Tresorit's DRM

A New Level of Security for Document Collaboration and Sharing

Cloud-based storage has made it easier for business users to share documents, but it has also opened up new vulnerabilities. Solutions that use client-side encryption, such as Tresorit, offer the most security for sensitive and private data as it travels from the user's desktop, to the cloud, and to the chosen collaborator's desktop. But what happens to documents after they have been shared and during the collaboration process?

TRESORIT DRM™ IS A GAME-CHANGER FOR SMB DATA SECURITY:

Unlike other cloud solutions, Tresorit DRM™ protects the data itself, not just the cloud infrastructure. DRM wards off a host of security concerns including attacks from external hacker as well as breaches from internal employees. Whether malicious or accidental, protecting against these breaches is vital: According to a PwC study of 9,600 businesses, current and former employees account for 31% and 27% of data breach incidents respectively.

DRM technology has been used by commercial publishers to protect digital works such as music, videos, and e-books, and by large enterprises to manage access to sensitive documents and control content sharing. Tresorit's DRM offers the same high-level of security offered by enterprise-grade solutions, but is much simpler to use – companies no longer need expensive infrastructure and large IT teams to have complete digital security.

Tresorit DRM™ complements the Tresorit cloud-storage solution: Files are protected in transit and on the cloud with end-to-end encryption via Tresorit's storage solution; DRM offers more control to businesses by extending security to documents once they have been shared.

DATA PROTECTION WITH TRESORIT DRM™

Tresorit DRM™ protects data by combining strict role definition, distributed control of data, and the ability to revoke access to files to ensure complete data security in the cloud and on user devices.

DEFINE ROLES

Document owners often need to provide different privileges to users to control who can view a file versus those who can print, edit, copy, or share it. With Tresorit DRM™, administrators can set access levels on all encrypted folders (known as tresors), defining roles across teams with ease. These granular permissions provide exceptional control for complex collaboration on sensitive documents. Once assigned, roles carry over to all of the user's devices, enforcing the granular policies that are mapped to each defined role:

{ tresor [tʀeʀzoʀʀ]
noun (German)
1. lockable, armoured cabinet }

		OWNER	MANAGER	EDITOR	READER
SIMPLE RIGHTS	view	✓	✓	✓	✓
	edit	✓	✓	✓	✗
	share	✓	✓	✗	✗
ADVANCED RIGHTS	delete a tresor	✓	✗	✗	✗
	print	✓	✓	✗	✗
	copy-paste	✓	✓	✗	✗
	print-screen	✓	✓	✗	✗
	forward	✗	✗	✗	✗

Table 1: Control Every Aspect of Document Collaboration by Defining Roles in Tresorit DRM™

DISTRIBUTED CONTROL OF FILES:

With Tresorit DRM™, distributed control carries over to any device or user, because all files are encrypted individually. Even if corporate files are leaked, intruders are unable to access them due to the combined encryption layers of both Tresorit DRM™ and the service that powers it, Microsoft's Rights Management Service (RMS). While Tresorit regulates security policies set by the owner of the content, Microsoft's underlying technology enables local control over data. If a user tries to share a document via email or copy it onto a thumb drive, the permission rights travel with the document: no one can open a DRM-protected document without permission.

MICROSOFT RMS AND DATA SECURITY

Microsoft provides the Rights Management Service (RMS) for Tresorit DRM™. Files stored with Tresorit DRM™ are protected with three separate layers:

- Microsoft RMS controls permission management on a file level, and Tresorit DRM™ provides control over a document and a secure channel to handle sensitive files.
- The second layer is Tresorit's end-to-end security, which uses client-side encryption to scramble files on the user's device before they are transferred to the cloud.
- The transfer process is protected with Transport Layer Security (TLS) a protocol for secure Internet communications that has eclipsed the previously used SSL protocol.

CAN MICROSOFT READ THE CONTENT OF DRM-ENABLED TRESORS?

Absolutely not. Tresorit DRM™ has a zero-knowledge design to ensure that neither Tresorit nor Microsoft servers have access to the uploaded information, and that user data cannot be exposed.

- First, Microsoft RMS servers do not have physical access to protected files at any stage of the process. This means that even with possession of the Content Key, they cannot use it to decrypt data.
- Second, Tresorit's client-side encryption is also applied to DRM protected files, so the content is encrypted before it is uploaded to the cloud. This means that Tresorit servers cannot ever read the client side encrypted data.

HOW DOES TRESORIT DRM™ WORK

Once DRM is enabled in the Tresorit app, the Tresorit client can apply file-level encryption to documents stored in DRM-enabled tresors. Currently, Tresorit's DRM service is available on Windows to secure documents created using Microsoft's Office applications. Tresorit DRM™ is powered by Microsoft's RMS, and uses its security solutions in the DRM design as described below [1].

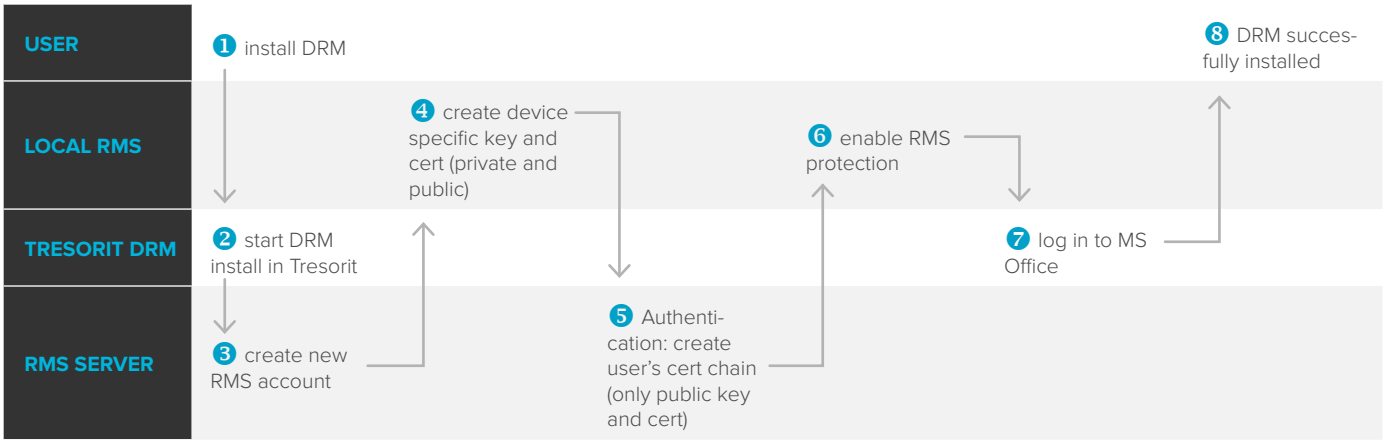
SECURING FILES WITH TRESORIT DRM™

After signing up for Tresorit Business, follow these steps:

1. Create a new tresor.
2. Set it up with DRM protection.
3. Install Tresorit DRM™ – this will run in the background and will take about a minute.
4. The DRM-protected tresor will be displayed with an additional shield symbolizing the extra layer of security.
5. Invite new members to share documents in a tresor, and set up permissions with a click.

TRESORIT DRM™ INSTALLATION

Users access Tresorit DRM™ by signing up to Tresorit Business; Tresorit will prompt them to download the DRM plugin. During installation, Tresorit DRM™ automatically creates the user's account on the Microsoft RMS servers and facilitates the creation of the user's own RMS public-private key pair and RMS certificate. The process also entails the exchange of public keys between the Microsoft RMS server and the user, and ends with Tresorit DRM™ signing the user into Microsoft Office.

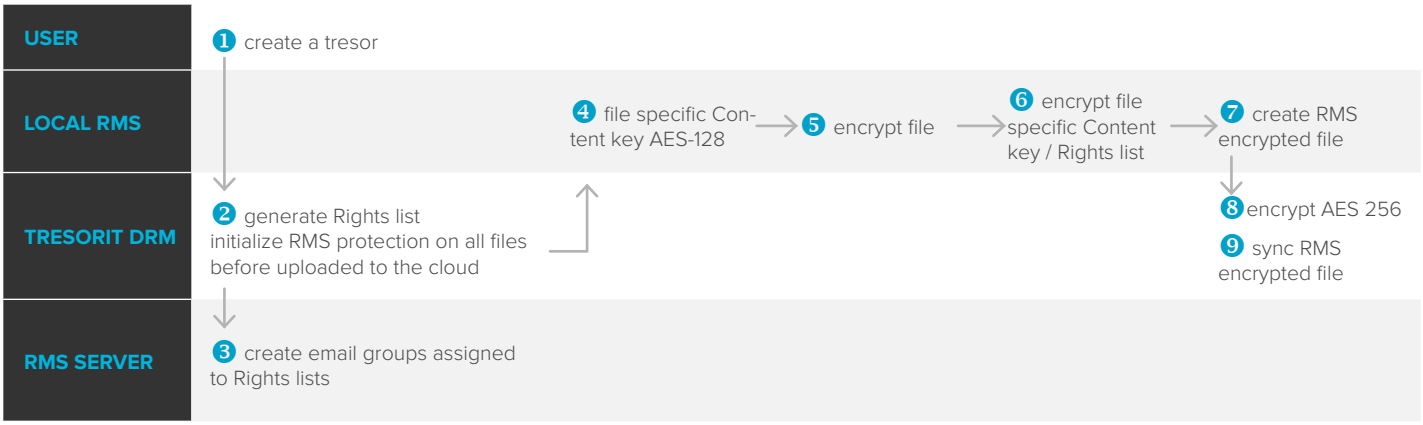


[1]For a more detailed description of Microsoft Rights Management Services, read this post by Dan Plastina, Microsoft developer's, on the official Microsoft TechNet blog.

CREATING A DRM PROTECTED TRESOR

When the user creates a DRM-protected tresor, Tresorit first generates a matching Rights List for each file. The Rights List contains three email groups, automatically created by Tresorit on Microsoft's servers. Tresorit DRM™ will ensure these email groups contain the email addresses of all Readers, Editors, and Managers of a tresor, and will assign their corresponding, pre-set access rights on the file level.

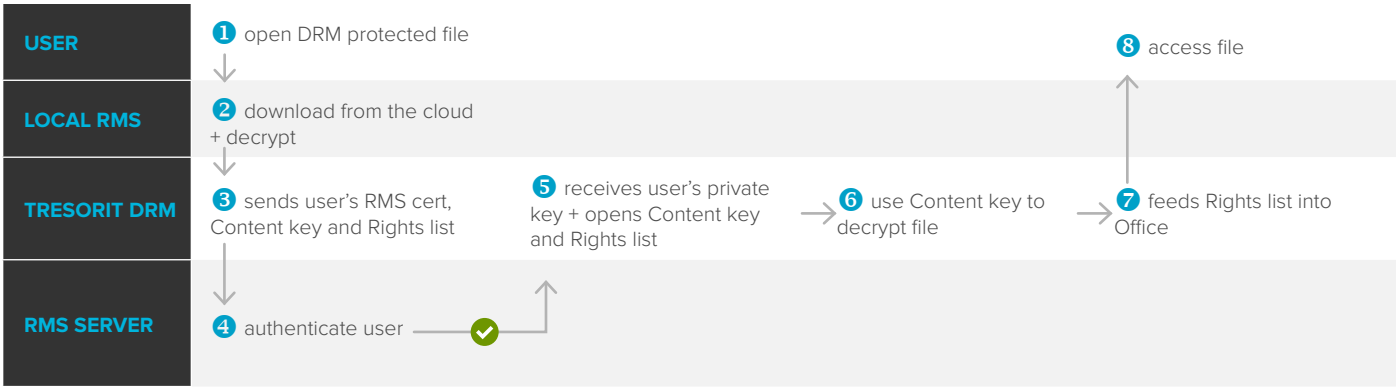
Tresorit also initializes Microsoft RMS protection for each file before upload. During this process, RMS creates a file-specific AES-128 Content Key, and encrypts each file with the corresponding Content Key, creating the 1st component of an RMS protected file. Once done, it combines each file's Content Key and Rights List, encrypting them with the Microsoft RMS server's public key. With this the 2nd component of the RMS-protected file is created. The final RMS protected file, made up of the encrypted file and matching 2nd component, is first encrypted with Tresorit's own AES-256 client-side protocol, then uploaded to the Tresorit cloud.



OPENING A DRM-PROTECTED FILE

When an authorized user has synced a DRM-protected file to their device via Tresorit, and opens it in Microsoft Office, the software contacts Microsoft RMS servers, sending along the user's RMS certificate and the encrypted 2nd component of the protected file. The RMS server uses its private key to decrypt the 2nd component, and gains access to both the file's Content Key and its Rights List.

Using the Rights List, the server checks whether the user has access to the protected content. If so, it sends the Content Key and Rights List back to the user's device, encrypting it with the user's RMS public key. Using the user's locally stored private key, RMS then accesses the Content Key and uses it to decrypt the local copy of the file. Once done, it loads both it and the Rights List into Microsoft Office, which grants access to the user, limiting his rights as outlined in the Rights List.

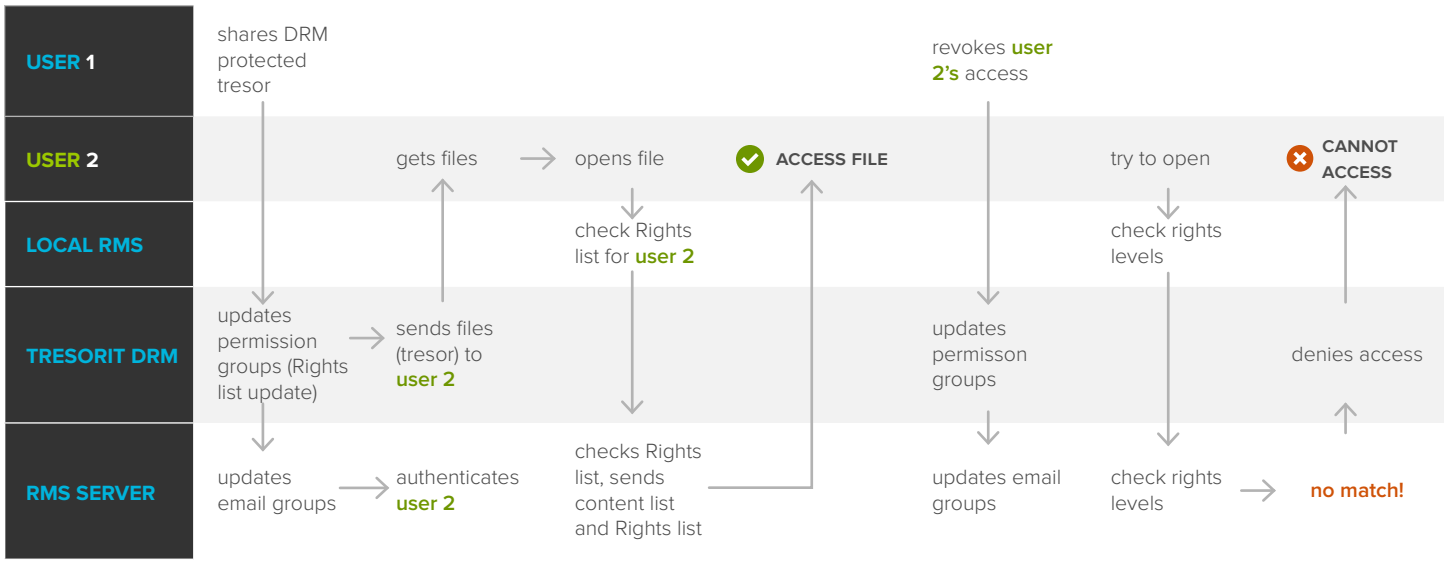


SHARING A DRM-PROTECTED FILE

When a user shares a DRM-protected file with a certain permission level, Tresorit DRM™ first updates the corresponding email group on the Microsoft RMS servers. As the invited member downloads an RMS-encrypted file through Tresorit, the same access process plays out that was outlined above: the RMS servers check for the user's access level. Once the user is granted access, they can start working with the shared documents according to the permission level set for him in Tresorit.

As the Rights List does not contain the users' email addresses directly, it's not necessary to re-encrypt protected files when changing permissions. The email groups for Readers, Editors, and Managers can be instantly updated by Tresorit DRM™ on the Microsoft RMS servers.

This means that even if a user had full access to the file a moment ago, as soon as permission is revoked, Microsoft Office will not permit him to open the file another time, ensuring that data stays under its owner's control, wherever it travels.



THE RIGHT SOLUTION FOR ADDED SECURITY

Tresorit's ultra-secure cloud collaboration service may be all a company needs to keep data safe while stored on the cloud and in transit to users. But companies that need to collaborate on sensitive documents need to protect information after it has been shared. Tresorit's DRM service makes secure and controlled collaboration possible for companies of all sizes. When Tresorit's cloud storage and sharing service is paired with the DRM service, companies now have end-to-end protection for data collaboration and security.