iQSol HSA
Hardware Security Appliance

iQSol
Security made in Austria.

iQSol HSA (Hardware Security Appliance)

Zertifikate sind ein wichtiger Vertrauensanker in der IT-Infrastruktur.

Ihre IT-Infrastruktur ist ein sensibler Bereich, denn hier arbeiten Menschen mit Daten und Systemen. Das macht sie besonders anfällig für Angriffe von außen, sei es durch Hacker oder Schadsoftware. Zudem ist nicht jeder Ihrer MitarbeiterInnen im Umgang mit der IT- Sicherheit versiert. Umso wichtiger ist es, dass Sie Standards setzen und Ihre IT-Infrastruktur schützen.

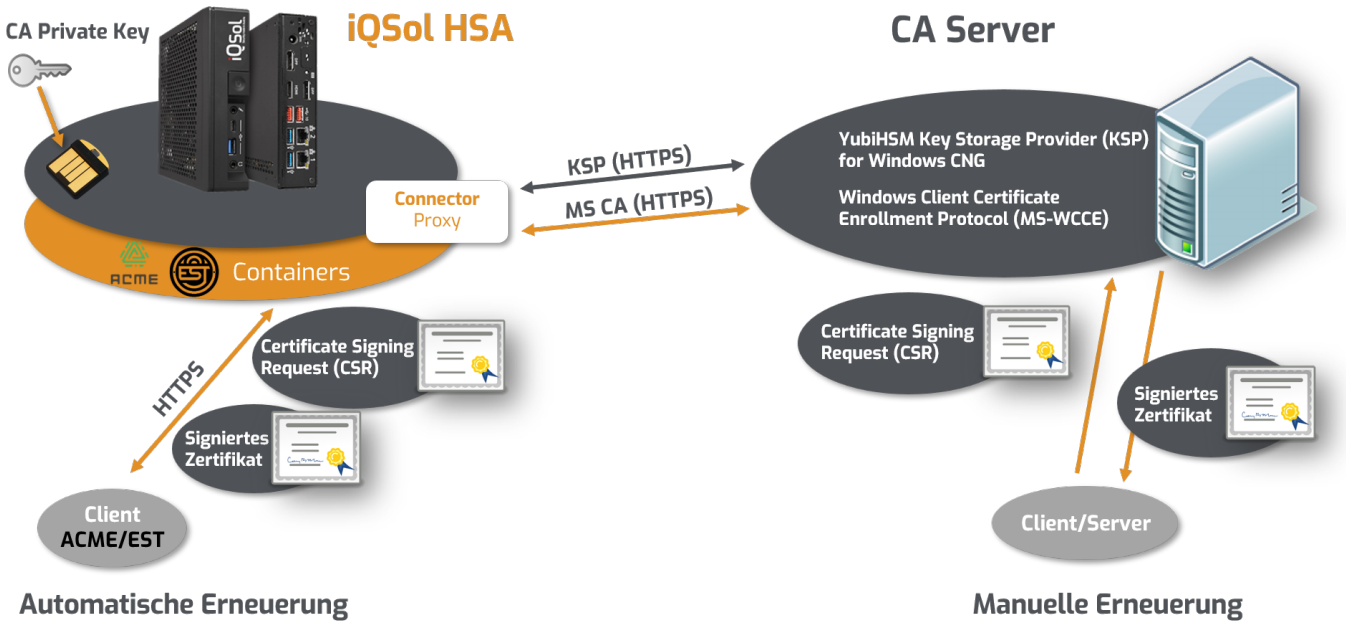
Schnelle und einfache HSM-Konfiguration für Ihre PKI.

Die **iQSol HSA** (Hardware Security Appliance) bietet die Möglichkeit, ein **YubiHSM** (Hardware Security Module) zur sicheren zentralen Erstellung und Speicherung von Zertifikaten im Netzwerk zur Verfügung zu stellen.

Zertifikate ausrollen und automatisch erneuern.

Mit dem iQSol HSA ACME/EST-Feature* werden Zertifikate ausgerollt und automatisch erneuert. Auch Linux-Systeme & andere ACME/EST-Client-fähige Systeme können ganz einfach mit Webserver-Zertifikaten versorgt werden.

Die iQSol HSA ist eine sehr kostengünstige, netzwerkbasierte HSM-Lösung. Mit dem ACME/EST-Feature können Zertifikate ausgerollt und automatisch erneuert werden. Einfach zu bedienen und für den Administrator ohne spezielle Kenntnisse nutzbar.



** Automatic Certificate Management Environment (ACME) / Enrollment over Secure Transport (EST)*

iQSol
Security made in Austria.

iQSol HSA & YubiHSM

Schnelle & einfache HSM-Konfiguration für Ihre PKI.

Mit der iQSol HSA können bis zu 16 PKI-Server an eine HSA angebunden werden. Dazu wird das YubiHSM in Domänen/Partitionen unterteilt und jeder Server hat nur Zugriff auf die eigenen Private Keys.

Warum Zertifikatsmanagement?

+ Durch Zertifikate ist in einer Microsoft-Umgebung eine **starke Authentifizierung mit Smartcards** statt Passwörtern möglich.
+ Gerade in Zeiten von Ransomware ist es sehr wichtig, die **Domain-Admin-Anmeldung** optimal mit Smartcards abzusichern.
+ Die Zertifikate sind aber auch für **wichtige Datenverbindungen innerhalb des Active Directory** notwendig (LDAPS, RDP-Verschlüsselung, usw.). Daher ist es notwendig, die Microsoft Zertifikatsinfrastruktur als Vertrauensanker gut abzusichern.

Vorteile der iQSol HSA mit YubiHSM

- Einfache, menügeführte Konfiguration der Appliance und des YubiHSM.
- Anbindung von bis zu 16 PKI-Servern an ein YubiHSM möglich.
- Die PKI-Server benötigen lediglich eine Netzwerkverbindung.
- Es wird kein physischer USB-Port benötigt.
- Einfaches, menügeführtes Erstellen von Backups auf ein zweites YubiHSM.
- Hochverfügbarkeit durch Clustering (2 Nodes).
- Wrap-Key Splitting
- Übergabe aller Logs via Syslog (auch verschlüsselt) an einen zentralen Logging-Server
- Erhöhte Sicherheit durch minimalistisches Systemdesign.

Wir bieten Ihnen innerhalb einer Appliance alles, was Sie für noch mehr Sicherheit benötigen:

- Konzept und Dokumentation zur Neuimplementierung einer Microsoft PKI mit der iQSol HSA/YubiHSM2 und zur Migration bestehender CAs in iQSol HSA/YubiHSM2

Technische Spezifikationen 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	-	-

iQSol HSA & ACME-Feature

Zertifikate ausrollen und automatisch erneuern.

Automatisiertes Zertifikatsmanagement spart Zeit und Kosten, indem die manuelle Verwaltung von Zertifikaten und Schlüsseln reduziert wird. Die Zertifikate sind immer auf dem neuesten Stand und das Risiko von Sicherheitsverletzungen und Ausfallzeiten wird erheblich reduziert.

Was ist ACME? Das **Automatic Certificate Management Environment (ACME) Protokoll** ist ein Kommunikationsprotokoll zur Automatisierung der Interaktion zwischen Zertifizierungsstellen und den Servern, welches **die automatische Bereitstellung einer Public-Key-Infrastruktur zu sehr geringen Kosten** ermöglicht.

Was ist EST? **Enrollment over Secure Transport (EST)** ist ein kryptografisches Protokoll, das die Ausstellung von Zertifikaten automatisiert. Es wird für PKI-Clients (Public Key Infrastructure) verwendet, die Clientzertifikate benötigen, die einer Zertifizierungsstelle (CA) zugeordnet sind. EST ersetzt den Bedarf an einer manuellen Zertifikatverwaltung, die riskant und fehleranfällig sein kann.

Die HSA bietet eine sehr einfache Möglichkeit, einen Windows CA Server um diese Funktionalität zu erweitern. Die dazu notwendigen Dienste laufen auf der iQSol HSA und ACME/EST-Clients kommunizieren mit der HSA, die dann die Anfragen über den CA Server abarbeitet.

Vorteile der iQSol HSA mit ACME/EST-Feature

- Einfache ACME/EST-Erweiterung für Windows CA Server.
- Einfacher Zertifikatsrollout - Zertifizierung über Domänenvalidierung.
- Reduktion der manuellen Verwaltung von Zertifikaten und Schlüsseln.
- Zertifikate entsprechen den aktuellen Sicherheitsstandards.
- Logs können via Syslog an zentralen Logging-Server übergeben werden (auch verschlüsselt).
- E-Mail Benachrichtigung über ablaufende Zertifikate.
- Hochverfügbarkeit durch Clustering (2 Nodes).
- Einfache menügesteuerte Konfiguration des ACME/EST-Servers auf der HSA.
- Benutzerhandbuch für die Konfiguration auf dem Windows CA Server.

iQSol GmbH, Petrusstraße 20, 3312 Oed T: +43 7472 207 67 E: office@iqsol.biz W: www.iqsol.biz