



Entrust Managed Services PKI Packages: Microsoft Mediaroom

Microsoft requires Mediaroom service providers to establish a highly trusted PKI environment for the Certification Authorities (CAs), servers and set-top clients in the Microsoft Mediaroom solution. Specifically, Microsoft requires a high level of protection around the keys that are the most costly to replace – the Root CA and Intermediate CA keys for a given service provider.

Entrust Managed Services PKI can help you establish, enhance and manage security across your environment by providing proven solutions that are compliant with your Microsoft Mediaroom solution. With Entrust, the offline CA infrastructure for delivering and managing certificates for Mediaroom-compliant solutions - PKI experts, secure facilities, policies, best practices and business controls - are already in place.

Entrust offers three packages to address Mediaroom requirements - Premium, Standard and Basic. Each package has a flexible term and corresponding cost structure. The following is a general description of the services available from Entrust, depending on the options selected.

Features / Package	Root & Intermediate CA	Hardware Security Module	Initial & Annual Audits	Disaster HSM & CA on standby	IPTV PKI Evaluation Workshop
Basic	✓	✓			Recommended
Standard	✓	✓	✓		Recommended
Premium	✓	✓	✓	✓	Recommended

Basic

This service offering includes the setup and on-going operation of a Root CA and an Intermediate CA in a secured facility. The Root CA and Intermediate CA will be setup and operated in accordance with Entrust’s Certification Practice Statement for Mediaroom services. Certification Authority key pairs are generated as part of a root key generation ceremony that will not be witnessed by an auditor and the private keys are stored in hardware security modules (“HSM”), using the Microsoft Mediaroom reference architecture. The Certification Authority’s

are kept in secure facilities to reduce risk of fraudulent creation of certificates. This involves secure physical access to the facility (card reader access), fire and alarm systems, a safe for key information, and trained security staff. Procedural controls, such as the role and authentication requirements required to perform sensitive Certification Authority functions, is also maintained to protect the security of the Certification Authority. The maximum number of valid Certificates will be limited to five hundred Certificates.

Standard

This service offering includes everything in the Basic offering as well as an auditor-witnessed Root Key Generation Ceremony and annual audits by an external 3rd party auditor selected and paid for by Entrust.

Premium

This full service offering includes everything that is in both the Basic and Standard packages as well as disaster recovery capabilities for the hardware security module and Certification Authority.

Feature Descriptions

Root & Intermediate CA - Following the Mediaroom Reference Architecture, all packages include the setup and on-going operation of a Root CA and an Intermediate CA in a secure facility. The Root CA and Intermediate CA will be operated in offline mode (powered down and stored in a secured location), except for issuing, renewing and revoking Certificates, issuing Certificate Revocation Lists or refreshing data backups for the disaster recovery site every time the Certification Authority is changed. Entrust will have a minimum of five business days to process each request submitted by the Registration Authority or Local Registration Authority to issue, renew and revoke Certificates.

Hardware Security Module (HSM) - The Certification Authority private key(s) will be stored in specialized, tamper-resistant hardware security modules that provide increased protection against unauthorized issuance of fraudulent certificates. An HSM provides a secure location to generate and store the CA signing (private) key in an encrypted state (unlike server software storage, where the private key resides in active memory and in an unencrypted state, making it more available to tampering). The private key digitally signs a Certificate without leaving the HSM.

Initial & Annual Audits – The Standard and Premium packages include the execution of an external auditor-witnessed root key generation ceremony for both the Root CA key and the Intermediate CA key within a secure vault. In addition, an external third-party auditor verifies on a regular basis that the certificate practice statement is followed.

Root key generation ceremony - The secure creation of the root key, or private key, is an integral part of the entire PKI system. A root key generation ceremony affirms that an organization's practices are followed and that no anomalies occurred that might later impugn the integrity of the root Certification Authority key pair.

Disaster HSM and CA on Standby – Disaster recovery ensures that your system can continue to issue certificates to subordinate online CAs and issue certificate revocation lists for validation of Certificates in the event of a catastrophe affecting the building housing the Certification

Authority at the primary site. The Entrust PKI maintains backup systems to reduce the risk that data is lost in the event of a total failure. These data backups and system software and hardware are made available at a secondary secure facility to assume the duties of the original servers when required. Entrust's Disaster Recovery Plan establishes procedures to recover a PKI following a disruption.

IPTV PKI Evaluation Workshop

For many customers the implementation of Microsoft Mediaroom is their first exposure to Public Key Infrastructure (PKI), especially the detailed policies and practices required by the IPTV PKI Evaluation. Yet the completion of this evaluation – and the understanding of the requirements it imposes on the proper operation of the CAs – is a mandatory step in receiving the Validation Object (VO) from Microsoft. With over 10 years experience in PKI policies and best practices, Entrust Professional Services has the in-depth knowledge customers require in preparing the IPTV PKI Evaluation and ensuring that their CAs are operated in a compliant manner.

Entrust Professional Services offers an IPTV PKI Evaluation Workshop consisting of up to three consecutive days onsite with key customer personnel to conduct a detailed walkthrough of the Microsoft PKI Evaluation for IPTV Edition 1.1 document as it relates to the customer hosted components. An Entrust Security Consultant leads the workshop, explaining in detail each requirement in the IPTV PKI Evaluation and how best to meet it within the customer's context. The Security Consultant completes the IPTV PKI Evaluation form as the workshop progresses – this form is ready for immediate submission to Microsoft. A key value to the customer is the close relationship between Microsoft and Entrust, resulting in expedited approval of the IPTV PKI Evaluation.

Additionally, a fundamental requirement of the IPTV PKI Evaluation is the preparation of a Certification Practice Statement– a structured document that describes the practices used to operate the CAs in a secure manner. The IPTV PKI Evaluation Workshop includes development of a skeleton CPS based on the customer's responses to the evaluation form. Finally, up to four hours post-workshop remote consulting services is included.