Program Requirements

SaaS eSeal Signing Service

Index

1 Program requirements

1.1 Introduction

Electronic trust services are services that increase confidence in online transactions among businesses and consumers. The eIDAS regulation, as European government decision, applies to this.
Within the Netherlands and within the European Union (EU) also these online services can be safely purchased or affairs with governments organizations can be arranged.

Kadaster signs its outgoing messages in the deed processing process with electronic seals. For trust services, a distinction is made between qualified and non-qualified services. The provision of qualified trust services is subject to stricter requirements under the eIDAS regulation than non-qualified services. This qualified service therefore offers additional guarantees. This schedule of requirements addresses the requirements set for the qualified seal signing service. The functional suitability requirements of the SaaS seal signing service are listed below.

1.2 Functional suitability requirements

Number	***Description***
	Requirements for auto-signing with seals functionality
FSS1.	The seal signing service must be capable of “unattended” automatic signing of high volumes of seal hashes.
FSS2.	The electronic seal signing service is certified and meets the eIDAS requirements for the “unattended” automated creation of qualified (QTSP) eIDAS seal signatures.
	Seal certificate requirements
FSS3.	The electronic seals used in the seal signing service are of a qualified level. The electronic seal service is on the European Commission list of the qualified trust service providers in accordance with the eIDAS Regulation, the List of Trusted Lists (LOTL).
FSS4.	The supplier has a role in the key ceremony with which the qualified seal is added to the seal signing service.
FSS5.	The seal to be created meets the requirements included in the schedule below. Part of the Kadaster requirement is that the 'common name' field must contain the text “Bewaarder”. This is required for production seal and also test seal certificate.

Field	Value
Common Name (CN)	**Bewaarder**
Organization Name (O)	**Dienst voor het Kadaster en de openbare registers**
Country (C)	**NL**
2.5.4.97	**NTRNL-08215619**

Number	***Description***
FSS6.	The root certificate and the intermediate certificates contains the mandatory fields: Common Name (CN), Organization Identifier (2.5.4.97), Organization (O) and as optionally the fields: Country (C), Organization Unit (OU), Locality (L). Other fields for example: email are not accepted. This is required for production seal and also test seal certificate.
	Interface requirements
FSS7.	The seal signing service supports signatures based on standard PKCS#1 for the qualified seal conform CSC specifications (https://cloudsignatureconsortium.org/.)
FSS8.	The seal signing service provides the signing of a single hash in a single service call.
FSS9.	The seal signing service (“Signing Server Application”) offers APIs (REST/JSON) interfaces to perform decoupled and fully automated signing. The integration between the Kadaster (“Signing Creation Application”) and the seal signing service (SSA) has been realized on the basis of remote services in accordance with CloudSignatureConsortium (CSC) specifications, as described in ETSI TS 119 432.
FSS10.	An API interface also provides an option to test in a test environment with a test seal.

1.3 Technical requirements

Number	*Description*
	Request format
T1.	The 'request' of the request REST/JSON API interface is the result of a hash function, where the hash function is executed with at least SHA256.
T2.	The format (encoded string) of the 'request' REST/JSON API remote signing interface is hex-encoded or base64-encoded.
T3.	The interface pattern for the request to the REST/JSON is synchronous and one signing per request.
	Response format:
T4.	The response from the seal signing service's REST/JSON API interface is a PKCS#1 RSA standard signature of the hash as input.
T5.	The PKCS#1 (Public-Key Cryptography Standards version 2.2 in accordance with RFC 8017) has been realized (at least) with an RSA2048 key bits size. Algorithm and key lengths must comply with the ETSI/eIDAS requirements at all times now and in the future. Other algorithms such as elliptic curves are not allowed.
T6.	The format (encoded string) of the response of the REST/JSON API remote signing interface is either hex-encoded or base64-encoded.
T7.	The public part of the seal certificate, which is used to sign a hash, is shared with Kadaster in order to be able to verify the signing.
T8.	The eseal signing certificate is according to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
T9.	The eseal signing certificate CRL according to the Section 5.2.3 of RFC 5280 accomplish the rule: the CRL number MUST be greater than the CRL number field in the immediately preceding CRL issued by this CA. CRL numbers are monotonically increasing.
	Authentication/authorization method:
T10.	The seal signing service requires no user interaction. (It implements automatic "unattended" seal signatures. The communication between the Kadaster 'Signing Creation Application' and the QTSP-eSeal service is authorized once by the Kadaster mandated auditor.)
T11.	The communication between the Kadaster service and the seal signing service QTSP ('Signing Server Application') remote signing service is authorized/authenticated according to the https://cloudsignatureconsortium.org security standards.

1.4 Performance requirements

The performance requirements are defined in number of transactions to be processed per day as well as the number of signing transactions per second at peak times.

Number	Description
PE1.	The seal signing service must be able to create 30000 seals signatures per day.
PE2.	Peaks of 5 seal signatures per second must be able to be processed.
PE3.	Performance per hash signing averages 500 ms.

1.5 Availability requirements

The availability indicates the time that the seal signing service is actually available for use.

Number	Description
BE1.	The target for the availability level of the seal signing service is an availability of at least 99.5%, during office hours and outside office hours (7 x 24 hours).
BE2.	The seal signing service will run 24x7, no downtime is necessary in normal operation.
BE3.	In case of an unexpected seal signing service production environment it is supposed to be solved as soon as possible, with a maximum allowable downtime of 4 hours.
BE4.	The test environment has a performance per hash signing 500 ms.
BE5.	The test environment has an availability of at least 95%, during office hours and outside office hours (7 x 24 hours).

1.6 Supplier requirements

Number	***Description***
LEV1.	The supplier appoints a permanent contact person and a permanent account manager for the client. These contact persons have permanent replacements.
LEV2.	Installation and implementation – insofar as carried out/supported by The supplier – are carried out by certified or authorized personnel. Kadaster may require a confidentiality statement.
LEV3.	The supplier will cooperate on a quarterly basis in contract management consultations between the supplier and Kadaster. The purpose of this consultation is to discuss invoicing, (new) developments and the quality and status of the service. The frequency of the consultation can be adjusted as needed and in mutual consultation.
LEV4.	The services and agreements between the client and the contractor are laid down in a Service Level Agreement. The contractor provides a draft for the SLA upon registration.
LEV5.	The supplier provides a monthly (self-service) report to Kadaster regarding the number of services provided in the form of signings, the service levels provided and any (security) incidents.
LEV6.	The supplier reports, at least 2 months in advance, changes to the interfaces or changes to the signing certificates and offers a test option on a specific test environment.
LEV7.	The supplier provides support for: solving incidents, updates to the services / certificates and other questions. If necessary, direct contact with the technical specialist will be possible.