iQSol HSA
Hardware Security Appliance

iQSol

Security made in Austria.

iQSol HSA (Hardware Security Appliance)

Certificates are an important anchor of trust in the IT infrastructure.

Your IT infrastructure is a sensitive area because it involves people working with data and systems. This makes it particularly vulnerable to external attacks, whether from hackers or malware. Not all of your employees are familiar with IT security. This makes it even more important that you set standards and protect your IT infrastructure.

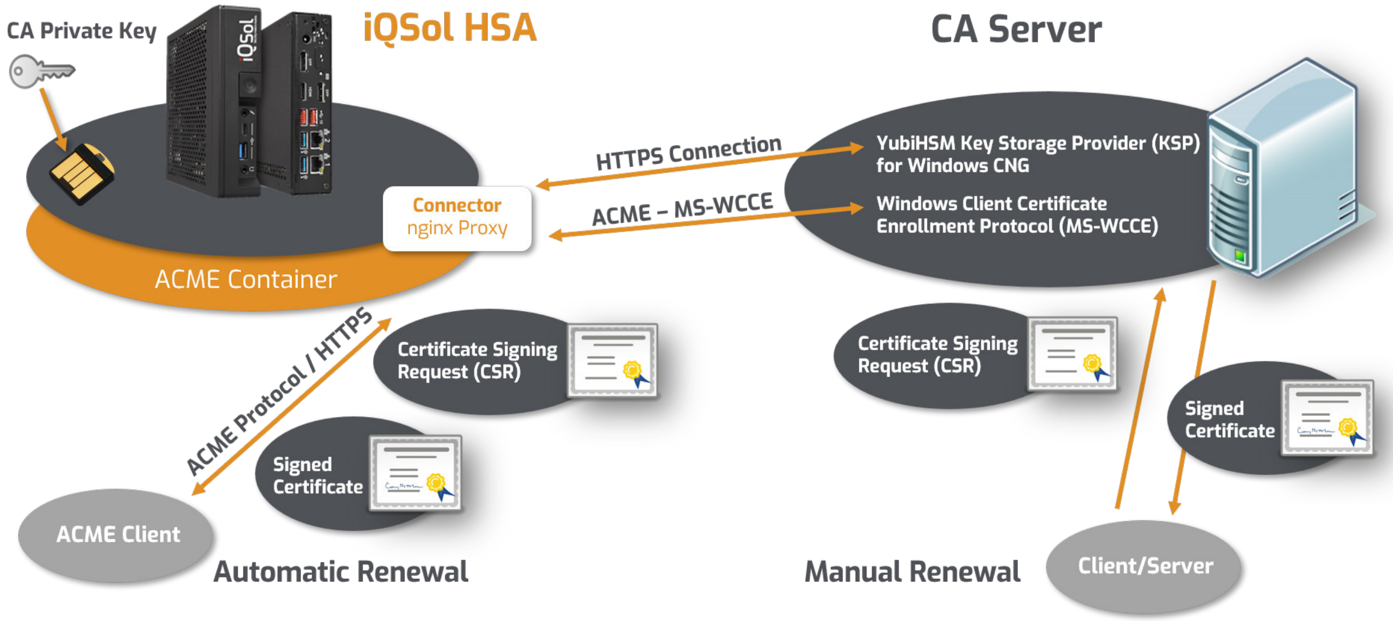
Fast and easy HSM configuration for your PKI.

The **iQSol HSA** (Hardware Security Appliance) offers the possibility to provide a **YubiHSM** (Hardware Security Module) for secure central generation and storage of certificates in the network.

Certificate deployment and automatically renewal.

With the iQSol HSA ACME feature, certificates are deployed and renewed automatically. Linux systems & other ACME client-enabled systems can also be easily provided with web server certificate.

The iQSol HSA is a very cost effective and network based HSM solution. With the ACME feature, certificates can be deployed and renewed automatically. It is easy to use and the administrator does not need any special knowledge.



iQSol HSA & YubiHSM

Fast and easy HSM configuration for your PKI.

With the iQSol HSA, up to 16 PKI servers can be connected to one HSA. For this purpose, the YubiHSM is divided into domains/partitions and each server only has access to its own private keys.

Why use certificate management?

- Certificates can be used in a Microsoft environment to **provide strong authentication using smart cards** instead of passwords.
- Especially in times of ransomware it is very important to secure the **domain admin login** with smart cards.
- Certificates are also required for **important data connections within Active Directory** (LDAPS, RDP encryption, etc.). Therefore, it is necessary to secure the Microsoft certificate infrastructure as an anchor of trust.

Advantages of iQSol HSA with YubiHSM

- Easy, menu-based configuration of the appliance and the YubiHSM.
- Up to 16 PKI servers can be connected to one YubiHSM.
- PKI servers require only network connection.
- No physical USB port required.
- Simple, menu-driven creation of backups on a second YubiHSM.
- High availability through clustering (2 nodes).
- Wrap Key Splitting
- All logs can be sent via syslog (also encrypted) to a central logging server.
- Increased security through minimalist system design.

We provide you with everything you need to get even more security in a single appliance:

- Concept and documentation for a new implementation of a Microsoft PKI with iQSol HSA/YubiHSM2 and for the migration of existing CAs to iQSol HSA/YubiHSM2.

iQSol HSA & ACME-Feature

Certificate deployment and automatically renewal.

Automated certificate management saves time and costs by reducing the manual management of certificates and keys. Certificates are always up to date and the risk of security breaches and downtime is reduced.

What is ACME?

The **Automatic Certificate Management Environment (ACME) protocol** is a communication protocol for automating the interaction between certification authorities and the servers, which enables **the automatic provision of a public key infrastructure at very low cost.**

The HSA provides a very simple way to add this functionality to a Windows CA server. The necessary services run on the iQSol HSA and ACME clients communicate with the HSA, which then processes the requests via the CA server.

Advantages of iQSol HSA with ACME Feature

- Easy ACME extension for Windows CA Server.
- Easy certificate rollout - certification through domain validation.
- Reduces manual management of certificates and keys.
- Certificates comply with the latest security standards.
- All logs can be sent via syslog (also encrypted) to a central logging server.
- E-mail notification when certificates are about to expire.
- High availability through clustering (2 nodes).
- Easy menu-driven configuration of the ACME server on the HSA.
- User manual for configuration on the Windows CA server.

Technical Specifications Hardware Security Appliance:

Modell	Cores	RAM	HDD	RAID	LAN	Dimension	Power Supply
HSA 1000	8	16GB	2x1TB SATA 7.2k	RAID 1	4x Gigabit Ethernet	19"1HE	Dual
HSA 200	2	8GB	256 GB SSD	-	2x Gigabit Ethernet	Desktop	Single
HSA VM	min. 4 Cores	min. 4GB RAM	min. 60 GB	-	min. 1x Gigabit Ethernet	-	-