Microsoft's Information Protection Software Development Kit Manual

By: Marhawe Asmerom

Microsoft Information Protection Software Development Kit Manual

The Microsoft Information Protection Software Development Kit (SDK) is the unification of classification, labeling, and protection services from Microsoft. Primarily used for third-party applications the kit allows for developers to use the SDK to build support for labels and client workstation. The utilization provides a security net for their applications to be secure from data breaches. The ability to be used cross-platform including Windows, macOS, and Ubuntu provides versatility and easy access to the product. This user manual contains a deep set of instruction, scenarios, and technical design description for the Microsoft Information.[i]

Technical Description

Microsoft Information Protection Software Development Kit is a software that can be used by organization's developers to protect their private information including financial reports, employee records, and company secrets. The SDK was initially released January 15, 2019 since then it has gone through its eleventh update with the most recent version released in August of 2021. The version being strictly for first-party usage it has broaden their services to provide meaningfully protection for third-party applications. [ii]

With the recent advancement in the software, it is easy accessible to download from the internet where nine different platforms are supported. Comprised of three separate software development kits including the Protection SDK, File SDK, and Protection SDK which are all tasked with different components of the overall Microsoft Information Protection SDK. It is important to note that these three software development kits can be used separated for their different capabilities. To get full functionality of software make sure to download all parts of the SDK. The three components cohesively come together before to provide effectively protection for private information.

Description of Components and Their Use Cases

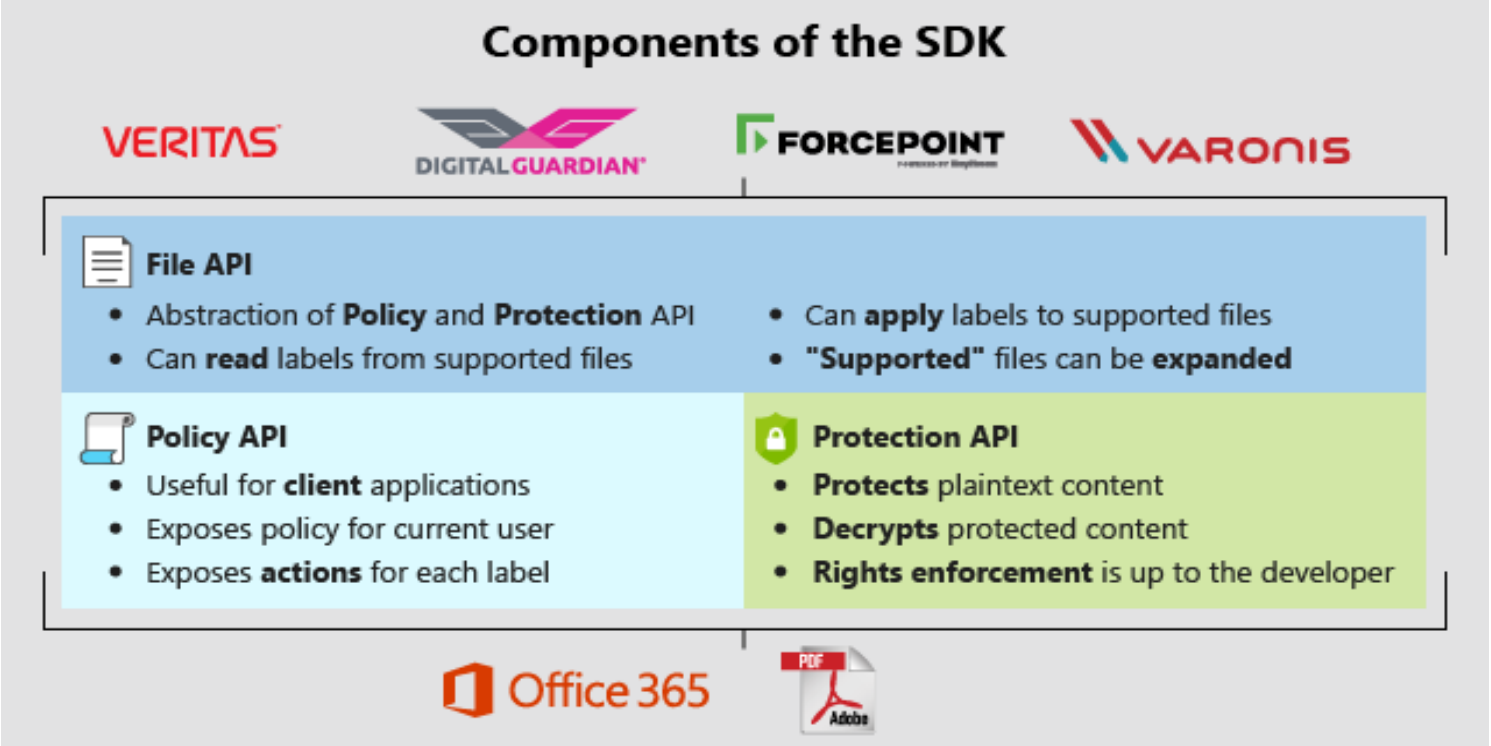

Figure 1 : Components of the SDK

Figure 2: Venn Diagram of MIP

File API Software Development Kit:

This is the main layer of the Microsoft Information Protection SDK. As the most commonly used component of SDK it is an abstraction of the other two APIs. It provides a simple interface to help read and assign labels to different file types. Labels are defined as the level of confidentially of the document being read.

Use Case – As a software engineer at a large corporation. To make sure the employees records and personal information are being protected and labeled on export based on the contents. While using the File API, you can check labels available then place the appropriate label. (Figure 1)[iii]

Policy API Software Development Kit:

The Policy SDK provides the developer an opportunity to retrieve labeling polices for a certain user. It essentially grabs the policy installed by the developer to retrieve the correct action. This component of the SDK is used mainly by client application because all it does is grab user policy.

Use Case – As a software engineer it is important to create a policy that based on contents it assigns labels and protections. When looking to apply labels in the application it is able display the list of labels, the users can select. The SDK exactly is what should be applied as far as content marking and protections. (Figure 1)[iv]

Protection API Software Development Kit:

Protection SDK provides the ability for software developers to protect content. The different protection actions including content marking, watermarking, rights enforcement for authorized users, and read only protections help contain sensitive information.

Use Case – As a financial institution looking to protect their customers banking records. You want to use the Protection SDK to create protection actions to disable printing of the file by unauthorized users. This protection of a content marking can make the information difficult for unauthorized consumers of the information. (Figure 1)[v]

Operating Description

The Microsoft Information Protection SDK is an effective, accessible way for users to develop policy to protect sensitive data. When all three components come together it creates a development kit that creates a safe environment for your data. With numerous uses case for each component it is important to realize how versatile the application is. When user downloads the application, they will be able to configure their application based on their personal and organizational needs.

Instructions

This section will provide the user with a detailed description of how to develop the Microsoft Information Protection SDK. It will detail how to configure your sensitive labels, client workstation, and register client application with Azure Active Directory. After the developer reads through this manual, they will have a good understanding of how to easily configure the Microsoft Information Protection SDK.

Prerequisites for Installing of Microsoft Information Protection

- Office 365 subscription – Microsoft 365 E3/E5, Enterprise Mobility and Security, Azure Information Protection Premium
- Policy configured in Office 365 Security and Compliance Center
- Visual Studio
- Platform / Operating System – Ubuntu, RedHat, Debian, macOS, Windows, Android, iOS
- Support Unified Labels [vi]

Directions

Follow the directions carefully to ensure proper use of the Microsoft Information Protection SDK.

Configure Sensitivity Labels

1. Install policies in an all advanced settings after your label including Microsoft 365 compliance center
2. For each label, the Azure portal displays only the display name which can be edited. The display name can be different from the label that is produced.
3. Once in the compliance center configure your sensitivity labels by adding protections at each level.
4. These protections will be used based on the contents found by Microsoft Information Protection SDK
5. Depending on the content it will be result in a protection action and label that is deemed necessary[vii]

Configure your client workstation

1. If you are using a Windows 10 workstation make sure to update your machine to the current version update.
2. Ensure Developer is enabled on your workstation by selecting the setting under “use developer features”
3. Install Visual Studio with the following tools and workloads. C++ Universal Windows Platform Development. Refer to the image below to see what optional workloads can be added for the development of the SDK. (Figure 3)

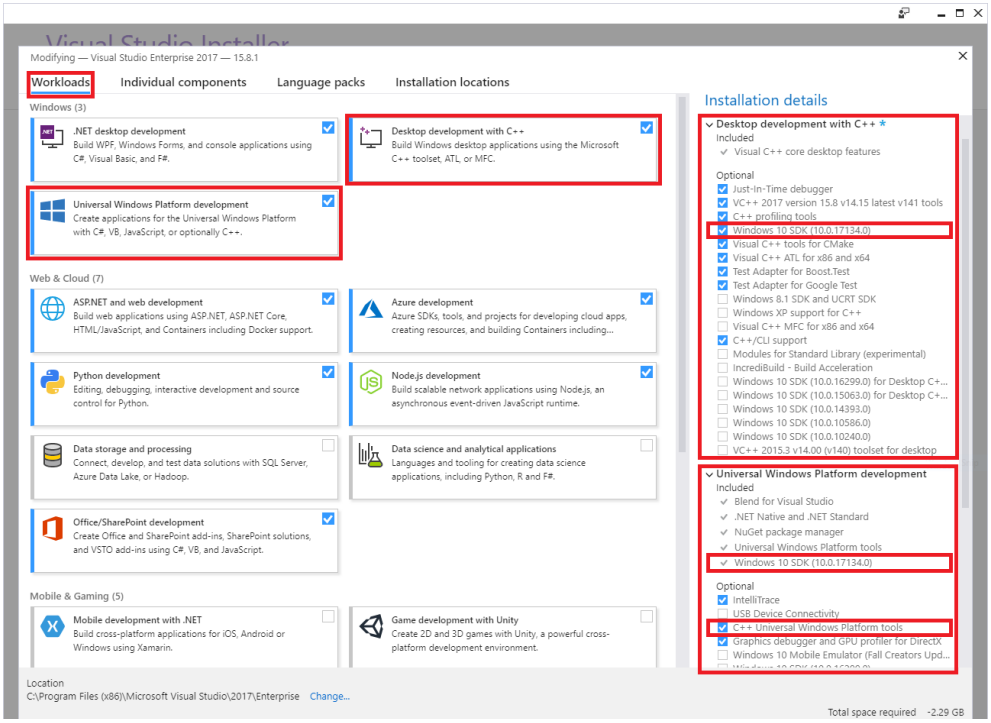

Figure 3 - MIP SDK Optional Workloads

4. Install the ADAL.PS Module by running the “install-module –name adal.ps” in the command prompt / terminal
5. Download the Files for the SDK based on the workstation operating system – refer to the perquisites to see what platforms are supported. [viii]

Register a client application with Azure Active Directory

1. Sign into the Azure portal with an active subscription and authorized application users.
2. Use the Directories + subscriptions filter to select the Azure Active Directory.
3. Under App Registrations select New Registrations then enter a display name for the application.
4. Specify who can use the application that is made and then register to complete the initial app registration. (Figure 4)

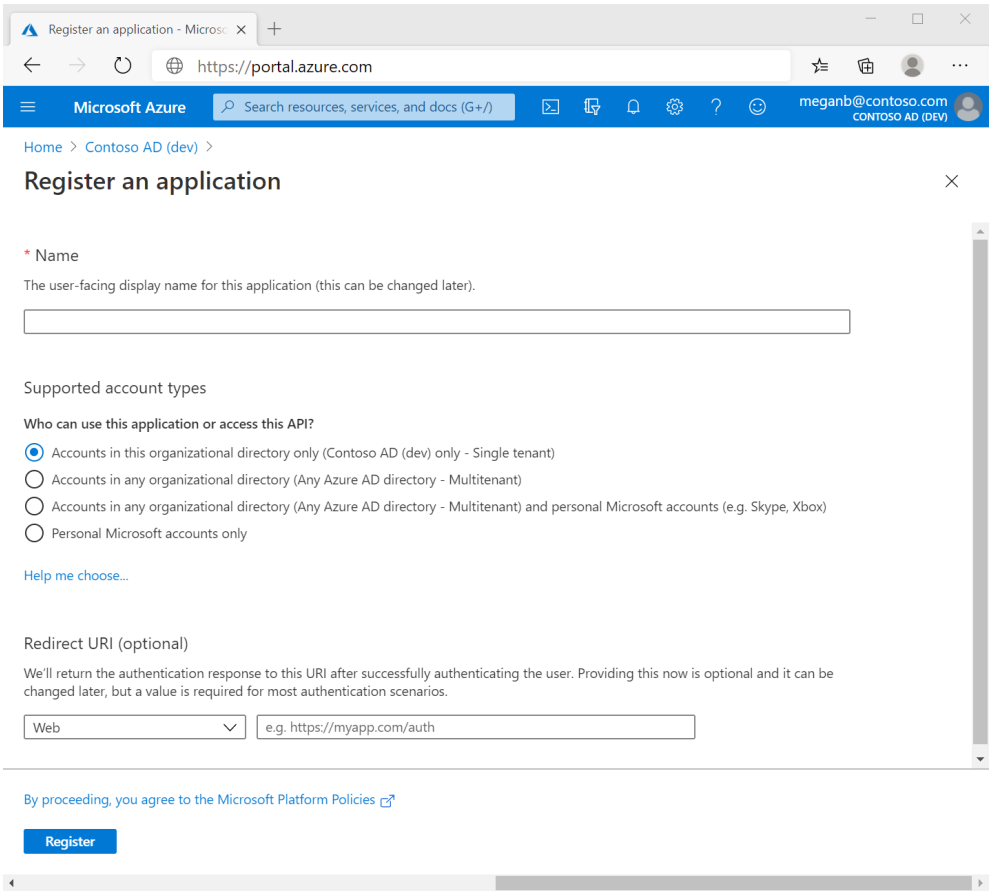

Figure 4: Register Application

5. Once configured figure out your platform settings for each application type by adding the platforms configuration under the add a platform tab. [ix]

Glossary

Azure Active Directory – enterprise identity service provides single sign-on, multifactor authentication, and conditional access to guard against 99.9 percent of cybersecurity attacks.

Command Prompt – the input field in a text-based user interface screen for an operating system or program

Content Marking – include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

First – Party – when the application or service is being used internally in this case in would Microsoft services

Interface – a device or program enabling a user to communicate with a computer

Microsoft Compliance Center – provides easy access to the data and tools you need to manage to your organization's compliance needs.

Operating System / Platform – system software that manages computer hardware and software resources.

Policy – how the developer decides retrieve the label based on the content found in the file

Sensitive Labels – Sensitivity labels are a means to classify your organization’s data in a way that shows how sensitive the data is.

Third-Party – when the application or service is being used externally elsewhere

Works Cited

[i] Moser, T. *Overview - Microsoft Information Protection SDK*. Microsoft Information Protection SDK. | Microsoft Docs. Retrieved February 27, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/overview

[ii] Moser, T. (2022, February 25). *Microsoft Information Protection (MIP) SDK version release history and support policy*. Microsoft Information Protection (MIP) SDK version release history and support policy | Microsoft Docs. Retrieved February 27, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/version-release-history

[iii] Moser, T. (2021, August 31). *Concepts - apis in the MIP SDK*. Concepts - APIs in the MIP SDK. | Microsoft Docs. Retrieved March 1, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/concept-apis-use-cases#file-sdk-use-cases

[iv] Moser, T. (2021, August 31). *Concepts - apis in the MIP SDK*. Concepts - APIs in the MIP SDK. | Microsoft Docs. Retrieved March 1, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/concept-apis-use-cases#policy-sdk-use-cases

[v] Moser, T. (2021, August 31). *Concepts - apis in the MIP SDK*. Concepts - APIs in the MIP SDK. | Microsoft Docs. Retrieved March 1, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/concept-apis-use-cases#protection-sdk-use-cases

[vi] Moser, T. (2021, November 20). *Microsoft Information Protection (MIP) SDK setup and configuration*. Microsoft Docs. Retrieved February 28, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/setup-configure-mip#sign-up-for-an-office-365-subscription

[vii] Didin, G. (2022, February 7). *Migrate azure information protection labels to Unified Sensitivity Labels - AIP*. Migrate Azure Information Protection labels to unified sensitivity labels - AIP | Microsoft Docs. Retrieved February 28, 2022, from https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-migrate-labels

[viii] Moser, T. (2021, November 30). *Microsoft Information Protection (MIP) SDK setup and configuration*. Microsoft Docs. Retrieved February 28, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/setup-configure-mip#configure-your-client-workstation

[ix] Moser, T. (2021, November 30). *Microsoft Information Protection (MIP) SDK setup and configuration*. Microsoft Docs. Retrieved February 27, 2022, from https://docs.microsoft.com/en-us/information-protection/develop/setup-configure-mip#register-a-client-application-with-azure-active-directory