



|  |
| --- |
| X-Road: Audit log events  **Specification** |
| Version: 10  25.11.2022  26 pages  Doc. ID: SPEC-AL |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| 10.05.2020 | 1.8 | Updated to match current implementation | Janne Mattila |
| 14.5.2021 | 1.9 | Added log entry for central server initialization | Teemu Kurki |
| 25.11.2022 | 1.10 | Added audit log event fields for timestamp service certificate changes | Eneli Reimets |

Table of Contents

[1 Introduction 5](#_Toc42083331)

[1.1 Format of the Audit Log Event 5](#_Toc42083332)

[1.1.1 Extended Audit Log Format for Security Server 5](#_Toc42083333)

[1.1.2 Common Value Structures of the Data Fields 6](#_Toc42083334)

[1.2 References 6](#_Toc42083335)

[2 Audit Log Events 7](#_Toc42083336)

[2.1 Central Server 7](#_Toc42083337)

[2.1.1 Common Events 7](#_Toc42083338)

[2.1.2 Members Events 7](#_Toc42083339)

[2.1.3 Security Servers Events 8](#_Toc42083340)

[2.1.4 Global Groups Events 9](#_Toc42083341)

[2.1.5 Central Services Events 9](#_Toc42083342)

[2.1.6 Certification Services Events 10](#_Toc42083343)

[2.1.7 Timestamping Services Events 11](#_Toc42083344)

[2.1.8 Management Requests Events 12](#_Toc42083345)

[2.1.9 Configuration Management Events 12](#_Toc42083346)

[2.1.10 System Settings Events 14](#_Toc42083347)

[2.1.11 Backup and Restore Events 14](#_Toc42083348)

[2.2 Security Server 15](#_Toc42083349)

[2.2.1 Common Events 15](#_Toc42083350)

[2.2.2 Initialization Events 15](#_Toc42083351)

[2.2.3 Security Server Clients Events 15](#_Toc42083352)

[2.2.4 System Parameters Events 18](#_Toc42083353)

[2.2.5 Keys and Certificates Events 20](#_Toc42083354)

[2.2.6 Backup and Restore Events 24](#_Toc42083355)

[2.2.7 API Key Management Events 24](#_Toc42083356)

[2.2.8 Technical Events 25](#_Toc42083357)

[2.3 Utility signer-console 25](#_Toc42083358)

License

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/3.0/.

# 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.

## 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.

Security server audit log contains some additional elements, described in the next chapter.

Section Error: Reference source not found lists all the possible (successful) event descriptions and corresponding set of data fields (some fields are optional).

### Extended Audit Log Format for Security Server

Security server uses REST APIs to update data, and a new audit log implementation adds some features that are useful in auditing updates done throught the API.

Example of extended audit log message for the security server:

2020-05-28T18:47:40+00:00 xroad-lxd-ss5 correlation-id: [e4591e2949c156e7] INFO [X-Road Proxy Admin REST API] 2020-05-28T18:47:40.801Z - {"event":"Edit service description","user":"xrd","auth":"Session","url":"/api/service-descriptions/210","data":{"clientIdentifier":{"xRoadInstance":"LXD","memberClass":"GOV","memberCode":"M5","subsystemCode":"AUDITLOGTEST2"},"wsdl":{"servicesAdded":["xroadSmallAttachment.v1"],"servicesDeleted":["xroadGetRandom.v1"]},"url":"http://xroad-lxd-cs.lxd/A.wsdl","serviceType":"WSDL","urlNew":"http://xroad-lxd-cs.lxd/B.wsdl"}}

Log contains (outside of the actual audit log event JSON) correlation-id element which can be used to associate audit log entry with a specific request, regular log entries and e.g. stacktraces from regular log.

Audit log event JSON contains these additional elements:

* auth
  + authentication type used for this API call
  + possible values:
    - Session – session based authentication (web application)
    - ApiKey - direct API call using API key authentication
    - HttpBasicPam – HTTP basic authentication with PAM login (for api key management API operations)
* url
  + url of called API endpoint
* warning
  + for failed events, boolean indicating whether the failure was caused by unhandled warnings

{

"event": "...",

"user": "...",

"reason": "...",

"warning": true,

"auth": "Session",

"url": "/api/service-descriptions/249",

"data": {"data\_field\_1": "data\_field\_1\_value", ...}

### 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.

## References

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

# Audit Log Events

## Central Server

### 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) |

### Initialization Events

The audit log events related to initialization.

|  |  |
| --- | --- |
| **Event** | **Data fields** |
| Initialize central server | * IntanceIdentifier – identifier of the instance for which central server is initialized * CentralServerAddress – IP address or hostname of the central server * HaNode – Which central server HA (High Availability) node it is. |

### 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 * 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 * 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 |
| Unregister 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 unregistered as client of the selected security server |

### Security Servers Events

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

|  |  |
| --- | --- |
| **Event** | **Data fields** |
| Edit security server address | * 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 |
| Delete security server | * 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 |
| Add authentication certificate for security server | * 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 |
| Delete authentication certificate of security server | * 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 |

### 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 |

### 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 |

### 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 |

### 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 * tsaCertHash – the hash of the timestamping service certificate * tsaCertHashAlgorithm – the hash algorithm used to calculate value of the field tsaCertHash |
| 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 |

### 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 |

### 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 |

### 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 |

### 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 |

## Security Server

### Common Events

The audit log events related to the UI logging.

|  |  |
| --- | --- |
| **Event** | **Data fields** |
| Log in user |  |
| Log out user |  |

### 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 | * ownerIdentifier – the owner identifier of the initialized security server * serverCode – the server code of the initialized security server |

### 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 orphaned client keys, certs and certificates | * 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 * 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 |
| Change owner | * clientIdentifier – the client identifier of the selected client * managementRequestId – the identifier of the corresponding management request in the central server * clientStatus – the status of the registered client |
| Add service description | * clientIdentifier – the client identifier of the selected client * url – the URL of the added service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 * disabled – the flag indicating whether the added WSDL and all its services were disabled * refreshedDate – the time when the added WSDL was refreshed |
| Delete service description | * clientIdentifier – the client identifier of the selected client * url – the URL of the service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 |
| Disable service description | * clientIdentifier – the client identifier of the selected client * url – the URL of the service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 * disabledNotice – the notice of the disabled WSDLs |
| Enable service description | * clientIdentifier – the client identifier of the selected client * url – the URL of the service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 |
| Refresh service description | * clientIdentifier – the client identifier of the selected client * url – the previous URL of the service description * serviceType – type of the service description: WSDL, REST, or OPENAPI3 * urlNew – the new URL of the service description * wsdl – wsdl data (only for type WSDL)   + servicesAdded – the list of services added during refresh   + servicesDeleted – the list of services removed during refresh |
| Edit service description | * clientIdentifier – the client identifier of the selected client * url – the URL of the added service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 * wsdl – wsdl data (only for type 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 * url – the URL of the added service description of the selected client * serviceType – type of the service description: WSDL, REST, or OPENAPI3 * 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 |
| 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 |

### 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 |

### 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  Event name is used if event fails before *Delete key from token and configuration part* is reached | * 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 and 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 |
| 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 * csrId – the identifier of the deleted certificate request |
| Generate key and CSR | * 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 * 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 |
| Import certificate from 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  Event name is used if event fails before it is known where certificate is delete from (configuration or token) |  |
| 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 |

### 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 |

### API Key Management Events

The audit log events related to API key management.

|  |  |
| --- | --- |
| **Event** | **Data fields** |
| API key create | * apiKeyId – identifier of the API key * apiKeyRoles – array containing the roles associated with the API key |
| API key update | * apiKeyId – identifier of the API key * apiKeyRoles – array containing the roles associated with the API key |
| API key remove | * apiKeyId – identifier of the API key * apiKeyRoles – array containing the roles associated with the API key |

### Technical Events

The audit log events related to technical events, such as authentication failures. Except for Key management API log in event, these events are only logged if they fail.

|  |  |
| --- | --- |
| **Event** | **Data fields** |
| Key management API log in |  |
| API key authentication |  |
| Auth credentials discovery |  |
| Access check  (if user did not have permission to do an operation which is not an audit logged event) |  |
| Authentication |  |

## 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 |