Autoenroll PKI

Introduction

Swiss IT Security AG
Etzelmatt 3
5430 Wettingen
Schweiz

+41 848 088 088
www.sits.ch
info@sits.ch

1. Introduction

true-Xtender Autoenroll PKI connects the Microsoft Autoenrollment function with a public PKI service of your choice. This lets you issue and manage certificates in-house as usual without having to set up, operate and maintain your own Microsoft CA.

Together with the keyon true-Xtender extensions from SITS, the Microsoft PKI is a comprehensive solution for the issuance and management of X.509 certificates.

Based on Microsoft PKI, X.509 certificates are issued and managed for comprehensive identity and access solutions.

The Autoenrollment function of the Microsoft PKI can be significantly extended with the true-Xtender Autoenroll PKI solution.

- Autoenrollment of public certificates. Any public CA that offers a web service interface can be integrated.
- Autoenrollment based renewal of certificates in the case of modifications of user or server attributes. Extended autoenrollment allows the update and renewal of certificates at any time.
- Rule based automated certificate revocation
- Flexible lifecycle management of user and server certificates
- Key archival and recovery
- Key history import
- Credential importer
- Certificate publishing to Intune managed accounts
- Account management web service

This document describes the features of true-Xtender Autoenroll PKI solution.

2. Architecture

Below diagram outlines the involved components to enable Autoenroll PKI.

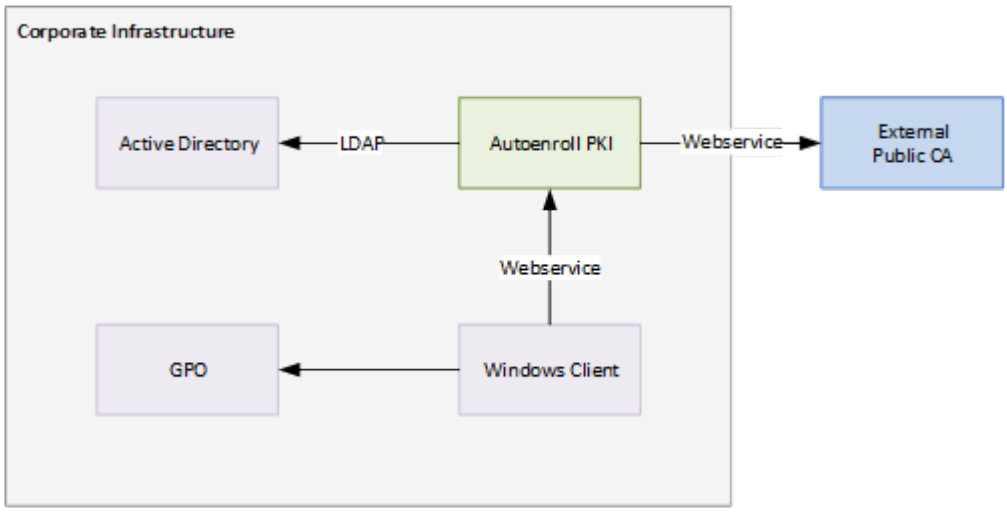


Image 1 - architecture overview

Component	Description
Active Directory	Used to authenticate accounts Used to retrieve account attributes for certificate content (any LDAP server possible)
GPO	Autoenrollment is configured via Group Policy
Windows client	Accounts receive certificates on their windows client
External Public CA	The CA that issues the certificates
Autoenroll PKI	The true-Xtender Autoenroll PKI enables certificate autoenrollment.

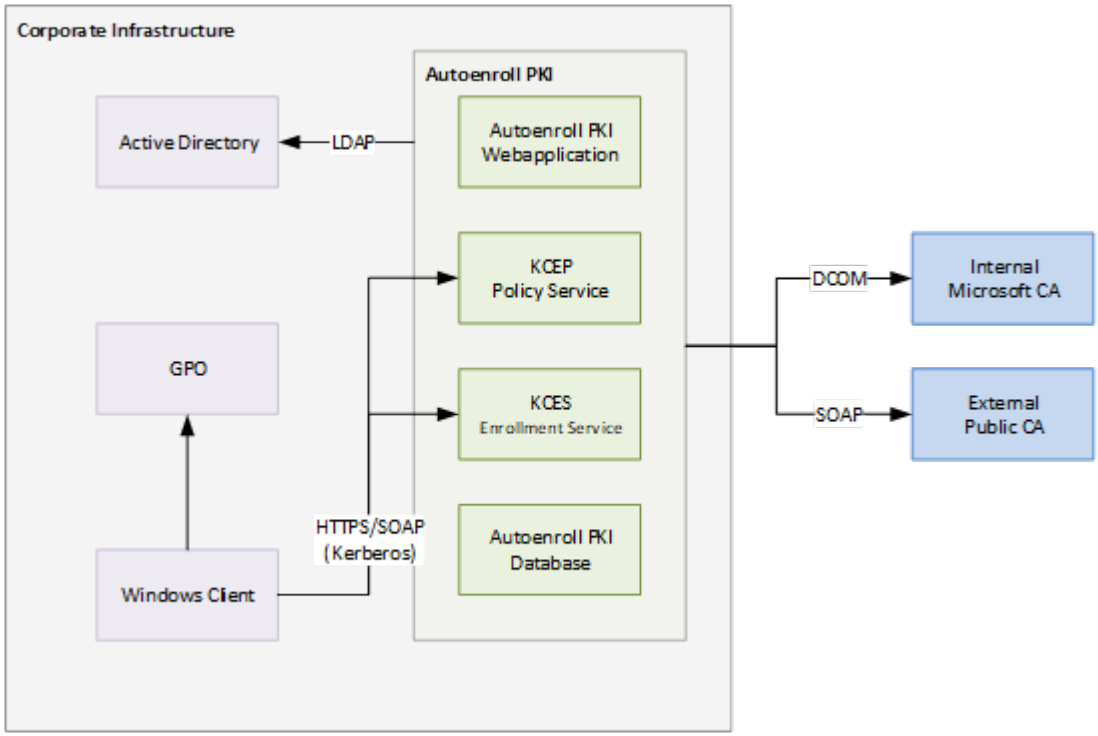


Image 2 - detailed architecture overview

- Autoenroll PKI connects to any LDAP server to retrieve account attributes which build the content of the certificate.
- The client connects to Autoenroll PKI application via HTTPS.
- The Autoenroll PKI connects to the Public CA via HTTPS over the internet.

3. Supported protocols and clients

The following protocols and Windows Client versions are supported.

Enrollment Protocol	Comment
CEP/CES including Key Archival	Windows 10 Windows 11
RPC/DCOM	To simulate an ADCS CA

4. Features

True-Xtender Autoenroll PKI has the following features:

1. Multiple certificate profiles
    1. Configuration of certificate profile per AD group
    2. Multiple AD groups for same certificate profile
2. Configurable notification thresholds per certificate profile
    1. Causes notification as threshold is reached
3. Configurable subject name and subject alternate name per certificate profile
    1. Dynamic content from account attributes and static content
    2. Account attribute changes can optionally enforce to re-issue certificates
4. Certificate Revocation
    1. Configurable auto revocation (revokes certificates where the account is no longer a member of an assigned AD group of configured certificate profile).
    2. Manual revocation per account and certificate
5. Key archival: Each issued certificate can be archived
    1. For installation on additional windows clients. If Active Directory credential roaming cannot be activated, the integrated credential importer application can be used instead.
    2. For installation on other devices
    3. Key recovery (e.g. for audit purposes, four-eye principle)
6. Certificate issuance status view
7. Real time certificate count per certificate profile
    1. Pending certificates (new, renew, modify)
    2. Issued certificates (new, renew, modify)
    3. Revoked certificates
8. Account and certificate search
9. Expiring certificate list (optionally exclude the accounts with already renewed certificates)
10. Email notification
11. Web Service for account administration
    1. Triggering of publishing tasks

2. Creation of shared accounts (e.g. for shared mailbox scenario)
12. Import of certificate history (per account) from archived from ADCS CA database or any PKCS#12 data.
13. Logging to log files and to the Windows event log

4.1. Feature Details

4.1.1. Feature Key Archival

Especially for encryption keys it is important, to be able to have the encryption key archived, so it can always be recovered for decryption purposes, even after the certificate was revoked or has expired. With Key Archival enabled, there is a Key Recovery process available that allows to download the archived keys of a specific account as a PKCS#12 file (PFX), e.g. for audit purposes by using an four-eye principle within the Autoenroll PKI application.

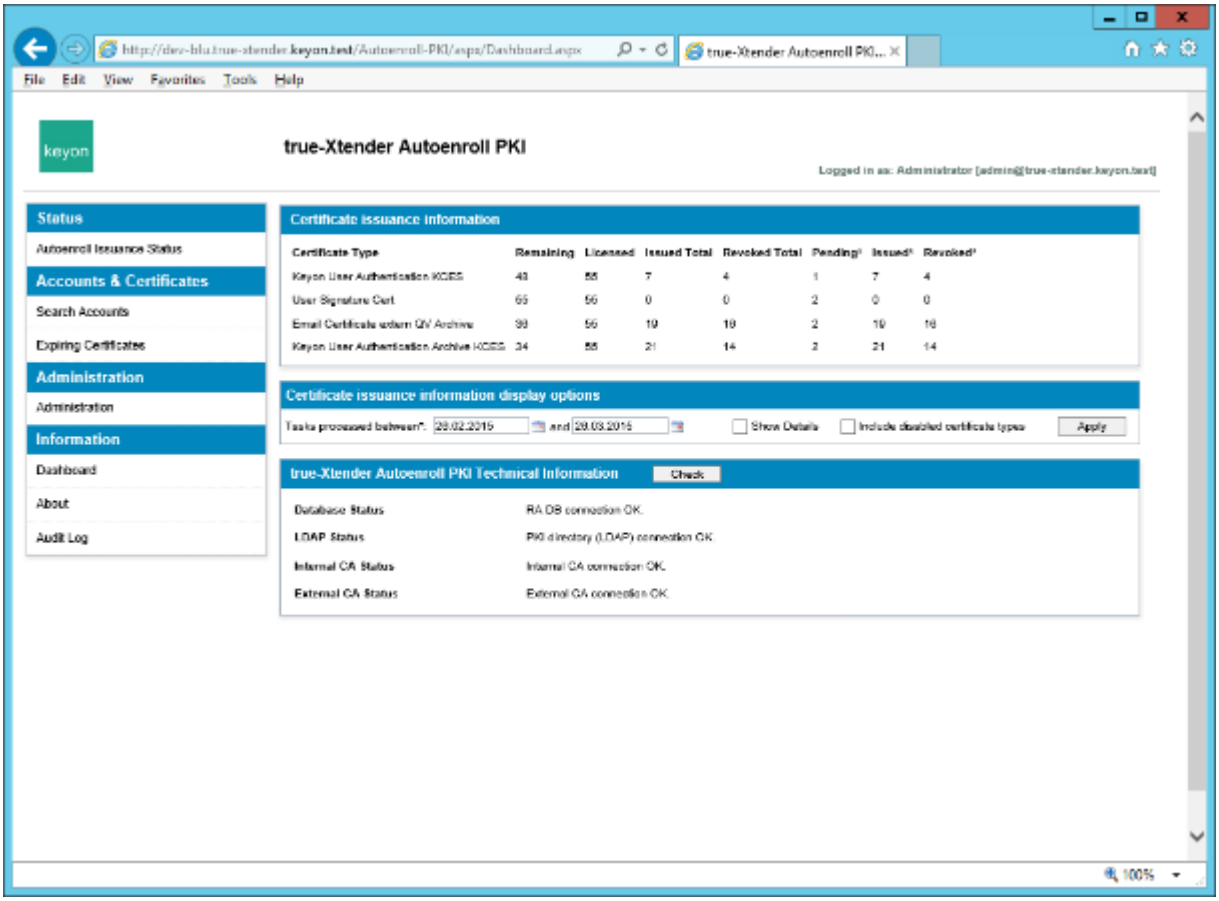
4.1.2. Feature Credential Importer

Certificates including private keys in the certificate store of a Windows account are automatically made available for the same account on multiple computers, if Windows Credential roaming is enabled. If for any reason (e.g. storage capacity) this Active Directory feature can't be enabled, Credential Importer provides a similar functionality. Credential Importer is an application that runs once for autoenroll enabled accounts on each user login, it verifies with Autoenroll PKI which certificates belongs to that account and installs missing certificates into the accounts certificate store. This works only for certificates with Key Archival enabled.

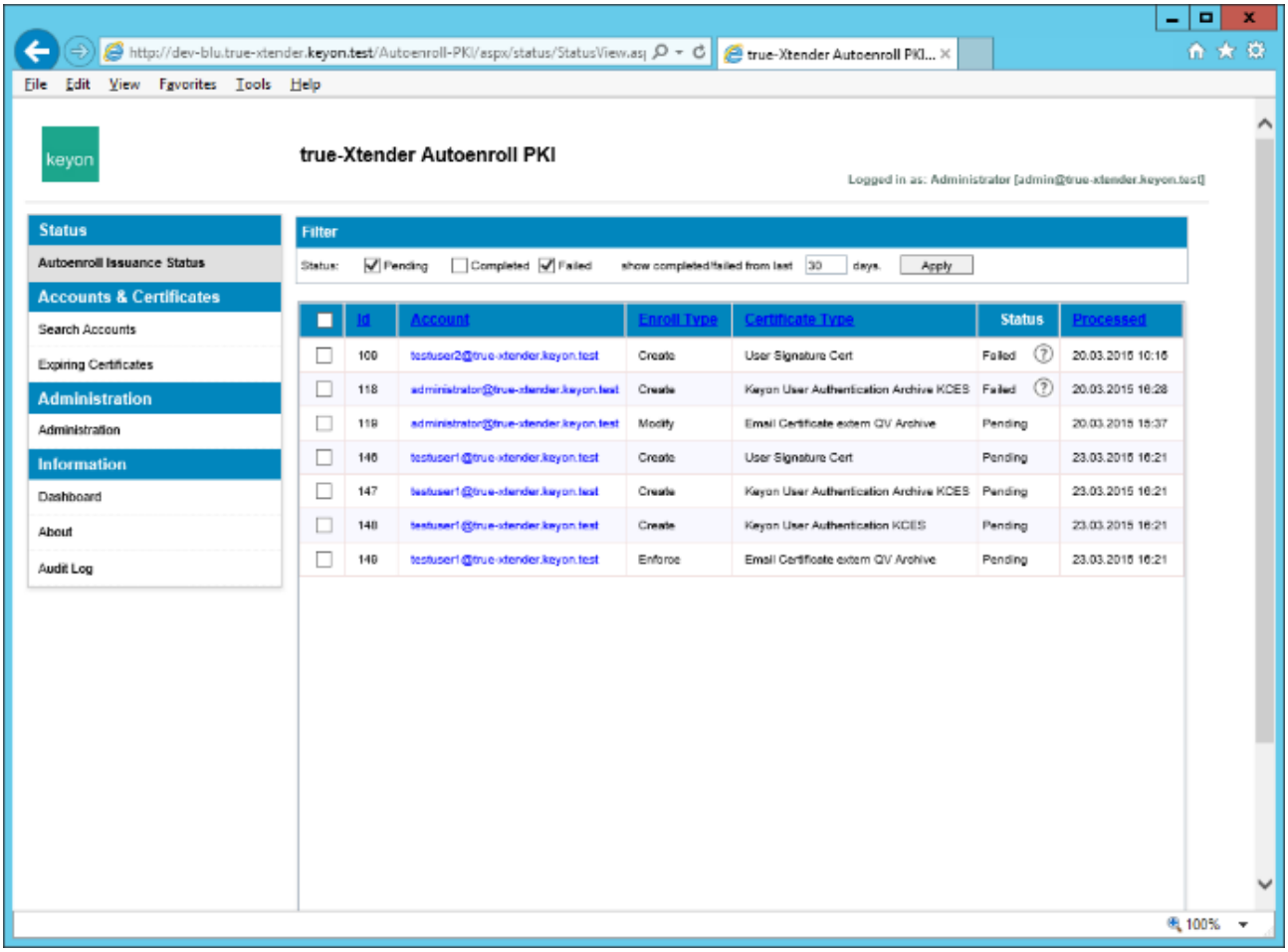
5. Administration web application

The following screenshots illustrate a set of the web application administration functions.

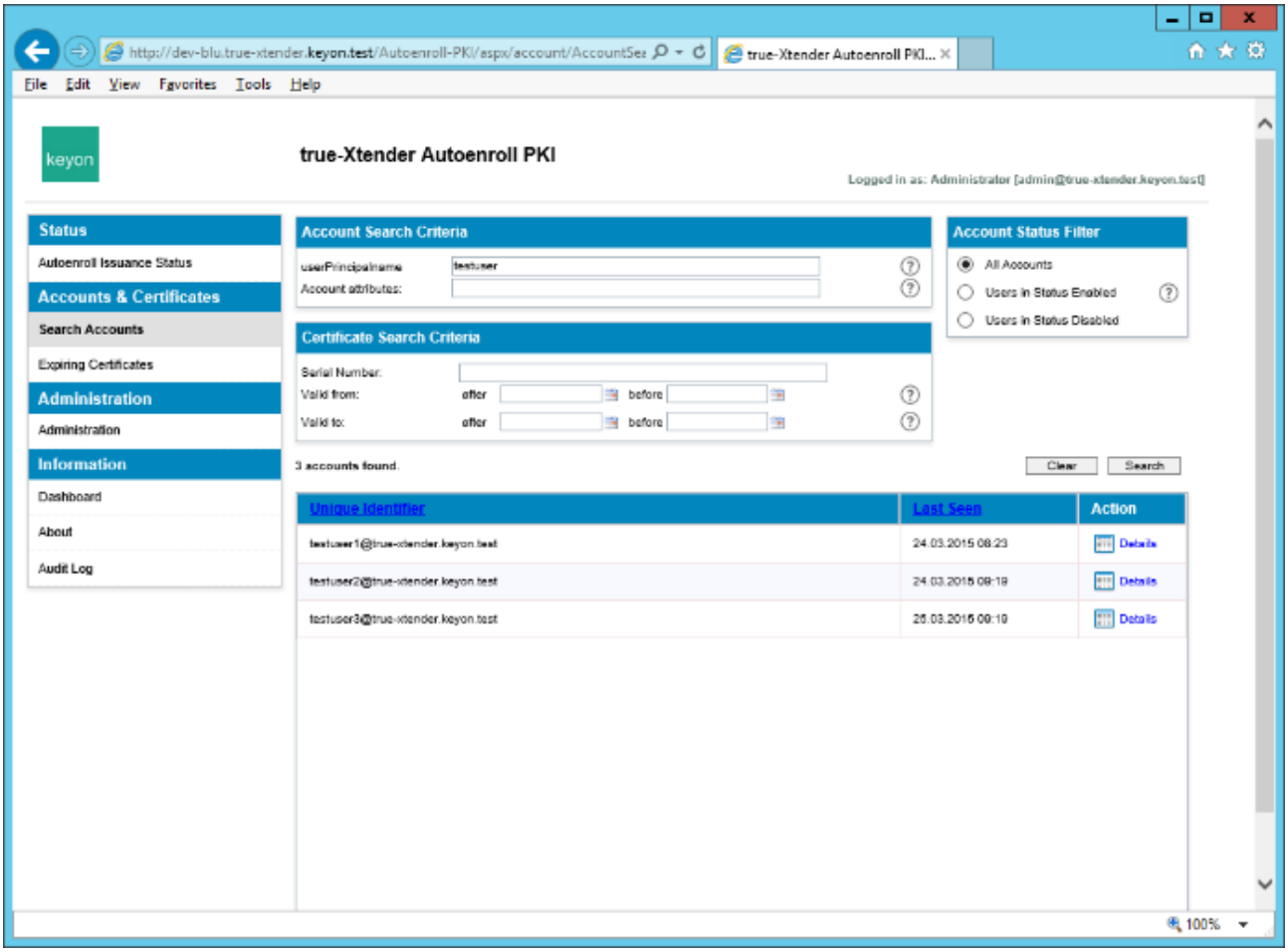
Dashboard



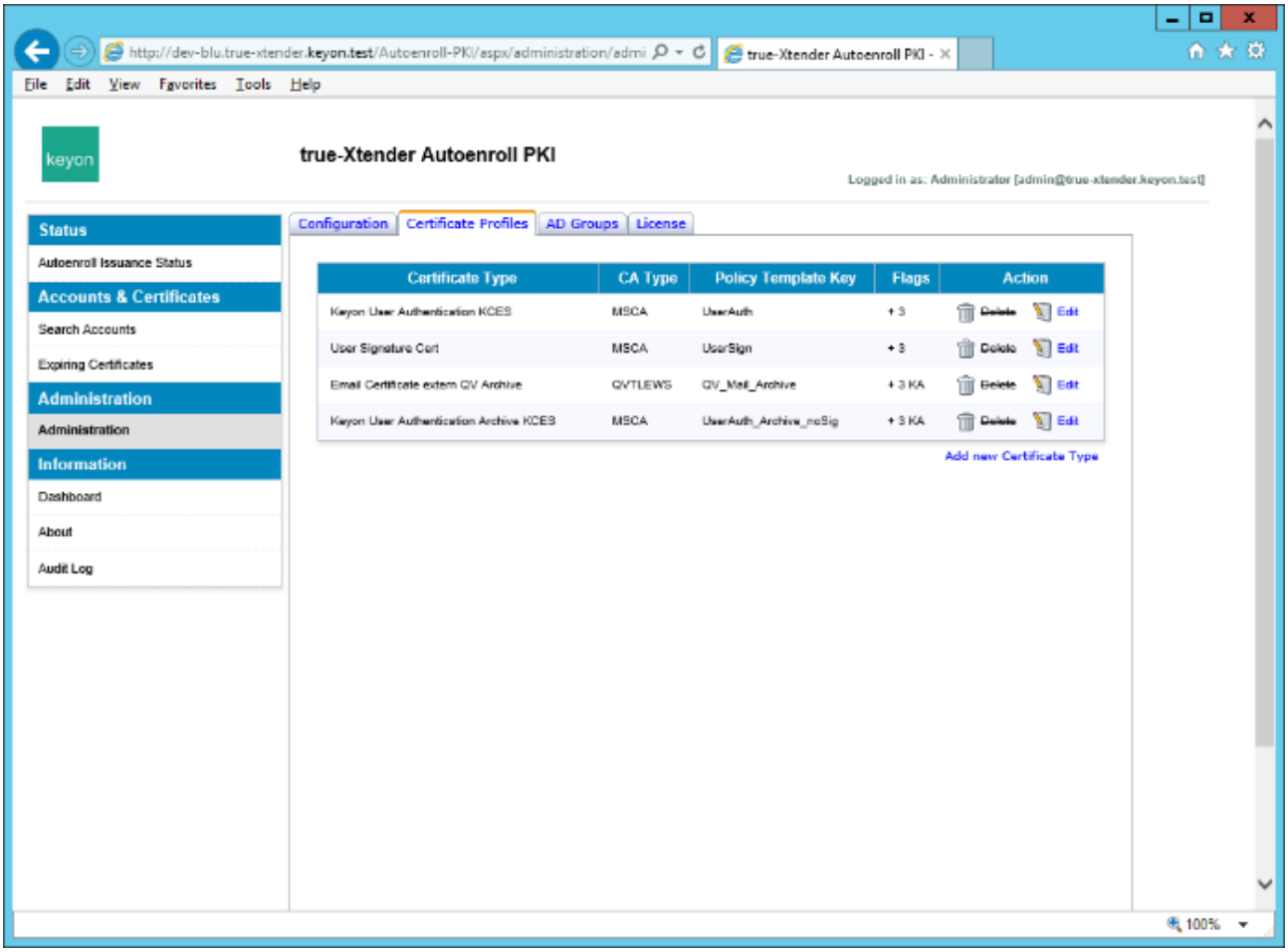
Certificate issuance status



Search functions



Administration



6. Security measures

The following security measures are implemented to prevent misuse of the Autoenroll PKI system.

1. Kerberos Windows Authentication for web service and web application authentication
2. Database encryption
3. Archived keys are encrypted using a symmetric database encryption key
4. The symmetric database encryption key is encrypted using encryption certificate(s) in HSM or soft token
5. Database integrity
6. Accounts and their stored archived keys are secured by database integrity means to detect and prevent misuse by copying database content
7. Integrity protected, comprehensive Audit log

Revision #2
★Created 2026-06-10 10:12:20 UTC by SITS
Updated 2026-06-10 10:12:21 UTC by SITS