÁTUMOK

XAdES, illetve bármely más adattípusú aláírás-formátum használata esetén, bármilyen kiterjesztésű bemeneti fájlformátum elfogadott, a kimeneti állomány pedig egy „.xml” vagy „.dosszie” kiterjesztésű és struktúrájú állomány lesz. **PAdES- (PDF) aláírás-formátumok használata esetén** ISO-32000-1 szabványnak megfelelő PDF-típusú (PDF.1.7+) állományokat fogad el a megoldás, a kimeneti állomány pedig ugyanaz a verziójú PDF-fájl-formátum lesz “.pdf” kiterjesztéssel.

HIGH AVAILABLITY (HA) TÁMOGATÁS

A SIGNASSIST CryptoServer képes nagy rendelkezésre állású, elosztott működésű hitelesítési környezet kialakítására.

E-KONVERZIÓ

A konverziós modul célja a papíralapú dokumentumokról történő hiteles elektronikus másolatkészítés során a hatályos jogszabályok által elvárt hitelesítési záradék elhelyezése az elektronikus dokumentumban.

INTEGRÁCIÓ - REST API, SOAP, CLI, NFS/PIPELINE

A hitelesítési feladatok során a SIGNASSIST alkalmazás a fenti integrációs interfészek támogatásával, többféle kapcsolódási alternatívát kínál az ügyfél műszaki igényeitől függően.

FŐBB FUNKCIÓK ÉS TULAJDONSÁGOK

- **tömeges elektronikus aláírás, bélyegzés, időbélyegzés** – bármilyen fájlformátumra alkalmazva
- **elektronikusan hitelesített állományok hitelesség ellenőrzése** (statikus legfelsőbb szintű és köztes megbízható kiadói lista vagy dinamikus EU TSL alapon)
- **aláírásképek elhelyezése** PDF-dokumentumokon
- **egyidejűleg több**, hitelesítést kérő és hitelesített állományokat fogadó rendszerrel képes együttműködni
- elektronikus dokumentumok **titkosítása és titkosított elektronikus dokumentumok visszafejtése**
- **több szoftveres, hardveres, NETLOCK | SIGN HIBRID aláíró kulcs** kezelése
- az összes eIDAS által szabványosított aláírás-formátum kezelése (ETSI Baseline XAdES, PAdES, CAdES, Asic és E-AKTA)
- **többféle kapcsolódási alternatíva más rendszerekhez** (pl. REST API, SOAP, NFS/PIPELINE, CLI)
- **hitelesítési folyamatvezérlési műveletek**, aláírási profilok és ezek közötti prioritássorrend, elő- és utóműveletek kezelése
- elektronikusan aláírt állományok **megküldése e-mailben**
- **redundancia**, nagyfokú rendelkezésre állás, skálázhatóság
- **naplózási folyamatok**, naplóarchiválás
- **eIDAS COMPLIANT** megoldás

EN

NETLOCK.HU/SIGNASSIST-EN

NETLOCK CRYPTOSERVER - SIGNASSIST

Automated authentication solution for enterprise systems

NETLOCK CryptoServer **SIGNASSIST** is a **modular, universal server-side authentication and process control application** that is **able to perform complex and large number of cryptographic operations and can be embedded in enterprise systems**. By means of NETLOCK CryptoServer, a high reliability, high security level centralized signature environment can be created that supports software, hardware (HSM) and remote NETLOCK SIGN based key management.

SUPPORTED PLATFORMS, SIGNATURE FORMATS AND COMPLIANCE

The NETLOCK CryptoServer SIGNASSIST module can also be run on **Microsoft Windows and LINUX** operating systems. The module supports **ETSI Baseline XAdES, PAdES, CAdES, ASIC & E-AKTA** signature and time stamp formats. NETLOCK CryptoServers are able to attach electronic signatures, electronic seals, as well as qualified time stamps and revocation information to the submitted documents **by using certificates issued in accordance with the provisions of Regulation 910/2014/EU (eIDAS) and Act CCXXII of 2015**.

SUPPORTED FILE FORMATS

When using XAdES or any other data-type signature formats, any extension of input file formats is accepted and the output file will be of „.xml" extension and structure. When using **PAdES (PDF)** signature formats, the application will accept PDF-type (PDF.1.7+) files conforming to ISO-32000-1 standard and the output file will be a PDF file format of the same version with „.pdf" extension.

HIGH AVAILABLITY (HA) SUPPORT

SIGNASSIST CryptoServer is able to create a high availability authentication environment in which each CryptoServer application can cooperate together.

E-CONVERSION

The purpose of the Conversion Module is to place an authentication clause, required by the legislation in force, in the electronic document while generating an authentic electronic copying of paper documents.

INTEGRATION

The SIGNASSIST authentication application **offers several (REST API, SOAP, CLI, NFS/PIPELINE) connectivity options** depending on the customer's technical requirements.

MAIN FUNCTIONS AND PROPERTIES

- **batch electronic signatures, seals, time stamps** – applied to any file format
- **verification** of authenticated documents (static or dynamic EU TSL based)
- **placing signature images** on PDF documents
- **simultaneous cooperation** with several systems that require electronic signature and accept e-signed files
- **encryption and decryption** of electronic documents
- managing multiple software, hardware & NETLOCK SIGN HIBRID signature keys
- handling **multiple types of signature formats** (ETSI Baseline, XAdES, PAdES, CAdES, Asic, E-AKTA)
- **multiple connectivity** alternatives to other systems (e.g. REST API, SOAP, NFS/PIPELINE, CLI)
- **signing process control** operations, signature profiles and their priority order, managing pre- and post-operations
- **redundancy, high availability, scalability**
- **PDF attachments**: attaching documents to a master PDF
- **e-mail forwarding**: sending electronically signed files via email using even dynamic e-mail addresses
- **logging** processes, log archiving
- **eIDAS COMPLIANT** solution