X-Road: Audit log events

Specification

Version: 1.8
25.02.2017

Doc. ID: SPEC-AL

Version history

Date	Version	Description	Author
11.09.2015	0.1	Initial version	Kristo Heero
14.09.2015	0.2	Bug fixes	Kristo Heero
16.09.2015	0.3	Made editorial changes in introduction	Margus Freudenthal
18.09.2015	1.0	Editorial changes made	Imbi Nõgisto
09.10.2015	1.1	Delete certificate/key events of security server updated	Kristo Heero
12.10.2015	1.2	Updated CSR generation events. Fields `nameExtractorMemberClass` and `nameExractorMethod` replaced with field `certificateProfileInfo`	Kristo Heero
20.10.2015	1.3	New events 'Add subsystem' and 'Register management service provider as security server client' added	Kristo Heero
21.10.2015	1.4	New fields `managementRequestId` and `keyLabel` added	Kristo Heero
23.10.2015	1.5	Data field of the event 'Edit WSDL' changed	Kristo Heero
8.12.2015	1.6	Added audit log events for TLS internal key certificate requests and certificate import	Ilkka Seppälä
10.05.2016	1.7	Merged changes from xtee6-doc repo. Added *New event 'Skip unregistration of authentication certificate' added* change made by Meril Vaht on 10.12.2015.	Kedi Välba
25.02.2017	1.8	Converted to Github flavoured Markdown, added license text, adjusted tables for better output in PDF	Toomas Mölder

Table of Contents

License

1. Introduction

X-Road central and security servers keep audit log. The audit log events are generated by user interfaces when the user changes system state or configuration. Additionally, the utility *signer-console* generates audit log events. The user actions are logged regardless of whether the outcome was a success or a failure.

This document provides complete list of all audit log events and theirs related data sets.

1.1 Format of the Audit Log Event

The audit log record contains description of the audit log event in JSON [JSON] format. The field `event` represents the description of the event, the field `user` represents the user name of the performer (events started by the system have the user name *system*), and the field `data` represents data fields related with the event:

```
{
"event": "...",
"user": "...",
"reason": "...",
"data": {"data_field_1": "data_field_1_value", ...}
}
```

In case of failure the event description ends with suffix `failed` and related data set may contain less data fields than normally. Also, an additional field `reason` for the error message will be added.

Section 2 lists all the possible (successful) event descriptions and corresponding set of data fields (some fields are optional).

1.1.1 Common Value Structures of the Data Fields

Values of data fields `memberIdentifier`, `clientIdentifier`, `ownerIdentifier`, `providerIdentifier`, and `serviceProviderIdentifier` have a common structure:

```
{
"xRoadInstance": "...",
"memberClass": "...",
"memberCode": "..."
}
```

where `xRoadInstance` is the X-Road instance, `memberClass` is the X-Road member class, and `memberCode` is the X-Road member code. In case of `clientIdentifier`, `providerIdentifier`, and `serviceProviderIdentifier` an optional field `subsystemCode` (the X-Road subsystem code) is present in the structure.

1.2 References

1. [JSON] Introducing JSON, http://json.org/

2. Audit Log Events

2.1 Central Server

2.1.1 Common Events

The audit log events related to the UI logging and the UI language settings.

Event	Data fields
Log in user	
Log out user	
Set UI language	- `locale` – the selected UI locale (e.g en)

2.1.2 Members Events

The audit log events related to configuration of the X-Road members.

Event	Data fields
Add member	- `memberName` – the member name of the added member - `memberClass` – the member class of the added member - `memberCode` – the member code of the added member
Edit member name	- `memberName` – the new member name of the edited member

Event	Data fields
- `memberClass` – the member class of the edited member - `memberCode` – the member code of the edited member	
Delete member	- `memberClass` – the member class of the deleted member - `memberCode` – the member code of the deleted member
Add security server	- `serverCode` – the server code of the added security server - `ownerClass` – the owner class of the added security server - `ownerCode` – the owner code of the added security server - `certHash` – the hash of the authentication certificate of the added security server - `certHashAlgorithm` – the hash algorithm used to calculate value of the field certHash
Add member to global group	- `groupCode` – the group code of the selected global group - `memberClass` – the member class of the member added to the selected group - `memberCode` – the member code of the member added to the selected group - `memberSubsystemCode` – the subsystem code of the member added to the selected group
Remove member from global group	- `groupCode` – the group code of the selected global group

Event	Data fields
- `memberClass` – the member class of the member removed from the selected group - `memberCode` – the member code of the member removed from the selected group - `memberSubsystemCode` – the subsystem code of the member removed from the selected group	
Add subsystem	- `memberClass` – the member class of the added subsystem - `memberCode` – the member code of the added subsystem - `memberSubsystemCode` – the subsystem code of the added subsystem
Delete subsystem	- `memberClass` – the member class of the deleted subsystem - `memberCode` – the member code of the deleted subsystem - `memberSubsystemCode` – the subsystem code of the deleted subsystem
Register member as security server client	- `serverCode` – the server code of the selected security server - `ownerClass` – the owner class of the selected security server - `ownerCode` – the owner code of the selected security server - `clientIdentifier` – the client identifier of the member registered as client of the selected security server

Event	Data fields
Unregister member as security server client - `ownerClass` – the owner class of the selected security server - `ownerCode` – the owner code of the selected security server - `clientIdentifier` – the client identifier of the member unregistered as client of the selected security server	- `serverCode` – the server code of the selected security server

2.1.3 Security Servers Events

The audit log events related to configuration of the X-Road security servers.

Event: Edit security server address

Data fields:

- `serverCode` – the server code of the edited security server
- `ownerCode` – the owner code of the edited security server
- `ownerClass` – the owner class of the edited security server
- `address` – the new address of the edited security server

Event: Delete security server

Data fields:

- `serverCode` – the server code of the deleted security server
- `ownerCode` – the owner code of the deleted security server
- `ownerClass` – the owner class of the deleted security server

Event: Add authentication certificate for security server

Data fields:

- `serverCode` – the server code of the selected security server
- `ownerCode` – the owner code of the selected security server
- `ownerClass` – the owner class of the selected security server
- `certHash` – the hash of the authentication certificate added to the selected security server
- `certHashAlgorithm` – the hash algorithm used to calculate value of the field certHash

Event: Delete authentication certificate of security server

Data fields:

- `serverCode` – the server code of the selected security server
- `ownerCode` – the owner code of the selected security server

- `ownerClass` - the owner class of the selected security server
- `certHash` – the hash of the deleted authentication certificate of the selected security server
- `certHashAlgorithm` – the hash algorithm used to calculate value of the field certHash

2.1.4 Global Groups Events

The audit log events related to configuration of the X-Road global groups.

Event	Data fields
Add global group	- code – the group code of the added global group

- description – the description of the added global group | | Edit global group description | - code – the group code of the edited global group
- description – the new description of the edited global group | | Delete global group | - code – the group code of the deleted global group
- description – the description of the deleted global group | | Add members to global group | - code – the group code of the selected global group
- description – the description of the selected global group
- memberIdentifiers – the list of member identifiers of the members added to the selected global group | | Remove members from global group | - code – the group code of the selected global group
- description – the description of the selected global group
- memberIdentifiers – the list of member identifiers of the members removed from the selected global group |

2.1.5 Central Services Events

The audit log events related to configuration of the X-Road central services.

Event	Data fields
Add central service	- serviceCode – the service code of the added central service

- targetServiceCode – the target service code of the added central service
- targetServiceVersion – the target service version of the added central service
- providerIdentifier – the provider identifier of the added central service | | Edit central service | - serviceCode – the service code of the edited central service
- targetServiceCode – the (new) target service code of the edited central service
- targetServiceVersion – the (new) target service version of the edited central service
- providerIdentifier – the (new) provider identifier of the edited central service | | Delete central service | - serviceCode – the service code of the deleted central service |

2.1.6 Certification Services Events

The audit log events related to configuration of the X-Road certification services.

Event	Data fields
Add certification service	- caId – the identifier of the added certification service

- caCertHash – the hash of the CA certificate of the added certification service
- caCertHashAlgorithm – the hash algorithm used to calculate value of the field caCertHash
- authenticationOnly – the authentication only flag of the added certification service
- certificateProfileInfo – the fully qualified (Java) class name that implements the CertificateProfileInfo interface of the added certification service | | Edit certification service settings | - caId – the identifier of the edited certification service
- authenticationOnly – the (new) authentication only flag of the edited certification service
- certificateProfileInfo – the fully qualified (Java) class name that implements the CertificateProfileInfo interface of the eddited certification service | | Delete certification service | - caId – the identifier of the deleted certification service | | Add intermediate CA | - caId – the identifier of the selected certification service
- intermediateCaId – the identifier of the intermediate CA added to the selected certification service
- intermediateCaCertHash – the hash of the intermediate CA certificate
- intermediateCaCertHashAlgorithm – the hash algorithm used to calculate value of the field intermediateCaCertHash | | Delete intermediate CA | - intermediateCaId – the identifier of the deleted intermediate CA | | Add OCSP responder of certification service | - caId – the identifier of the selected certification service
- ocspId – the identifier of the OCSP responder added to the selected certification service
- ocspUrl – the URL of the added OCSP responder
- ocspCertHash – the hash of the added OCSP responder certificate
- ocspCertHashAlgorithm – the hash algorithm used to calculate value of the field ocspCertHash | | Add OCSP responder of intermediate CA | - intermediateCaId – the identifier of the selected intermediate CA
- ocspId – the identifier of the OCSP responder added to the selected intermediate CA
- ocspUrl – the URL of the added OCSP responder
- ocspCertHash – the hash of the added OCSP responder certificate
- ocspCertHashAlgorithm – the hash algorithm used to calculate value of the field ocspCertHash | | Edit OCSP responder | - ocspId – the identifier of the edited OCSP responder
- ocspUrl – the (new) URL of the edited OCSP responder
- ocspCertHash – the (new) hash of the edited OCSP responder certificate
- ocspCertHashAlgorithm – the hash algorithm used to calculate value of the field ocspCertHash | | Delete OCSP responder | - ocspId – the identifier of the deleted OCSP responder |

2.1.7 Timestamping Services Events

The audit log events related to configuration of the X-Road timpestamping services.

Event	Data fields
Add timestamping service	- tsaId – the identifier of the added timestamping service

- tsaName – the name of the added timestamping service
- tsaUrl – the URL of the added timestamping service
- tsaCertHash – the hash of the timestamping service certificate
- tsaCertHashAlgorithm – the hash algorithm used to calculate value of the field tsaCertHash | | Edit timestamping

service | - tsaId – the identifier of the edited timestamping service

- tsaName – the (new) name of the edited timestamping service
- tsaUrl – the (new) URL of the edited timestamping service | | Delete timestamping service | - tsaId – the identifier of the deleted timestamping service
- tsaName – the name of the deleted timestamping service
- tsaUrl – the URL of the deleted timestamping service |

2.1.8 Management Requests Events

The audit log events related to the management requests.

Event	Data fields
Revoke client registration request	- requestId – the identifier of the revoked request
Revoke authentication certificate registration request	- requestId – the identifier of the revoked request
Approve registration request	- requestId – the identifier of the approved request
Decline registration request	- requestId – the identifier of the declined request

2.1.9 Configuration Management Events

The audit log events related to configuration management.

Event	Data fields
Re-create internal configuration anchor	- anchorFileHash – the hash of the re-created internal configuration anchor file

- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash | | Generate internal configuration signing key | - tokenId – the identifier of the token used to generate the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the generated signing key
- keyLabel – the label of the generated key
- certHash – the hash of the generated signing certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Activate internal configuration signing key | - tokenId – the identifier of the token owning the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the activated signing key | | Delete internal configuration signing key | - tokenId – the identifier of the token owning the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the deleted signing key | | Re-create external configuration anchor | - anchorFileHash – the hash of the re-created external configuration anchor file

- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash | | Generate external configuration signing key | - tokenId – the identifier of the token used to generate the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the generated signing key
- certHash – the hash of the generated signing key certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Activate external configuration signing key | - tokenId – the identifier of the token owning the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the activated signing key | | Delete external configuration signing key | - tokenId – the identifier of the token owning the signing key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the deleted signing key | | Add trusted anchor | - anchorFileHash – the hash of the added anchor file
- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash
- instanceIdentifier – the X-Road instance identifier of the added anchor
- generatedAt – the UTC time when anchor file was generated
- anchorUrls – the configuration download URLs of the added anchor | | Delete trusted anchor | - anchorFileHash – the hash of the deleted anchor file
- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash
- instanceIdentifier – the X-Road instance identifier of the deleted anchor | | Log in to token | - tokenId – the identifier of the token logged in
- tokenSerialNumber – the serial number of token
- tokenFriendlyName – the friendly name of token | | Log out from token | - tokenId – the identifier of the token logged out
- tokenSerialNumber – the serial number of token
- tokenFriendlyName – the friendly name of token | | Upload configuration part | - sourceType – the source type (internal or external) of the uploaded configuration part
- contentIdentifier – the content identifier of the uploaded configuration part
- partFileName – the internal name of the configuration part file
- uploadFileName – the name of the uploaded configuration part file
- uploadFileHash – the hash of the uploaded configuration part file
- uploadFileHashAlgorithm – the hash algorithm used to calculate value of the field uploadFileHash |

2.1.10 System Settings Events

The audit log events related to the system settings.

Event	Data fields
Edit central server address	- address – the new address of the central server
Register management service provider as security server client	- serverCode – the server code of the management services' security server

- ownerClass – the owner class of the management services' security server
- ownerCode – the owner code of the management services' security server
- clientIdentifier – the client identifier of the registered management service provider | | Edit provider of management services | - serviceProviderIdentifier – the new service provider identifier of the management service
- serviceProviderName – the new service provider name of the management service | | Add member class | - code – the code of the added member class
- description – the description of the added member class | | Edit member class description | - code – the code of the edited member class
- description – the new description of the edited member class | | Delete member class | - code – the code of the deleted member class |

2.1.11 Backup and Restore Events

The audit log events related to backup and restore.

Event	Data fields
Back up configuration	- backupFileName – the name of the created backup file
Upload backup file	- backupFileName – the name of the uploaded backup file
Delete backup file	- backupFileName – the name of the deleted backup file
Restore configuration	- backupFileName – the name of the backup file used to restore configuration

2.2 Security Server

2.2.1 Common Events

The audit log events related to the UI logging and the UI language settings.

Event	Data fields
Log in user	
Log out user	
Set UI language	- locale – the selected UI locale (e.g en)

2.2.2 Initialization Events

The audit log events related to initialization.

Event	Data fields
Initialize anchor	- anchorFileHash – the hash of the initialized anchor file

- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash
- generatedAt – the UTC time when the anchor file was generated | | Initialize server configuration | - ownerI-

dentifier – the owner identifier of the initialized security server

- serverCode – the server code of the initialized security server |

2.2.3 Security Server Clients Events

The audit log events related to the security server clients configuration.

Event	Data fields
Add client	- clientIdentifier – the client identifier of the added client

- isAuthentication – the information system authentication type of the added client
- clientStatus – the status of the added client | | Register client | - clientIdentifier – the client identifier of the registered client
- managementRequestId – the identifier of the corresponding management request in the central server
- clientStatus – the status of the registered client | | Unregister client | - clientIdentifier – the client identifier of the unregistered client
- managementRequestId – the identifier of the corresponding management request in the central server
- clientStatus – the status of the unregistered client | | Delete client | - clientIdentifier – the client identifier of the deleted client | | Delete client certificates | - clientIdentifier – the client identifier of the client which certificates and certificate requests were deleted
- certHashes – the list of hashes of the deleted certificates
- certHashAlgorithm – the hash algorithm used to calculate hash values of the field certHashes
- certRequestIds – the list of identifiers of the deleted certificate requests | | Add WSDL | - clientIdentifier – the client identifier of the selected client
- wsdlUrl – the URL of the added WSDL of the selected client
- disabled – the flag indicating whether the added WSDL and all its services were disabled
- refreshedDate – the time when the added WSDL was refreshed | | Delete WSDL | - clientIdentifier – the client identifier of the selected client
- wsdlUrls – the list of URLs of the deleted WSDLs of the selected client | | Disable WSDL | - clientIdentifier – the client identifier of the selected client
- wsdlUrls – the list of URLs of the disabled WSDLs of the selected client
- disabledNotice – the notice of the disabled WSDLs | | Enable WSDL | - clientIdentifier – the client identifier of the selected client
- wsdlUrls – the list of URLs of the enabled WSDLs of the selected client | | Refresh WSDL | - clientIdentifier – the client identifier of the selected client
- wsdls – the list of the refreshed WSDLs of the selected client. The list item contains of the following data fields:
  - wsdlUrl – the URL of the WSDL
  - servicesAdded – the list of services added during refresh
  - servicesDeleted – the list of services removed during refresh | | Edit WSDL | - clientIdentifier – the client identifier of the selected client
- wsdl – the edited WSDL of the selected client. The value of the field is a structure containing the following data fields:

  - wsdlUrl – the previous URL of the WSDL
  - wsdlUrlNew – the new URL of the WSDL
  - servicesAdded – the list of services added by the new WSDL
  - servicesDeleted – the list of services removed by the new WSDL | | Edit service parameters | - clientIdentifier – the client identifier of the member provided the edited services
- wsdlUrl – the URL of the WSDL of the edited service
- services – the list of the edited services. The list item contains of the following data fields:
  - id – the identifier of the service
  - url – the URL of the service
  - timeout – the timeout of the service
  - tlsAuth – the flag indicating whether the certificate of the service provider should be verified for TLS connections | | Add access rights to service | - clientIdentifier – the client identifier of the member provided the selected service
- serviceCode – the selected service code
- subjectIds – the list of the selected subject identifiers to which the access of the selected service granted | | Remove access rights from service | - clientIdentifier – the client identifier of the member provided the selected service
- serviceCode – the selected service code
- subjectIds – the list of the selected subject identifiers from which the access of the selected service denied | | Add access rights to subject | - clientIdentifier – the client identifier of the member provided the selected service
- subjectId – the selected subject identifier
- serviceCodes – the list of the service codes which access granted to the selected subject | | Remove access rights from subject | - clientIdentifier – the client identifier of the member provided the selected service
- subjectId – the selected subject identifier
- serviceCodes – the list of the service codes which access denied to the selected subject | | Set connection type for servers in service consumer role | - clientIdentfier – the client identifier of the selected client
- isAuthentication – the new information system authentication type of the selected client | | Add internal TLS certificate | - clientIdentfier – the client identifier of the selected client
- certHash – the hash of the certificate added to the selected client
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash
- uploadFileName – the name of the uploaded certificate file | | Delete internal TLS certificate | - clientIdentfier – the client identifier of the selected client
- certHash – the hash of the certificate deleted from the selected client
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Add group | - clientIdentifier – the client identifier of the selected client
- groupCode – the code of the local group added to the selected client
- groupDescription – the description of the added local group | | Edit group description | - clientIdentifier – the client identifier of the selected client
- groupCode – the code of the edited local group of the selected client
- groupDescription – the new description of the edited local group | | Add members to group | - clientIdentifier – the client identifier of the selected client

- groupCode – the code of the selected local group of the selected client
- memberIdentifiers – the list of member identifiers of members added to the selected local group | | Remove members from group | - clientIdentifier – the client identifier of the selected client
- groupCode – the code of the selected global group of the selected client
- memberIdentifiers – the list of member identifiers of the removed members | | Delete group | - clientIdentifier – the client identifier of the selected client
- groupCode – the code of the deleted local group of the selected client
- groupDescription – the description of the deleted local group |

2.2.4 System Parameters Events

The audit log events related to the system parameters.

Event	Data fields
Generate certificate request for TLS	- subjectName – the subject name of the generated certificate request
Import TLS certificate from file	- certHash – the hash of the generated internal TLS certificate

- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Upload configuration anchor | - anchorFileHash – the hash of the uploaded anchor file
- anchorFileHashAlgorithm – the hash algorithm used to calculate value of the field anchorFileHash
- generatedAt – the UTC time when the anchor file was generated | | Add timestamping service | - tspName – the name of the added timestamping service
- tspUrl – the URL of the added timestamping service | | Delete timestamping service | - tspName – the name of the deleted timestamping service
- tspUrl – the URL of the deleted timestamping service | | Generate new internal TLS key and certificate | - certHash – the hash of the generated internal TLS certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash |

2.2.5 Keys and Certificates Events

The audit log events related to keys and certificates management

Event	Data fields
Log in to token	- tokenId – the identifier of the token logged in

- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token | | Log out from token | - tokenId – the identifier of the token logged out
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token | | Generate key | - tokenId – the identifier of the token used to generate the key
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token

- keyId – the identifier of the generated key
- keyLabel – the label of the generated key
- keyFriendlyName – the friendly name of the generated key | | Delete key from configuration | - tokenId – the identifier of the token where the deleted key located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the deleted key
- keyFriendlyName – the friendly name of the deleted key
- keyUsage – the key usage of the deleted key | | Delete key from token | - tokenId – the identifier of the token where the deleted key located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the deleted key
- keyFriendlyName – the friendly name of the deleted key
- keyUsage – the key usage of the deleted key | | Generate CSR | - tokenId – the identifier of the token used to generate the certificate request
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key used to generate the certificate request
- keyFriendlyName – the friendly name of key
- keyUsage – the key usage
- clientIdentifier – the client identifier of the client which certificate request was generated
- subjectName – the subject name of the generated certificate request
- certificationServiceName - the name of the approved certification service for which the CSR was generated
- csrFormat – the format (PEM / DER) of the generated CSR file | | Delete CSR | - tokenId – the identifier of the token where the key of the deleted certificate request located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key related to the deleted certificate request
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the deleted certificate request | | Import certificate from file | - certFileName – the name of the imported certificate file
- certHash – the hash of the imported certificate file
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash
- keyUsage – the key usage of the imported certificate
- clientIdentifier – the client identifier of the member constructed from signing certificate | | Import certificate from token | - tokenId – identifier of the token where imported certificate located

- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key related to the imported certificate
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the imported certificate
- certHash – the hash of the imported certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash
- clientIdentifier – the client identifier of the member constructed from signing certificate | | Delete certificate from configuration | - tokenId – the identifier of token where the key of the deleted certificate located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the deleted certificate
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the deleted certificate
- certHash – the hash of the deleted certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Delete certificate from foken | - tokenId – the identifier of token where the key of the deleted certificate located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the deleted certificate
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the deleted certificate
- certHash – the hash of the deleted certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Enable certificate | - tokenId – the identifier of token where the key of the enabled certificate located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the enabled certificate
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the enabled certificate
- certHash – the hash of the enabled certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Disable certificate | - tokenId – the identifier of the token where the key of the disabled certificate located
- tokenSerialNumber – the serial number of the token

- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the disabled certificate
- keyFriendlyName – the friendly name of the key
- keyUsage – the key usage
- certId – the identifier of the disabled certificate
- certHash – the hash of the disabled certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash | | Register authentication certificate | - tokenId – the identifier of token where key of authentication certificate locates
- tokenSerialNumber – the serial number of token where key of authentication certificate locates
- tokenFriendlyName – the friendly name of token where key of authentication certificate locates
- keyId – the identifier of key of registered authentication certificate
- certId – the identifier of registered authentication certificate
- certHash – the hash of registered authentication certificate
- certHashAlgorithm – the hash algorithm used to calculate value of field certHash
- address – the address of security server which authentication certificate was registered
- managementRequestId – the identifier of the corresponding management request in the central server
- certStatus – the status of registered certificate | | Unregister authentication certificate | - tokenId – the identifier of the token where the key of the authentication certificate located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the unregistered authentication certificate
- certId – the identifier of the unregistered authentication certificate
- certHash – the hash of the unregistered authentication certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash
- managementRequestId – the identifier of the corresponding management request in the central server
- certStatus – the status of the unregistered certificate | | Skip unregistration of authentication certificate | - tokenId – the identifier of the token where the key of the authentication certificate located
- tokenSerialNumber – the serial number of the token
- tokenFriendlyName – the friendly name of the token
- keyId – the identifier of the key of the unregistered authentication certificate
- certId – the identifier of the unregistered authentication certificate
- certHash – the hash of the unregistered authentication certificate
- certHashAlgorithm – the hash algorithm used to calculate value of the field certHash
- certStatus – the status of the unregistered certificate | | Set friendly name to token | - tokenId – the identifier of the selected token
- tokenSerialNumber – the serial number of the selected token
- tokenFriendlyName – the new friendly name of the selected token | | Set friendly name to key | - keyId – the identifier of the selected key

- keyFriendlyName – the new friendly name of the selected key |

2.2.6 Backup and Restore Events

The audit log events related to backup and restore.

Event	Data fields
Back up configuration	- backupFileName – the name of the created backup file
Upload backup file	- backupFileName – the name of the uploaded backup file
Delete backup file	- backupFileName – the name of the deleted backup file
Restore configuration	- backupFileName – the name of the backup file used to restore configuration

2.3 Utility signer-console

The audit log events logged by the utility signer-console.

Event	Data fields
Set a friendly name to the token	- tokenId – the entered token identifier

- tokenFriendlyName – the new friendly name for the entered token | | Set a friendly name to the key | - keyId – the entered key identifier
- keyFriendlyName – the new friendly name for the entered key | | Activate the certificate | - certId – the identifier of the activated certificate | | Deactivate the certificate | - certId – the identifier of the deactivated certificate | | Delete the key from token | - keyId – the identifier of the deleted key | | Delete the certificate | - certId – the identifier of the deleted certificate | | Delete the certificate request | - certRequestId – the identifier of the deleted certificate request | | Import a certificate from the file | - certFileName – the name of the imported certificate file
- clientIdentifier – the client identifier of the member constructed from signing certificate
- keyId – the identifier of the key to which the certificate was imported. | | Log into the token | - tokenId – the identifier of the token logged in | | Initialize the software token | - tokenId – the identifier of the initialized token | | Generate a key on the token | - tokenId – the identifier of the token used to generate the key
- keyId – the identifier of the generated key
- keyLabel – the label of the generated key | | Generate CSR | - keyId – the identifier of the key used to generate the certification request
- keyUsage – the key usage
- clientIdentifier – the client identifier of the client which certificate request was generated
- subjectName – the subject name of the generated certification request
- csrFormat – the format (PEM / DER) of the generated CSR file |