



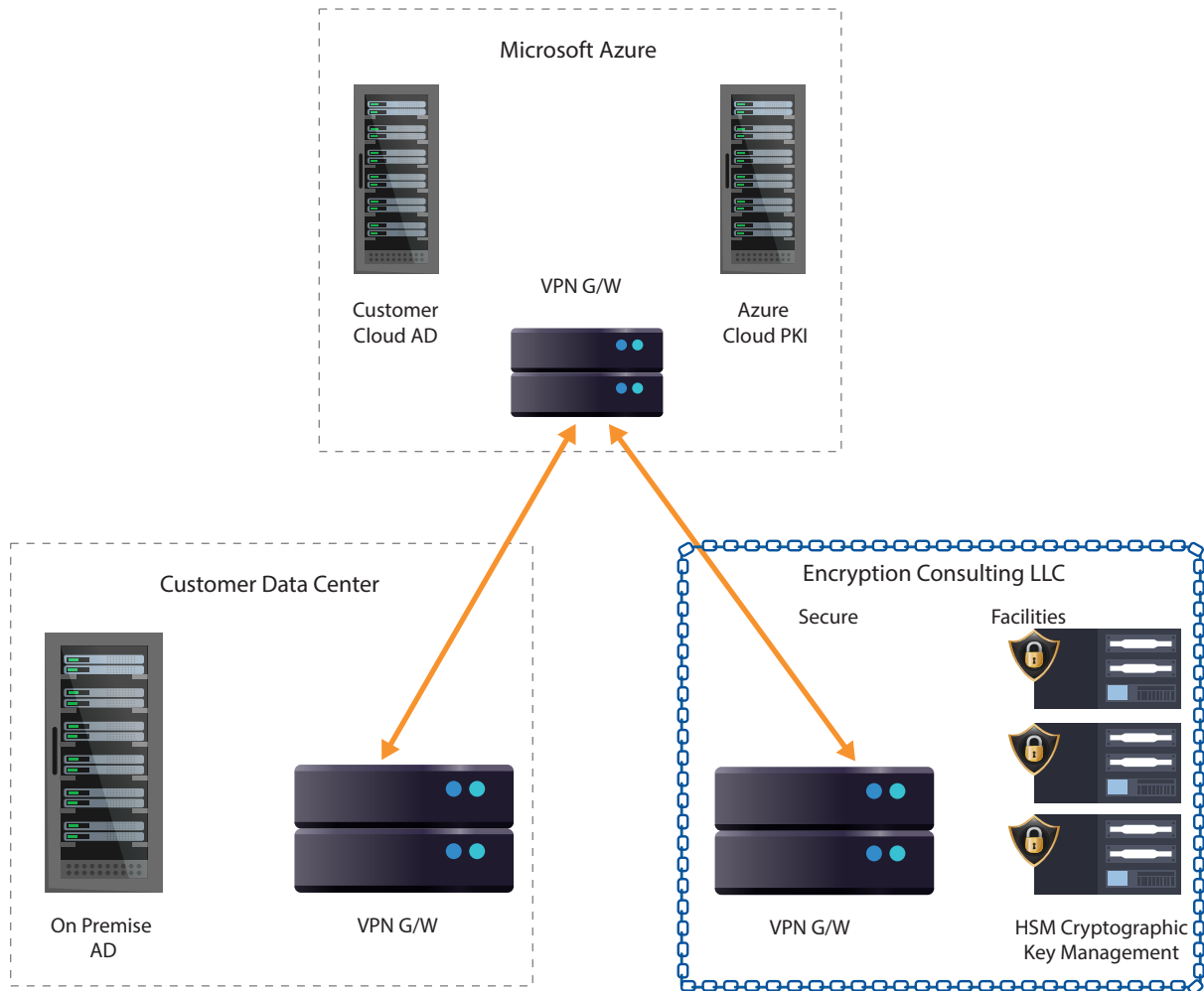
**PKI AS A SERVICE
FROM**



An efficient and secure way to manage access using trusted credentials. Your own dedicated Microsoft PKI delivered as a PKI as a service, hosted in Azure.

FEATURES

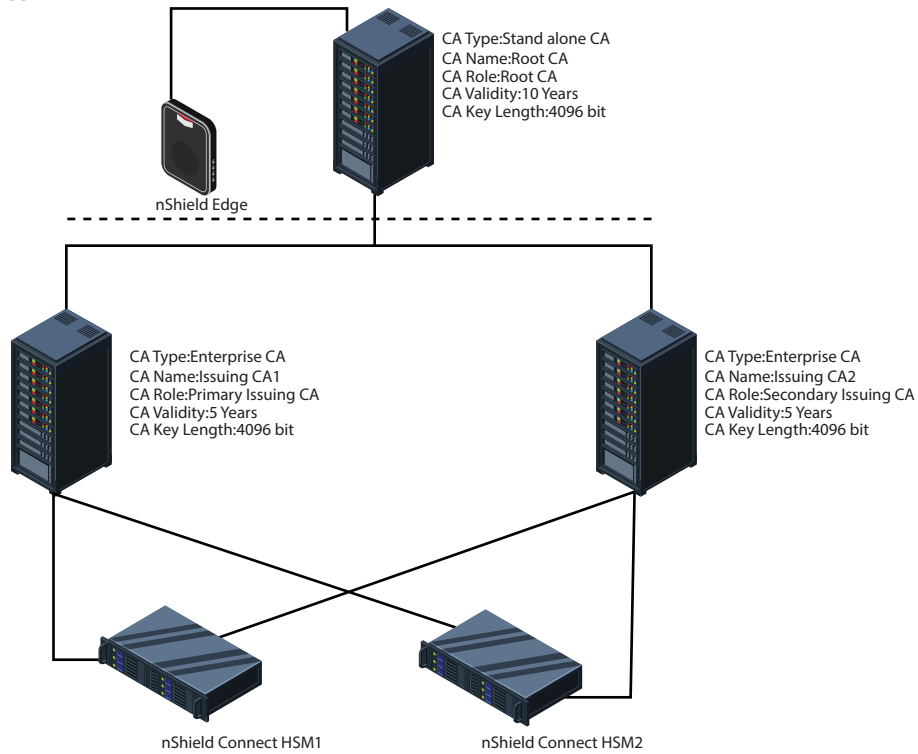
- ▶ Encryption Consulting’s PKI as a Service offers you a customizable, high-assurance Microsoft PKI designed and built to the highest NIST standards.
- ▶ It’s a low risk solution that gives you full control of your PKI without having to worry about the complexity.



AN ENTERPRISE PKI IN THE CLOUD

Many organizations are moving core components of their infrastructure to the cloud to enable cost savings and provide scalability. When running a PKI, the challenge is to both secure the root as an offline resource and to separately manage the Root CA and issuing sub-CAs which need to be accessible online for certificate requests and issuances. Encryption Consulting has the expertise and secure environment necessary to hold the Root Private Key offline and also to manage the signing of keys used for online RAs and issuing sub-CAs.

By default customers will have a two-tier PKI CA hierarchy. All CAs within this CA hierarchy will only issue CA and end-entity certificates for internal usage. Customer PKI CA hierarchy consists of a single PKI Root CA and two or more PKI Issuing CAs as per their requirements.



So now you can have your own two-tier Enterprise PKI in Azure, with your own dedicated, compliant offline Root CA and high-assurance sub-CA infrastructure. We deploy to industry best practice, with supporting policy and procedures tailored to your own organization's compliance requirements. The PKI as a Service from Encryption Consulting will provide you with robust infrastructure and a solid foundation for your corporate PKI requirements.

THE CONTROL YOU WANT

Encryption Consulting will deploy and manage your PKI using a fully developed and tested set of policies and procedures control over your PKI and its associated business policies and procedures will always remain with you. Furthermore, for security reasons the root and issuing will be held in FIPS140-2 Level 3 HSMs hosted either in your secure datacenter or at Encryption Consulting datacenter in Dallas, Texas.

HOSTED ROOT CA

The trust anchor of a PKI is a high-assurance Root CA.

- ▶ If you choose to use our Root Service, your Root will be hosted securely in our SOC2-certified datacenter in Dallas, Texas.
- ▶ If required, we can support customers participation in the Root CA build, and will undertake a Key Signing Ceremony (KSC) with you for this purpose. This is the event where the protected key material for the CA is created and implemented according to your policy.
- ▶ As this is your PKI, you are the only one who has access to the Root CA private keys; these are protected by a quorum of HSM control keys of which you hold the majority share. This means that no one can initialize the Root to create additional Sub-CAs or revoke Sub-CAs without your presence.
- ▶ After the KSC, Encryption Consulting will facilitate Root CRL signings as often as required. Signings will be undertaken under the accreditation and compliance requirements for the specific Root CA, according to its policy.

ADDITIONAL SERVICES

Encryption Consulting can also offer further services related to the Root CA such as:

- ▶ Sub CA signings
- ▶ Root CA and sub CA certificate lifecycle management advice (e.g. hashing algorithms / cryptographic algorithms)
- ▶ Policy / certificate profile advice
- ▶ Root maintenance
 - ▶ Root migration / rollover



BENEFITS OF PKI AS A SERVICE BY ENCRYPTION CONSULTING

- ▶ Bespoke design fits your business requirements
- ▶ Quick and simplified deployment using tested templates and dedicated policy
- ▶ Eliminate the need to employ PKI/ HSM skilled SME
- ▶ Securely integrated into AD in a Microsoft supported model
- ▶ AD extended into Azure IaaS, while you remain in full control
- ▶ Reduces risk by maintaining PKI security scheme assurance processes
- ▶ Provides best practice PKI management processes for your business
- ▶ Efficient control of certificate lifecycle to manage risks
- ▶ Apply digital signatures to your contracts, documents, web forms, emails
- ▶ Delivers remote monitoring and trouble-shooting of PKI resources running in Azure
- ▶ Provides cost savings over in-house PKI deployments

KEY FEATURES AND TECHNICAL SPECIFICATIONS

- ▶ Customer specific Certificate Policy and Certification Practice Statement
- ▶ Bespoke design and controls, specific to customer requirements
- ▶ Certificates for devices, computers, domain controller, Wi-Fi, SSL, TLS, users
- ▶ Full support for Microsoft device auto-enrolment and Microsoft Express Route
- ▶ Cryptographic keys stored/managed outside of Azure in ultra-secure facility
- ▶ Only you can access the HSM stored Private Keys
- ▶ Secure integration between on-premise and Azure servers, using protected VPN
- ▶ Azure provides high SLAs in line with your own corporate requirements



130 N Preston Rd, Prosper, TX 75078, USA |
+1- 469-815-4136 | info@encryptionconsulting.com
www.EncryptionConsulting.com

Find us:
"EncryptionConsulting" on



CONFIDENTIALITY. INTEGRITY. AVAILABILITY.