WISeKey PKI Technology

CertifyID GuardianXM

Description

Microsoft Active Directory Certification Services (ADCS) is widely used in the Enterprise environments, but it lacks important features for advanced PKI implementations.

WISeKey is a long-lasting Microsoft Technology Partner and has extensive experience deploying and leveraging Microsoft ADCS for complex environments. This experience has led to the development of software modules that complement Microsoft ADCS.

WISeKey's CertifyID GuardianXM enhances ADCS in such a way that can serve advanced scenarios, like mission-critical infrastructures or PKI for Publicly Trusted Certificates.

Features & benefits

CertifyID GuardianXM adds database redundancy and resiliency to Windows Certificate in order to provide high availability services. It is a standard exit module which is installed on Windows Certificate Services. The module stores all Certificates and related information such as Certificate Status History (the changes of a certificate status during its lifecycle) in an SQL database. This database can be mirrored or replicated at an offsite location to provide effective disaster recovery.

Features:

- CA Disaster Recovery – allows recovery of the Certificates Services database to its 100% valid state following data corruption or loss
- Improve the efficiency of certificate management activities by implementing a central certificate information database to support lookup and reporting
- Implement near-real time data updates
- Implements batch load/update/audit capability allowing mass loading and update
- Compatibility with Windows Server up to 2016 version

CertifyID Guardian also provides important reporting analysis and audit tools, allowing administrators to track:

- Number of Certificates per user – How many Certificates have been issued to an individual user? Has any user requested more that one Certificate of the same type, or did any user request several Certificates from different Certificates Authorities?
- Who's got a certificate – If you goal is to fully deploy Certificates, it would be good to know if all users belonging to a given domain or Organizational Unit (OU) have requested a Certificate already. Using WISeKey Guardian the administrator can check which users in Windows Active Directory have requested a Digital Certificate
- Request peaks (day/month) – Determine how your Certificate Authorities are utilized
- What Certificates types are issued – determine what kind of certificates have been issued based on the certificate templates in use

Why WISeKey PKI technology is different?

WISeKey is a leading eSecurity company, with 20 years of experience in information security and trusted digital identities. Acting as both a PKI technology supplier and a Trusted Certification Authority, delivering services using our own technology ensures that our products are up-to-date with the modern customer needs and regulations for PKI.

All Certificates aren't equal… Choosing WISeKey is the wise choice

PKI As A Service

Corporate customers not willing to implement their own PKI platform can also benefit of our trusted "PKI As A Service" (Managed PKI) services offering. This service is built with our URA and enables:

- Multiple Certificate Templates
- Multi-Tenant access, isolating the data of each customer
- Possibility to deploy dedicated CAs for the customer, or use WISeKey's Trusted CAs
- Possibility to deploy a fully dedicated and isolated infrastructure, not sharing any resource with other customers

Our MPKI service doesn't require the installation of any local infrastructure, and it's delivered from WISeKey's owned secure datacenter in Switzerland, ensuring the privacy of your data according to the highest standards.

For more information:
wisekey.com
sales@wisekey.com