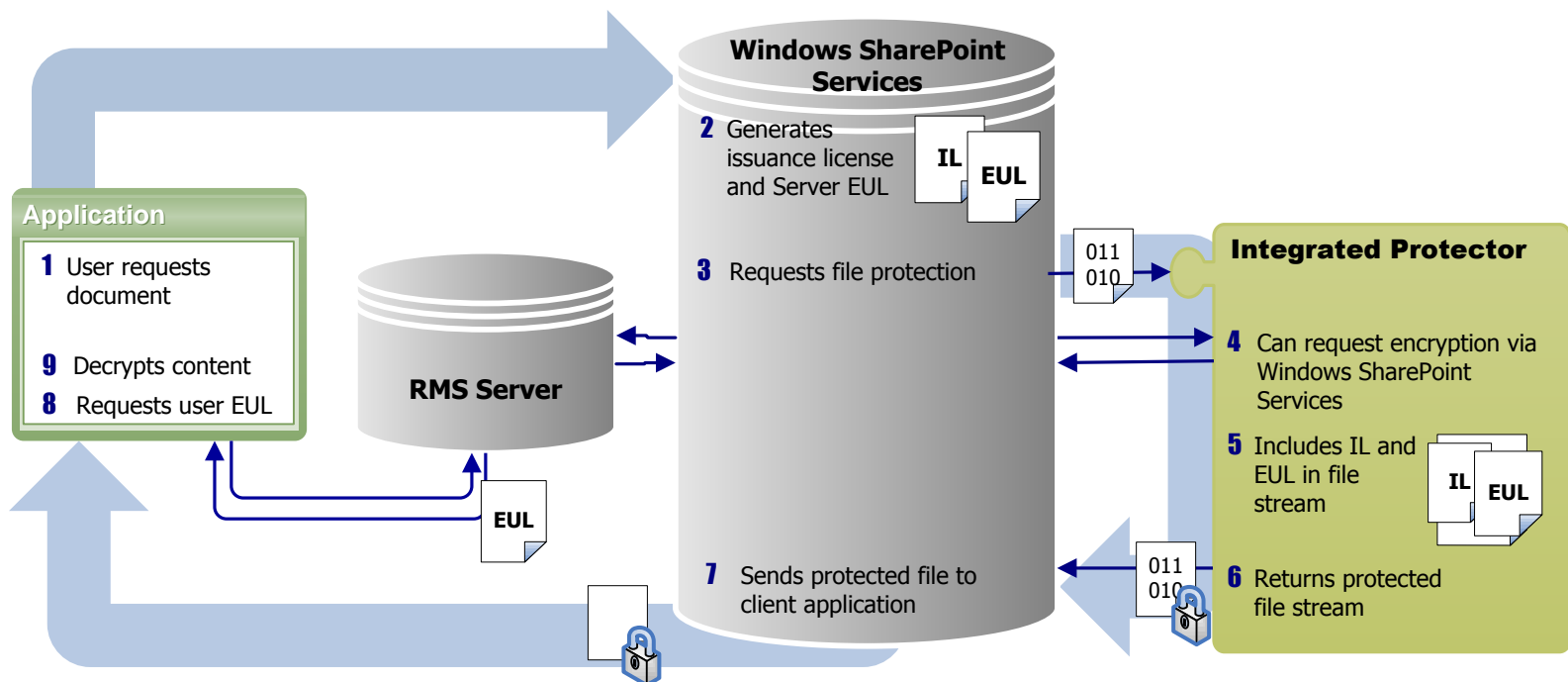


Information Rights Management in Windows SharePoint Services 3.0

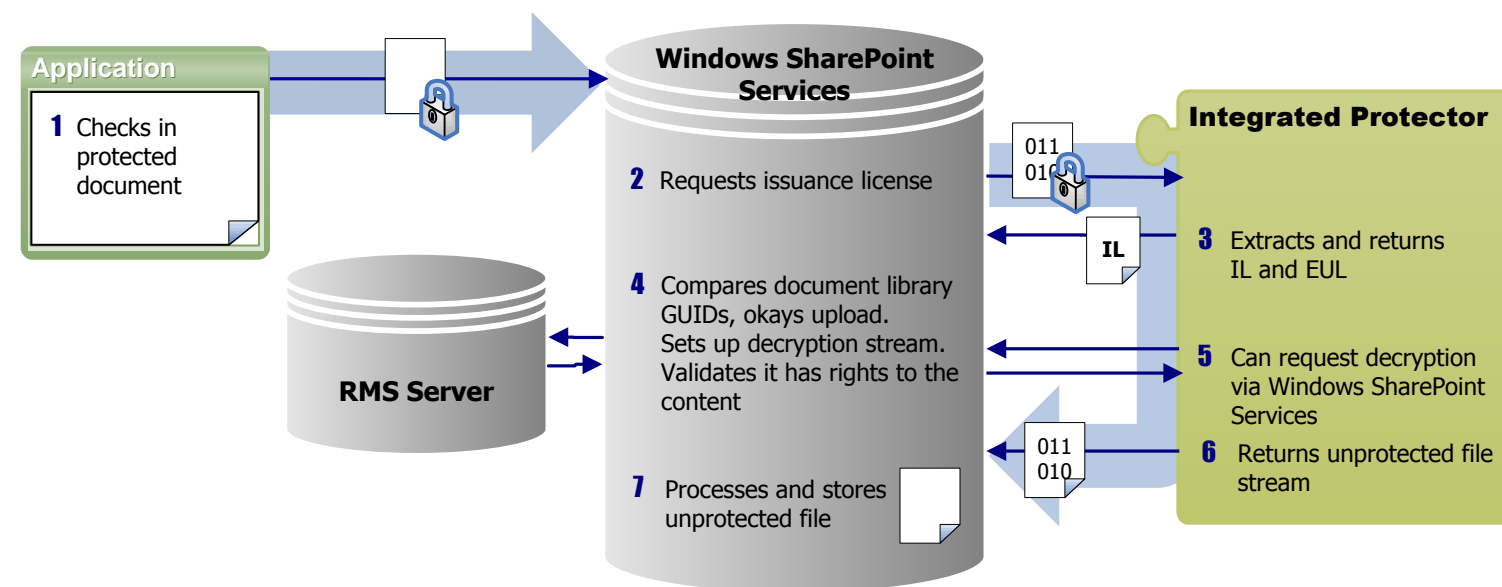
Microsoft® Windows® SharePoint® Services 3.0 enables administrators to apply Microsoft Information Rights Management (IRM) to document libraries and item attachments. IRM lets you create a persistent set of access controls that live with the content, helping you control access to files even after a user downloads them. You can even create IRM protectors, custom assemblies that plug into the IRM framework in Windows SharePoint Services and control the conversion of your custom file types to and from their encrypted, rights-managed formats. You can create two types of custom protectors:

Integrated Protectors Integrated protectors use Windows SharePoint Services to access the Windows Rights Management Services (RMS) platform in order to generate protected versions of files, and to remove protection from rights-managed files.

When a user requests a document of a file type that is rights-managed by an integrated protector, Windows SharePoint Services generates an issuance license (IL) and end user license (EUL) for the document. The integrated protector generates a protected file stream of the document that includes the IL and EUL; the protector can request RMS encryption through Windows SharePoint Service to accomplish this.

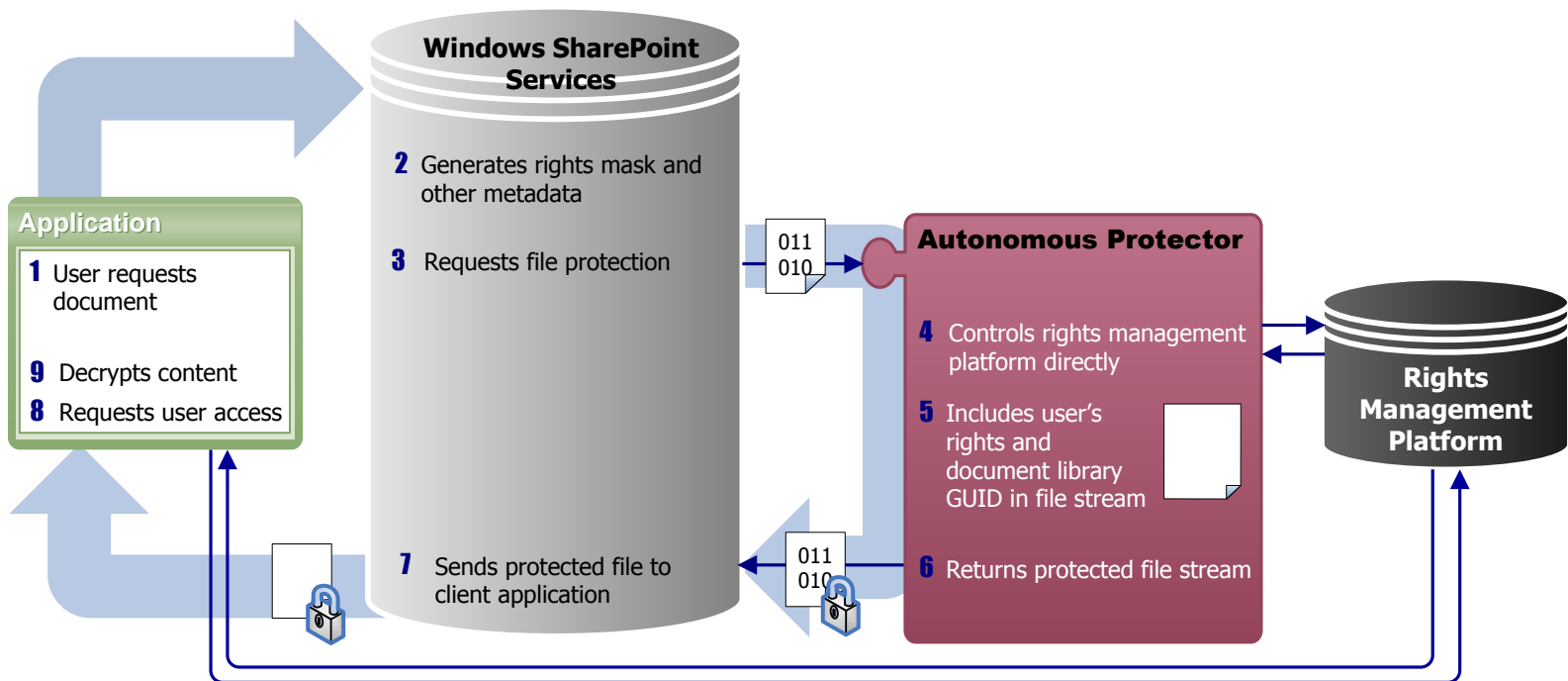


When a user uploads a document of a file type that is rights-managed by an integrated protector, the protector extracts the IL and passes it to Windows SharePoint Services, which compares the document library GUID in the IL with the target library GUID to ensure the file belongs in the target library. The protector then generates an unprotected file stream of the document, requesting RMS decryption through Windows SharePoint Service if necessary.



Autonomous Protectors Autonomous protectors, on the other hand, configure and execute the entire rights-management process by themselves.

When a user requests a document of a file type that an autonomous protector rights manages, Windows SharePoint Services provides the protector rights data and other document metadata, which the protector uses to configure and execute its own rights-management process to produce a rights-managed version of the requested file.



When a user uploads a document of a file type that is rights-managed by an autonomous protector, the protector passes the document library GUID back to Windows SharePoint Services, which uses it to ensure the file belongs in the target library. The protector then generates an unprotected file stream of the document, configuring and executing the decryption process itself.

