Architecture Design Document



Information Protection Using Azure Rights Management Services

Prepared for

[Customer Name]

June 20, 2014

Version .1

Prepared by

**Author**

Add Author Position to Doc Properties

Add Author Email to Doc Properties

Contributors

**Add Contributors to Doc Properties**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1.0 | Initial version for discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 6](#_Toc391036260)

[1.1 Azure Rights Management Services Terminology 6](#_Toc391036261)

[2 Solution Objectives Summary 7](#_Toc391036262)

[2.1 Scope 8](#_Toc391036263)

[2.2 Out of Scope 9](#_Toc391036264)

[2.3 Technical Requirements 10](#_Toc391036265)

[3 Solution Environment 11](#_Toc391036266)

[3.1 Client and Applications for Azure Rights Management Services 11](#_Toc391036267)

[3.2 Usage Scenarios 12](#_Toc391036268)

[*3.2.1* Usage Scenario *X* – *Scenario name* 12](#_Toc391036269)

[4 Solution Architecture 12](#_Toc391036270)

[4.1 Azure RMS Service Architecture Components 13](#_Toc391036271)

[4.1.1 Azure Active Directory 14](#_Toc391036272)

[4.1.2 Azure RMS Service 15](#_Toc391036273)

[4.1.3 Logging Services 16](#_Toc391036274)

[4.1.4 Client-Side Components 17](#_Toc391036275)

[5 Azure RMS Design Decisions 20](#_Toc391036276)

[5.1.1 Active Directory Considerations 20](#_Toc391036277)

[5.1.2 Azure RMS Templates 20](#_Toc391036278)

[5.1.3 Mobile Devices 21](#_Toc391036279)

[5.1.4 RMS PowerShell and File API 21](#_Toc391036280)

[5.1.5 Microsoft RMS Software Development Kit (SDK) 22](#_Toc391036281)

[5.1.6 Solution Design - Client 22](#_Toc391036282)

[5.1.7 Server Integration Options 26](#_Toc391036283)

[6 Conclusion 30](#_Toc391036284)

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar mark-ups in red. To turn this feature off, do the following:

1. Click **File**.
2. Click the **Options** on the left.
3. Click **Proofing**.
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl + H to open the **Find and Replace** box
2. Make sure your cursor is in the **Find what** box.
3. Click the **More** button at the bottom left.
4. Click the **Format** button at the bottom left and select **Style**.
5. Scroll down, locate select the **Visible Guidance**.
6. Make sure the **Replace with** box is empty.
7. Click **Replace All**.
8. If not empty - click the format button in the lower left-hand corner. Scroll down and choose **(no style)**, then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Introduction

This document describes the architecture of an Azure Rights Management Services solution for [Customer Name], based on the design decisions made during the Envisioning Workshop delivered on <date>.

* 1. Azure Rights Management Services Terminology

| **Terms** | **Explanations** |
| --- | --- |
| Azure RMS | Azure Rights Management Services  This is a technology that provides persistent protection to digital data using encryption, certificates, and authentication. Authorized recipients or users must acquire a license in order to consume the protected files, according to the rights, or business rules, set by the content owner. |
| Azure RMS Architecture | This refers to the entire suite of Azure RMS components, including Azure RMS service, logging services, and RMS-enabled applications and their dependencies, such as Azure Active Directory (AAD). |
| RMS-protected Content | Digital information that is protected by Azure RMS technology. |
| IRM | Information Rights Management, which refers to the Azure RMS supporting features in Microsoft Office 2010/2013 Professional Plus, the RMS App, and any other product like SharePoint and Exchange. Other editions of Microsoft Office also support IRM but in a read-only fashion. This term does not refer to the overall Azure RMS Platform, which can be used by other applications. |
| Encrypt content | This describes the process of converting information into a form that can be read only by a specific receiver. Encryption is an effective way to help keep information secure. To decipher a file that has been encrypted, the receiver must have the secret key or password that will translate it.  In an Azure RMS context, this term suggests that not only will the content be encrypted using the encryption key, but the RMS information will also be attached to the content. |
| Decrypt content | This describes the process of making encrypted data readable again by converting cipher text to plaintext.  In an Azure RMS context, this term suggests that not only will the content be decrypted the content using decryption key, but the content will also be converted back to the original plain content. |
| XrML | eXtensible rights Markup Language  The XML-based format that is used by Azure RMS for all of the licenses it supports, including machine certificates, rights account certificates, client licensor certificates, use licenses, publishing licenses, and server licensor certificates. Licenses are documents that specify the policy applied to protected content. |

**Table 1 –** Rights Management Terminology

1. Solution Objectives Summary

The proposed solution comprises the system components, which work together to address all requirements of <<Customer Name>> using the Azure Rights Management Services platform, and set the correct customer expectations on the desired solution and overall project direction.

The major objective of this proposed solution is to use Azure RMS to protect confidential documents against security threats, such as information disclosure in <<Customer Name>>. In particular, the solution will:

*Paste the customer’s information protection business needs as surveyed during the Envisioning Workshop. The scenarios listed below are provided as examples.*

1. Protect information from unauthorized view and unwanted disclosure by encrypting the sensitive contents and by applying granular rights protection to the actual contents.
2. Enable Regulatory Compliance and IP Protection, enabling archival of RMS-protected e-mails and documents, and effectively logging the users’ document consumption activities.
3. Improve Security on Business Process Automation, which allows existing workflow to extend information protection to business process automation.
4. Enforce Corporate Policy and controlling Information Protection centrally, which makes centrally managed document protection efficient and allows inspection and audits, if necessary.
5. Enable Communication in Mixed Environments, allowing users to view file contents without RMS-Enabled versions of Office, through the RMS App or through XPS
6. Limit protected content authoring capability to certain users.

In the following sections the requirements for the solution are listed, and the scope of the solution and the summary of the usage scenario are described. There is a thorough description of all parts of the solution and a description of how the solution can be implemented in the <<Customer Name>> corporate environment.

*Customize this list according to the scenarios surveyed during the Envisioning Workshop. The scenarios listed below are provided as examples.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***#*** | ***Scenario*** | ***Business Requirements*** | ***Risk Identified*** | ***RMS Usage*** |
| *1* | *Executive Board Documentation Protection* | *Restrict access to critical information to BDM only.* | *Information printed and e-mails forwarded to additional chiefs, managers, or other personnel in the company.* | *Deploy “One-click” RMS Policy Templates allowing CxOs to restrict information flow among them.* |
| *2* | *Business Strategy and Competitive Documentation Protection* | *Mitigate information disclosure to external parties or competitors.* | *Sales Personnel who leave the company exchange critical information with external parties, thus affecting business plans.* | *Deploy restrictive policies that require personnel to connect every week (via license expiration), which will prevent people who leave the company from having access to files.* |
| *3* | *<<Company Name>> Internal Employees Information Only* | *Restrict access to information classified as Internal User Only.* | *There are no controls to prevent information/document exchange with Vendors and Temporary employees.* | *Implement RMS Policy Templates that allow limited access to Internal Use/ Employees Only documents.* |
| *4* | *Mobile Device consumption* | *View protected content on mobile devices* | *Employees receive protected content on mobile devices and cannot view it.* | *Deploy the RMS Sharing Application and AD RMS Mobile extension to view protected content.* |

**Table 2 –** <<Customer Name>> Business Requirements and Usage Scenarios

* 1. Scope

The following items are in scope of the solution design:

*Paste the requirements agreed for the solution as defined during the Envisioning Workshop. The items listed below are provided as examples.*

* Protect Data in Use
  + Protection of information included in emails through policy, encryption and access controls via the application of the Do Not Forward option in Outlook and the usage of Rights Policy Templates.
  + Protection of Word, Excel and PowerPoint documents through encryption and enforcement of restricted rights via the usage of Rights Policy Templates.
  + Protection of Word, Excel and PowerPoint documents through encryption and enforcement of restricted rights via manual assignment of rights.
  + Protection of text and image files, using the RMS App, through encryption and enforcement of restricted rights via the usage of Rights Policy Templates.
  + Protection of text and image files, using the RMS App, through encryption and enforcement of restricted rights via manual assignment of rights.
  + Protection of files of any file type with wrapper-based protection, using the RMS App, to control initial access and expiration.
* Protect Data in Motion
  + Automated protection of information included in emails based on content and context at the email server (Exchange Server 2010/2013) level.
  + Protected document exchange between divisions of the organization.
* Protect Data at Rest
  + Automated protection of information stored in sensitive document libraries at the SharePoint Server level.
  + Automated protection of information stored in file servers at the file server level using File Classification Infrastructure (FCI).
  + Automated protection of information stored in users’ Document folder at the file server level using File Classification Infrastructure (FCI) and Work Folders.
* Administration
  + Optimized design for a globally distributed environment.
  + Centralized management and reporting.
  + High availability of the platform components.
* Protected access to licensing services from the Internet without the need for VPN access.
  1. Out of Scope

The following items remain “out of scope” of the Azure Rights Management Services design;

*Paste the exclusions agreed for the solution during the engagement planning. The items listed below are provided as examples.*

* Support for restricting granular-level permissions with document types other than Office, XPS, text, and image files. Such support can be implemented through custom development or third party solutions based on Azure Rights Management Services.
* Integration with Hardware Security Modules for key protection.
* Implementation of two-factor authentication to the Azure RMS services.
* Data classification or automated protection of documents other than that provided by File Classification Infrastructure, SharePoint Server, and Exchange Server.
  1. Technical Requirements

*Below are some of the typical technical requirements for Azure RMS solutions. Please customize them for your customer according to the information surveyed prior to and during the Envisioning Workshop.* *The scenarios listed below are provided as examples.*

* Supporting Microsoft Office 2013/2010 Professional Plus and Office 2013/2010 Enterprise to enable content protection
* Allowing appropriate rights permissions/restrictions to be set according to users and groups.
* Supporting data classification by using Rights Policy Templates to provide data labeling services.
* Supporting the data retention policy by setting expiration dates on RMS-protected contents.
* Enabling offline usage, except for when the users access the content for the first time.
* Enabling offline usage, including for first time usage through Exchange pre-licensing.
* Enabling access to the contents from the Internet through a Corporate Virtual Private Network (VPN).
* Enabling service availability 24 hours x 365 days by utilizing the fully redundant Azure RMS service.
* Enabling appropriate logging actions performed on the system.
* Protecting from information disclosure by applying RMS encryption using standard algorithms, such as AES and RSA.
* Enabling the capability of Backup / Restore / Disaster Recovery processes.
* Enabling the creation of Rights-Protected content on the server side for certain applications.
* Enabling multi-forest integration.
* Provide access to documentation to authorized users from the Internet.
* Integrating with on-premises Exchange 2010/2013 servers to provide OWA access to different browsers | Journal Decryption | Transport Protection Rules | Transport Decryption | Search Indexing | Outlook Protection Rules.
* Integrating with Exchange Online services to provide OWA access to different browsers | Journal Decryption | Transport Protection Rules | Transport Decryption | Search Indexing.
* Integrating with on-premises SharePoint 2010/2013 servers to provide the automatic protection of documents stored in sensitive document libraries upon download.
* Integrating with on-premises File Classification Infrastructure to provide automatic protection of documents stored on file servers, based on content and/or location.

1. Solution Environment

The solution is expected to operate in the current environment at <<Customer Name>>. This environment has the following characteristics relevant to Azure RMS.

* 1. Client and Applications for Azure Rights Management Services

*Below are some of the typical RMS Clients and applications. Please customize them for your customer. The scenarios listed below are provided as examples.*

The solution design is based on the following RMS clients and applications:

* **Computer Requirements**
  + All clients are using Windows 7 or Windows 8
  + Clients are members of the <<CUSTOMERDOMAINNAME>> Active Directory Forest/domain
* **User Requirements**
  + Users are regular employees, contract employees, or guests, members of the <<CUSTOMERDOMAINNAME>> Active Directory Forest/domain
* **Application Requirements**
  + Clients use Microsoft Office 2010/2013 <indicate edition> that supports RMS Capabilities
  + The RMS client v2.1 or later or RMS App is installed on the clients
  + XML Paper Specification (XPS) Writer/Viewer is installed on the clients
  + Rights Management Sharing Application (RMS-App) is installed on the clients
  1. Usage Scenarios

*Below is a template for Azure RMS Usage scenarios. Please include one heading for each intended scenario. The scenario list does not need to be exhaustive; this section just enumerates the scenarios discussed during the Envisioning Workshop that explain the decisions made.*

The solution was designed based on a certain usage scenarios. This section describes some of the examples identified during the Envisioning Workshop.

* + 1. Usage Scenario *X* – *Scenario name*

Scenario description: *<<briefly describe the scenario, for example “Managers and other full time employees sharing sensitive documents through email with authorized third parties, and wanting to limit further propagation of the shared information”>>.*

Document types: <<Specify Office documents, email, others>>

Intended audience for the information: <<Specify target authorized audience, such as all internal employees, managers, partners, ad-hoc specific individuals, etc.>>.

Rights needed by the intended audience: <<specify if the intended audience needs any specific access level such as being able to print, copy or resend the content to other individuals>>.

Additional restrictions: <<specify if documents need any additional restrictions such as expiration, requirements for online licensing, etc.>>

1. Solution Architecture

<<Customer Name>> chose to use Azure Rights Management Services to build an Information Protection solution that can address all business and technical requirements.

Azure RMS is an information protection service provided by Microsoft that works with client and server-side applications to help safeguard the digital content—no matter where it goes—for people who need to protect sensitive Web content, documents, e-mail and other forms of digital information. Users can define exactly who can open, read, modify, and redistribute the content. Organizations can create rights policy templates that enforce policies that can be applied to content. Responding to customer demand for improved content protection, Microsoft designed Azure RMS as an extensible platform, capable of integration into third-party applications as well as into Microsoft Office starting with Office 2010.

Azure RMS allows documents to be shared as well as sent in e-mail messages while helping maintain control over who can view or edit the document, as well as who can print, extract information or perform other operations on the content. Once a document or e-mail message is protected with this technology, the access and usage restrictions are enforced no matter where the information goes; even if the file is sent outside the firewall. Because RMS protection is embedded in the protected file, usage restrictions will persistently be enforced.

* 1. Azure RMS Service Architecture Components

*Below are the main Azure RMS Service components. Please customize the list for your customer.*

The following components are part of the Azure RMS architecture; in this section we present general considerations about each specific role and usage.





* + 1. Azure Active Directory

Azure Active Directory (AAD) is a core architecture component used by Azure RMS. The following services are provided when Azure RMS is in place:

* **Authentication Services**
  + Azure RMS relies on AAD to authenticate users who participate in the Azure RMS environment. Because of this, there is no anonymous-access to Azure RMS.
* **Group Membership**
  + Because users can belong to many different groups in multiple domains/forests in the Azure RMS environment, it might be necessary to validate effective user permissions assigned to groups using group expansion in order to guarantee the appropriate user rights.

Azure Active Directory can be synchronized with on-premises Active Directory using the Directory Synchronization Tool. Optionally, you can also implement Active Directory Federation Services (AD FS) to pass authentication back through federation and complete it against the on-premises Active Directory.

* + 1. Azure RMS Service

Azure RMS is an Azure service that provides information protection by using encryption and policy to help secure documents, files, and emails. The Azure RMS service provides the following functionality:

* **Certification Service**
  + Certification refers to the account certification and activation activities performed by Azure RMS. Each user must acquire a set of certificates that identity that particular user to be able to participate in the Azure RMS platform.
* **Licensing Service**
  + Licensing refers to the set of operations by which the Azure RMS Service grants access to protected content to authorized users. The Azure RMS Service grants a use license for each document to authorized users
* **Rights Policy Templates**
  + Rights policy templates specify a predefined set of rights and conditions that can be applied to protected content, simplifying the RMS Protection for common or daily-use scenarios to the end-users. Azure RMS administrators create and manage rights policy templates.
  + When publishing protected content, the author selects the rights policy template to apply from the templates that are available on the local computer. To make rights policy templates available for use, the administrator must deploy them to user computers or the client computer should have access to a shared folder.
  + When a user attempts to consume content protected through a template, the Azure RMS Service retrieves the latest version of the rights policy template that was used to publish the content from the configuration database and issues a license based on that template.
* **Azure RMS Trusts**
  + In Azure RMS, trust relationships are implied with any other organization supported by Azure Active Directory, including users with Office 365 or using RMS for Individuals. Users can collaborate with external parties who have Azure Active Directory, without the need to configure a trust relationship.
  + Note that this trust relationship provides the ability to collaborate; it does not automatically grant external users access to protected content. External users must be explicitly mentioned in the permission policy.
    1. Logging Services

Azure RMS provides access to tenant logs using Windows Azure storage. RMS can log every request that it makes for an organization, which includes requests from users, actions performed by RMS administrators in an organization, and actions performed by Microsoft operators to support an RMS deployment. RMS writes logs in W3C extended log format into an Azure storage account that you provide. You can then direct these logs into a repository of your choice (such as a database, an online analytical processing (OLAP) system, or a map-reduce system) to analyze the information and produce reports. This information is useful for a variety of reasons:

* **Analyzing data access for business insight:** 
  + These logs can be used to create reports and drive insights such as: who is accessing sensitive data, what devices are being used for access, which locations are users accessing data from, and report on which users have read a given document.
* **Monitoring for abuse**
  + Logs can be accessed in near-real-time (delay: < 15 minutes). This allows administrators to continuously monitor usage of the Microsoft RMS assets. For example, tenant administrators may want to be alerted if there is a spike in access of assets after business hours (why someone is trying to open lots of critical documents in a short time), or if the same user is accessing from two different IP addresses within 15 minutes (have passwords been compromised), or if someone is trying to read content from a remote location (we don’t have any staff there).
* **Performing Forensics**.
  + When there is an information leak the logging information can help determine the users that recently accessed the leaked document and what information a specific user accessed recently.

RMS logging is optional. When you use RMS logging, there is no change in how RMS works and the logging process itself is free. However, you must provide an Azure storage account for the logs and you will be charged for this storage.

* + 1. Client-Side Components

The client-side components of RMS are:

* **Rights Management Services Client**
  + The RMS Client is software designed for client computers to help protect access to and usage of information flowing through applications that use Azure RMS.
  + The latest version of the RMS Client 2.1 should be deployed to all clients. It is available as a free download from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=38396) (http://www.microsoft.com/en-us/download/details.aspx?id=38396).
  + Note that Windows 7 already includes an outdated version of the Rights Management Service Client. This version should be replaced with the latest version as referenced above.
  + Installing this client places software on your computer that allows RMS-enabled applications to work with Azure RMS to provide licenses for publishing and consuming RMS-protected information. If a previous version of the RMS Client is installed on a computer, installing this Client will replace it. Once installed, the Client will be ready for use by applications designed to support Azure RMS, providing the user with access to RMS features.
  + Note that the latest version of the RMS Client is included in the Rights Management Sharing Application software package.
* **RMS enabled applications**.
  + RMS protection is a persistent document-level protection technology that helps protect digital information from unauthorized use. Applications such as Microsoft Office 2013 Professional Plus and Microsoft Office 2010 Professional Plus, support for RMS protection through their IRM features. The Windows XPS client also provides such support.

**Additional components:**

* **Rights Management Sharing Application (RMS App)**. 
  + The Rights Management Sharing Application (RMS App) is a user-driven application which allows user to protect and consume files of any file format. The RMS App can be used to protect files of any file type using a built-in right click protection option. Protected Office files open in the native application. Protected PDF files open in RMS-aware PDF readers. Protected text and image files open in the RMS App reader. Files of any other file type are protected with a wrapper-based protection. These files are decrypted and then opened in the native application. Unlike the file types mentioned above, the wrapper-based protection provides support for initial authentication and expiration; however, it does not support granular-level permissions.
  + The RMS App also supports the Share Protected feature in the Office user interface. This one-click button allows users to send a protected version of the document via email, and apply ad hoc protection on the file.
  + The RMS App supports mobile devices to allow for the consumption of protected content. Additionally, third party applications can be utilized to extend mobile device support to pdf and other file formats.
* **XML Paper Specification (XPS) client**.
  + XPS is a general purpose page description language that makes portable and secure documents possible for all applications. XPS describes electronic paper in a way that can be read by hardware, software, and humans. With XPS, documents can print more reliably, can be shared more easily, can be archived with confidence, and are more secure.
  + Microsoft has integrated XPS-based technologies into Microsoft Office 2013/2010 and the Microsoft Windows 8 and Windows 7 operating systems but XPS itself is platform independent, openly published, and available royalty-free. Microsoft is using XPS to bring additional document value to its customers, its partners, and the computing industry.
  + In Windows 8 and Windows 7, XPS document features are already in place. You can generate XPS files from any application that can print to a standard printer by printing and selecting the Microsoft XPS Document Writer as the printer. You can view XPS documents by simply double-clicking on them. They will automatically open inside an XPS viewer. For earlier versions of the Windows OS, you can [download](http://www.microsoft.com/whdc/xps/viewxps.mspx) the Microsoft XPS Document Writer to generate XPS files from any Windows application and an XPS viewer to see the results.
  + The XPS client included with Windows 8 and Windows 7 Vista and the .Net framework 3.0 is an RMS-enabled application so that any XPS Document can be protected with Azure RMS.
  + XPS can thus be used to deliver protected documents for applications that do not natively support Azure RMS, even in cases where the target users do not have access to the source applications.

1. Azure RMS Design Decisions

*This section includes all the architectural decisions made during the Envisioning Workshop. List under each heading the decisions made.*

During the Envisioning Workshop, design decisions were made together with <<Customer Name>> after careful consideration of the alternatives, best practices and needs. These decisions, that guided the architecture developed, are enumerated below.

* + 1. Active Directory Considerations

*Active Directory is a key component of an Azure RMS implementation; Please insert AD diagram obtained from the customer.*

The following diagram presents the Active Directory Architecture in which Azure RMS will be implemented in <<Customer Name>>:

*Insert AD Diagram here*

* + 1. Azure RMS Templates

*Please provide the strategy defined for template usage. If the definition is to centralize templates and access them remotely, replace the following paragraph.*

<<Customer Name>> has decided to deploy the RMS Policy Templates to all client machines, and all the XML files will need to be copied to client machines. This will provide users with the capability to assign permissions to documents either in the Intranet, on the Internet or when offline.

Templates should always be designed so that they follow a uniform taxonomy that makes it easy for users to select the right Rights Policy Template.

*Select the right one among the following paragraphs based on the definition for template policy.*

At <<Customer Name>> templates will be defined to limit usage of protected information to different employee levels and roles.

At <<Customer Name>> templates will be defined to scope content to different organizations and departments.

At <<Customer Name>> templates will be defined to reflect different data classifications based on Business Impact.

At <<Customer Name>> templates will be defined to reflect different data classifications based on specific content such as PII or Intellectual Property.

At <<Customer Name>> templates will be defined to scope content to audiences such as Full Time Employees, Contractors, Partners, etc.

Details on the different templates to be used will be defined in the Detailed Design Document.

* + 1. Mobile Devices

*Please provide any info about mobile devices in customer environment, and security implications (if any).*

<<Customer Name>> has decided to allow users to utilize protected content on mobile devices.

*Insert WAP/AD FS/mobile device diagram here.*

*Provide any info regarding AD FS URLs, or relying parties configuration in AD FS.*

*Detail if AD FS is already implemented in the organization, and if a trust is already established.*

* + 1. RMS PowerShell and File API

*Please provide any info about the customization needed in customer environment, and security implications (if any).*

*Please provide any info about whether the RMS PowerShell or File API will be used in the customer environment and, if so, how it will be used*

<<Customer Name>> has decided to use the RMS PowerShell or File API to enable the following scenarios:

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Details** | **PowerShell** | **File API** |
| Bulk protection | Use Azure RMS to selectively bulk protect items in certain locations | Can be used to select multiple files and pipeline the request to File API or a personalized application | Can protect multiple files on a directory or pipelined |
| Bulk un-protection | Use Azure RMS to selectively bulk unprotect items in certain locations | Can be used to select multiple files and pipeline the request to File API or a personalized application | Can un-protect multiple files on a directory or pipelined |
| Manual protection | Use Azure RMS to manually protect files or folders | Can be used to select a single or multiple files or a folder and pipeline the request to File API or a personalized application | Can protect single or multiple files on a directory |

* + 1. Microsoft RMS Software Development Kit (SDK)

*Please provide any info about whether the RMS SDK will be used in the customer environment and, if so, how it will be used*

The RMS SDK 2.1 platform enables developers to build applications that leverage RMS to provide information protection. The RMS SDK 2.1 handles complex security practices such as key management, encryption and decryption processing, and offers a simplified API for easy application development.

<<Customer Name>> has decided to use the RMS SDK to enable the following scenarios:

|  |  |
| --- | --- |
| **Scenario** | **Details** |
| Extend RMS granular permissions to additional file formats | Extend granular permissions to the following:   * CAD files |
| Encrypt data at rest | Automatically encrypt sensitive information upon download from SAP applications |

The RMS SDK 2.1 is available from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=38397) (<http://www.microsoft.com/en-us/download/details.aspx?id=38397>).

* + 1. Solution Design - Client

*Please customize this section for your customer.*

The RMS Client is installed on end-user machines and is required to communicate between the Azure RMS service and Azure RMS-aware applications such as Microsoft Word 2013. There are three different versions of the RMS Client:

* RMS Client 2.x: This is the latest version of the RMS Client.
* RMS Client 1 SP2 (KB979099): This is the update to the RMS Client 1, which prevents users from receiving error messages related to the application manifest expiry feature in the RMS Client 1.
* RMS Client 1: This client is included in the Windows 7 and Windows Vista operating systems; however, it must be updated to the RMS Client SP2. If automated updates are being applied to client systems it is likely that this client is in-place already

The latest version of the RMS Client is required on all client machines running Windows 7/Windows Server 2008 or higher. Windows Vista and earlier do not support Azure RMS.

The activation of the RMS client software establishes a lockbox and computer certificate for the currently logged-on user. Activation is a local process and does not require a network connection. Once activation is successful, the first use of Azure RMS by an enabled application obtains a user certificate for the user. The RMS client can be installed on each client computer in the organization by using SMS, Group Policy, Windows Update, or an administrative script.

* + - 1. Azure RMS Client

*Please customize the list according to your customer’s software versions.*

| **OS** | **Requirement** | **Deployment mechanism** |
| --- | --- | --- |
| Windows 8  Windows 7  Windows Server 2012 R2  Windows Server 2012  Windows Server 2008 R2  Windows Server 2008 | Rights Management Service Client 2.1 (<http://www.microsoft.com/en-us/download/details.aspx?id=38396>) | Microsoft Update/SCCM |

* + - 1. Rights Management Sharing Application

*If the RMS App will be used in the customer environment, customize this section accordingly.*

|  |  |  |  |
| --- | --- | --- | --- |
| **OS** | **Requirement** | **Deployment mechanism** |  |
| Windows 8  Windows 7 | Microsoft Rights Management sharing application for Windows (<http://www.microsoft.com/en-us/download/details.aspx?id=40857>) | GPO/SMS/SCCM/Embedded in OS image/manual installation/other |  |
| Windows RT  iOS Mobile Devices  Android Mobile Devices | Microsoft Rights Management Sharing application (<https://portal.aadrm.com/home/download>) | Windows Intune/manually through the App Store |  |

* + - 1. XML Paper Specification (XPS) client

*If XPS will be used in the customer environment, customize this section accordingly.*

|  |  |
| --- | --- |
| OS | [Requirements](http://www.microsoft.com/whdc/xps/viewxps.mspx) |
| Windows 8 and Windows 7 | None (already includes XPS Viewer) |

* + - 1. Operating System and RMS Enabled Applications

*Please customize this section for your customer.*

|  |  |  |  |
| --- | --- | --- | --- |
| OS | Office Version | Office Products | Editions |
| Windows 8.1, Windows 8 and Windows 7 , Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 | Microsoft Office 2013  Microsoft Office 2010 | Microsoft Office Word  Microsoft Office Excel  Microsoft Office PowerPoint  Microsoft Office Outlook  Microsoft Office InfoPath | Microsoft Office 2013 Professional Plus (Read and author content)  Microsoft Office 2010 Professional Plus (Read and author content)  All other versions of Office 2010 and 2013, including Office readers (Read content) |
| Windows Server 2008  Windows Server 2008 R2  Windows Server 2012  Windows Server 2012 R2 | Microsoft Office SharePoint 2010 Standard  Microsoft Office SharePoint 2010 Enterprise  Microsoft Office SharePoint 2013 Standard  Microsoft Office SharePoint 2013 Enterprise | - | - |

* + - 1. Azure RMS Service Discovery and Configuration Settings – Internal Client

*Please customize this section for your customer.*

The client deployment can be achieved using software distribution infrastructure such as Microsoft System Center Configuration Manager or AD Group Policy (Software Distribution). It is recommended to distribute the RMS client ahead of or at the same time as any deployment of Office so that the RMS users who try to use the IRM functionality will not be asked to download and install the RMS client software.

The following table presents the client configuration settings to be deployed for standard internal clients.

|  |  |  |
| --- | --- | --- |
| Configuration Setting | Provider | Explanation |
| *RMS Client Deployment* | *SCCM/GPO/Other* |  |
| *RMS App* | *SCCM/GPO/Other* |  |
| *XPS Viewer* | *SCCM/GPO/Other* |  |
| *Office 2013/2010 Professional* | *SCCM/GPO/Other* |  |

* + - 1. RMS Service Discovery and Configuration Settings – External Client

*Please customize this section for your customer.*

Users working from their home machines or partners accessing information from non-domain-joined machines will need special configurations. The deployment mechanisms for those configurations are explained in the table below.

|  | **Configuration Setting** | **Provider** | **Explanation** |
| --- | --- | --- | --- |
| **1** | *RMS Client Deployment* | *Script or manually Configured* |  |
| **2** | *RMS App* | *Script or manually Configured* |  |
| **3** | *XPS Viewer* | *Script or manually Configured* |  |
| **4** | *Office 2013/2010 Professional* | *Script or manually Configured* |  |
| **5** | *Others (Optional) Trusted Root CA Configuration* | *Script or manually Configured* |  |

* + - 1. Simple Delegation

Simple delegation for Azure RMS enables you to have the same access rights to protected content that are assigned to one person delegated to other individuals within their organization. Simple delegation provides the ability to have content rights assigned to executives and managers be easily and effectively delegated to their assistants. This enables the assistants to have the same level of access permission to Information Rights Management (IRM)-protected content as the executive.

<<Customer Name>> has decided to enable simple delegation to support this scenario.

* + 1. Server Integration Options
       1. Integration with SharePoint 2013/2010

*If SharePoint 2013/2010 libraries are in use at the customer, or plan to be used, and need to be integrated with Azure RMS for automated content protection, list the libraries to be integrated below.*

Microsoft SharePoint Server 2013/2010 can be configured to provide automatic protection to documents downloaded from its libraries based on the users’ permissions over those document libraries. The following SharePoint libraries are expected to be integrated with Azure RMS:

| **SharePoint Server** | **Library/List** | **Forest** | **SharePoint version** | **Extranet** | **AD FS enabled** |
| --- | --- | --- | --- | --- | --- |
| **SharePoint01** | **ManagementPlans** | Corp | SharePoint Server 2013/2010 Enterprise (x64) | No |  |
| **SharePointExtranet** | **PriceLists** | Extranet | SharePoint Server 2013/2010 Enterprise (x64) | Yes | With Contoso |

* + - 1. Exchange Prelicensing

*If the requirements for Exchange Prelicensing are met (listed in the table below) indicate if Exchange Prelicensing will be enabled.*

Internal deployments of Microsoft Exchange Server 2010 and Exchange Server 2013 can be configured to automatically acquire and deliver licenses to content delivered to the appropriate clients. Following are the requirements to enable Exchange Pre-licensing.

| **Component** | **Version** | **Minimum version needed** | **Can be upgraded** |
| --- | --- | --- | --- |
| **Exchange Hub Transport Servers** | Exchange Server 2013, Exchange Server 2010 | Exchange Server 2010 | Yes |
| **Office Client** | Office 2010 Enterprise | Office 2010 | No upgrade necessary |
| **Windows Phone** | 7.5 | 6.0 | No upgrade necessary |

Based on these requirements it is decided that Exchange pre-licensing will be enabled.

* + - 1. Integration with On-premises Exchange Server 2013/2010

*Include this section if your customer has Exchange Server 2010/2013 deployed and wants to implement the integration functionality indicated below. Customize according to your customer’s environment and requirements.*

<<Customer Name>> has deployed Exchange 2010/2013 as their email infrastructure. Exchange 2010/2013 can be integrated with Azure RMS to provide specific enhanced functionality.

The functionality in the table below will be implemented as part of this deployment.

| **Capability** | **Purpose** | **Details** |
| --- | --- | --- |
| **Transport Decryption** | Enable server Antivirus scanning to scan protected messages (available on specific antivirus software) | To be used with anti-virus and antispam transport agents |
| **Transport Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Indicate rules to be implemented* |
| **Data Loss Prevention** | To protect messages with sensitive information | *Indicate DLP Policies to be implemented* |
| **Outlook Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Indicate rules to be implemented*  *Specify if the rules will be mandatory*  *Confirm Outlook 2010 or later is available in the clients* |
| **Journal Decryption** | To provide automated decryption of messages sent to the journaling mailbox | *Indicate objectives of journaling mailbox* |
| **OWA IRM** | To enable users to author and consume protected content inside a browser | *Indicate browser platforms to be used.*  *Indicate if Exchange Server 2010 SP1 or later will be used, enabling in-browser attachment viewing.* |

* + - 1. Integration with Exchange Online

*Include this section if your customer uses Exchange Online/Office 365 and wants to implement the integration functionality indicated below.*

<<Customer Name>> is using Exchange Online as part of their email platform. Exchange Online in Office 365 can be integrated with Azure RMS to provide specific enhanced functionality.

The functionality in the table below will be implemented as part of this deployment.

| **Capability** | **Purpose** | **Details** |
| --- | --- | --- |
| **Transport Decryption** | Enable server Antivirus scanning to scan protected messages (available on specific antivirus software) | To be used with anti-virus and antispam transport agents |
| **Transport Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Indicate rules to be implemented* |
| **Data Loss Prevention** | To protect messages with sensitive information | *Indicate DLP Policies to be implemented* |
| **Journal Decryption** | To provide automated decryption of messages sent to the journaling mailbox | *Indicate objectives of journaling mailbox* |
| **OWA IRM** | To enable users to author and consume protected content inside a browser | *Indicate browser platforms to be used.*  *Indicate if Exchange Server 2010 SP1 will be used, enabling in-browser attachment viewing.* |

<<Customer Name>> understands that implementing this integration between Exchange Online and their on Azure RMS deployment requires exporting the Azure RMS cluster’s private key inside a Trusted Publishing Domain and importing it into the Exchange Online service in order to enable the service to perform the necessary encryption and decryption operations.

* + - 1. Integration with FCI and Work Folders

*Include this section if your customer has FCI deployed and wants to implement the integration functionality indicated below. Customize according to your customer’s environment and requirements.*

<<Customer Name>> has deployed FCI on their file servers. FCI in Windows Server 2012 R2 and Windows Server 2012 can be integrated with Azure RMS to provide specific enhanced functionality.

<<Customer Name>> has also deployed Work Folders on their file servers. Work Folders in Windows Server 2012 R2 and Windows 8.1 provides enhanced RMS protection to the end point.

The functionality in the table below will be implemented as part of this deployment.

| **File Server** | **Folder Classifier** | **Content Classifier** | **Forest** | **FCI version** | **Extranet** |
| --- | --- | --- | --- | --- | --- |
| **FileServer01** | **ManagementPlans** | String Patterns:   * Confidential * Project Alpha   Regular Expressions:   * Social Security numbers | Corp | Windows Server 2012 | No |
| **FileServer Extranet** | **PriceLists** | String Patterns:   * Confidential * Project Alpha   Regular Expressions:   * Social Security numbers | Extranet | Windows Server 2012 | Yes |



1. Conclusion

During the Envisioning Workshop, we presented technical information about the technology, as well as best practices and recommendations based on field experience deploying the platform.

Based on those recommendations, the information provided by <<Customer Name>>, and the discussions had during the session, a general architecture was defined that should be able to cover <<Customer Name>> information protection needs as stated at the beginning of the session. This architecture should not, at this point, be considered final. Further revision of the environment and the requirements should be performed as <<Customer Name>> becomes more familiar with the product and the solution proposed. As revisions are made to the design, a final architecture should be developed which can be applied to a production environment in the form of a Proof of Concept that will enable <<Customer Name>> to test the technology in their environment to obtain the necessary validation before deploying the technology at a large scale.