# RSA® CONFERENCE CHINA 2012

RSA信息安全大会2012

## THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

# Rights Management Services and the Information Protection Ecosystem

**Gagan Gulati**

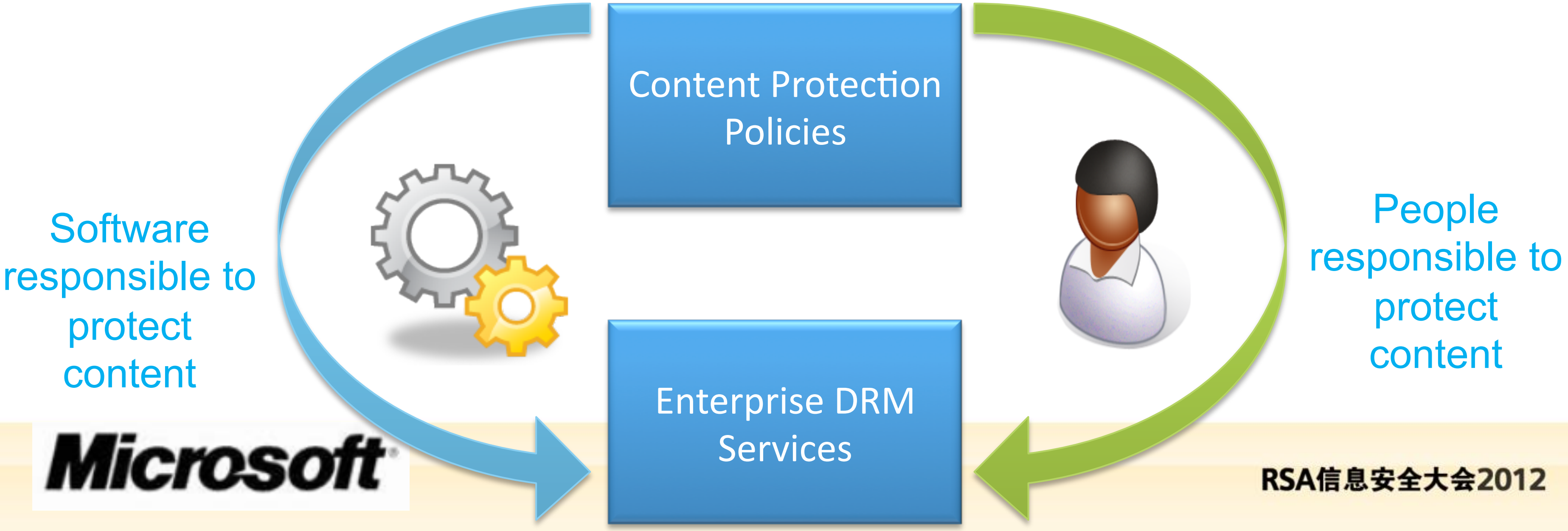
**Microsoft Corporation**

RSA CONFERENCE
CHINA 2012

# Foreword: Definitions and Approaches

- **Protection:** Encryption + Policy + Policy enforcement
  - **Encryption:** Targets securing data in transit or at rest but only until consumed
  - **Policy:** Definition of who (identity) can do what (conditions) on a protected item
  - **Policy Enforcement:** App-specific code to enforce common, standardized behaviors

- **Enterprise Rights Management (ERM):**
  Relies on 'users' or 'SPO libraries' to apply Protection to documents
- **Content-Aware Data Leakage Protection (DLP):**
  Relies on 'agents' to apply Protection (encryption + policy) to content



Content Protection Policies
Software responsible to protect content
People responsible to protect content
Enterprise DRM Services

# The changing landscape

# Industry trends driving customers and Microsoft

Externalization of IT

Applications are on-premises and in the cloud

Consumerization of IT

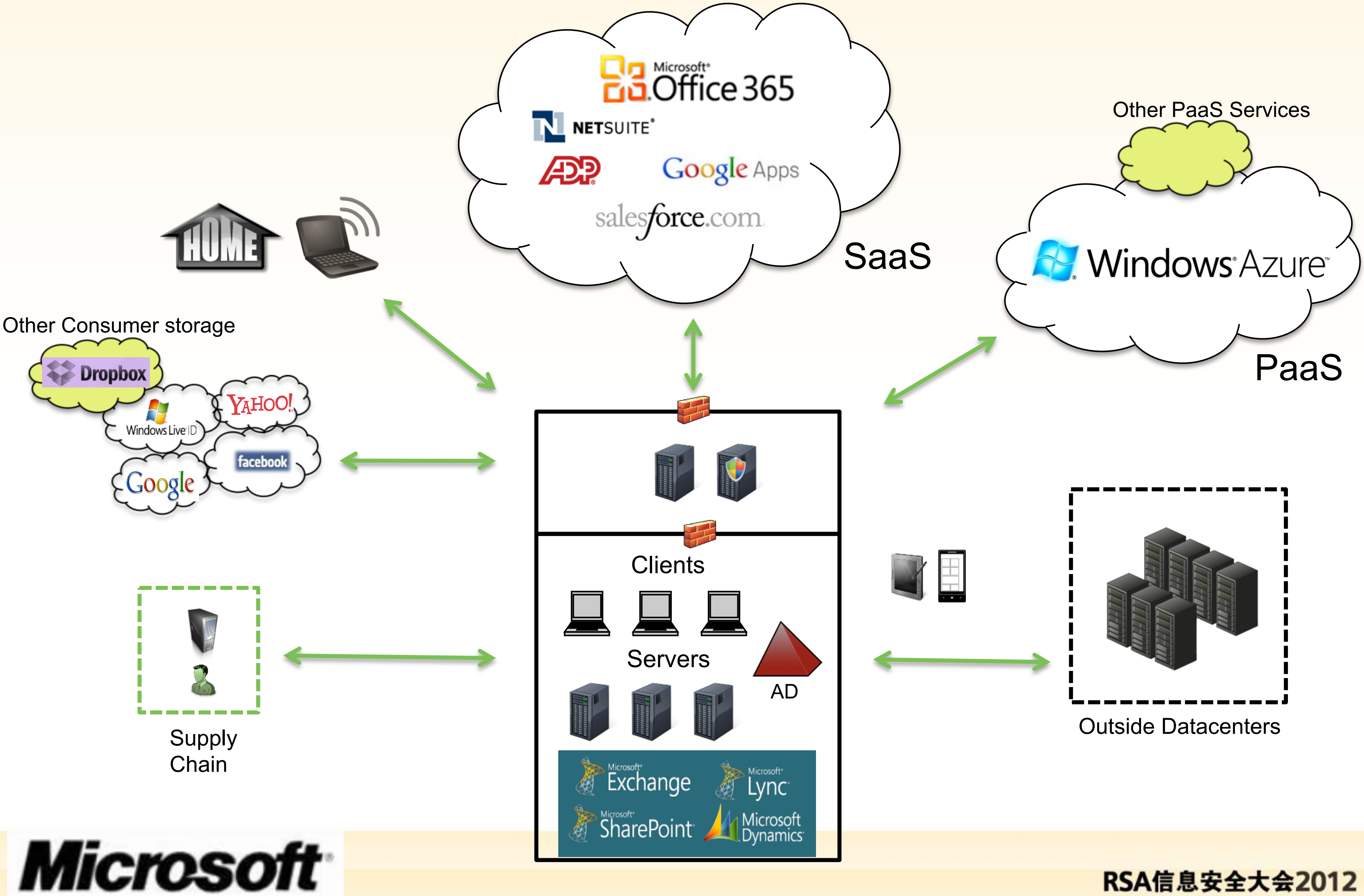
Users need access, from any device

Explosion of Information

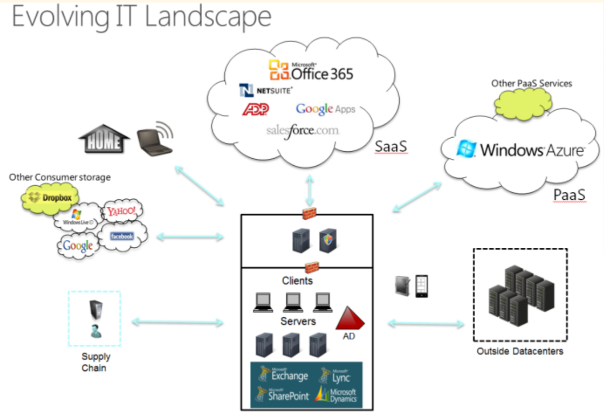
Dispersed enterprise data needs to be protected

The traditional perimeter is rapidly eroding
A form of protection that does not require a classic ‘boundary’ is required

# Evolving IT Landscape



# Info Protection Requirements



- **Data is protected at the source**
  - Modern apps save directly to ‘foreign storage’ so they must encrypt before data leaves the app
- **Data is protected in ‘usable chunks’**
  - Use patterns are at the document level; not at the full drive level (e.g.: BitLocker)
  - Especially true on constrained-resource mobile devices; on shared cloud-based storage

# Info Protection Requirements

- **Very strong encryption at rest; pretty good protection in apps is fine**
  - Assume the data is exposed to adversaries when at rest (pre-authorization)
  - Presume the user is “trustworthy but possibly absent minded” (post-authorization)
  - Flexible activation model supports the most important of auditing or offline use; ITPro decides
- **Per-app policies and customization(s) to increase usability (reduce friction)**
  - Automatic RM (CA-DLP); Per-application optimizations (Outlook vs Word); App Context Matters

# Satisfying Customer Needs: Approaches

- **Protect files with EFS**
  - Everyday Metaphor: Locking bike rack – useful at that particular location but nowhere else.
  - Once a good idea **but not very useful in modern times…** who has only one device?

- **Lock up personal data stores with BitLocker / BitLocker to Go**
  - Everyday Metaphor: Lock on the front door of your home. Good, but once open, everyone gets in.
  - Great way to protect against lost laptops and other assert but not at a granular level

- **Rights Management on-premises, in the cloud, across ‘tenants’ and to guests**
  - Everyday Metaphor: Certified mail that, when closed, requires re-certification before reuse.
  - Protection for data ‘in the wild’ with flexible terms-of-use, and transport agnostic

# Satisfying Customer Needs: Approaches

- **SharePoint ‘Secured Libraries’**
  - Everyday Metaphor: A well run public Library who’s librarian actually asks to see your identity
  - Great way to host data that can be centralized; data that leaves is protected

- **Pro-active protection (aka DLP) via Exchange, FOPE, FCI, ISV offers, etc.**
  - Everyday Metaphor: A persistent yard caretaker for your ‘digital landscape’
  - Volunteer application of RM will only get you so far → DLP offers at strategic points does wonders!

**Combined, these offers give you protection of lost assets, data in repositories, data in flight (protected or not), and IT controlled* auditing of data usage.**

# Satisfying Customer Needs: Investments

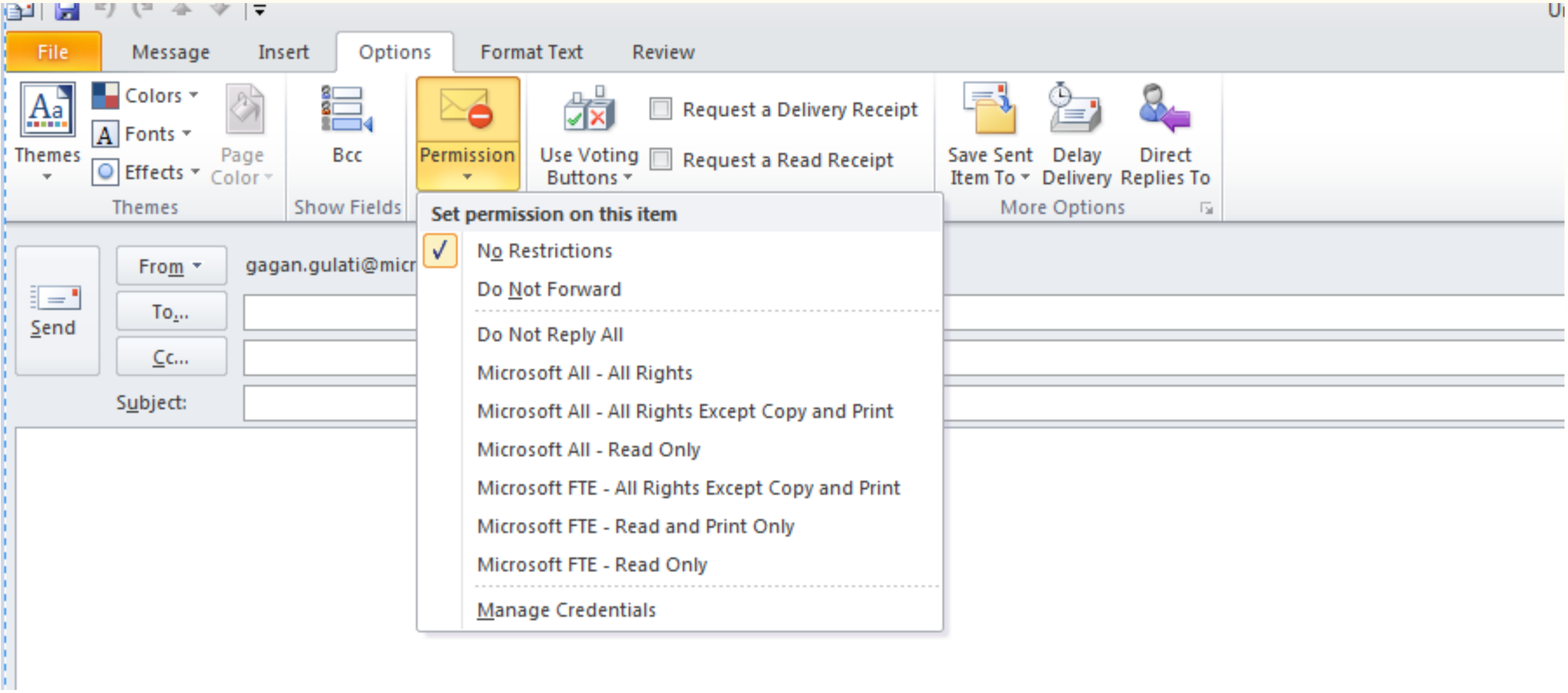
- **Application Reach: “Let me protect my documents as part of my work flow”**
  - Office and Office 365 supports RMS today… and continuing to improve
  - Key file formats within reach: PDF, TXT, Visio, Project
  - Massive outreach underway with new, far-simpler SDK (4000 vs 200 lines of code)
  - Generic Protection with ‘Rights Protected Folder’ format
- **Device Reach: “Let me use RM protected documents anywhere”**
  - Supported on Windows, Windows Phone 7.5+, Office 365, and Mac
  - Action(s) underway for iOS, Android(s), and Metro
  - Interest in devices using Linux

# Satisfying Customer Needs: Investments

- **Operational Readiness: “I can use RMS in my organization”**
  - ERM as base capability (substrate)
    - Microsoft’s AD RM offer lead by a wide margin in base capabilities, reach, and use.
  - DLP for automated protection of relevant content
    - Microsoft Office, Windows Server FCI, Microsoft FOPE, Office 365 and many other partners combine to support more than user-applied data protection in the Rights Management format
  - Reporting for validation of efforts (compliance)
    - Microsoft FOPE and many other partners combine (past and future) to support this need.
  - **Vibrant solutions ISV community**
    - Many very useful offers layered over core MSFT IRM platform: Gigatrust, Secure Island, etc.

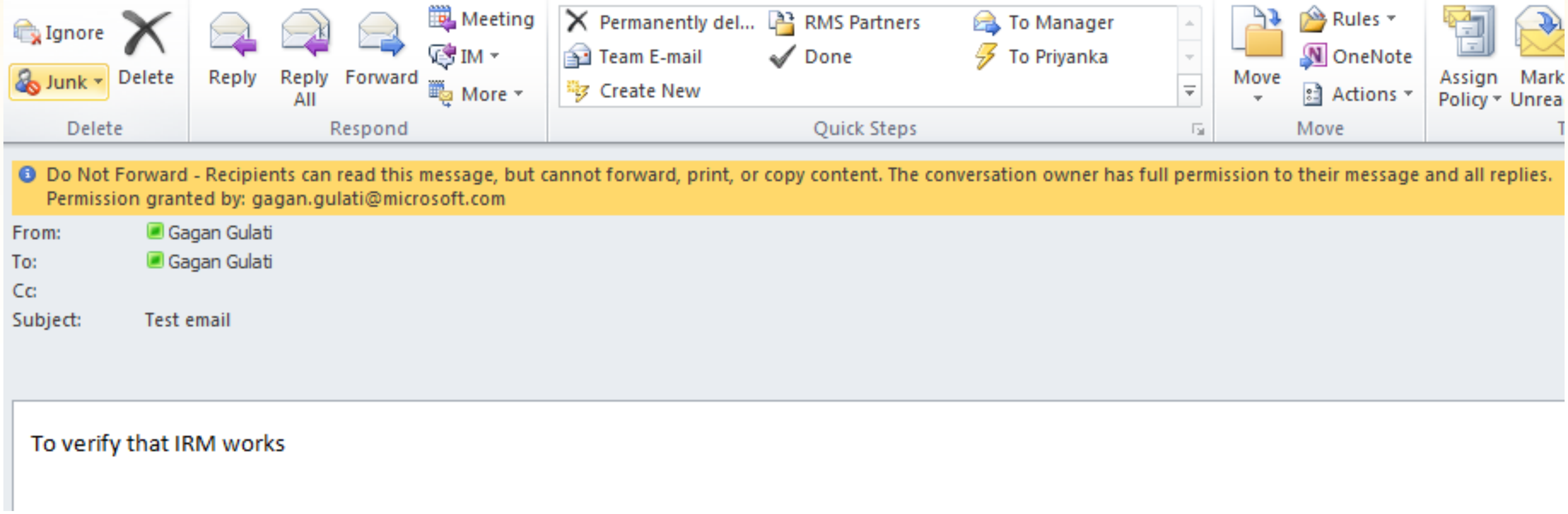
# AD RMS offerings for developers

# Outlook: Publisher



From: gagan.gulati@micr

# Outlook: Receiver

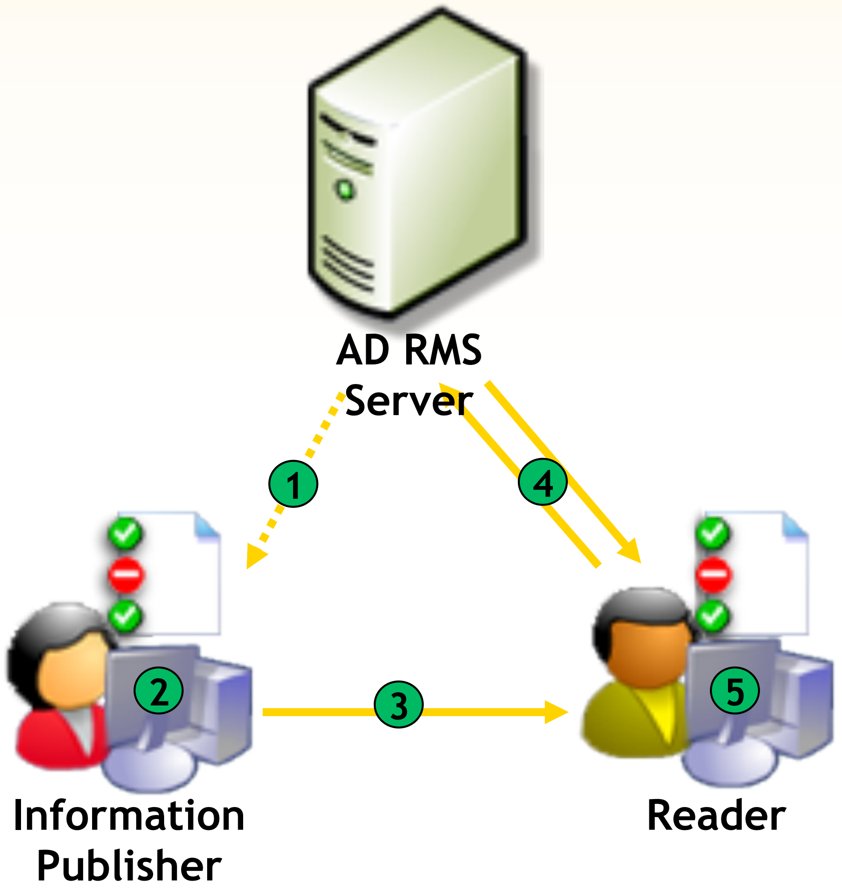


Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: gagan.gulati@microsoft.com

From: Gagan Gulati
To: Gagan Gulati
Cc:
Subject: Test email

To verify that IRM works

# AD RMS Workflow



1. Publisher gets the required certificates and templates to allow Rights Management
2. Publisher defines a set of usage rights and rules for their file; Application encrypts the file
3. Publisher distributes file
4. Reader clicks file to open, the application calls to the RMS server which validates the user
5. Application renders file and enforces rights

# What is a Rights-Enabled Application

- AD RMS relies on rights-enabled applications to:
  - Create policies (Do not Print, Do not Forward, Reply All)
  - Encrypt documents
  - Enforce restrictions
- An AD-RMS-enabled application is a regular application, enhanced to work with AD RMS
  - Use AD RMS SDK to enhance your application

# A bit of history: MSDRM

- MSDRM was the first client/SDK/API provided to support Rights Management Services

- MSDRM was a low-level API
  - It required significant understanding of AD RMS functionality
  - It required significant development and testing investment
  - It bound an application to specific behaviors in AD RMS
    - E.g. specific cryptography

# AD RMS SDK 2.0 (MSIPC)

- Released in May 2012 for Windows
- Very low integration cost
- Microsoft-internal Rights Management implementations moving to the new SDK (Office 15, SharePoint and later Exchange)

- Quotes from Office devs
  - *"The benefits of MSIPC being in Office are huge… has cut out weeks and weeks from our schedule of learning about RACs, CERTs, CLCs and how everything works"*
  - *"I accidentally send an IRM'd email with big attachments (9MB) the perf changes were amazing. It took Office 15-25seconds to open the e-mail and in the future it will takes 2-3 seconds."*

# MSIPC: AD RMS SDK 2.0

| Developer Cost | MSDRM (old) | MSIPC (new) |
|---|---|---|
| **API surface** | 84 functions | 20 functions (of which a few are needed) |
| **Cost of integration** | ~4000 lines of code | ~200-400 lines of code |
| **Ramp up time** | Detailed knowledge of Certificates, formats and topologies, multi-threaded only | Basic understanding of rights enforcement only |
| **Requires Update to support new functionality** | Yes (significant changes might be required) | No |
| **New RMS features guaranteed to work** | No (for Crypto-agnosticism, cert formats, revocation scenarios) | Yes |
| **Multi-topologies support** | Significant development and test cost | Free (just works with all topologies) |
| **Servicing** | MSDRM features are a little bit different on every OS version | Consistent feature behavior as MSIPC is Out of Band. You can bundle update. |

# What's next for AD RMS SDK

# What's Next: AD RMS iOS SDK

- Consume protected content on an iOS device
- We have a team actively working on the SDK
- We are signing up ISVs now!

iOS SDK Beta ready to release in Fall, 2012

# What’s Next: File API

File API

- Access and create AD RMS protected files without worrying about file formats
- Tighter integration, high performance
- Protector model: File format owners ship protectors, customers buy protectors
- Office + Generic Protector bundled free with runtime
- Works with AD RMS and AADRM

File API Beta ready to release in Fall, 2012.

# Additional Resources

- AD RMS SDK 2.0 available on Microsoft download center
- Here are some resources you'll find invaluable:
  - Download Link: https://connect.microsoft.com/site1170/
    - 1-box test environment
    - Quick Start guide for building a simple Rich Client application

# Thank You

RSA CONFERENCE
CHINA 2012