IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PASAFESHARE LLC , Plaintiff, v. MICROSOFT CORPORATION, Defendant.	Case No. 6:20-cv-00397 Jury Trial Demanded

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff paSafeShare LLC ("paSafeShare"), by and through its undersigned counsel, files this Complaint against Microsoft Corporation ("Microsoft") for patent infringement of United States Patent Nos. 9,455,961, 9,615,116, and 10,095,848 (collectively, the "patents-in-suit") (Exhibits 1-3) and alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

THE PARTIES

2. Plaintiff paSafeShare LLC is a limited liability company of New Jersey, having its principal place of business at 1 Shawnee Court, Colts Neck, New Jersey 07722.

3. On information and belief, Defendant Microsoft Corporation is a corporation organized and existing under the laws of the State of Washington with its principal place of business located at One Microsoft Way, Redmond, WA 98052. Microsoft may be served with process through its registered agent for service in Texas: Corporation Service Company, 211 East 7th Street, Suite 620, Austin, Texas 78701.

4. On information and belief, since at least November 1993, Microsoft has been registered to do business in the State of Texas under Texas SOS File Number 0010404606.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

6. Microsoft is subject to this Court's personal jurisdiction in accordance with due process and/or the Texas Long Arm Statute because, in part, Microsoft "[r]ecruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state." *See* Tex. Civ. Prac. & Rem. Code § 17.042.

7. Microsoft has already submitted to the jurisdiction of this Court in patent litigations bearing docket numbers: 6:19-cv-00399-ADA and 1:19-cv-00874-ADA.

8. This Court has personal jurisdiction over Microsoft because Microsoft (directly and/or through its subsidiaries, affiliates, or intermediaries) has committed and continues to commit acts of direct and indirect infringement in this judicial district in violation of at least 35 U.S.C. §§ 271(a) and (b). In particular, on information and

belief, Microsoft makes, uses, offers for sale, and sells licenses for, or provides access to, products and/or services that infringe the patents-in-suit, and induces others to use the infringing products and/or services.

9. This Court also has personal jurisdiction over Microsoft because Microsoft has sufficient minimum contacts with this forum as a result of business conducted within the State of Texas and this judicial district. In particular, this Court has personal jurisdiction over Microsoft because, *inter alia*, Microsoft, on information and belief: (1) has substantial, continuous, and systematic contacts with this State and this judicial district; (2) owns, manages, and operates facilities in this State and this judicial district; (3) enjoys substantial income from its operations and sales in this State and this judicial district; (4) employs Texas residents in this State and this judicial district, and (5) solicits business and markets products, systems and/or services in this State and this judicial district including, without limitation, related to the accused instrumentalities.

10. Microsoft has purposefully availed itself of the privileges of conducting business within this judicial district; has established sufficient minimum contacts with this judicial district such that it should reasonably and fairly anticipate being hauled into court in this judicial district; has purposefully directed activities at residents of this judicial district; and at least a portion of the patent infringement claims alleged in this Complaint arise out of or are related to one or more of the foregoing activities.

11. Venue is proper in this judicial district pursuant to 28 U.S.C. § § 1391(b)-(d) and/or 1400(b). Microsoft is registered to do business in the State of Texas,

maintains a regular and established place of business within this judicial district, and has committed acts of infringement in this judicial district.

12. On information and belief, Microsoft maintains a significant physical presence in this judicial district, including its corporate sales office locations, retail store locations, and datacenter locations (hereinafter collectively referred to as "Microsoft's Regular and Established Business Locations").

13. On information and belief, Microsoft operates multiple corporate sales offices in this judicial district including, without limitation, offices located at 10900 Stonelake Boulevard, Suite 225, Austin, TX, USA 78759,[1] and Concord Park II, 401 East Sonterra Boulevard, Suite 300, San Antonio, TX, USA 78258.[2]

14. On information and belief, Microsoft markets, offers to sell, and/or sells products through its corporate sales offices located in this judicial district including, but not limited to, the accused instrumentalities.

15. On information and belief, Microsoft operates multiple retail stores in this judicial district including, without limitation, stores located at 3309 Esperanza Crossing, Suite 104, Austin, TX, USA 78758,[3] and 15900 La Cantera Parkway, Suite 6560, San Antonio, TX, USA 78256.[4]

16. On information and belief, Microsoft maintains a list of certified learning partners in this judicial district that offer training solutions and certification in

[1] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[2] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[3] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[4] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.

Microsoft technology.[5] For example, on information and belief, at the ONLC Training Center, 700 Lavaca Street, Suite 1400, Austin, Texas 78701, Microsoft Certified Trainers offer training and courses in Microsoft Azure Security Technologies.[6]

17. On information and belief, Microsoft has spent at least tens of millions of dollars on networking and server infrastructure to support Microsoft Azure located in the State of Texas and in this judicial district.

18. On information and belief, Microsoft owns and operates multiple datacenters in this judicial district including, without limitation, data centers located at 5150 Rogers Road, San Antonio, TX 78251; 5200 Rogers Rd, San Antonio, TX 78251; 3823 Weisman Blvd, San Antonio, TX 78251; and 15000 Lambda Drive, San Antonio, TX 782245 (collectively, "Microsoft's Datacenter Locations").

19. On information and belief, Microsoft's Azure global infrastructure includes 58 regions worldwide. On information and belief, one of those regions is known as the "South Central US."

[5] *See* https://www.microsoft.com/en-us/learning/partners.aspx.
[6] *See* https://www.onlc.com/training/azure/austin-downtown-tx.htm.

https://azure.microsoft.com/en-us/global-infrastructure/regions/

20. Microsoft provides a list of Azure products and services available in the "South Central US" region, including but not limited to Azure Information Protection. *See* https://azure.microsoft.com/en-us/global-infrastructure/services/?regions=non-regional,us-south-central&products=all.

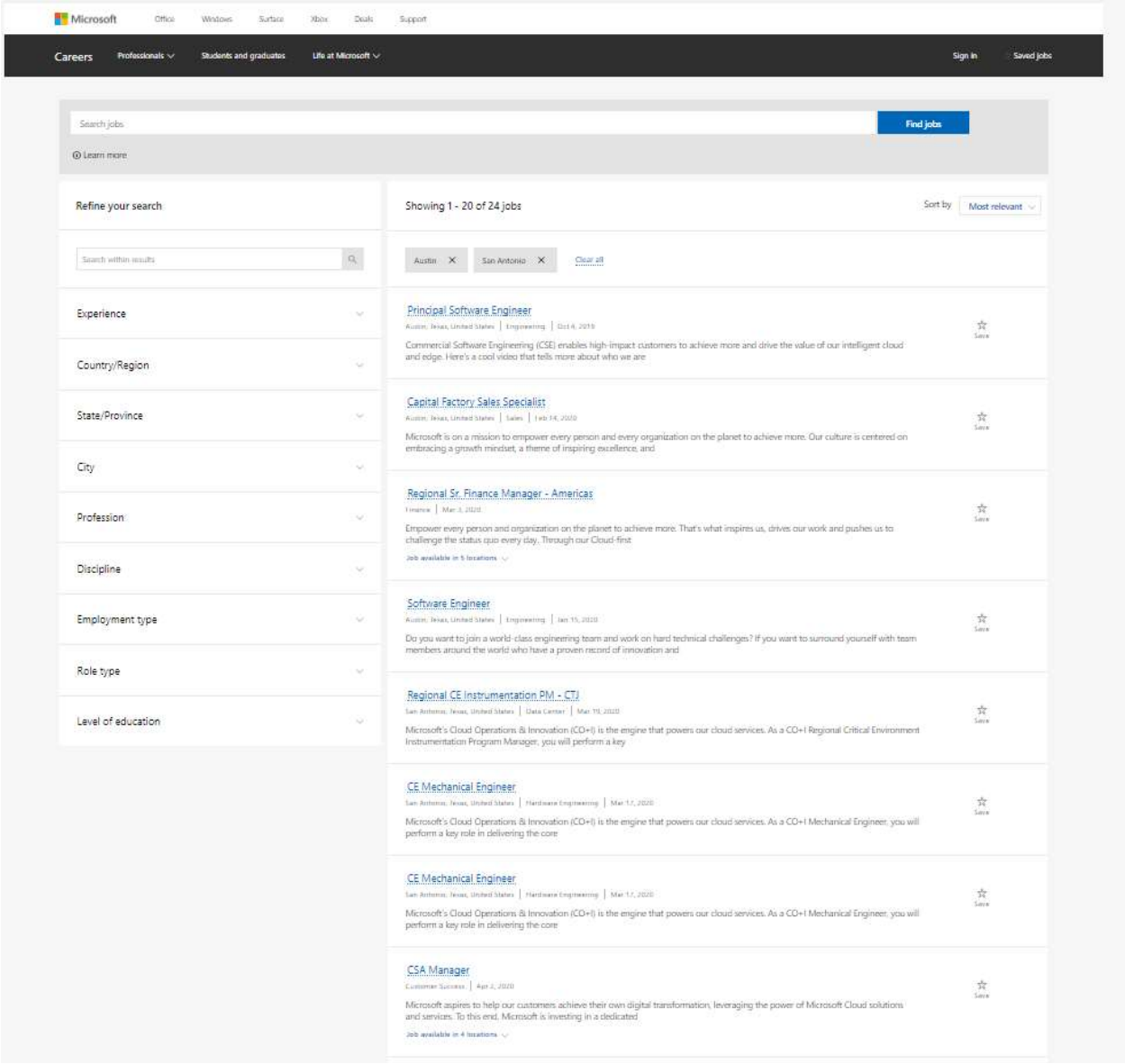
21. On information and belief, a substantial portion of the "South Central US" region's Azure network and server infrastructure is housed and operated in Microsoft's Datacenter Locations.

22. On information and belief, Microsoft has 36 H-1B labor condition applications for people employed in Austin, Texas.[7] On information and belief, Microsoft has 17 H-1B labor condition applications for people employed in San Antonio, Texas.[8] Employees holding an H-1B visa are employed in a specialty occupation that requires "theoretical and practical application of a body of highly specialized knowledge . . . and attainment of a bachelor's or higher degree in the specific specialty." *See generally* 8 U.S.C. § 1184. As such, Microsoft employees in Austin, Texas and San Antonio, Texas are highly specialized and important to the operation of Microsoft.

23. Microsoft lists job openings on its website for positions in this judicial district.

[7] *See* https://h1bsalary.online/index.php?searchtext=MICROSOFT+CORPORATION&year=&minsalary=&state=&worksite_city=AUSTIN%2CTX&job_title=.

[8] *See* https://h1bsalary.online/index.php?searchtext=MICROSOFT+CORPORATION&year=&minsalary=&state=&worksite_city=San+Antonio&job_title=.



https://careers.microsoft.com/us/en/c/data-center-jobs (visited on 4/9/2020).

BACKGROUND

24. The patents-in-suit are the result of paSafeShare's years of research, design and development of innovative and proprietary content distribution technologies.

25. Dr. Madhav S. Phadke and Kedar M. Phadke, co-inventors of the patents-in-suit, have over 50 years of combined experience in software development and technical consulting.

26. Dr. Madhav S. Phadke is a recognized leader in engineering design optimization and test methods. In the late 1980s, Dr. Phadke authored the first engineering textbook on robust design methods in the United States, *Quality Engineering Using Robust Design* (Prentice Hall, 1989). Dr. Phadke is also an ASQ Fellow and a recipient of the 2011 IEEE Region 1 Innovation Award.

27. In 1990, Dr. Phadke founded Phadke Associates, Inc. ("Phadke Associates"), a global consultancy and software services company. Phadke Associates develops and markets software tools for systems engineering process improvement and design and test optimization. Prior to founding Phadke Associates, Dr. Phadke was a manager in AT&T Bell Labs, a visiting scientist at the IBM Watson Research Center, and a Research Associate at the Army Math Research Center.

28. Dr. Phadke's son, Kedar M. Phadke, joined the family business in 2004 as Vice President of Phadke Associates. Mr. Phadke holds a Bachelor of Science in Economics from the Wharton School, University of Pennsylvania.

29. While working at Phadke Associates, the father-son duo noticed a significant oversight in existing content distribution security. In particular, they realized that while sensitive data could be protected in transmit by various security techniques (e.g., password-protected documents, access restricted web portals), there was no way to protect unwanted distribution by the recipient of the data.

30. In 2010, Dr. Madhav and Kedar Phadke founded paSafeShare LLC to address the deficiencies in existing content distribution security.

31. In or around mid-2010, Dr. Madhav and Kedar Phadke began developing technology related to secure content distribution.

32. The patents-in-suit relate, in part, to the persistent protection of content distributed within and across firewalls.

United States Patent No. 9,455,961

33. On September 27, 2016, the United States Patent and Trademark Office ("USPTO") duly and legally issued United States Patent No. 9,455,961 ("the '961 patent") entitled "System, Method and Apparatus for Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke. A true and correct copy of the '961 patent is attached as Exhibit 1.

34. The '961 patent is presumed valid under 35 U.S.C. § 282.

35. paSafeShare owns all rights, title, and interest in the '961 patent.

United States Patent No. 9,615,116

36. On April 4, 2017, the USPTO duly and legally issued United States Patent No. 9,615,116 ("the '116 patent) entitled "System, Method and Apparatus for Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke. A true and correct copy of the '116 patent is attached as Exhibit 2.

37. The '116 patent is presumed valid under 35 U.S.C. § 282.

38. paSafeShare owns all rights, title and interest in the '116 patent.

U.S. Patent No. 10,095,848

39. On October 9, 2018, the USPTO duly and legally issued United States Patent No. 10,095,848 ("the '848 patent) entitled "System, Method and Apparatus for

Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke. A true and correct copy of the '848 patent is attached as Exhibit 3.

40. The '848 patent is presumed valid under 35 U.S.C. § 282.

41. paSafeShare owns all rights, title and interest in the '848 patent.

CLAIMS FOR RELIEF

Count I – Infringement of United States Patent No. 9,455,961

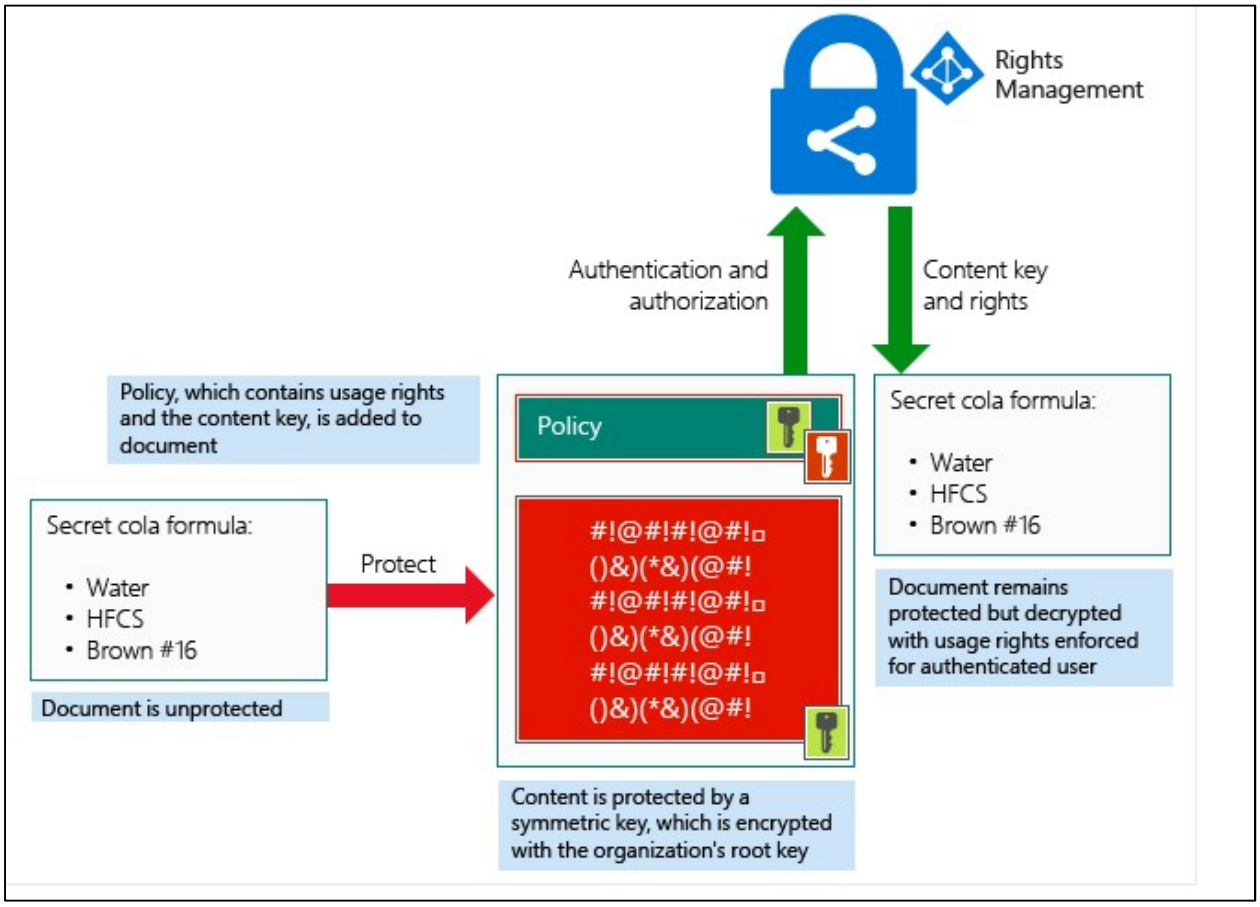
42. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

43. Microsoft makes, uses, sells, offers for sale, imports, and/or provides access to products and/or services for securely distributing content.

44. On information and belief, Microsoft makes, uses, sells, offers to sell, imports and/or provides access to Azure Information Protection, Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Active Directory, Azure Key Vault, Microsoft Office 365, and Microsoft Azure RMS-enlightened client programs and services (collectively, the "Microsoft Azure RMS Platform")[9].

[9] RMS clients include, but are not limited to, Windows 10(x86, x64), Windows 8.1 (x86, x64), Windows 8 (x86, x64), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include, but are not limited to, Office 365 ProPlus, Office 365 Enterprise E5, Office 365 Enterprise E4, Office 365 Enterprise E3, Office 365 Government G4, Office 365 Government G3, Office 365 Education A5, Office 365 Education A4, Office 365 Education A3, Office 365 Education A1, Office 365 Office Professional 2019, Office Professional 2016, Office Professional 2013, and Office Professional 2010. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications#footnote-1.

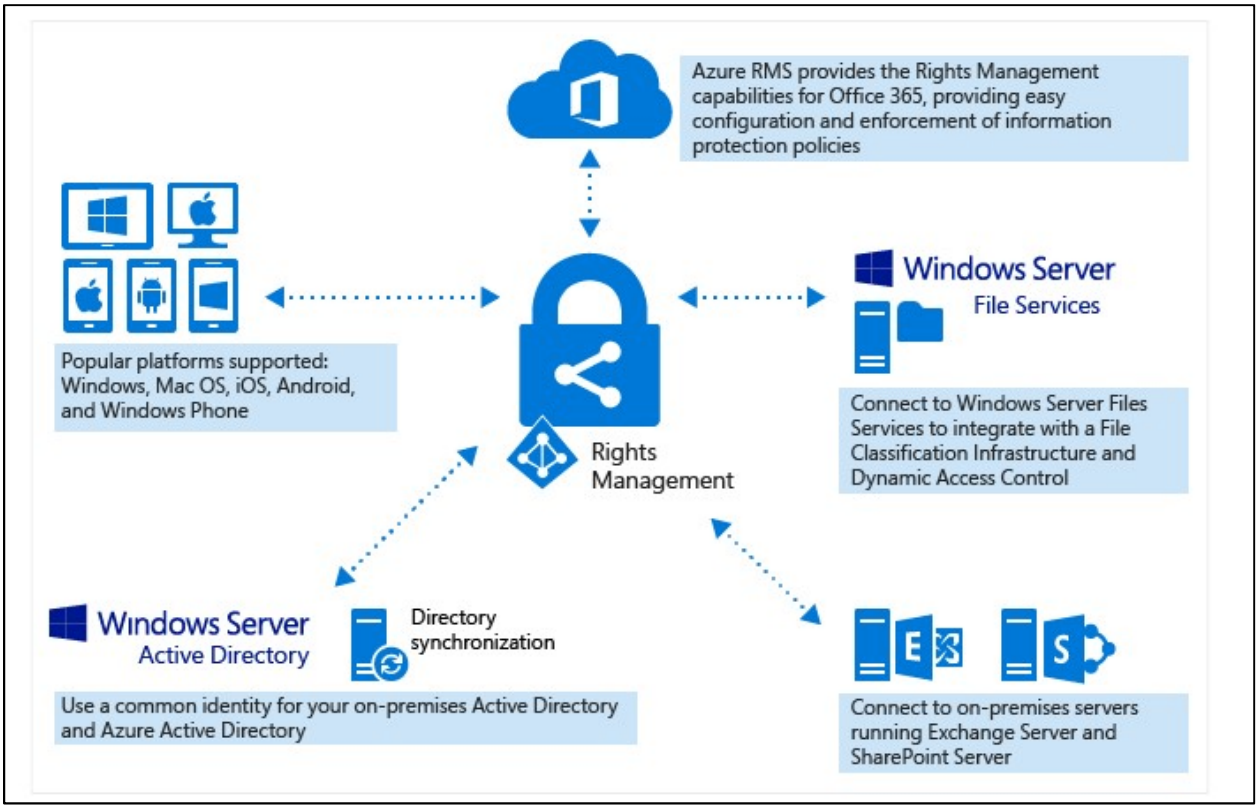
45. On information and belief, the Microsoft Azure RMS Platform practices a method for securely distributing content. Specifically, on information and belief, the Microsoft Azure RMS Platform uses Microsoft Azure RMS technology to protect documents and emails using labels and policies defined by an administrator.[10]



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

[10] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.

46. On information and belief, Microsoft Azure RMS is a cloud-based service running on Microsoft Azure instances.

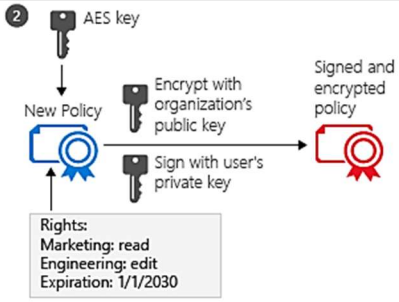


What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

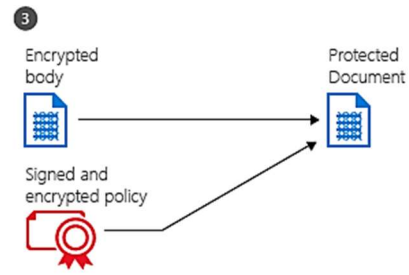
47. On information and belief, the Microsoft Azure RMS Platform generates, at a server (e.g., a Microsoft-designed physical and/or virtual Hardened Security Appliance in the Azure cloud) in communication with a network (e.g., the Internet), a protected document package (PDP) (e.g., protected document) including encrypted content or a link to encrypted content (e.g., encrypted body and/or encrypted usage policy), and a Publisher Key (PK) (e.g., AES key) for decrypting said encrypted content

for presentation of said content by an authorized user via a Limited Capability Viewer (LCV) (e.g., Microsoft Office 365 application, such as Word).

What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.



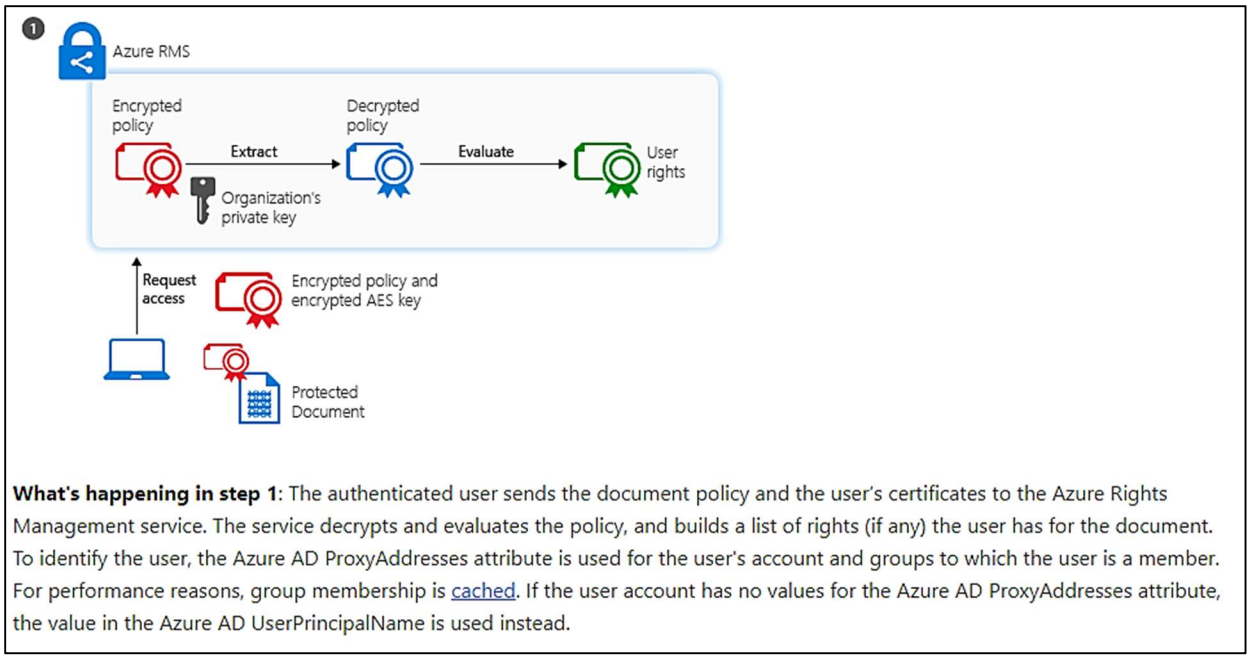
What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").



What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

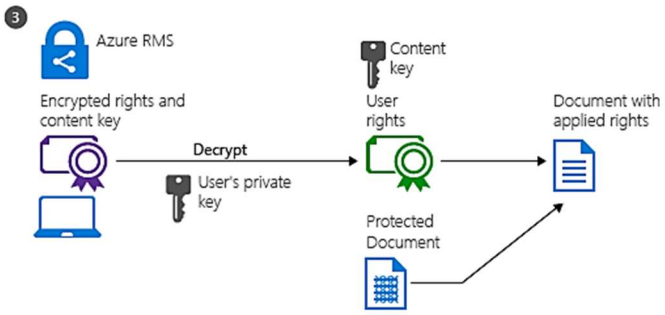
48. On information and belief, the Microsoft Azure RMS Platform generates software instructions that, when executed by a processor at a user device (e.g., personal computer) of a proposed authorized user, cause the user device to generate a Content Consumer License Request (CCLR) identifying said PK (e.g., AES key).



What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

49. On information and belief, the authorized user comprises a user having a Content Consumer License (CCL) (e.g., Azure RMS use license) compatible with the PK (e.g., AES key) to enable decryption of the encrypted content (e.g., encrypted body and/or encrypted usage policy) by the PK included within the PDP (e.g., protected document).



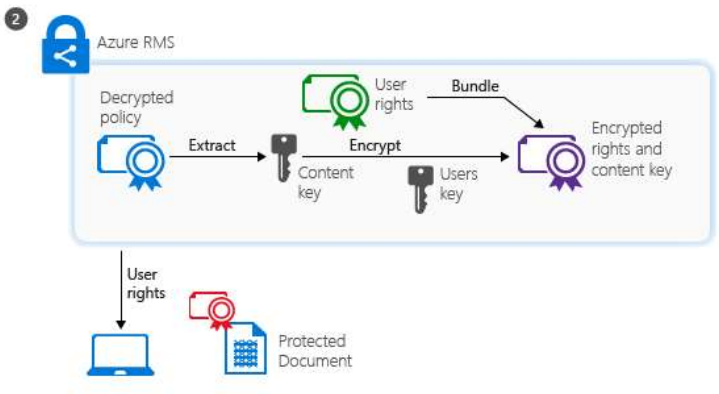
What's happening in step 3: Finally, the RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document's body as it is needed and render it on the screen.

The client also decrypts the rights list and passes them to the application, which enforces those rights in the application's user interface.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

50. On information and belief, the Microsoft Azure RMS Platform propagates, via the network (e.g., the Internet), the PDP (e.g., protected document) toward at least one user.

51. On information and belief, in response to receiving from a proposed authorized user a CCLR identifying the PK (e.g., AES key), the Microsoft Azure RMS Platform propagates a CCL (e.g., Azure RMS use license) compatible with the PK toward the proposed authorized user.



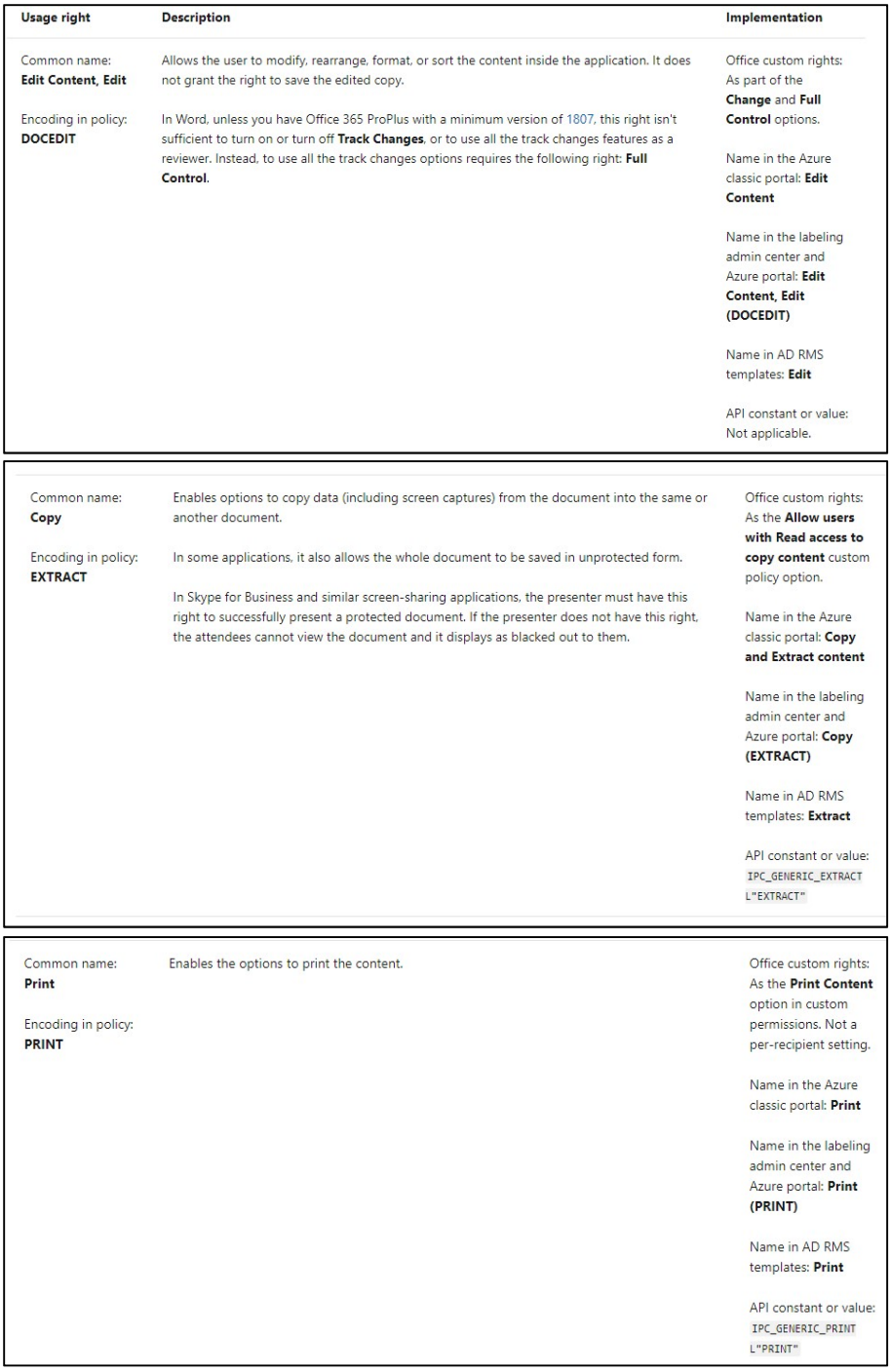
What's happening in step 2: The service then extracts the AES content key from the decrypted policy. This key is then encrypted with the user's public RSA key that was obtained with the request.

The re-encrypted content key is then embedded into an encrypted use license with the list of user rights, which is then returned to the RMS client.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

52. On information and belief, the proposed authorized user is an unauthorized user where received PDP license requirements are not satisfied.

53. On information and belief, the LCV (e.g., Microsoft Office 365 application) is configured to restrict editing, printing and copying of the content.



Usage right	Description	Implementation
Common name: **Edit Content, Edit** Encoding in policy: **DOCEDIT**	Allows the user to modify, rearrange, format, or sort the content inside the application. It does not grant the right to save the edited copy. In Word, unless you have Office 365 ProPlus with a minimum version of 1807, this right isn't sufficient to turn on or turn off **Track Changes**, or to use all the track changes features as a reviewer. Instead, to use all the track changes options requires the following right: **Full Control**.	Office custom rights: As part of the **Change** and **Full Control** options. Name in the Azure classic portal: **Edit Content** Name in the labeling admin center and Azure portal: **Edit Content, Edit (DOCEDIT)** Name in AD RMS templates: **Edit** API constant or value: Not applicable.
Common name: **Copy** Encoding in policy: **EXTRACT**	Enables options to copy data (including screen captures) from the document into the same or another document. In some applications, it also allows the whole document to be saved in unprotected form. In Skype for Business and similar screen-sharing applications, the presenter must have this right to successfully present a protected document. If the presenter does not have this right, the attendees cannot view the document and it displays as blacked out to them.	Office custom rights: As the **Allow users with Read access to copy content** custom policy option. Name in the Azure classic portal: **Copy and Extract content** Name in the labeling admin center and Azure portal: **Copy (EXTRACT)** Name in AD RMS templates: **Extract** API constant or value: `IPC_GENERIC_EXTRACT` `L"EXTRACT"`
Common name: **Print** Encoding in policy: **PRINT**	Enables the options to print the content.	Office custom rights: As the **Print Content** option in custom permissions. Not a per-recipient setting. Name in the Azure classic portal: **Print** Name in the labeling admin center and Azure portal: **Print (PRINT)** Name in AD RMS templates: **Print** API constant or value: `IPC_GENERIC_PRINT` `L"PRINT"`

Configuring Usage Rights For Azure Information Protection, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited April 2020).

54. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platform in regular business operations.

55. On information and belief, the Microsoft Azure RMS Platform is available to businesses and individuals throughout the United States.

56. On information and belief, the Microsoft Azure RMS Platform is provided to businesses and individuals located in the Western District of Texas.

57. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '961 patent by making, using, selling, offering for sale, importing and/or providing access to products and/or services for securely distributing content, including but not limited to the Microsoft Azure RMS Platform.

58. By making, using, testing, offering for sale, and/or selling products for securely distributing content, including but not limited to the Microsoft Azure RMS Platform, Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '961 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a)

59. On information and belief, Microsoft also indirectly infringes the '961 patent by actively inducing infringement under 35 USC § 271(b).

60. On information and belief, Microsoft has been on notice of the '961 patent at least as early as the date of service of this Complaint.

61. On information and belief, Microsoft intends to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platform

and has knowledge that the inducing acts cause infringement or is willfully blind to the possibility that its inducing acts cause infringement.

62. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '961 patent. Microsoft performs the acts that constitute induced infringement, and induce actual infringement, with knowledge of the '961 patent and with the knowledge that the induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platform, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platform to use the products in a manner that directly infringe one or more claims of the '961 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platform in a manner that directly infringes one or more claims of the '961 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '961 patent. On information and belief, Microsoft engages in such inducement to promote the sales of the Microsoft Azure RMS Platform, e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '961 patent. Accordingly, Microsoft has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '961 patent, knowing that such use constitutes infringement of the '961 patent.

63. Microsoft's direct and/or indirect infringement has damaged paSafeShare and paSafeShare is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count II – Infringement of United States Patent No. 9,615,116

64. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

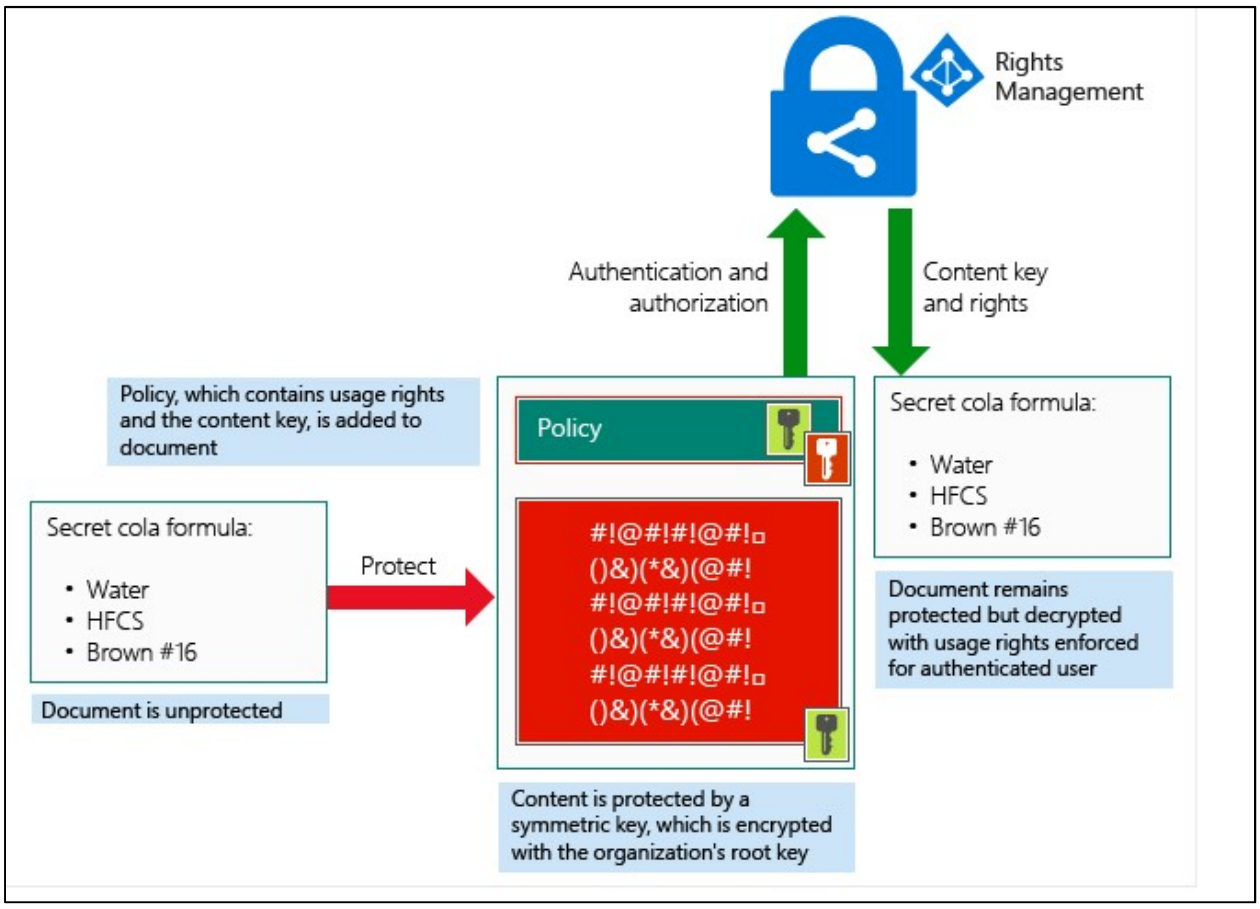
65. Microsoft makes, uses, sells, offers for sale, imports, and/or provides access to products and/or services for securely distributing content.

66. On information and belief, Microsoft makes, uses, sells, offers to sell, imports and/or provides access to Azure Information Protection, Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Active Directory, Azure Key Vault, Microsoft Office 365, and Microsoft Azure RMS-enlightened client programs and services (collectively, the "Microsoft Azure RMS Platform")[11].

67. On information and belief, the Microsoft Azure RMS Platform practices a method for securely distributing content. Specifically, on information and belief, the

[11] RMS clients include, but are not limited to, Windows 10(x86, x64), Windows 8.1 (x86, x64), Windows 8 (x86, x64), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include, but are not limited to, Office 365 ProPlus, Office 365 Enterprise E5, Office 365 Enterprise E4, Office 365 Enterprise E3, Office 365 Government G4, Office 365 Government G3, Office 365 Education A5, Office 365 Education A4, Office 365 Education A3, Office 365 Education A1, Office 365 Office Professional 2019, Office Professional 2016, Office Professional 2013, and Office Professional 2010. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications#footnote-1.

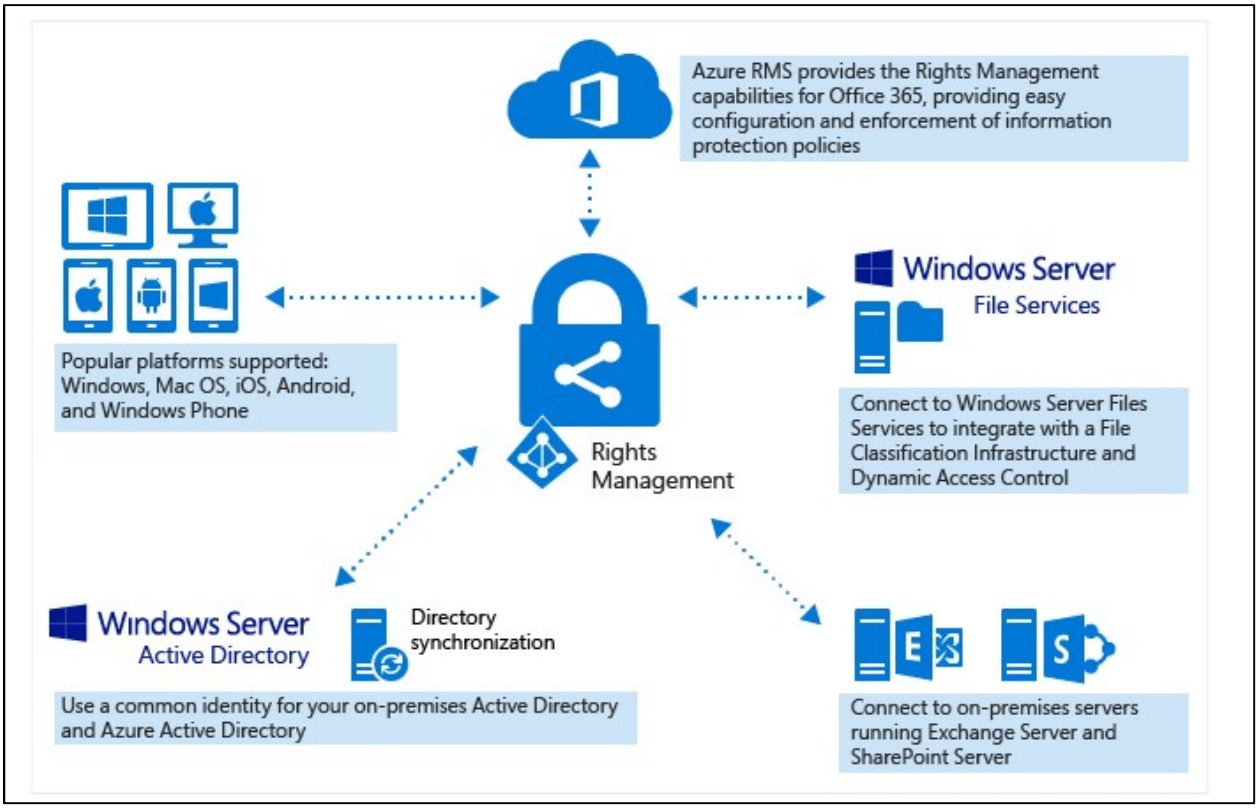
Microsoft Azure RMS Platform uses Microsoft Azure RMS technology to protect documents and emails using labels and policies defined by an administrator.[12]



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

68. On information and belief, Microsoft Azure RMS is a cloud-based service running on Microsoft Azure instances.

[12] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.

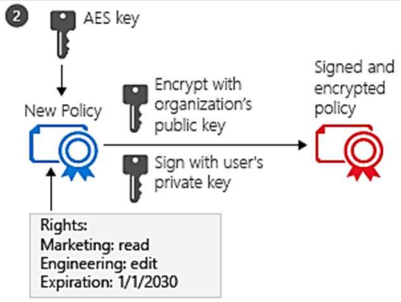


What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

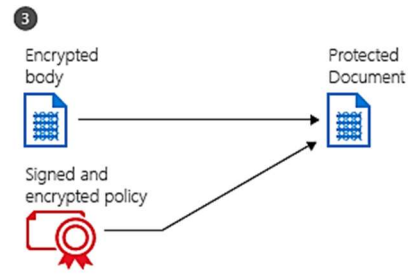
69. On information and belief, the Microsoft Azure RMS Platform generates, at a server (e.g., a Microsoft-designed physical and/or virtual Hardened Security Appliance in the Azure cloud), a protected document package (PDP) (e.g., protected document), the PDP including encrypted content (e.g., encrypted body and/or

encrypted usage policy), and a Publisher Key (PK) (e.g., AES key) associated with the encrypted content.

What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.



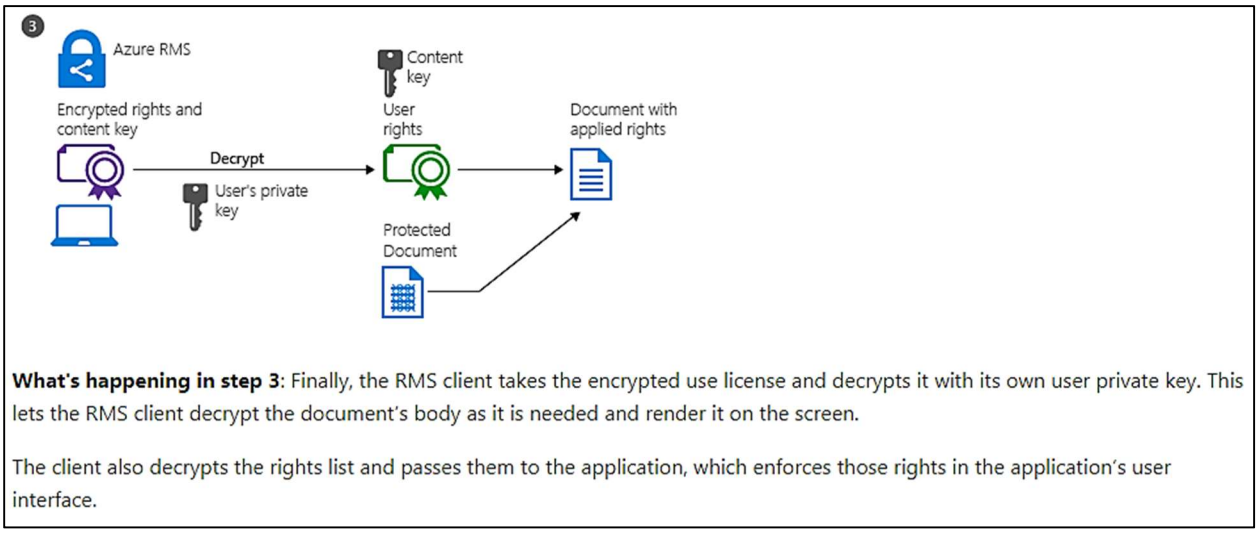
What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").



What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

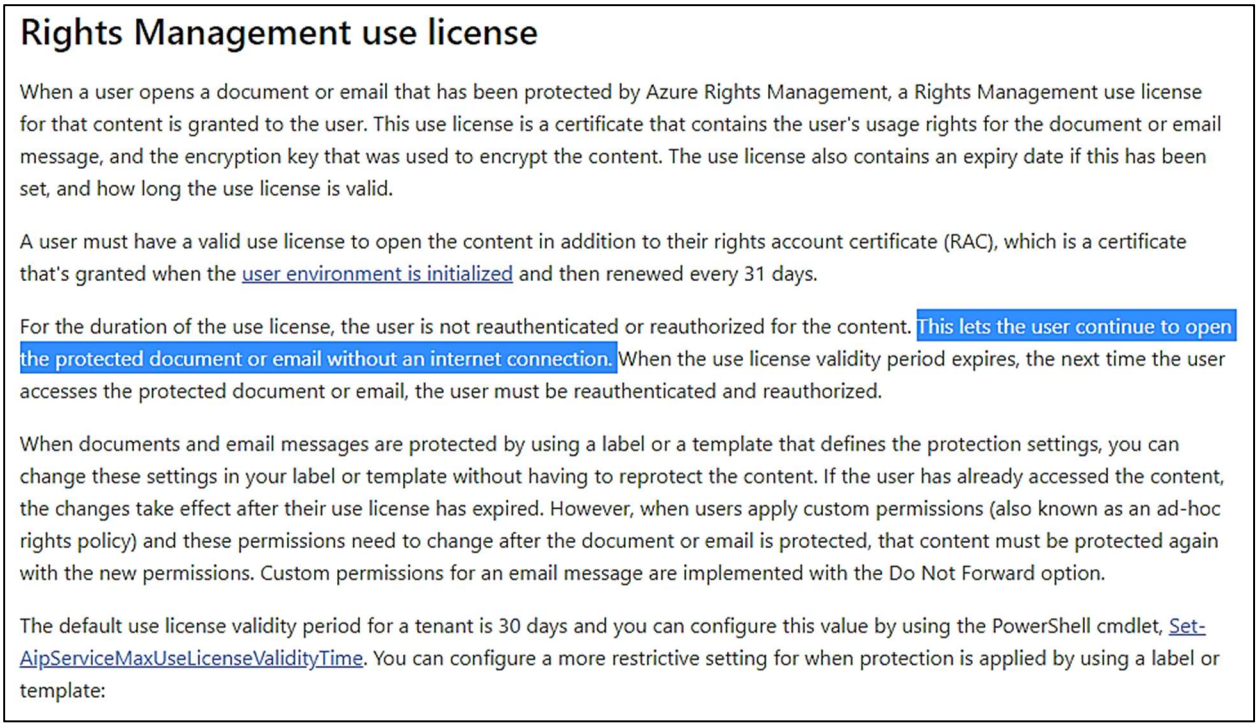
How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

70. On information and belief, the PK (e.g., AES key) enables decryption of the encrypted content for presentation via a Limited Capability Viewer (LCV) (e.g., a Microsoft Office 365 application, such as Word) of an authorized user device.



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

71. On information and belief, the authorized user device comprises a user device (e.g., personal computer) having a Content Consumer License (CCL) (e.g., Azure RMS use license) compatible with the PK (e.g., AES key) to enable presentation via the LCV (e.g., Microsoft Office 365 application) of locally stored encrypted content from the PDP (e.g., protected document).



Rights Management use license

When a user opens a document or email that has been protected by Azure Rights Management, a Rights Management use license for that content is granted to the user. This use license is a certificate that contains the user's usage rights for the document or email message, and the encryption key that was used to encrypt the content. The use license also contains an expiry date if this has been set, and how long the use license is valid.

A user must have a valid use license to open the content in addition to their rights account certificate (RAC), which is a certificate that's granted when the user environment is initialized and then renewed every 31 days.

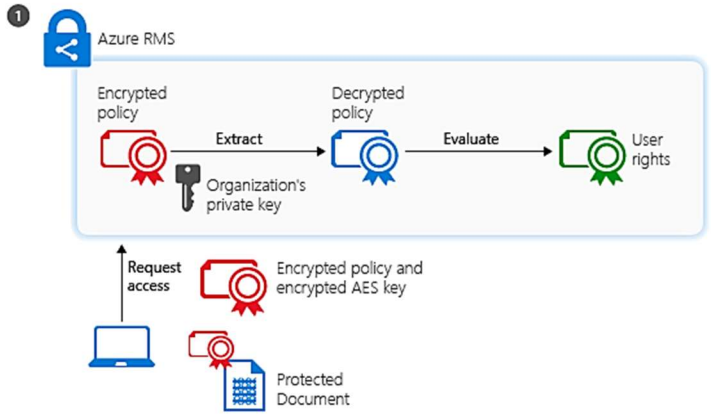
For the duration of the use license, the user is not reauthenticated or reauthorized for the content. This lets the user continue to open the protected document or email without an internet connection. When the use license validity period expires, the next time the user accesses the protected document or email, the user must be reauthenticated and reauthorized.

When documents and email messages are protected by using a label or a template that defines the protection settings, you can change these settings in your label or template without having to reprotect the content. If the user has already accessed the content, the changes take effect after their use license has expired. However, when users apply custom permissions (also known as an ad-hoc rights policy) and these permissions need to change after the document or email is protected, that content must be protected again with the new permissions. Custom permissions for an email message are implemented with the Do Not Forward option.

The default use license validity period for a tenant is 30 days and you can configure this value by using the PowerShell cmdlet, Set-AipServiceMaxUseLicenseValidityTime. You can configure a more restrictive setting for when protection is applied by using a label or template:

Configuring Usage Rights for Azure Information Protection, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited April 2020).

72. On information and belief, the PDP (e.g., protected document) includes software instructions that, when executed by a processor at a proposed authorized user device (e.g., personal computer), cause the proposed authorized user device to generate a Content Consumer License Request (CCLR) identifying the PK (e.g., AES key).

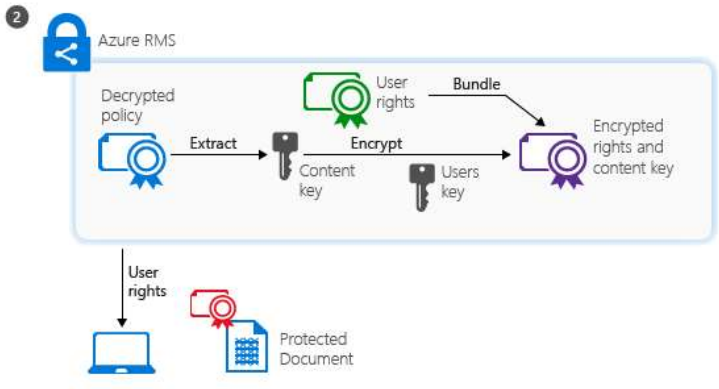


What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

73. On information and belief, the Microsoft Azure RMS Platform propagates the PDP (e.g., protected document) toward at least one authorized or proposed authorized user device (e.g., personal computer).

74. On information and belief, the Microsoft Azure RMS Platform receives from a proposed authorized user device (e.g., personal computer) having the PDP (e.g., protected document) a CCLR identifying the PK (e.g., AES key).



What's happening in step 2: The service then extracts the AES content key from the decrypted policy. This key is then encrypted with the user's public RSA key that was obtained with the request.

The re-encrypted content key is then embedded into an encrypted use license with the list of user rights, which is then returned to the RMS client.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

75. On information and belief, the Microsoft Azure RMS Platform propagates a CCL (e.g., Azure RMS use license) compatible with the PK (e.g., AES key) toward the proposed authorized user device (e.g., personal computer) if the CCLR is valid.

76. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platform in regular business operations.

77. On information and belief, the Microsoft Azure RMS Platform is available to businesses and individuals throughout the United States.

78. On information and belief, the Microsoft Azure RMS Platform is provided to businesses and individuals located in the Western District of Texas.

79. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '116 patent by making, using, selling, offering for sale, importing and/or providing access to products and/or services for securely distributing content, including but not limited to the Microsoft Azure RMS Platform.

80. By making, using, testing, offering for sale, and/or selling products for securely distributing content, including but not limited to the Microsoft Azure RMS Platform, Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '116 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a)

81. On information and belief, Microsoft also indirectly infringes the '116 patent by actively inducing infringement under 35 USC § 271(b).

82. On information and belief, Microsoft has been on notice of the '116 patent at least as early as the date of service of this Complaint.

83. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platform and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement.

84. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '116 patent. Microsoft performs the acts that constitute induced infringement, and induces actual infringement, with knowledge of the '116 patent and with the knowledge that the

induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platform, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platform to use the products in a manner that directly infringe one or more claims of the '116 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platform in a manner that directly infringes one or more claims of the '116 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '116 patent. On information and belief, Microsoft engages in such inducement to promote the sales of the Microsoft Azure RMS Platform, e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '116 patent. Accordingly, Microsoft has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '116 patent, knowing that such use constitutes infringement of the '116 patent.

85. Microsoft's direct and/or indirect infringement has damaged paSafeShare, and Microsoft is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count III – Infringement of United States Patent No. 10,095,848

86. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

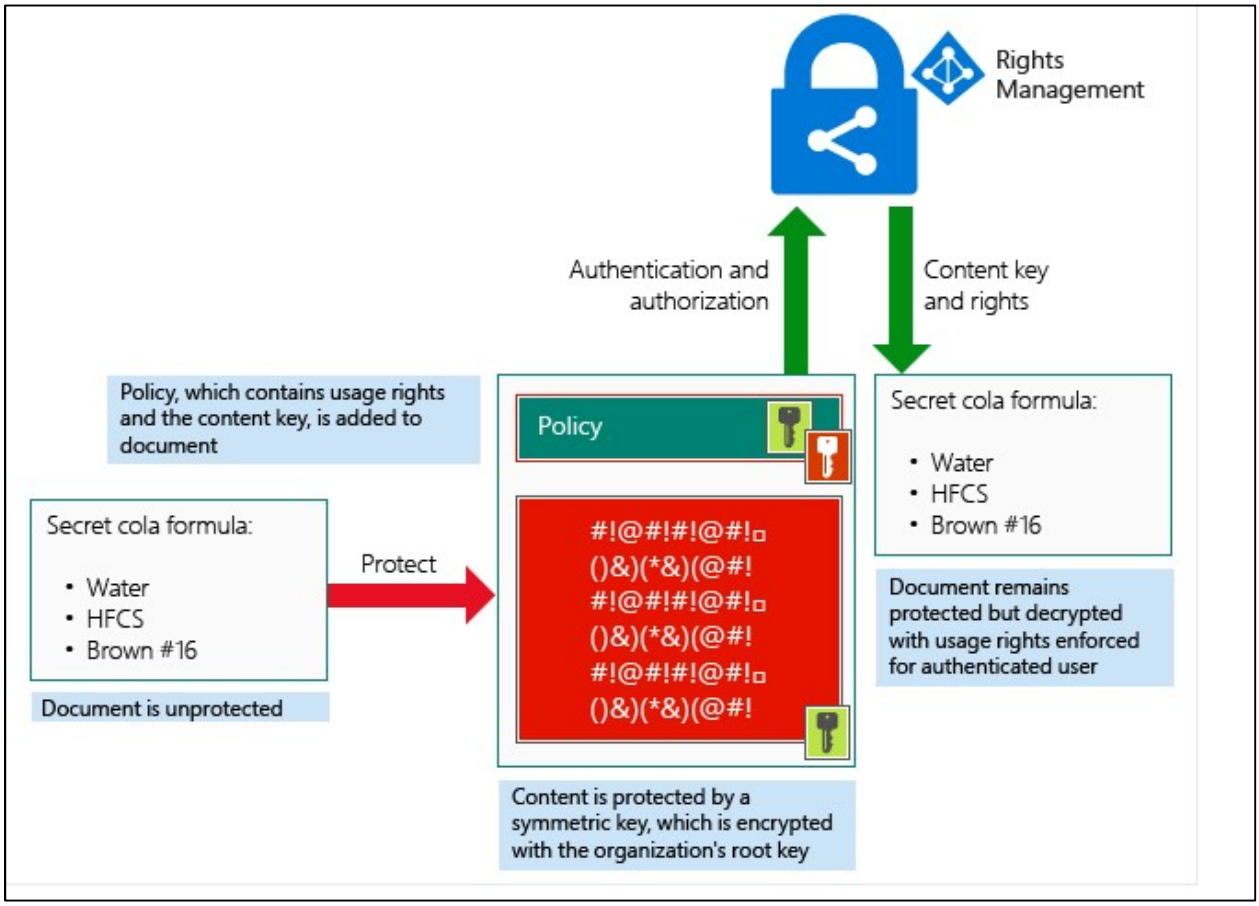
87. Microsoft makes, uses, sells, offers for sale, imports, and/or provides access to products and/or services for securely distributing content.

88. On information and belief, Microsoft makes, uses, sells, offers to sell, imports and/or provides access to Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Active Directory, Azure Key Vault, Microsoft Office 365, and Microsoft Azure RMS-enlightened client programs and services (collectively, the "Microsoft Azure RMS Platform").[13]

89. On information and belief, the Microsoft Azure RMS Platform practices a method for securely distributing content. Specifically, on information and belief, the Microsoft Azure RMS Platform uses Microsoft Azure RMS technology to protect documents and emails using labels and policies defined by an administrator.[14]

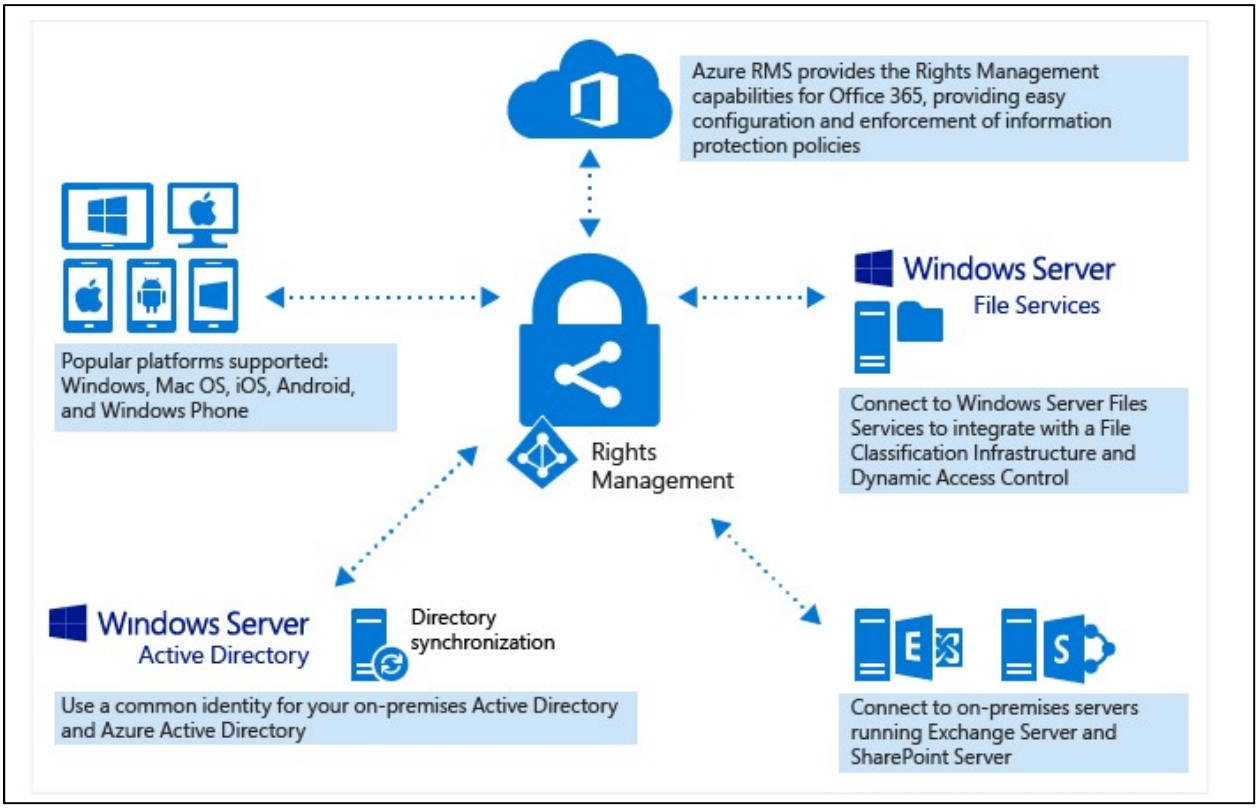
[13] RMS clients include, but are not limited to, Windows 10(x86, x64), Windows 8.1 (x86, x64), Windows 8 (x86, x64), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include, but are not limited to, Office 365 ProPlus, Office 365 Enterprise E5, Office 365 Enterprise E4, Office 365 Enterprise E3, Office 365 Government G4, Office 365 Government G3, Office 365 Education A5, Office 365 Education A4, Office 365 Education A3, Office 365 Education A1, Office 365 Office Professional 2019, Office Professional 2016, Office Professional 2013, and Office Professional 2010. *See* https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications#footnote-1.

[14] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

90. On information and belief, Microsoft Azure RMS is a cloud-based service running on Microsoft Azure instances.

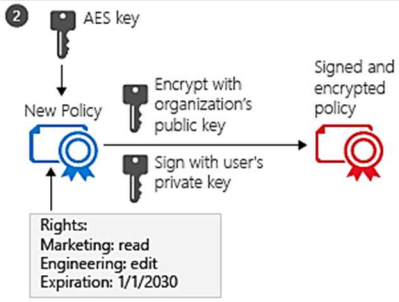


What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

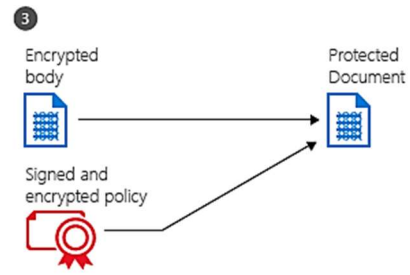
91. On information and belief, the Microsoft Azure RMS Platform generates, at a server (e.g., a Microsoft-designed physical and/or virtual Hardened Security Appliance in the Azure cloud) in communication with a network (e.g., the Internet), a protected document package (PDP) (e.g., protected document) including encrypted content or a link to encrypted content (e.g., encrypted body and/or encrypted usage policy), and a Publisher Key (PK) (e.g., AES key) for decrypting the encrypted content

for presentation of said content by an authorized user via a Limited Capability Viewer (LCV) (e.g., a Microsoft Office 365 application, such as Microsoft Word).

What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.



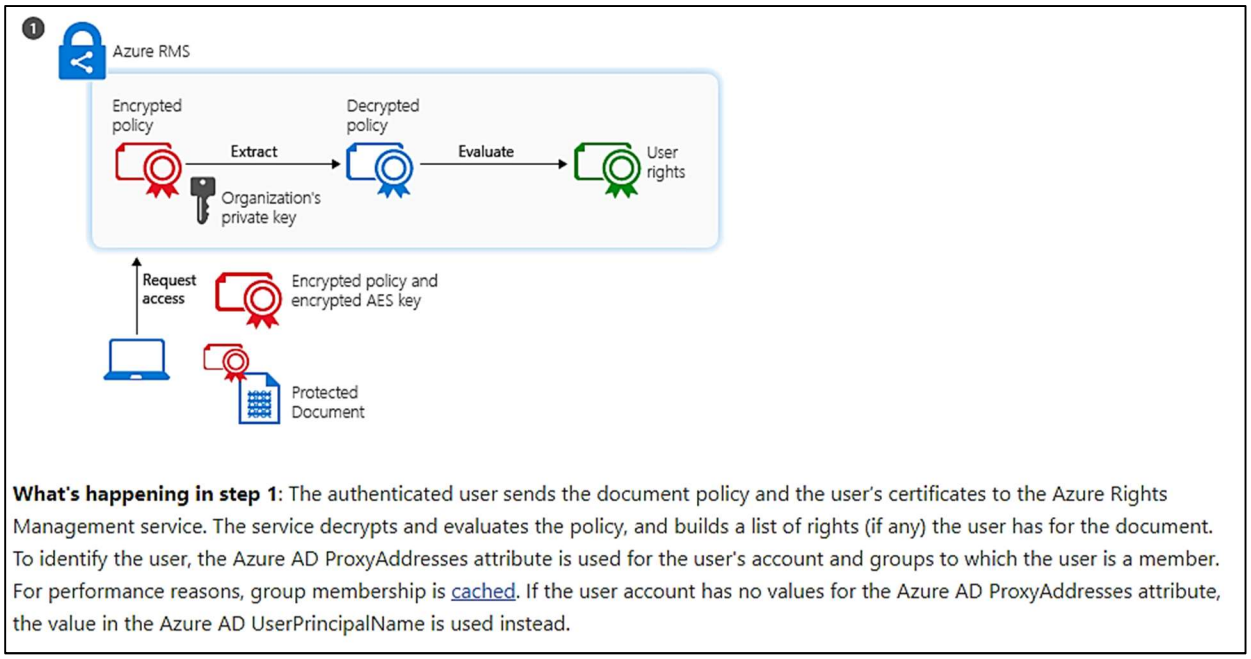
What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").



What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

92. On information and belief, the Microsoft Azure RMS Platform generates software instructions that, when executed by a processor at a user device (e.g., personal computer) of a proposed authorized user, cause the user device to generate a Content Consumer License Request (CCLR) identifying the PK (e.g., AES key).

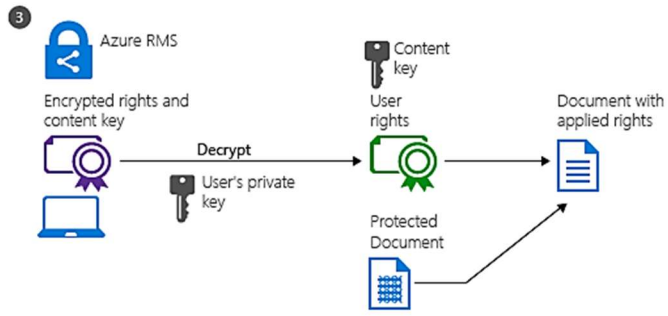


What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

93. On information and belief, the authorized user comprises a user having a Content Consumer License (CCL) (e.g., Azure RMS use license) compatible with the PK (e.g., AES key) to enable decryption of the encrypted content (e.g., encrypted body and/or encrypted usage policy) by the PK included within the PDP (e.g., protected document) and use of decrypted content in accordance with advanced permissions

(e.g., Azure usage rights) indicated via the CCL. *See* https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights.



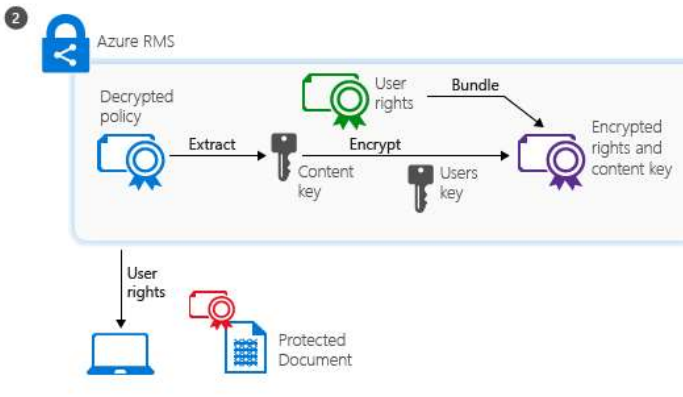
What's happening in step 3: Finally, the RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document's body as it is needed and render it on the screen.

The client also decrypts the rights list and passes them to the application, which enforces those rights in the application's user interface.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

94. On information and belief, the Microsoft Azure RMS Platform propagates, via the network (e.g., the Internet), the PDP (e.g., protected document) toward at least one user.

95. On information and belief, in response to receiving from a proposed authorized user a CCLR identifying said PK (e.g., AES key), the Microsoft Azure RMS Platform propagates a CCL (e.g., Azure RMS use license) compatible with the PK toward the proposed authorized user.



What's happening in step 2: The service then extracts the AES content key from the decrypted policy. This key is then encrypted with the user's public RSA key that was obtained with the request.

The re-encrypted content key is then embedded into an encrypted use license with the list of user rights, which is then returned to the RMS client.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

96. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platform in regular business operations.

97. On information and belief, the Microsoft Azure RMS Platform is available to businesses and individuals throughout the United States.

98. On information and belief, the Microsoft Azure RMS Platform is provided to businesses and individuals located in the Western District of Texas.

99. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '848 patent by making, using, selling, offering for sale, importing and/or providing access to products and/or services for securely distributing content, including but not limited to the Microsoft Azure RMS Platform.

100. By making, using, testing, offering for sale, and/or selling products for securely distributing content, including but not limited to the Microsoft Azure RMS Platform, Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '848 Patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a)

101. On information and belief, Microsoft also indirectly infringes the '848 patent by actively inducing infringement under 35 USC § 271(b).

102. On information and belief, Microsoft has been on notice of the '848 patent at least as early as the date of service of this Complaint.

103. On information and belief, Microsoft intends to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platform and has knowledge that its inducing acts cause infringement or is willfully blind to the possibility that its inducing acts cause infringement.

104. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '848 patent. Microsoft performs the acts that constitute induce infringement, and induce actual infringement, with knowledge of the '848 patent and with the knowledge that its

induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platform, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platform to use the products in a manner that directly infringe one or more claims of the '848 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platform in a manner that directly infringes one or more claims of the '848 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '848 patent. On information and belief, Microsoft engages in such inducement to promote the sales of the Microsoft Azure RMS Platform, e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '848 patent. Accordingly, Microsoft has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '848 patent, knowing that such use constitutes infringement of the '848 patent.

105. Microsoft's direct and/or indirect infringement has damaged paSafeShare and paSafeShare is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

JURY DEMANDED

106. Pursuant to Federal Rule of Civil Procedure 38(b), paSafeShare requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

paSafeShare respectfully requests this Court to enter judgment in paSafeShare's favor and against Microsoft as follows:

a. finding that Microsoft has infringed one or more claims of the '961 patent;

b. finding that Microsoft has infringed one or more claims of the '116 patent;

c. finding that Microsoft has infringed one or more claims of the '848 patent;

d. awarding paSafeShare damages under 35 U.S.C. § 284, or otherwise permitted by law, including supplemental damages for any continued post-verdict infringement;

e. awarding paSafeShare pre-judgment and post-judgment interest on the damages award and costs;

f. awarding cost of this action (including all disbursements) and attorney fees pursuant to 35 U.S.C. § 285, or as otherwise permitted by the law; and

g. awarding such other costs and further relief that the Court determines to be just and equitable.

Dated: May 14, 2020

Respectfully submitted,

/s/Raymond W. Mort, III

Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com

THE MORT LAW FIRM, PLLC
100 Congress Avenue, Suite 2000
Austin, Texas 78701
Tel/Fax: 512-865-7950

Attorneys for paSafeShare LLC

OF COUNSEL:

Ronald M. Daignault*
Chandran B. Iyer*
Stephanie Mandir *
GOLDBERG SEGALLA
rdaignault@goldbergsegalla.com
cbiyer@goldbergsegalla.com
smandir@goldbergsegalla.com
711 Third Avenue, Suite 1900
New York, New York 10017
Telephone: (646) 292-8700

* *pro hac vice* motion to be filed