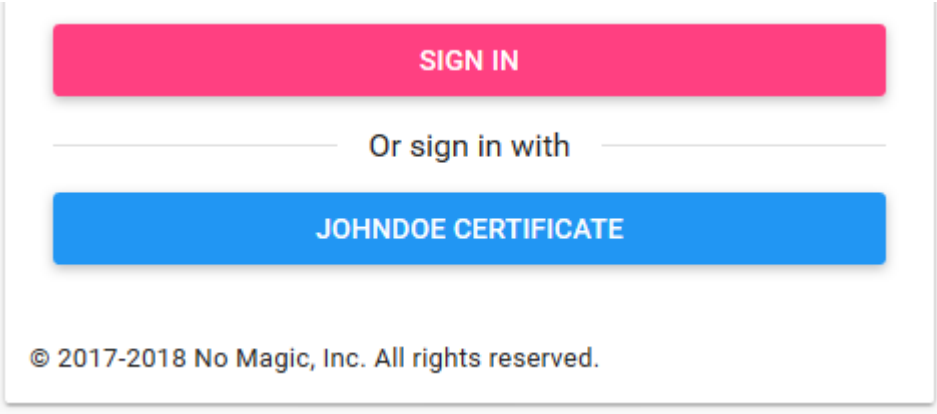
Authentication by certificate

The following parameters are utilized to authenticate the user by using certificates, e.g., certificates from CAC cards.

Parameter	Required	Description	Default value
server.ssl.client-auth	no	A flag indicating if a client certificate is needed or wanted. This flag is required if certificate authentication is enabled. The available value is **want**.	want
server.ssl.trust-store	no	The path to a truststore file in the file system. It can be relative to the Authentication Server directory or absolute. The path is required if certificate authentication is enabled. All certificates added into the */config/truststore* directory will be imported into the truststore file.	config/truststore.jks
server.ssl.trust-store-type	no	A Truststore type, required if certificate authentication is enabled. The available type is **JKS**.	JKS
server.ssl.trust-store-password	no	A Truststore password, required if certificate authentication is enabled and the truststore is password-protected.	secret
authentication.certificate.enabled	no	An option that enables or disables certificate authentication. Available values are **true** and **false**.	false
authentication.certificate.username. template	no	A template used to create a username from the subject DN (Distinguished Name) stored on the certificate. This template is required if certificate authentication is enabled. The template can contain ASCII characters as well as placeholders in round brackets that are replaced with relative distinguished name (RDN) values from the DN, as, for example, when the subject DN on the certificate is *CN=JohnDoe, O=MyCompany,C=GB*: • Template: *(CN)*, username: *JohnDoe* • Template: *(O)-(CN)*, username: *MyCompany-JohnDoe* • Template: *CERT_(CN)*, username: *CERT_ JohnDoe*	(CN)
authentication.certificate.displayname. template	no	A template used to create a display of the subject DN (Distinguished Name) stored on a certificate. This template is required if certificate authentication is enabled. The template is specified the same way as a username template, except that the display name is used for display purposes only. The display name is shown on the authentication button, which authenticates the user using a selected certificate. For example, when the subject DN on the certificate is *CN=JohnDoe,O=MyCompany,C=GB*, and the display template is *(CN) CERTIFICATE*, the following authentication button will be displayed: 	(CN)
authentication.certificate.revocation. list.file	no	The absolute path to the certificate revocation list (CRL) file, if it is stored on the filesystem. Multiple files are available if there are several certificate revocation lists. If there are multiple files, separate each file by a comma (for example, <Path and file name 1>,<Path and file name 2>, <Path and file name 3>).	-
authentication.certificate.revocation. list.url	no	The URL of the certificate revocation list (CRL) file, if it is available on the web. Multiple URLs are available if there are several certificate revocation lists. If there are multiple URLs, separate each URL by a comma (for example, <URL1>,<URL2>, <URL3>).	-

A configuration example

```
server.ssl.trust-store=config/truststore.jks
server.ssl.trust-store-password=YOUR_TRUSTSTORE_PASSWORD
server.ssl.trust-store-type=JKS
server.ssl.client-auth=want
authentication.certificate.enabled=true
authentication.certificate.username.template=(O)-(CN)
authentication.certificate.displayname.template=(CN)'s Smart Card
```