

# Authentication by certificate

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

| 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 <b>want</b> .                                                                                                                                                                                                                                                                                         | want          |
| authentication.certificate.enabled              | no       | An option that enables or disables certificate authentication. Available values are <b>true</b> and <b>false</b> .                                                                                                                                                                                                                                                                                                                                          | false         |
| authentication.certificate.headers.enabled      | no       | An option that enables or disables certificate authentication when authentication server is under proxy. Available values are <b>true</b> and <b>false</b> . This option by default is hidden and should be used only if authentication server is not accessible without a proxy.                                                                                                                                                                           | false         |
| authentication.certificate.username.source      | no       | Source of the username. Available values: <b>dn</b> (if the username is constructed from the Subject Distinguished Name) or <b>san</b> (if the username is constructed from the Subject Alternative Name).                                                                                                                                                                                                                                                  | dn            |
| authentication.certificate.username.san.type    | no       | If <i>authentication.certificate.username.source</i> value is <b>san</b> , this parameter specifies the type of SAN to use. Available values:<br><br><b>0</b> - other name,<br><br><b>1</b> - RFC 822 name,<br><br><b>2</b> - DNS name,<br><br><b>4</b> - directory name (in case of this type parameter <i>authentication.certificate.username.template</i> is required).                                                                                  | 4             |
| authentication.certificate.username.template    | no       | Template that is used to create username from the subject DN (Distinguished Name) or SAN (Subject Alternative Name) of type 4 stored on the certificate. Required if certificate authentication is enabled.<br><br>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.                                                                         | (CN)          |
| authentication.certificate.displayname.source   | no       | Source of the display name on login page. Available values: <b>dn</b> (if the username is constructed from the Subject Distinguished Name) or <b>san</b> (if the username is constructed from the Subject Alternative Name).                                                                                                                                                                                                                                | dn            |
| authentication.certificate.displayname.san.type | no       | If <i>authentication.certificate.displayname.source</i> value is <b>san</b> , this parameter specifies the type of SAN to use. Available values:<br><br><b>0</b> - other name,<br><br><b>1</b> - RFC 822 name,<br><br><b>2</b> - DNS name,<br><br><b>4</b> - directory name (in case of this type parameter <i>authentication.certificate.displayname.template</i> is required).                                                                            | 4             |
| authentication.certificate.displayname.template | no       | Template that is used to create a display of the subject DN (Distinguished Name) or SAN (Subject Alternative Name) of type 4 stored on the certificate. Required if certificate authentication is enabled.<br><br>The template specified the same way as username template, except that display name is used for display purposes only. Display name is shown on authentication button that enables the user to authenticate with the selected certificate. | (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.<br><br>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.<br><br>If there are multiple URLs, separate each URL by a comma (for example, <URL1>,<URL2>,<URL3>).                                                                                                                                                                                   | -             |

## A configuration example

```
server.ssl.client-auth=want
authentication.certificate.enabled=true
authentication.certificate.username.source=san
authentication.certificate.username.san.type=4
authentication.certificate.username.template=(0)-(CN)
authentication.certificate.displayname.source=dn
authentication.certificate.displayname.template=(CN)'s Smart Card
```

