Microsoft tartalomvédelmi megoldások

Micskei Zoltán

BME

OVITÓL AZ EGYETEMIG AZ OKTATÁSBAN
Microsoft

Társ a Tanulásban program

Tartalomvédelem

- Digitális tartalmak elterjedése
- Tartalom tulajdonosa tudja szabályozni a *hozzáférést*
- Állományok biztonságos átvitele és tárolása
- Klasszikus fájlvédelemnél *finomabb granularitású* hozzáférés

Rights Management Services

(RMS)

Társ a Tanulásban program

Microsoft NetworkShop 2005

Tartalom

- **RMS szerepe, céljai**
- RMS architektúrája
- RMS működése
- RMS további funkciói

Védelmi megoldások

- Titkosítás
  - Csak hozzáférhet – nem férhet hozzá
- Tűzfal
  - Ha egyszer megkerülték, nem véd
- Fájl hozzáférési listák (ACL)
  - Kevés jog (írás, olvasás)
  - Kikerülhető ha hozzáférünk a HW-hez
- Ennél finomabb szabályozás kell

RMS

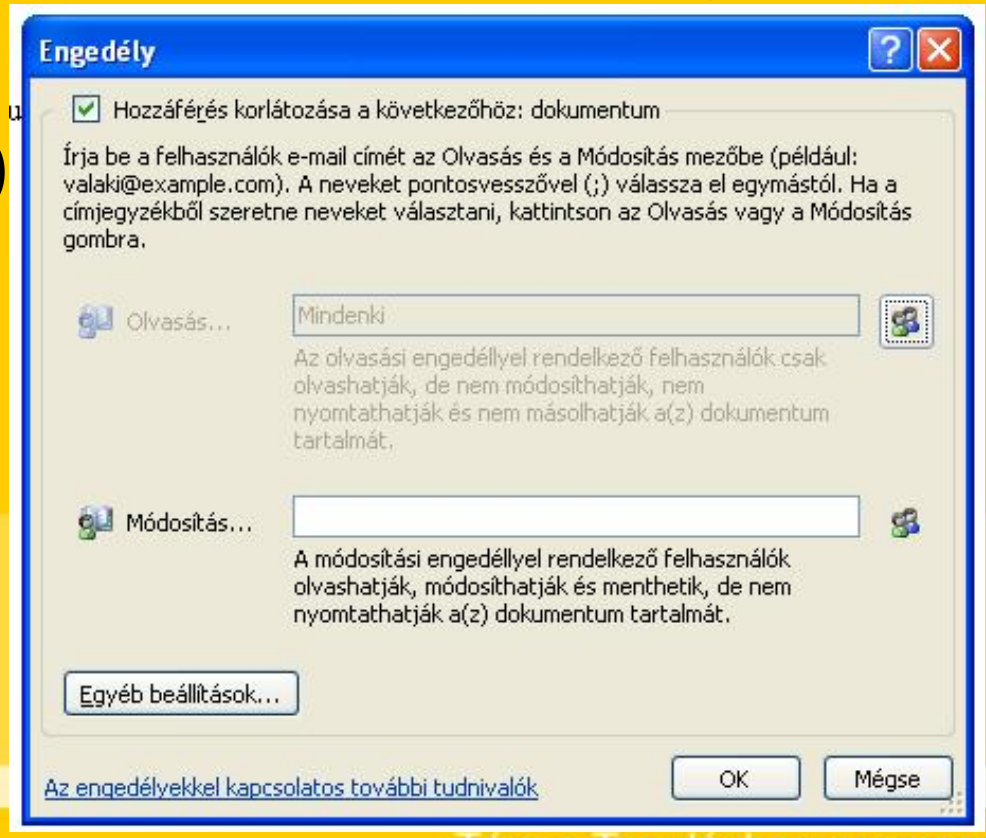
- Infrastruktúra dokumentumok korlátozott használhatóságának megadására
- A védelem a vállalati hálózatból kikerült dokumentumokon is megmarad
- „Policy enforcement solution”
  - Egyértelmű legyen, hogy milyen műveleteket hajthat végre az a dokumentumon, aki hozzáfért.

Kiadható jogok

- Jogok:
  - Írás, olvasás, mentés másként
  - Válasz, továbbítás, makrók engedélyezése
  - Nyomtatás
  - Elévülés (adott napon, adott nap múlva)
  - Alkalmazás-specifikus név-érték párok
- Ezekből saját sablonok állíthatóak össze

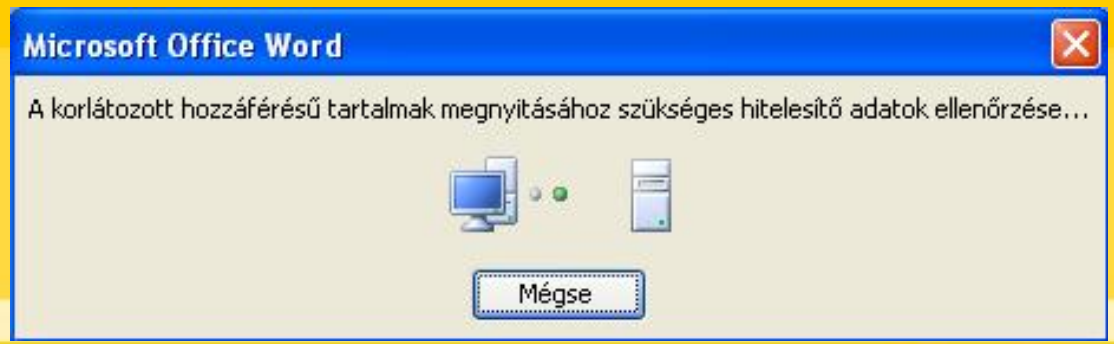
RMS használata – I.

- RMS-t támogató alkalmazással a dokumentumot tartalomvédelemmel látjuk el:
  - Dokumentumot titkosítja (AES 128 bit)
  - Tanúsítványt rendel hozzá (XrML leírás), hogy ki milyen műveleteket hajthat végre vele



RMS használata – II.

- Megfelelő kliens (Office 2003, IE Add-on) megpróbálja megnyitni
- Dokumentumban szereplő licenc szerverhez csatlakozik (Webszolgáltatás)
- Beszerzi a licencet és eltárolja (ha lehet) későbbi használatra



Microsoft NetworkShop 2005

Tartalom

- RMS bemutatása, szerepe, céljai
- **RMS architektúrája**
- RMS működése
- RMS további funkciói

Szerver oldali komponensek

- Windows Server 2003
- Active Directory
  - Felhasználó e-mail címe kitöltve
- Microsoft Message Queue: loggoláshoz
- SQL Server 2000 vagy MSDE 2000
- RMS Server komponens telepítése
  - Opcionális: hardver támogatás a kulcsok tárolásához
- Internet kapcsolat az első szerver bejegyzéséhez (enrollment)

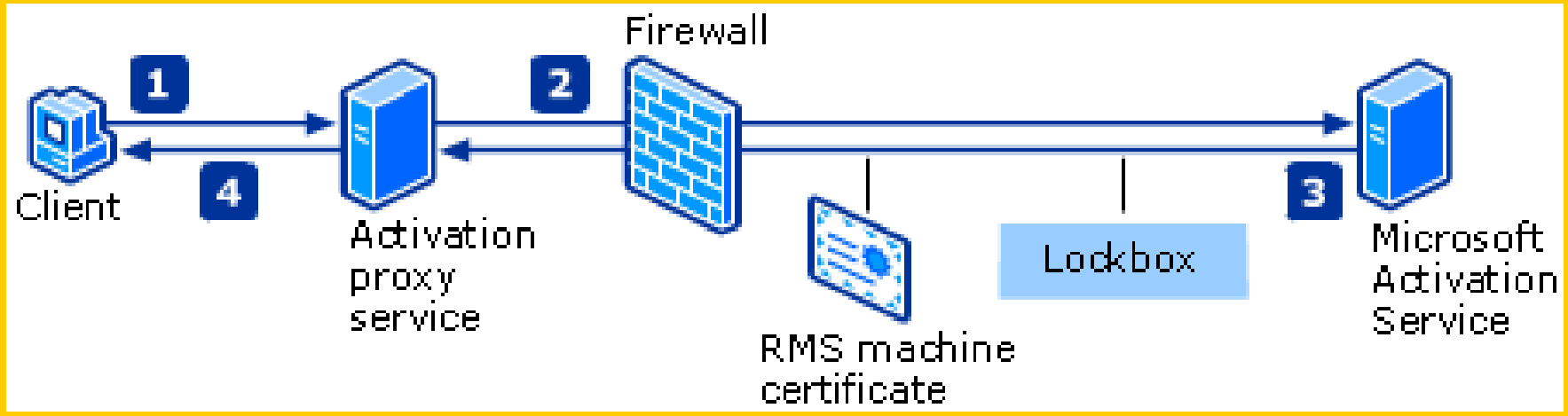
Szerver enrollment

- Első RMS szerver telepítésekor:
  - Szervezet RMS kulcsának generálása
  - Az RMS verzióját, a használandó URL-t és kulcspár nyilvános részét elküldi a Microsoft RMS Server Enrollment szolgáltatásának (megbízható harmadik fél).
  - Válaszként megérkezik az RMS Licensor Certificate, mely a további licencek előállításához szükséges.

Kliens

- RMS-re felkészített alkalmazás (Office 2003, Internet Explorer Add-On, saját készítése: RMS SDK)
- Használatához külön RMS Client licenc szükséges: RMS Licensing
- RMS Client tool:
  - RMS használatához szükséges dll-k
  - Telepítése során aktiválja a gépet:

Kliens aktiválás



- Elküldi a gép hardver azonosítójának hash-ét
- Létrejön:
  - Lockbox (secrep.dll): számítógép privát és publikus kulcsának tárolására, RMS-t használó alkalmazások ellenőrzése
  - RMS machine certificates: a gép publikus kulcsát tartalmazza a Microsoft RMS Activation Service által aláírva.

Felhasználó hozzáadás

- RAC (rights account certificates): Egy felhasználót és egy aktivált számítógépet rendel össze.
- Tartalmazza a *felhasználó nyilvános kulcsát*
- és a gép publikus kulcsával titkosítva a *felhasználó privát kulcsát*
- Akkor jön létre, amikor a felhasználó ezen a gépen először védett tartalomhoz fér hozzá

XrML

- Jogosultságok leírására szolgáló XML
-
-

```
-<license>
   <!- - Anyone can print the book located at the specified URL - ->
  -<grant>
     <mx:print/>
    -<digitalResource>
       <nonSecureIndirect URI="http://www.contentguard.com/sampleBook.spd"/>
     </digitalResource>
   </grant>
  -<issuer>
     <!- - The issuer's signature - ->
    +<dsig:Signature>
    -<details>
       <timeOfIssue>2000-01-27T15:30:00</timeOfIssue>
     </details>
   </issuer>
 </license>
```

Licencek

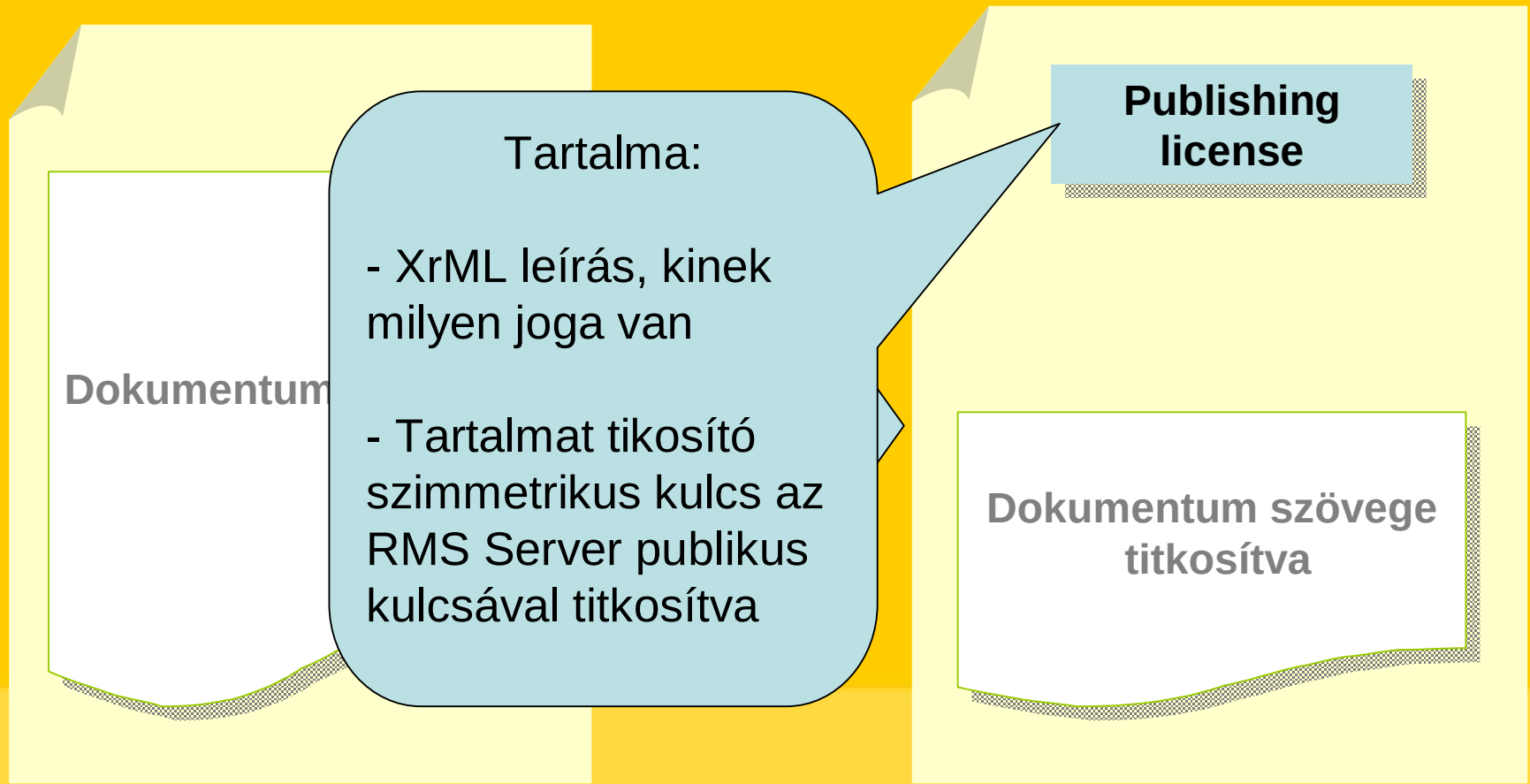
- Publish: tartalom levédésekor kerül bele a dokumentumba, megadja, hogy ki mit csinálhat.
  - Tartalmazza a dokumentum titkosításához használt szimmetrikus kulcsot, az RMS Server publikus kulcsával kódolva.
- Use: engedély egy felhasználónak, hogy hozzáférhet egy védett dokumentumhoz.
  - Tartalmazza a dokumentum titkosításához használt szimmetrikus kulcsot, a felhasználó publikus kulcsával kódolva.

Microsoft NetworkShop 2005

Tartalom

- RMS bemutatása, szerepe, céljai
- RMS architektúrája
- **RMS működése**
- RMS további funkciói

Tartalomvédelem bekapcsolása



Védett dokumentum megnyitása

1. Szerver dekódolja a Publish licencet
2. A megkapott szimmetrikus tartalom kulcsot kódolja a felhasználó publikus kulcsával
3. Így előáll a Use licenc

RMS szerver

2. Licenc kérés

PL

RAC

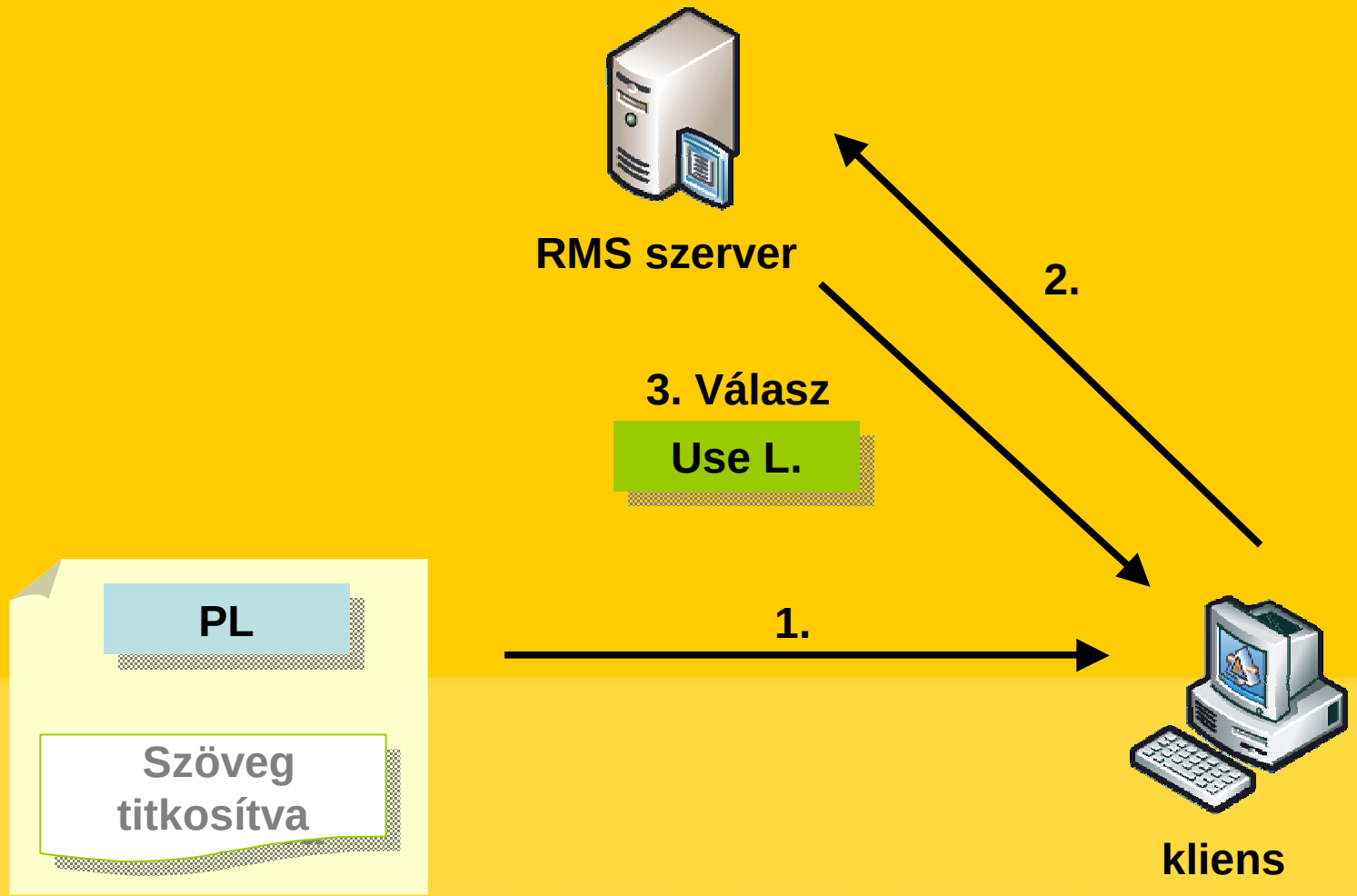
PL

Szöveg titkosítva

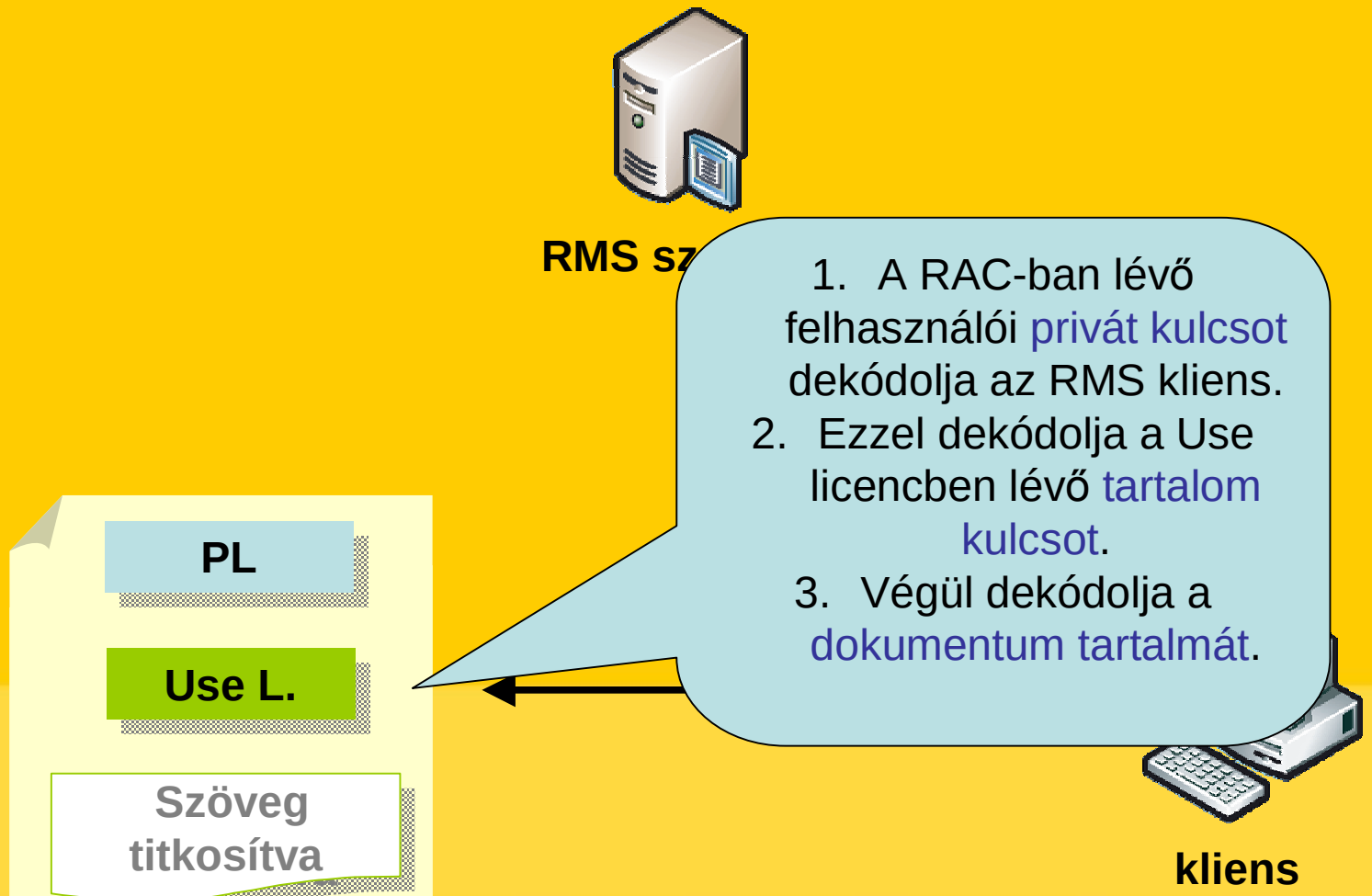
1. megnyitja

kliens

Védett dokumentum megnyitása



Védett dokumentum megnyitása



Tartalom

- RMS bemutatása, szerepe, céljai
- RMS architektúrája
- RMS működése
- **RMS további funkciói**

RMS skálázása

- Oldalra skálázás:
  - Web Service load balancing
- Hierarchia létrehozása
  - Root RMS server
  - Alá rendelhetők licensing szerverek, melyek csak publishing és use licenceket állítanak ki

SDK

- RMS Server SDK
  - SOAP metódusok leírása
  - Meglévő dokumentum-kezelő rendszerbe RMS beépítése
- RMS Client SDK
  - Saját alkalmazás hogy készítsen RMS által védett fájlokat
  - Security Guidelines, API hívások, példakódok

Értékelés

- Előnyök
  - Robosztus, skálázható architektúra
  - Testreszabható szolgáltatások
- Kérdéses:
  - Függés az MS Enrollment és Activation Servervices-től
  - SP1-ben kiszedik az Activation Servicest

További információ

- Szalontay Zoltán – A Windows tartalomvédelmi szolgáltatása (Technet)
- http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx
- Technical Overview of Windows RMS
- RMS Deployment Guide
- RMS Information on Technet

Digital Rights Management

DRM

Társ a Tanulásban program

Digital Rights Management

- WMV, WMA fájlokhoz korlátozás rendelése
  - Megnézésükhöz a lejátszó programnak be kell szereznie egy licencet
- Új lehetőségek:
  - Akár csak egy szám megvétele
  - Közvetlenül a szerzőtől akár
  - Kölcsönzés, korlátozott számú használat
  - A fizikai hordozóeszköz nem növeli az árat
  - Könnyű áttölteni mobil eszközre
- Azonban sokakban kétségek:
  - Cenzúra, tartalom későbbi elérhetetlensége, eszközök inkompatibilitása

További információ

- Microsoft DRM honlap
  - SDK a DRM technológia alkalmazásához hardver eszközben, saját alkalmazásban, webhelyen
- Wikipedia: DRM
  - Technológiák, jogi háttér, érvek-ellenérvek
- Pl.: http://teka.origo.hu – Videotéka Microsoft DRM technológiával
- Sokféle egyéb DRM technológia:
  - Rhapsody (RealNetworks), iTunes (Apple)

Köszönöm a megtisztelő figyelmet!

Kérdések

Amire már nem jutott idő az előadásban

Társ a Tanulásban program

Megbízható partner

- Üzlettársunk is szeretné elolvasni a tartalomvédett dokumentumokat
- Publikálhatjuk az RMS szolgáltatásokat
- Megbízhatunk az Ő általa kiállított RAC-okban, így nekik is adunk use licencet
- Ha nincs RMS-ük, akkor külön Passport fiókokban is megbízhatunk
- Vagy importálhatják a server licensor certificate-ünket, így Ők is tudnak use licenset kiadni a mi publish licencünkhöz

Tanácsok

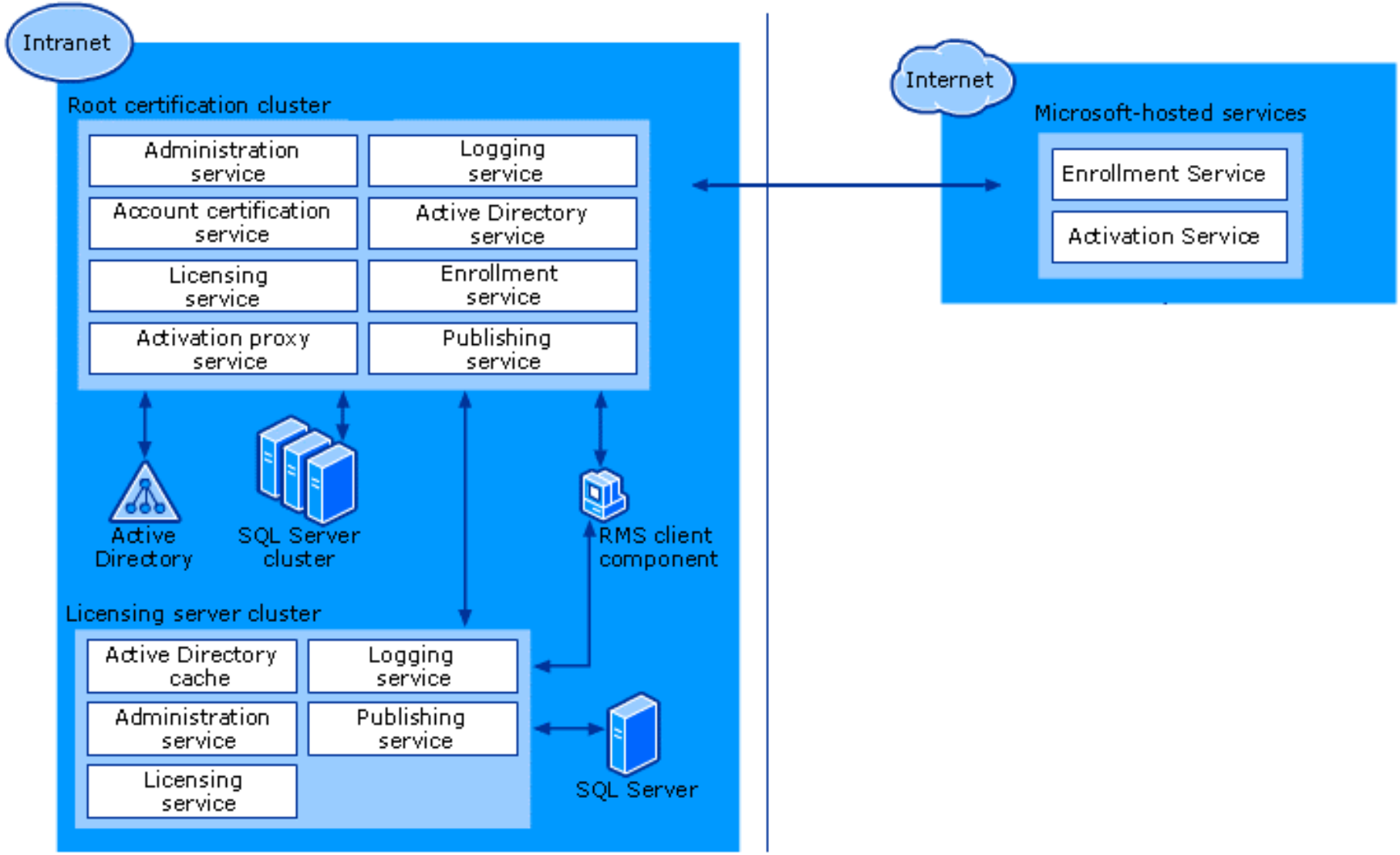
- Csoportoknak osszunk jogokat, ne egyéneknek
- RMS eltávolításának külön folyamata van, lásd itt. RMS Server privát kulcsát eltávolítás után is őrizzük meg!
- .NET webes alkalmazás, a nyomkövetés szükség esetén ugyanúgy bekapcsolható

Telepítés után létrejön

- Service connection point (SCP) az Active Directory-ban a Services konténerben (kliensek ez alapján találják meg az RMS-t webszolgáltatásokat)
- Webalkalmazás web szolgáltatásokkal

RMS szerverek feladata

- **Subenrollment: a később beállított licenc szervereket lépteti elő**
- **Activation proxy: Internet proxy a kliensek lockbox kérése esetén**
- **Certification: rights account certificate-ek kiosztása a felhasználóknak**
- **Publishing: publishing licencek**
- **Licensing: use licencek kiosztása.**


Intranet
Root certification cluster
Administration service
Logging service
Account certification service
Active Directory service
Licensing service
Enrollment service
Activation proxy service
Publishing service
Active Directory
SQL Server cluster
RMS client component
Licensing server cluster
Active Directory cache
Logging service
Administration service
Publishing service
Licensing service
SQL Server
Internet
Microsoft-hosted services
Enrollment Service
Activation Service

Tanúsítványok

- Server licensor certificates: root certification server nyilvános kulcsát tartalmazza (az MS Enrollment Service privát kulcsával aláírva)
- Kiadhat vele:
  - **Publishing licenses**
  - **Use licenses**
  - **Client licensor certificates**
  - **Rights policy templates**
  - **Rights account certificates to clients**
  - **Server licensor certificates to licensing servers**

Kliens használat ideiglenes kulcsokkal

- **Client enrollment.** If client computers will be used to publish rights-protected information when they are not connected to the corporate network, a local enrollment process is required. Client computers enroll with the root installation server or a Windows RMS licensing server and receive rights management client licensor certificates, which enable users to publish rights-protected information from those computers without being connected to the corporate network.

Kulcsok

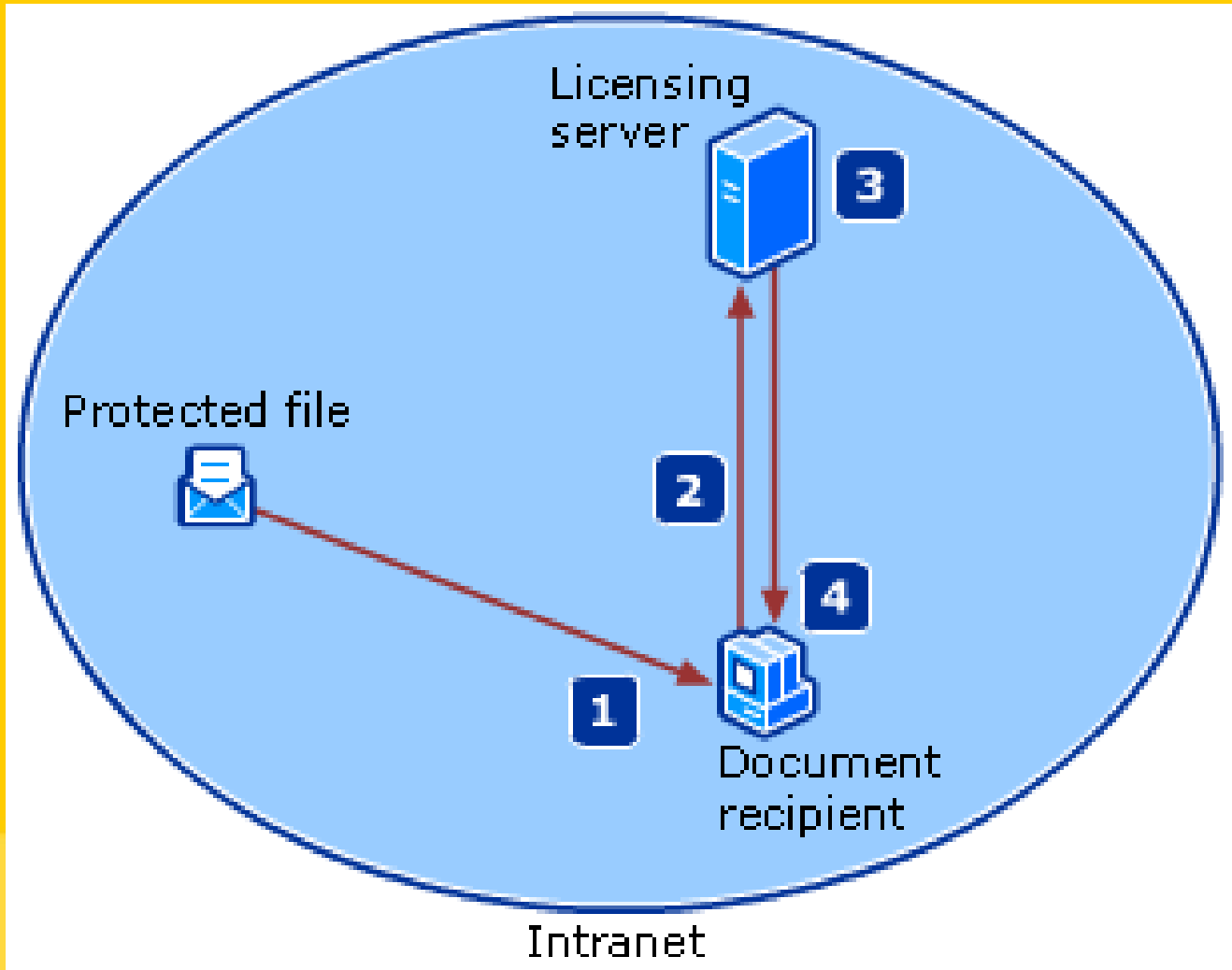
- Tartalom titkosítása (Office 2003): 128-bit AES.
- RMS server kulcs: 2048-bit
- Felhasználó kulcsa: 1024-bit
- Számítógép kulcsa: 512-bit RSA

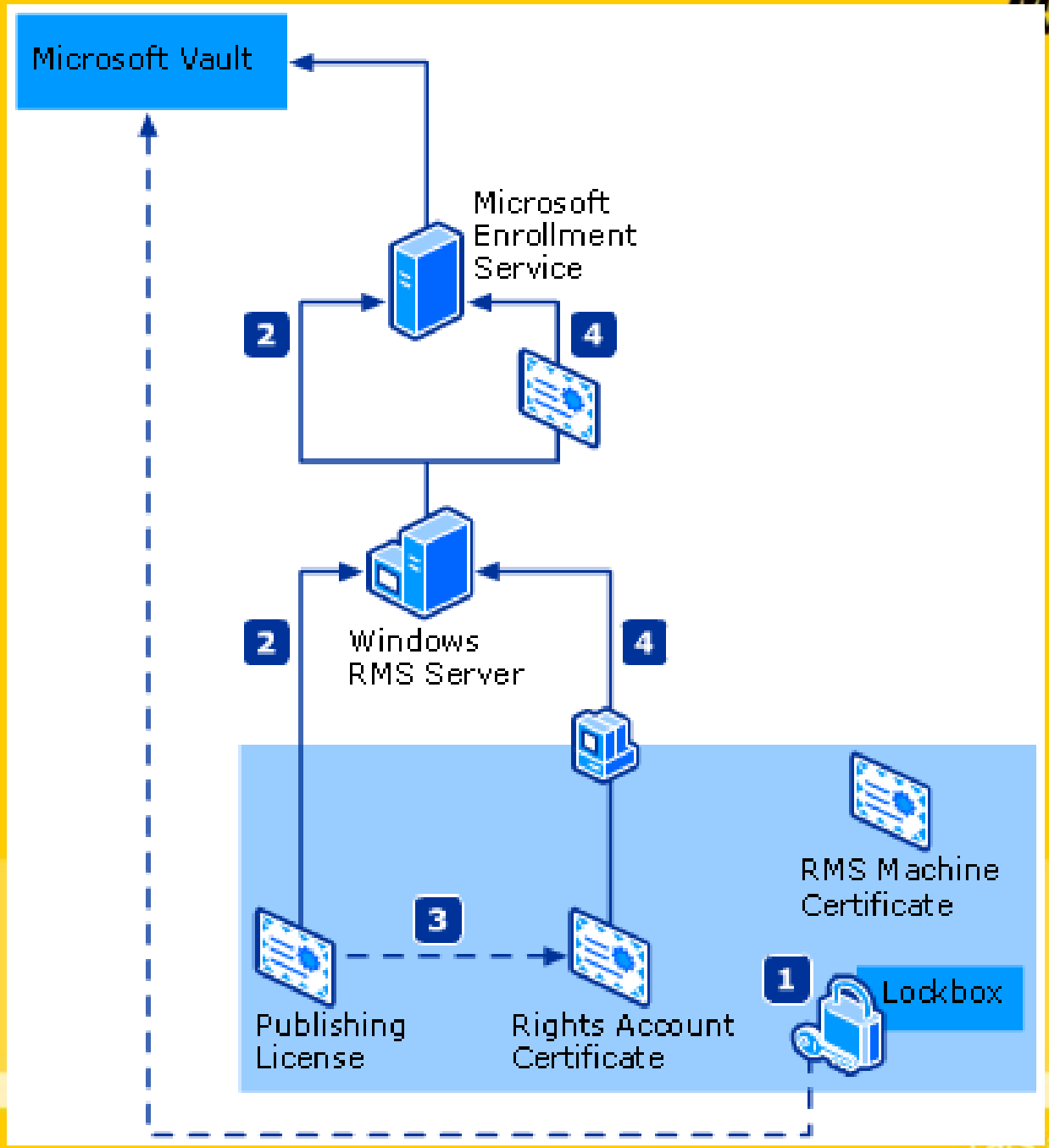
Adminisztráció

- RMS supports a special super users group that has full control over all RMS-protected content.
- Kizárások: lockbox version, OS version (98 és Me), felhasználó, alkalmazás

Kliens

- Lockbox:
  - The lockbox contains the computer's private key and is the core client-side security principal for encryption and decryption. In addition, it validates RMS-enabled applications as well as ensures machine integrity. Each lockbox is built on a hardware identifier, so that the lockbox is both unique and bound to a specific computer.
- Machine certificate:
  - The machine certificate contains a corresponding public key for the computer.


Licensing server
3
Protected file
2
4
1
Document recipient
Intranet


Microsoft Vault
Microsoft Enrollment Service
2
4
Windows RMS Server
2
4
RMS Machine Certificate
3
1
Lockbox
Publishing License
Rights Account Certificate