MANAGEMENT WITH ENTRUST MANAGED PKI

Secure and enable your evolving enterprise with trusted identity with the world's leading PKI provider on your side. With Entrust Managed PKI CA (Pro+) Services, our experts help enterprises manage their Entrust PKI, helping ensure best practices, policies, and procedures are applied to user/ device identities (certificates).

Service	Service Description	mPKI Pro + NA	mPKI Pro + UK
Customer CA entry (standard configuration of allowed searchbase)	Deployment of the customer's searchbases (e.g., people, devices), and specific certificate policies for the customers. Commonly the certificate policies will simply be a copy of the default policies.	Y	Y
Administration services (URS/UMS)	Basic certificate management capability; includes the provisioning of two LRAs who may require hardware access tokens or any other applicable key storage mechanisms. *UK MPKI - Standard: UMS, Optional: URS*	Y	Y
Enrollment protocols supported during onboarding (CSRES, MDMWS, MDMWS-SCEP, CSR-SCEP, EST, CMPv2)	Support to enrollment protocols (certificate signing requests – CSRs). *UK MPKI - Standard: CSRES, CSR-SCEP, Optional: MDMWS, MDMWS-SCEP, EST, CMPv2)*	Y	Y
New digital ID configuration	Enrollment protocol is already configured and supported within the deployed MPKI service.	Y	Y
Email notification	Automated email messages to administrators or users to notify an event occurrence. *UK MPKI - Doesn't support*	Y	N
Certificate expiry notifications	Configurable automated expiry notification of certificates to users or administrators. *UK MPKI - Doesn't support*	Y	N
Configurable search base (restricted configuration of OUs)	Configuration of OUs - Initial setup is restricted to administrators, devices, and people; MAC/other custom requirements are addressed through this custom search base setup. *UK MPKI: Optional*	Y	Y
Role-based administration controls	Ability to create multiple roles with permissions over different user sets/groups. *UK MPKI: Optional*	Y	Y
Secure email exchange within/ between the organization(s) by publishing encryption certificates over internet via LDAP	Encryption of email between users requires access to a recipient's encryption certificate. Customers that wish to exchange email within their organization or between organizations may request that Entrust provide access to their encryption certificate over the public internet. *UK MPKI: Does not support this use case of encryption certificates being made available via LDAP via internet. LDAP replication is also not supported due to the local GDPR & other regulations.*	$$*	N
UMS (and URS) customer Logo	Ability to upload the customer logo. *UK MPKI: Does not support*	Y	N
LDAP replication	Customers that need to have their end-user certificates copied into customer-operated directories can utilize the LDAP replication service. LDAP replication is a directory independent process; the customer may operate any LDAP-compliant directory with the requisite object classes. *UK MPKI: Does not support*	$$*	N

ENTRUST

MPKI ENTERPRISE CA (PRO+) SERVICES

Service	Service Description	mPKI Pro + NA	mPKI Pro + UK
Custom cert types (same as digital ID)	Customer may request specialized certificate modification including Adobe signing, or specific extended key usage settings.	Y	Y
Delta CP/CPS	Customized certificate policy and practices statements based on our core policy documents tailored to the customer's specific implementation. *UK MPKI: Does not support as base CP/CPS is not followed*	Y	N
Additional issuing CAs	Any additional issuing certificate authorities (CA) that need to be added post onboarding for either production or test instance.	$$*	$$*
Audited root key generation ceremony	Generating the CA keys in a trusted manner, observed by a third party that can testify to the procedures that were performed and ensure the integrity and trust in the infrastructure for both the customer and third parties.	Y	Y
Audit logs, system audits	Access to audit logs and system audits - separated out for a specific customer. *UK MPKI: Supports RA logs only, via raw SPLUNK feed. Doesn't support audit logs and system audits; as per scheme regulation audit logs and system logs cannot be shared.*	Y	N
OCSP	Dedicated customers can optionally request OCSP for an additional price. NFI and Fed CAs have OCSP available to all customers.	$$*	$$*
mPKI - Technical Account Manager	• Single point of contact from highly experienced support agent • Quarterly SLA Performance reporting • Monthly emailed Service Activity Report (LRA verification, enhancements reqs, bugs, etc.) *UK MPKI: Not available*	$$*	N
mPKI - Premium Technical Account Manager	• Single point of contact for support oversight and advocacy • Monthly Conf-call SLA Performance reporting • Monthly Conf-call Service Activity Report (LRA verification, enhancements reqs, bugs, etc.) • TAM delivered Operational Activity briefings – customized per customer • Personal High Severity Incident Care • 10 hrs/yr TAM-driven mPKI operations Service Consultation - Additional hours of Service Consultation billed as T&M • 2 annual conf-call service review meetings (use cases, expansion opportunity, roadmap discussions, etc.) • 1 annual on-site visit for technical and service review assessments *UK MPKI: Not available*	$$*	N
CA Gateway	Enterprise PKI Certificate Lifecycle Management and operational management across all your Entrust certification authorities (CAs)	$$*	$$*
Test CA	Provided in line with the Dedicated CA package. Though Silver support is applicable by default, SLA commitment is not applicable for Test CA.	$$*	$$*
Managed EDC root CA	Offline root CA hosted and managed by Entrust	$$*	$$*
Enrollment protocols supported post onboarding	CSRES, MDMWS, MDMWS-SCEP, CSR-SCEP, EST, CMPv2	$$* (Annual Service)	$$* (Annual Service)
Third-party integrations (CAGW, customer premises integration)	Any Non-Entrust product, as per customer request, being integrated to work with MPKI hosted solutions are referred to as third-party integrations.	$$*	$$*

*$$ - Available for additional cost

Learn more at entrust.com

ENTRUST