

# AD RMS (engl. Active Directory Rights Management Services) implementacija



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Module Overview*

- AD RMS Overview
- Deploying and Managing an AD RMS Infrastructure
- Configuring AD RMS Content Protection
- Configuring External Access to AD RMS



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Lesson 1: AD RMS Overview*

- What Is AD RMS?
- Usage Scenarios for AD RMS
- Overview of the AD RMS Components
- AD RMS Certificates and Licenses
- How AD RMS Works



**Algebra**

visoka škola za  
primijenjeno računarstvo

- Information protection technology *What Is AD RMS?*
- Designed to reduce information leakage
- Integrated with Windows operating systems, Microsoft Office, Exchange Server, and SharePoint Server
- Based on Symmetric and Public Key Cryptography
- Protects data at rest, in transit, and in use



**Algebra**

visoka škola za  
primijenjeno računarstvo

## *Usage Scenarios for AD RMS*

- Prevent the transmission of sensitive information
- Comply with privacy regulations
- Can be used with encryption to protect data in transit and at rest



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Overview of the AD RMS Components*

- AD RMS cluster
- AD RMS server
  - Licenses AD RMS-protected content
  - Certifies identity of trusted users and devices
- AD RMS client
  - Built into Windows Vista, Windows 7, and Windows 8
  - Interacts with AD RMS-enabled applications
- AD RMS-enabled applications
  - Allows publication and consumption of AD RMS-protected content
  - Includes Microsoft Office, Exchange Server, and SharePoint Server
  - Can be created using AD RMS SDKs.



## *AD RMS Certificates and Licenses*

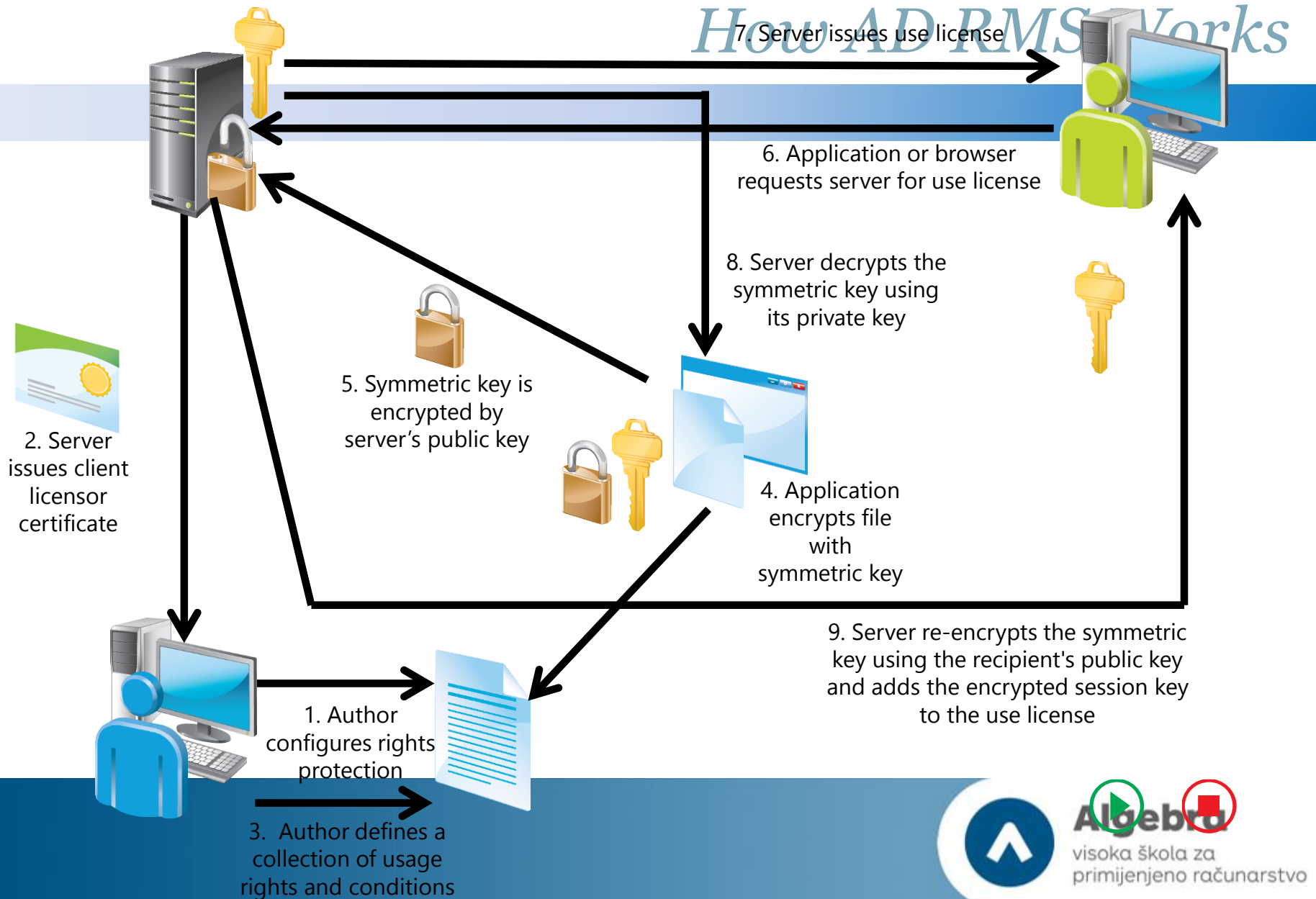
- AD RMS certificate and licenses include:
  - Server licensor certificate
  - AD RMS machine certificate
  - Rights Account Certificate
  - Client licensor certificate
  - Publishing license
  - End-user license



**Algebra**

visoka škola za  
primijenjeno računarstvo

# How AD RMS Works





# *Lesson 2: Deploying and Managing an AD RMS Infrastructure*

- AD RMS Deployment Scenarios
- Configuring the AD RMS Cluster
- AD RMS Client Requirements
- Implementing an AD RMS Backup and Recovery Strategy
- Decommissioning and Removing AD RMS



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *AD RMS Deployment Scenarios*

- Deployment scenarios for AD RMS are:

- AD RMS in a single forest
- AD RMS in multiple forests
- AD RMS used on an extranet
- AD RMS integrated with AD FS



**Algebra**

visoka škola za  
primijenjeno računarstvo

AD RMS configuration includes configuring of following:

## *Configuring the AD RMS Cluster*

- New or join existing cluster
- Configuration database location
- Service account
- Cryptographic mode
- Cluster key storage
- Cluster key password
- Cluster website
- Cluster address
- Server certificate
- Licensor certificate
- SCP registration



**Algebra**

visoka škola za  
primijenjeno računarstvo

## AD RMS Client Requirements

- Client included in Windows Vista and newer operating systems
- Client included in Windows Server 2008 and newer operating systems
- Client available for download for previous versions of Windows operating systems, and Mac OS X
- AD RMS-enabled applications include Office 2007, Office 2010, and Office 2013
- Exchange Server 2007, Exchange Server 2010, and Exchange Server 2013 support AD RMS
- AD RMS clients needs RMS CAL



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Implementing an AD RMS Backup and Recovery Strategy*

- Back up private key and certificates
- Ensure that the AD RMS database is backed up regularly
- Export templates to back them up
- Run the AD RMS server as a virtual machine, and perform full server backup



**Algebra**

visoka škola za  
primijenjeno računarstvo

## *Decommissioning and Removing AD RMS*

- Decommission an AD RMS cluster prior to removing it
  - Decommissioning provides a key that decrypts previously published AD RMS content
  - Leave server in decommissioned state until all AD RMS-protected content is migrated
- Export the server licenser certificate prior to uninstalling the AD RMS role



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Lesson 3: Configuring AD RMS Content Protection*

- What Are Rights Policy Templates?
- Providing Rights policy Templates for Offline Use
- What Are Exclusion Policies?
- AD RMS Super Users Group
- AD RMS Integration with Dynamic Access Control



**Algebra**

visoka škola za  
primijenjeno računarstvo

## *What Are Rights Policy Templates?*

- Allow authors to apply standard forms of protection across the organization
- Different applications allow different forms of rights
- Can configure rights related to viewing, editing, and printing documents
- Can configure content expiration rights
- Can configure content revocation



**Algebra**

visoka škola za  
primijenjeno računarstvo



# *Providing Rights policy Templates for Offline Use*

- Ensure that templates are published to a shared folder
- Enable the AD RMS Rights Policy Template Management (Automated) Scheduled Task
- Edit the registry key and specify the shared folder location



**Algebra**

visoka škola za  
primijenjeno računarstvo

## Allows you to: *What Are Exclusion Policies?*

- Block specific users from accessing AD RMS–protected content by blocking their RAC
- Block specific applications from creating or consuming AD RMS–protected content
- Block specific versions of the AD RMS client



**Algebra**

visoka škola za  
primijenjeno računarstvo

## *AD RMS Super Users Group*

- Super users group members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the super users group is configured.
- Super users group:
  - Is not configured by default
  - Can be used as data recovery mechanism for AD RMS–protected content
    - Can recover content that has expired
    - Can recover content if the template is deleted
    - Can recover content without requiring author credentials
  - Must be an Active Directory group with an assigned email address.



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *AD RMS Integration with Dynamic Access Control*

- DAC applies encryption by using AD RMS
- DAC protects documents even if inadvertently saved, sent, or processed incorrectly
- DAC extends AD RMS to the file server



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Lesson 4: Configuring External Access to AD RMS*

- Options for Enabling External Users with AD RMS Access
- Implementing Trusted User Domain
- Implementing TPD
- Sharing AD RMS–Protected Documents by Using a Microsoft Account
- Considerations for Implementing External User Access to AD RMS
- Windows Azure AD Rights Management



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Options for Enabling External Users with AD RMS Access*

- Trusted User Domains
  - Exchange protected content between two organizations
- Trusted Publishing Domains
  - Consolidate AD RMS architecture
- Federation Trust
  - One AD RMS infrastructure is accessible to AD FS partners
- Windows Live ID
  - Allow stand alone users access to AD RMS content
- Microsoft Federation Gateway
  - Allow an AD RMS cluster to work with Microsoft Federation Gateway without requiring a direct Federation Trust



## *Implementing Trusted User Domain*

- Allows AD RMS to service requests to users with RACs from different AD RMS clusters
- TUDs:
  - Support exclusions to individual users and groups
  - Can be one-way or bidirectional
- Must export TUD from partner before importing TUD locally



**Algebra**

visoka škola za  
primijenjeno računarstvo

## *Implementing TPD*

- Allows a local AD RMS deployment to issue EULs to content protected by a partner AD RMS cluster
- Involves importing the SLC of the partner AD RMS cluster
- No limit to the number of supported TPDs



**Algebra**

visoka škola za  
primijenjeno računarstvo



# *Sharing AD RMS–Protected Documents by Using a Microsoft Account*

- Provide RACs to users who are not part of an organization
- Users with Microsoft Accounts can consume AD RMS–protected content
- Users with Microsoft Accounts cannot publish AD RMS–protected content



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Considerations for Implementing External User Access to AD RMS*

- Use Windows Live ID to issue RACs to users who are not part of organizations, and who need to consume content
- Use TUD for RACs issued by a different AD RMS cluster
- Use TPD to allow local RACs to access remotely published AD RMS content
- Use Federation Trust between organizations that have a federated relationship
- Use Microsoft Federation Gateway when no direct federated relationship exists



**Algebra**

visoka škola za  
primijenjeno računarstvo

# *Windows Azure AD Rights Management*

- Windows Azure Rights Management is IRM-based cloud service protection
- Windows Azure Right Management is available in Office 365 Enterprise E3 and Office 365 ProPlus
- Windows Azure AD Rights Management provides:
  - IRM integration with Microsoft Office
  - Exchange Online IRM integration
  - SharePoint Online IRM integration



**Algebra**

visoka škola za  
primijenjeno računarstvo