

# Krestfield PKCloud

## Specifications

version 2.1  
Copyright Krestfield 2020

---

### Operating Systems

- Windows Server (2012 R2, 2016, 2019)
- Solaris (10, 11.x)
- Linux (Amazon Linux, CentOS, Debian, Red Hat, SUSE, Ubuntu)

### Hardware Security Modules

Any PKCS#11 compliant HSM but tested with:

- Azure Key Vault
- Google KMS
- nCipher range
- AWS CloudHSM
- Thales/Gemalto Luna
- Thales/Gemalto Data on Demand Cloud HSM
- Utimaco
- Thales PayShield (PKI operations only)

Contact Krestfield support to discuss support for other HSMs

### Algorithm Support

- RSA
- ECDSA (including NIST recommended, SECG and Brainpool defined curves)
- AES
- SHA-1, SHA-2 and SHA-3

### Signature Formats Supported

- PKCS#7
- Raw/PKCS#1

### Revocation Checking

- CRL
- OCSP (including IdenTrust requirements and response caching)

### Interfaces

- Restful API (JSON over HTTP/HTTPS)
- C# and Java thin client

### Java

- Java 8 to Java 14 – Oracle and OpenJDK