Microsoft

# Azure Information Protection

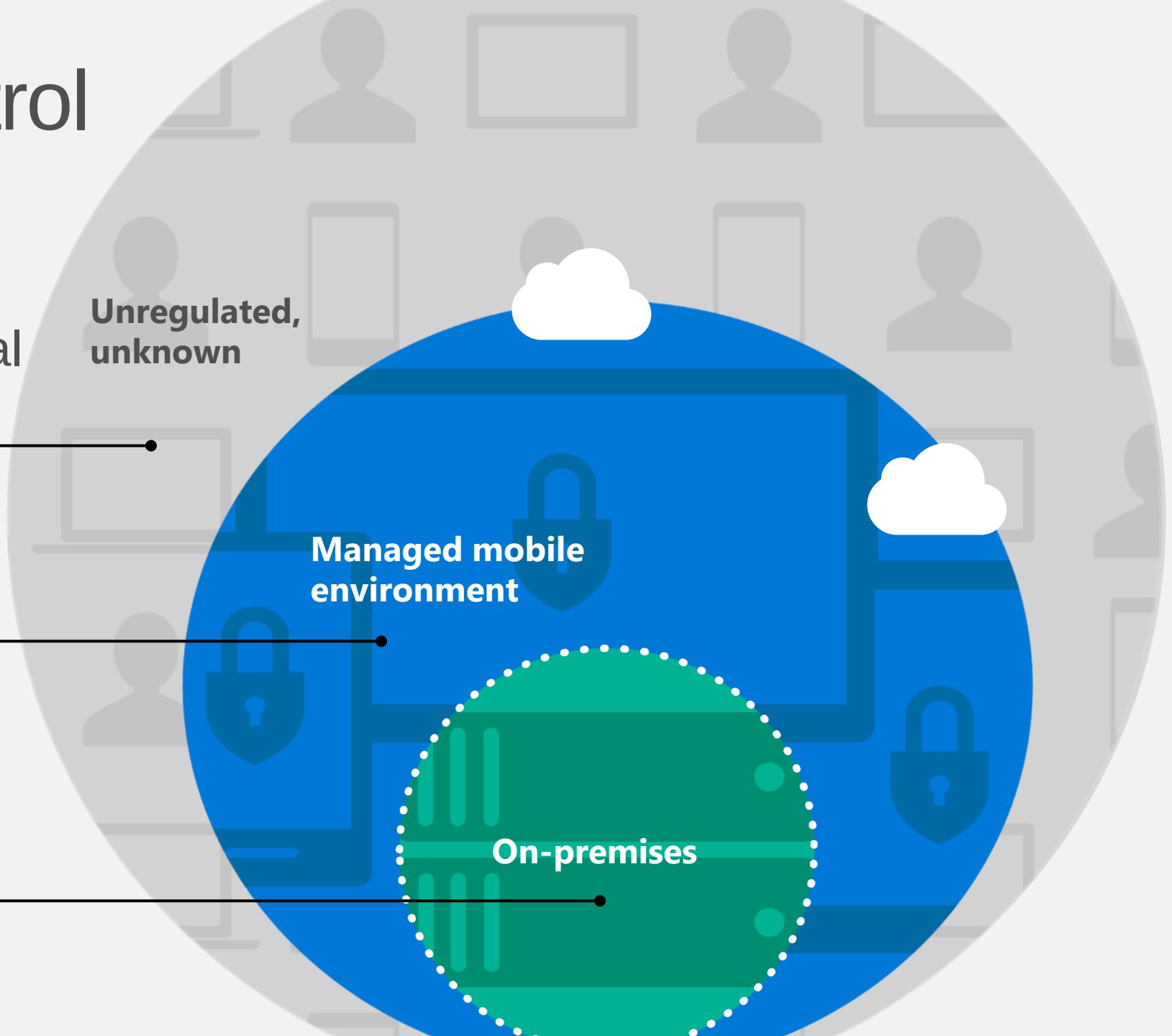
Raúl Moros Peña ramoro@Microsoft.com
Technology Solutions Professional - Enterprise Mobility+Security

# How much control do you have?

Hybrid data = new normal
It is harder to protect

Identity, device management protection

Perimeter protection



# The evolution of Azure RMS


Classification & labeling

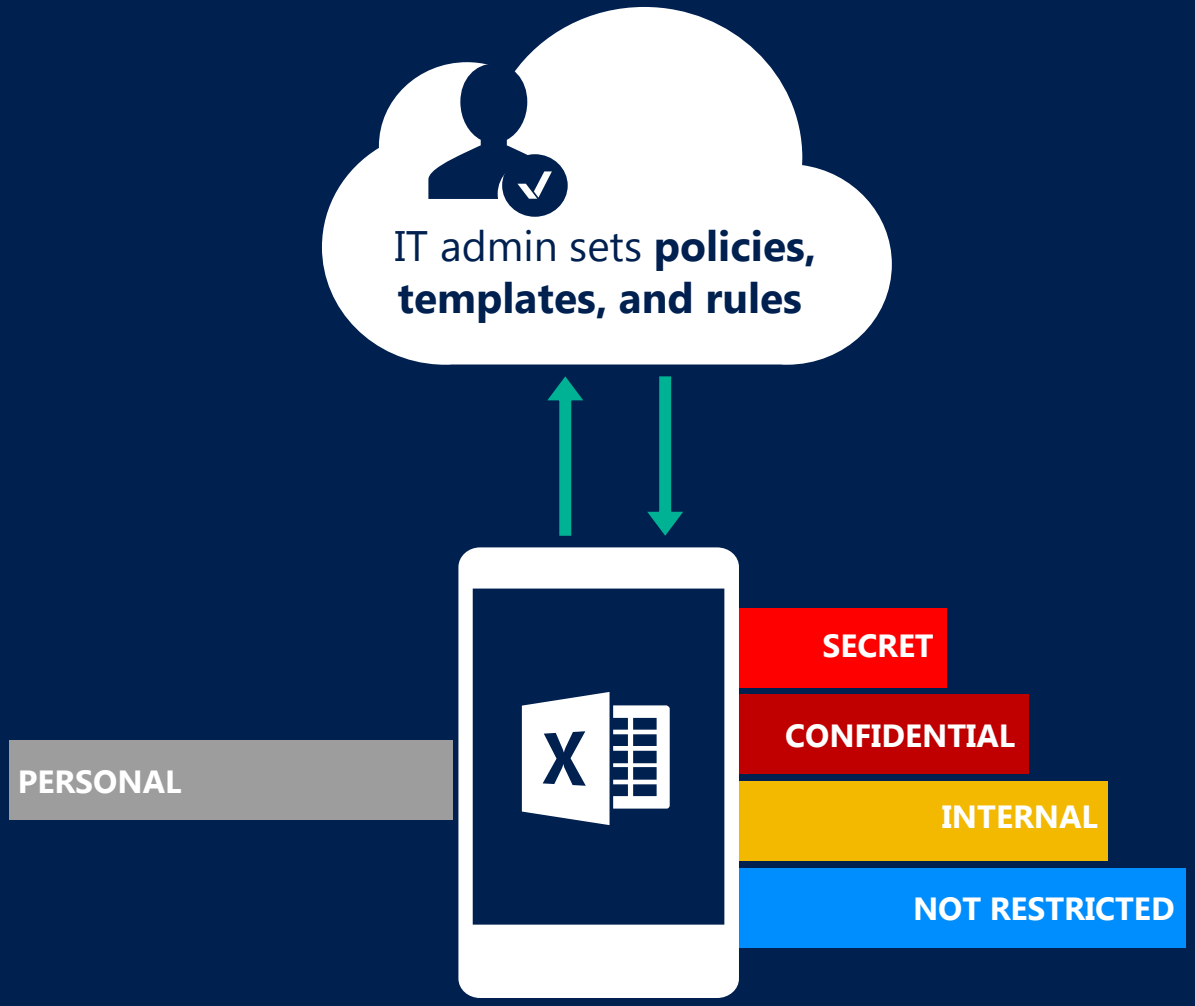
Protect

Monitor & respond

# The evolution of Azure RMS

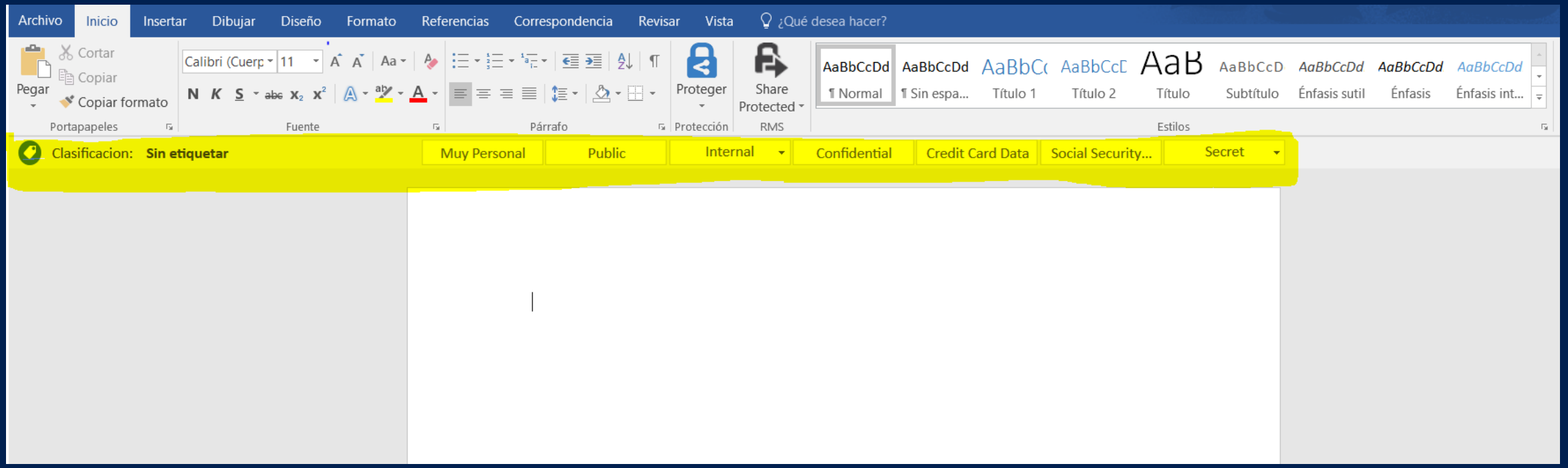
# Classify Data – Begin the Journey

## Classify data based on sensitivity




- Start with the data that is most sensitive
- IT can set automatic rules; users can complement it
- Associate actions such as visual markings and protection

# Classification



# How Classification Works

## Automatic

Policies can be set by IT Admins for automatically applying classification and protection to data

## Recommended

Based on the content you're working on, you can be prompted with suggested classification

## Reclassification

You can override a classification and optionally be required to provide a justification

## User set

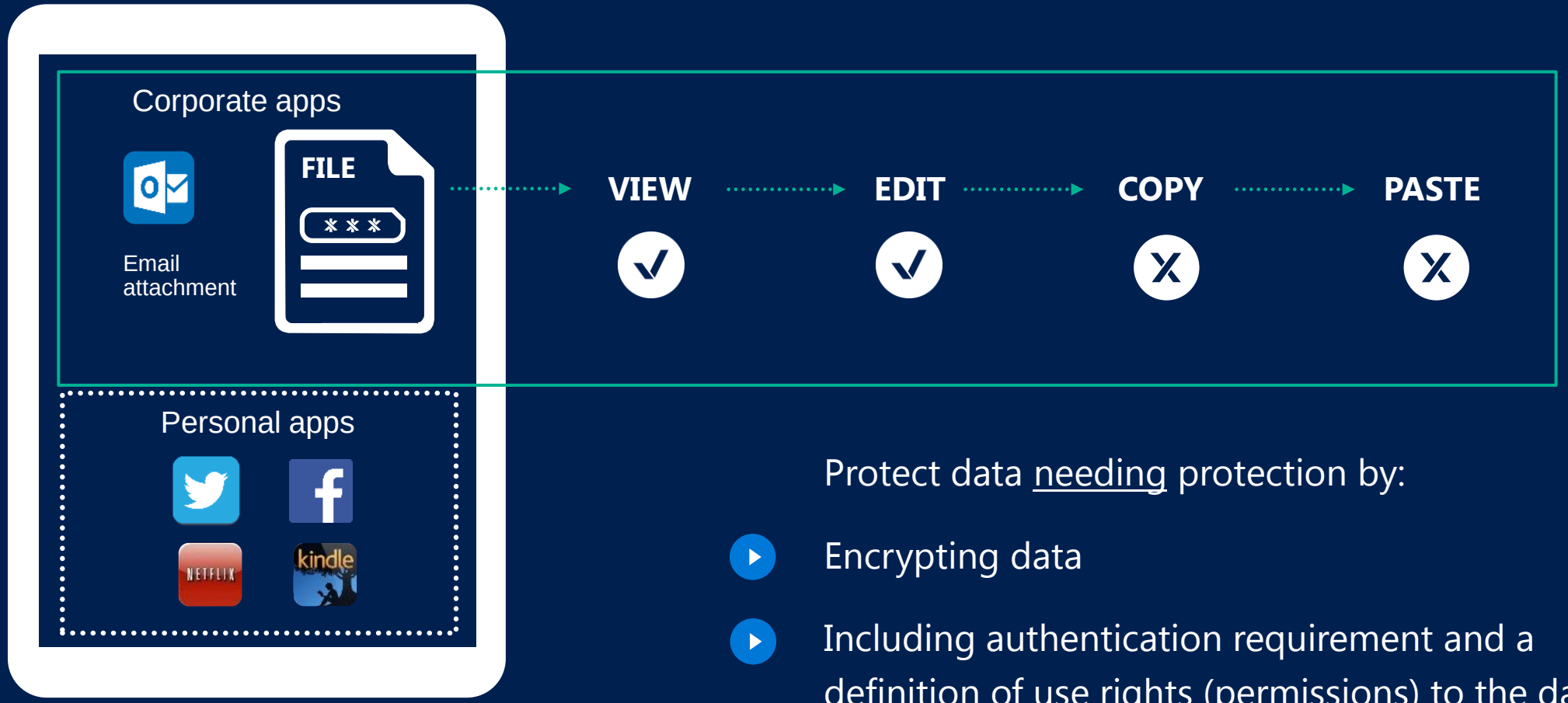
Users can choose to apply a sensitivity label to the email or file they are working on with a single click

# **Apply labels** based on classification

## Persistent labels that travel with the document


- Labels are metadata written to documents
- Labels are in clear text so that other systems such as a DLP engine can read it

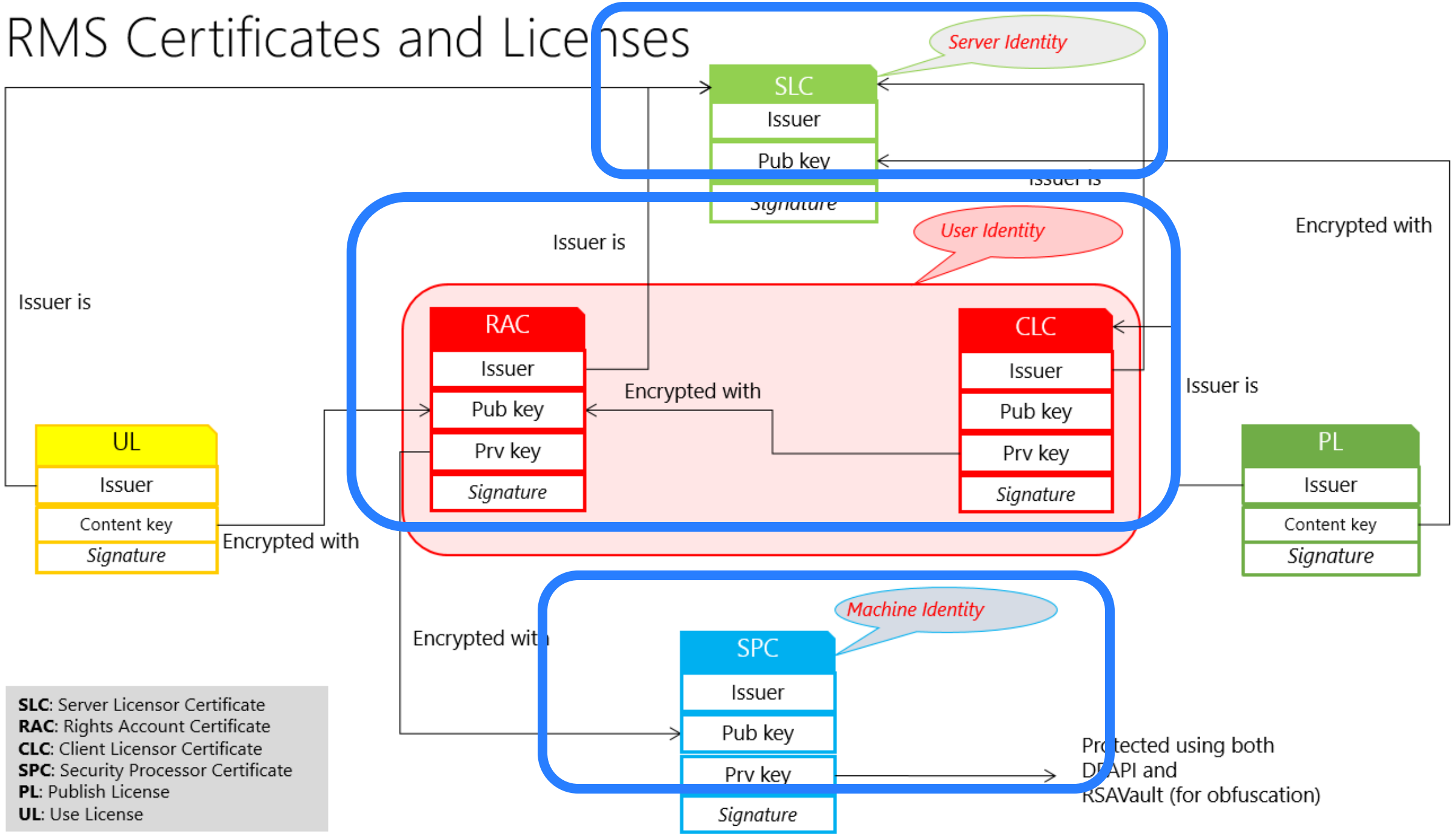
# **Protect data** against unauthorized use




Protect data <u>needing</u> protection by:

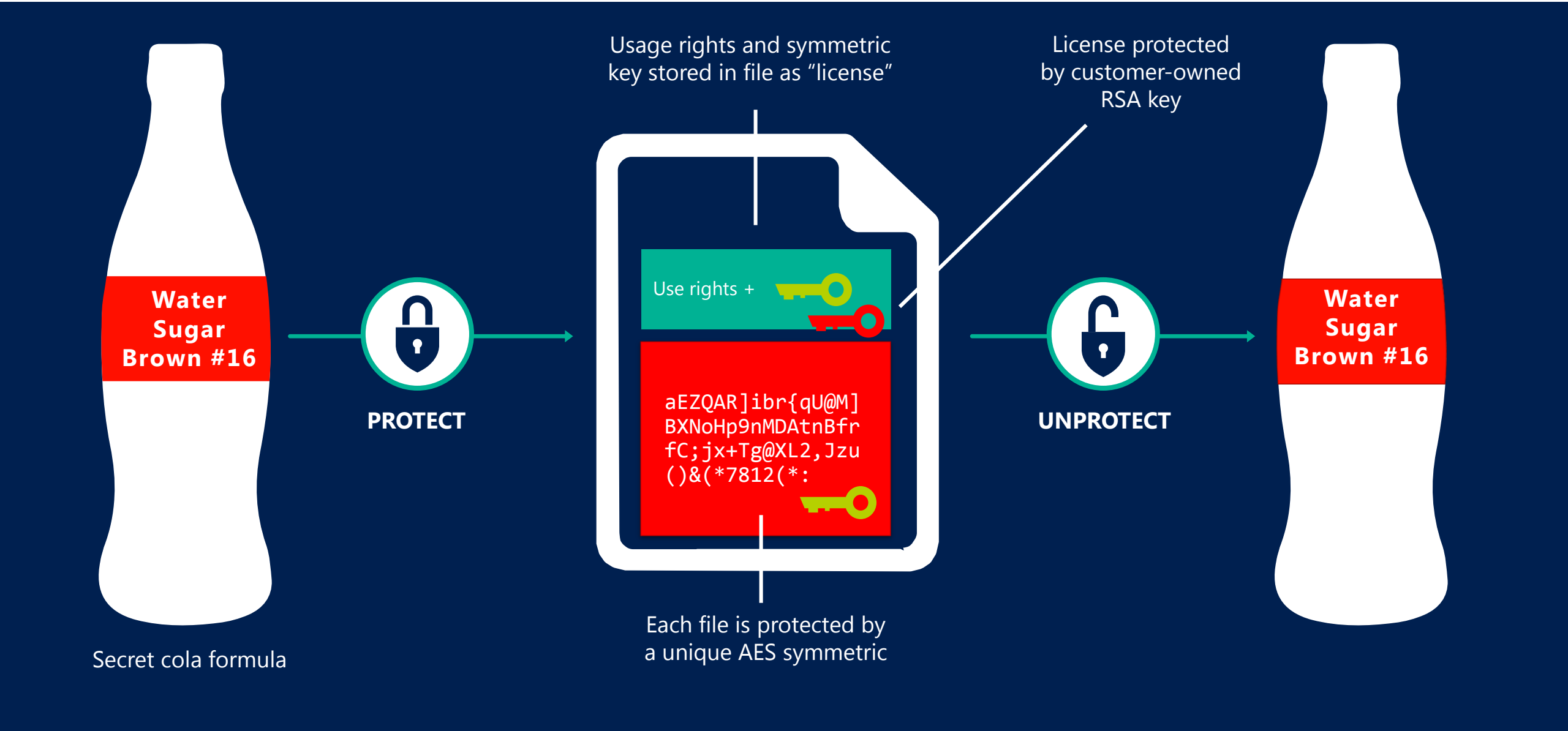
- Encrypting data
- Including authentication requirement and a definition of use rights (permissions) to the data
- Providing protection that is persistent and travels with the data

# RMS Certificates and Licenses



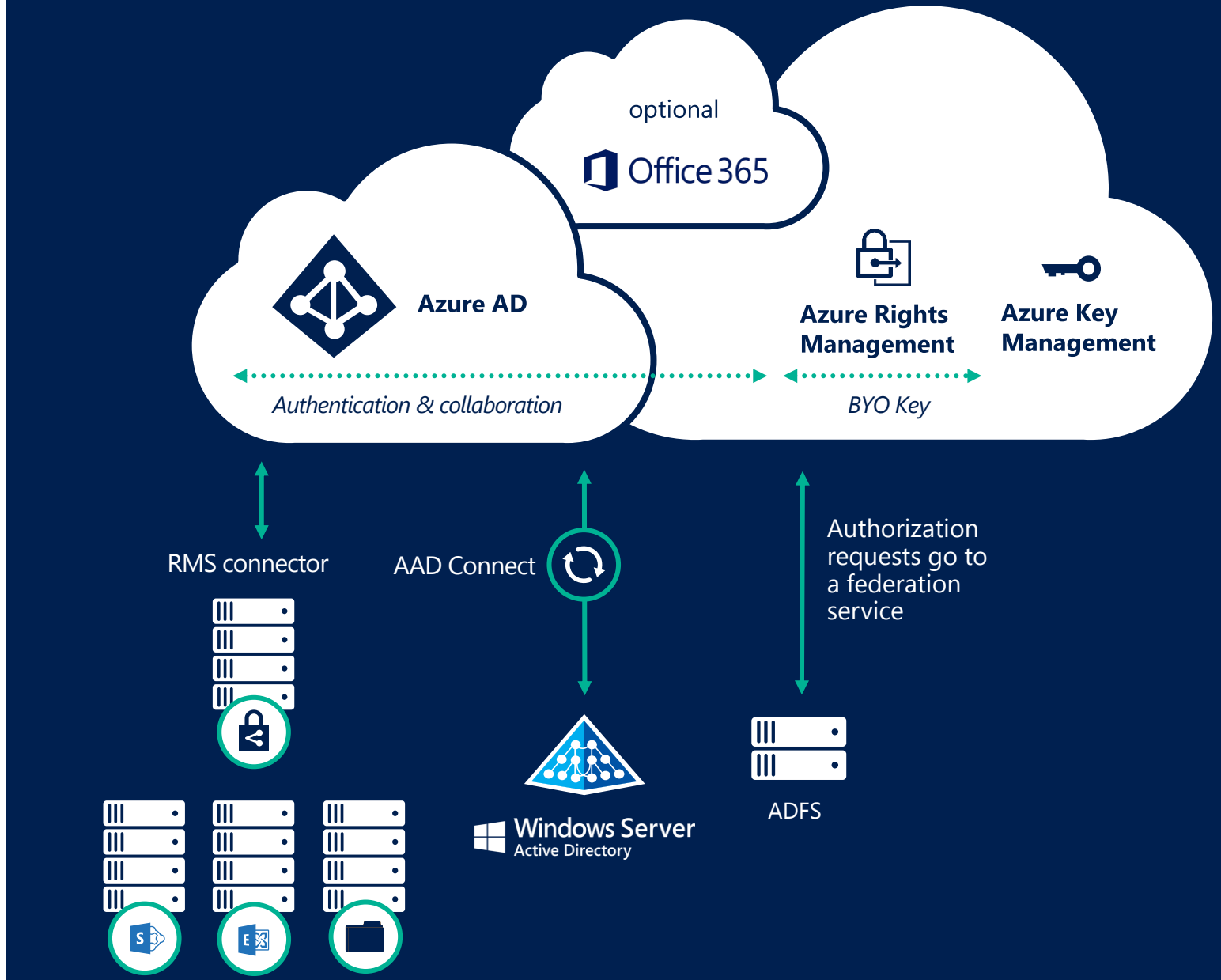

**SLC**: Server Licensor Certificate
**RAC**: Rights Account Certificate
**CLC**: Client Licensor Certificate
**SPC**: Security Processor Certificate
**PL**: Publish License
**UL**: Use License

# How Protection Works

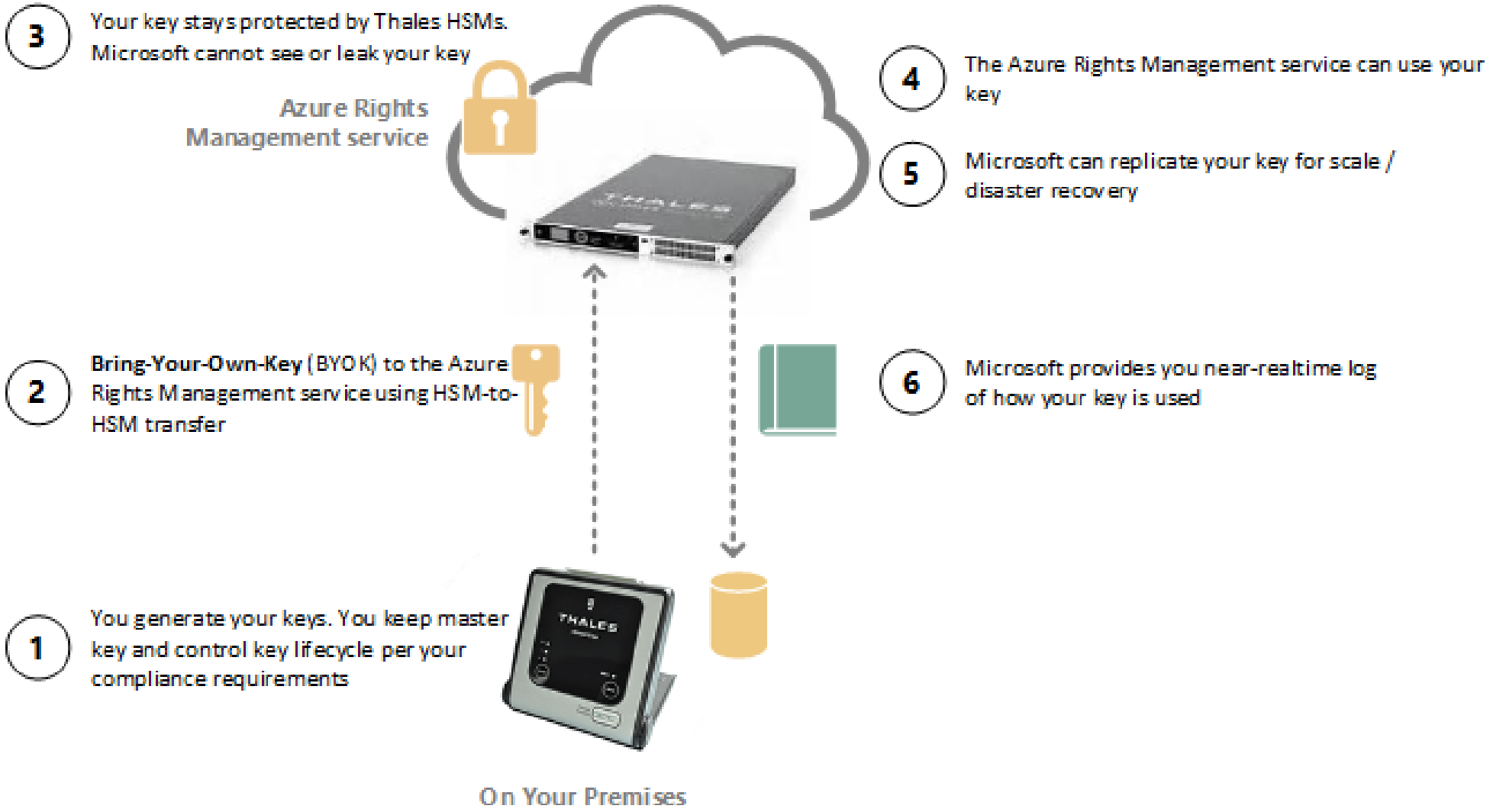


# Topology

- Data protection for organizations at different stages of cloud adoption
- Ensures security because sensitive data is never sent to the RMS server
- Integration with on-premises assets with minimal effort

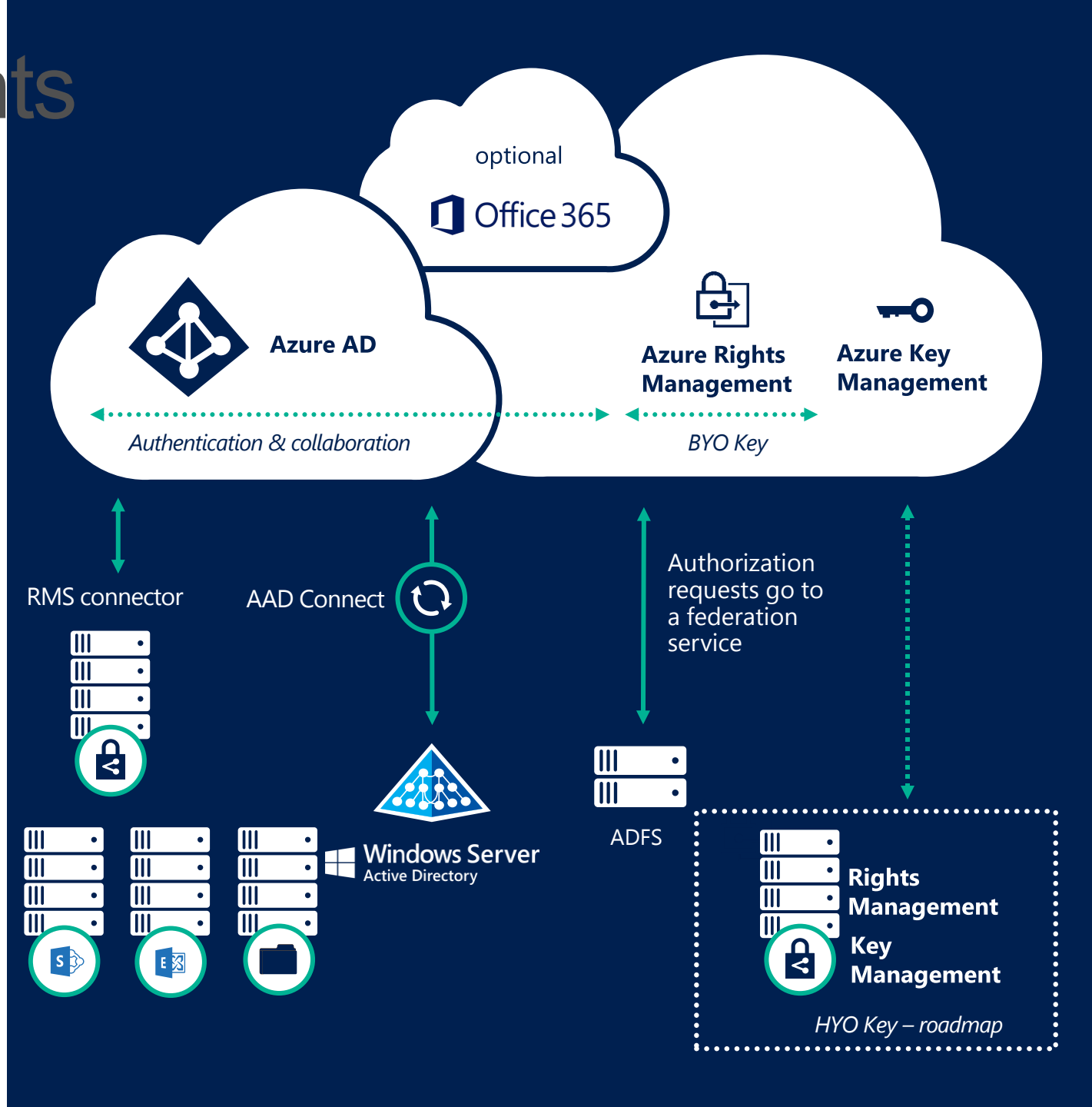


# Bring Your Own Key



# Regulated Environments Topology

- Data protection for organizations at different stages of cloud adoption
- Ensures security because sensitive data is never sent to the RMS server
- Integration with on-premises assets with minimal effort
- Hold your key on premises (roadmap)



# Resources

**Follow** @ https://twitter.com/TheRMSGuy

**Technical Documentation** @ https://docs.microsoft.com

**For questions email** AskIPteam@Microsoft.com

**IT Pro Blog** @ https://blogs.technet.microsoft.com/enterprisemobility/

Download @ https://www.microsoft.com/en-us/download/details.aspx?id=53018

Product page @ https://www.microsoft.com/en-us/cloud-platform/azure-information-protection

© 2016 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.