PKIaaS Offline Root - Service Description/Onboarding Checklist

Service Description

Feature/Capability	Service Description	In Scope	Out of Scope
Root Certificate Authority (CA) Key Storage/Backup	HSM leveraged to protect Offline Root Certificate Authority (CA) Database (DB) protection and signing keys	Redundant pair of Entrust nShield network HSMs leveraging unique security world per Offline Root Certificate Authority (CA). 1/4 OCS quorum 2/8 ACS quorum Certificate Authority (CA) key files backed up to centralized RFS server which replicates to DR.	SafeNet/Thales HSM Customer ability to own/control quorum
Access Control	Posture for allowing inbound/ outbound access to Offline Root Certificate Authority (CA) UK MPKI - Standard: UMS, Optional: URS	Unless the customer requests for air gapped environment we will stick to powered down Root CA. There is no extra charge for managing the Root CA in an air gapped environment.	
Root Certificate Authority (CA) Distinguished Name (DN) Structure	Distinguished name of the Root Certificate Authority (CA)	Customer requested Distinguished Name (DN) through onboarding checklist	
Root Certificate Authority (CA) Lifetime	Lifetime of the Root Certificate Authority (CA) certificate	Customer requested lifetime through checklist (Default: 10 years)	
Root Certificate Authority (CA) Key Algorithms	Algorithms used to sign Root Certificate Authority (CA)	Customer requested lifetime through checklist (Default: RSA-2048, SHA-256)	RSA-2048 only allowed through 2030.
Root Certificate Authority (CA) Validation Services	Validation services leveraged to support revocation checking and certificate validation	HTTP CRL (Akamai) OCSP (Akamai)	LDAP CRL
Root Certificate Authority (CA) CRL Lifetime	Lifetime of the Root Certificate Authority (CA) CRL	1 year lifetime with pre-update of 6 months	Customized CRL lifetime or pre-update threshold
KGC Audit	Audit of the Root Certificate Authority (CA) signing ceremony	Ideally we can bulk issue keys and have auditor witness creation of keys at one time. Each following KSC would not need to be audited since they would be using pre-generated keys.	Extra cost if customer requires independent third-party audit.
CP/CPS	Policy and practices statement governing Offline Root Certificate Authority (CA)	Offline Root is supported as part of Entrust Managed PKI and PKIaaS CP/CPS	
Sub Certificate Authority (CA) Issuance	Issuance of subordinate Certificate Authority (CA)s	4 service requests (Includes signing within the request) allowed with the base package annually for PKIaaS customers. For mPKI customers, we can accommodate additional service requests (Includes signing within the request) at an additional cost.	

PKIaaS Offline Root - Service Description/Onboarding Checklist

Key Difference Between Standalone Offline Root vs. PKIaaS Offline Root

	Standalone Offline Root	PKIaaS Offline Root
Service	Publish ARL once in a year	Maximum 4 service requests (Ex: Publishing ARL, Subordinate Cert issuance). i.e. In one service request, customer can provide multiple CSRs for proxy certs - This will be treated as one service request.
Service Flavor for US vs UK MPKI	For US MPKI, Entrust MPKI to act as a Policy Authority. For UK MPKI, Customer acts as the policy Authority for UK MPKI.	MPKI to own/control quorum.

Learn more at entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223