Information Rights Management

2nd User Group Meeting

March 25th - 26th, 2014

eberhard@keyon.ch, CEO

V1.3, 2014 March

AD-RMS expertise

- Partnership with Microsoft and SecureIslands
- Support of large financial institutes in the global technical and organizational integration of MS AD-RMS and SI IQP

Corporate PKI

Software Engineering

IT- and Mobile Security

Digital Signature Services

Identity & Access Management

Security- and Business Consulting

Data Leakage Prevention & Information Rights Management

keyon

www.keyon.ch / info@keyon.ch

AD-RMS

our understanding…

AD-RMS major features

- Comprehensive technology to protect confidential data across major platforms (Windows, iOS, Android, Mac)
- Security is intrinsically tied to data, no dependency to other security measures
- Flexible management of users and roles (joiners / movers / leavers / deputies / auditors / legal investigators)
- Online- and offline capabilities

AD-RMS is the answer to

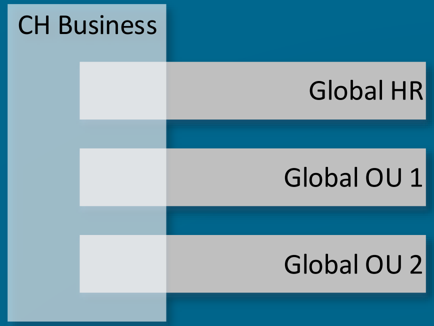
- How to efficiently prevent loss of confidential data?
- How to classify and protect data on premise and in the cloud?
- How to separate business data from IT support personnel?
- How to separate organizational units or jurisdictions from each other?

MS AD-RMS / SI IQP

major use-cases and features

Major features implemented

- Data is classified and protected (if confidential classified)
- RMS protection profiles define “leakage” boundaries. They act in addition to access control on file shares / SharePoint



- Data is automatically protected
  - on download from specific web applications
  - in Outlook if certain text-patterns are found in the email / attachments (pop-up windows for user justification)
  - if copied to specific folders

Major features implemented

- Data is automatically un-protected
  - for email journaling (super user rights)
  - to interoperate with third party secure email solutions (individual user rights)
  - on upload to trusted applications (mostly used for legal investigation)
  - if copied to specific folders (mostly used for legal investigation)
- User is notified whenever he tries to transmit data containing certain text patterns
- Automatic content marking for MS Office documents containing certain text patterns (visual appearance of the term “Confidential”)

Major features implemented

- Regional licensing servers fenced with firewalls. No use license can be retrieved to open an RMS protected document outside that region.
- Self-services provided to:
  - managers for user and role management
  - application owners to easily enable IRM protection of their applications
    - `http://servicename/ApplicationPath/IRM_Apply_Confidential_HrProfile/Path2`
    - `\\sharename\AnyPath\IRM_Apply_Confidential_OU1Profile\AnyOtherPath`

MS AD-RMS / SI IQP

experiences, challenges and requests

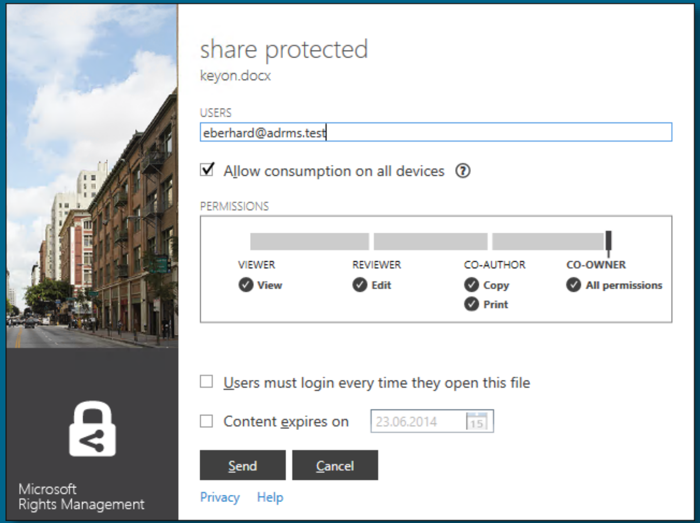
To P or not to P – Facts about .pfiles

- Microsoft introduced two levels of RMS protection

Level	Description	File-types
Native	• Provides a strong level of protection that includes both encryption and enforcement of rights. • The content is shown using RMS enabled applications (such as MS Office, Foxit Reader of MS IP Viewer)	MS Office, PDF, text, images • .docx -> .docx • .pdf -> .pdf • .txt -> .ptxt
Generic	• Provides a level of protection that includes file encapsulation in an encrypted container (.pfile) and authentication to verify if a user is authorized to open the file • The content is shown using standard, non RMS enabled applications (lack of enforcement of rights)	Other files than above • .csv ->.csv.pfile • .vsdx -> .vsdx.pfile

To P or not to P – Issue

- .pfile approach is not enterprise ready
  - Allow consumption on all devices is a great idea and easily enables non MS platforms to open RMS protected documents using RMS Sharing Applications.
  - The problem is that no templates can be applied and even native RMS documents (e.g. MS Office or PDF) end up with the .pfile extensions. Such documents are treated as unprotected documents inside the application (e.g. Word), no RMS rights are enforced at all. Furthermore the file is opened in read-only mode and, once edited, has to be stored into a separate file.



share protected

keyon.docx

USERS

eberhard@adrms.test

☑ Allow consumption on all devices

PERMISSIONS

VIEWER	REVIEWER	CO-AUTHOR	CO-OWNER
✓ View	✓ Edit	✓ Copy ✓ Print	✓ All permissions

☐ Users must login every time they open this file

☐ Content expires on 23.06.2014

To P or not to P – Request

- Extend the native approach (.p<ext>)
  - It would be required to extend the native approach to other major file-types.
  - Microsoft Office should honor any Office related .p<ext> file-types, especially .pcsv and .prtf. Such file-types should provide the same RMS related user experience in MS Office as native Office file-types.
  - Microsoft Outlook should apply top-down inheritance using .p<ext> file-types whenever possible.
  - Consider automated migration scenarios when new .p<ext> file-types are introduced.

Protection of Emails – Facts

- If an email is RMS protected in Outlook the RMS protection is top-down inherited to attachments where applicable (i.e. MS Office file-types).
- Using SI IQP RMS inheritance can be extended to additional file-types (e.g. .pdf, .txt, etc.).

Protection of Emails – Issue, Request

- Relationship between RMS protection and classification
  - RMS protection should be consistently tied together with the corresponding classification. This is currently not the case. RMS protected attachments are not being classified along the top-down inheritance in Outlook.
  - Additionally a GUI would be required where a user can easily manage the RMS protection / classification of the email body and all attachments in Outlook before the email is being sent.

Protection of Emails

- Insufficient RMS information about the sender
  - RMS protected data can be sent to any recipient even the sender has no access to it.
  - Option 1:
    No issue because the recipient anyway needs to be entitled to open the RMS protected document.
  - Option 2:
    Issue because the recipient might be entitled to open the RMS protected document but would not have access to the data through file shares / SharePoint (access control).
  - Request:
    Provide a rule set in Outlook based on the senders RMS capabilities related to the RMS protected attachments.

Protection of Emails

- Insufficient RMS information about the recipients
  - Provide a rule set in Outlook based on the recipients RMS capabilities related to the RMS protected attachments. This measure will lower the number of support requests.

Further requests

- Enhance Exchange to unprotect any RMS protected data for journaling
- Enhance the search capabilities on RMS protected documents in Outlook, Windows Desktop Search, MS FAST
  - Local based, user centric search index protected with Windows Data Protection API
  - Centralized search index protected with a corresponding RMS template
- RMS enable Calendar, Contact and Tasks transmission in Outlook and provide an Outlook API to scan the content of such items

Further requests

- Provide policy based issuing of use licenses
  - User identifying attributes, especially the email address, may change (marriage, gender change) or may be re-used (joiners and leavers). The licensing server should issue use licenses accordingly
    - Issue a use license if just the email address of the user has changed
    - Do not issue a use license if the user has been applied in the AD after the document has been protected
- Provide policy based deletion of cached use licenses, provide a better protection of the RAC
  - Having access to the users desktop, RMS protected documents can be opened even the corresponding use license / RAC has expired.

Further requests

- Dedicated deputy role for ad-hoc protection
  - Today “simple delegation” gets a delegate full rights to all RMS protected data of the delegator (including template based protection). Since line-managers may be located somewhere outside a specific region they should not get access to regional RMS templates. Therefore an delegation model for ad-hoc protection would be required.

Q&A

Thank you for your attention

eberhard@keyon.ch, CEO