[MS-RMSOD]: Rights Management Services Protocols Overview

Errata below are for Protocol Document Version V7.0 – 2015/06/30.

Errata Published*	Description
2015/07/20	In various places in Section 2.5.4, Use Case Descriptions, corrected information related to the service connection points and GICURL value. Changed text is in bold.
	In Section 2.5.4.2, Bootstrap RMS Client - RMS Client Application, changed from:
	6. To publish offline, the user has to have a separate signing certificate that is bound to the user's identity in RMS. The client first finds the service location, by deriving it from a publishing license (PL) or by discovering it from the directory service.<5> The client then sends a request to the publishing RMS server to retrieve the CLC.
	<5> Section 2.5.4.2: Windows RMS clients search Active Directory for the security processor certificate (SCP) unless one of the following registry keys is present:
	…
	Windows RMS servers search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://<server name>/_wmcs/certification.
	Changed to:
	6. To publish offline, the user has to have a separate signing certificate that is bound to the user's identity in RMS. The client first finds the service location, by deriving it from a publishing license (PL) or by discovering it from the directory service.<5> The client then sends a request to the publishing RMS server to retrieve the CLC.
	<5> Section 2.5.4.2: Windows RMS clients search Active Directory for the service connection point (SCP) unless one of the following registry keys is present:
	…
	Windows RMS servers search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://<server name>/_wmcs/certification/certification.asmx.
	In Section 2.5.4.4, Find Service Locations for Client - RMS Server, changed from:
	Main success scenario
	…
	5. At least one of the responses includes a valid set of security processor certificates (SCPs) for the services requested. This can be an SCP pointing to the other RMS server that responded or an SCP that is known to that server.
	Changed to:
	Main success scenario
	…
	5. At least one of the responses includes a valid set of service connection points (SCPs) for the services requested. This can be an SCP pointing to the other RMS server that responded or an SCP that is known to that server.

*Date format: YYYY/MM/DD