Signant DevOp Security

Last updated: 09.01.2023

Content

Purpose

The purpose of this document is to provide transparent information on security- and operational management data related to Signant services for electronic identification, digital signatures and archive with LTV maintenance.

Overview

Signant is an online service for digital signatures. The service enables you to create signature postings and retrieve digital signatures from your business associates. Signant provides advanced electronic signature by means of PAdES documents. This is a strong electronic signature defined by the acts related to electronic signatures, which sets high standards for authentication of document contents and validation of signatures.

How it works

The basic concept of Signant as a signature portal is as follows (see Figure 1 Signant basic workflow). The posting owner uploads documents to be signed to the service and register signatories. The signature center notification module will then start to request the signatories of their signatures. The signatories connect to the signature center by mean an online web interface. After all the signatories have signed the document online, the posting owner can download signed documents. If selected the Signed documents are automatically committed to the online archive.

Figure 1 Signant basic workflow

Technical environments

The Signant development ant test life cycle includes three separated environments:

I. Production environment
II. Pre-production and integrational test environment
III. Test and development

The technical environments comprise the following technology components:

- Load balancer
- Web servers
- SQL database server
- File storage server
- Hardware security module (HSM), and hosted hard tokens
- Power and network infrastructure

Production environment

The production environment is the environment in which the Signant services is performed and that meets all the specified requirements for performance, durability and security. The production environment is exposed to public usage and interacts with production environments from the featured eID-providers.

Location:	Amazon Webservices region Frankfurt
Data backup:	Amazon Webservices region Frankfurt
HSM:	Amazon CloudHSM region Frankfurt
Hard tokens:	Datacenter in Oslo

Pre-production and integrational test environment

The pre-production and integrational test environment is the environment in which the service is made available to integrational customers and 3-party vendors to test their integrated functionality. This environment is exposed to public usage and interacts with test-environments from the featured eID-providers.

Location:	Amazon Webservices region Frankfurt
Data backup:	Amazon Webservices region Frankfurt
HSM:	Amazon CloudHSM region Frankfurt
Hard tokens:	Datacenter in Oslo

Test and development

The test and development environment is the environment in which the service is developed and tested with new functionality. This environment is only available to the Signant development team.

Location:	Datacenter in Oslo

Security

Internal organization

The security organization consist of the Board, Administration & Management, Development and Operation staff members, and Development & Quality Assurance.

The Board of Directors is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the Chief Executive Officer (CEO).

The Executive Directors give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the Security Committee (SC) chaired by the Chief Security Officer (CSO).

Security objectives

Perspective	Objective	Location
Operations	Production environment containing • Customer documents • Customer meta data • Customer user information • Customer certificates hard token	Oslo, Frankfurt

Security description

Internal operational security

The security objectives are secured by means of physical, digital and organizational control mechanisms. The production environment is both physically and digitally isolated from unauthorized personnel.

Authorization to the production environment
Only Signant DevOp staff members are granted access to the production environment.

Authentication to the production environment
Digital access to the production environment is controlled by means of two factor authentication.

External operational security

All communication with Signant is secured by means of SSL Evident encryption connection (HTTPS). This protects data and documents to and from the production environment database and file server.

All user access and login to Signant requires PKI authentication from the supported e-ID providers. All user access and operations are logged.

Confidentiality, data integrity and availability

Data and personal data are only available to the operations personnel. All user access and operations are logged. All Maestro employees and operations personnel are subject to a Non Disclosure Agreement.

Access recovery, and recovery of data after an incident

The provider restores availability and access to data and service in line with the Service Level Agreement. The provider maintains traceability of events and the ability to re-construct data from backup. Backup is performed on a daily basis to a geographical separated location from the production environment.

Testing and evaluation of technical and organisational measures:

The provider conducts testing and evaluation of its own technical and organisational measures. Tests and review of security policy and security organization are carried out regularly and at least once annually.

Physical security and Environmental Protection

Physical security and environmental protection of the production environment is defined by controls provided by the cloud provider. For Amazon Web Services see the System and Organization Controls Reports (AWS SOC).

Data durability, backup and deletion in the production environment

Documents committed to the e-signature service is stored in the production environment in order to be made available for the signatories to apply their signatures. The time to delete a signature posting is customizable for each submission. A signature posting can be made available up to one year after submission to the service. The current time to delete from backup storage is one year.

Signant Archive with LTV maintenance is optional, and data committed to the Signant Archive with LTV maintenance is not deleted automatically.