# Windows Hello白皮书

## Windows Hello

Windows Hello是一种生物特征鉴权方式，它为生物特征鉴权带来系统支持，通过使用你的脸部、虹膜或指纹等生物特征来解锁设备。有了它，您可以方便地访问自己的Windows10设备。这种技术比传统密码更加安全。用户就是可以解锁Windows、应用、数据甚至网站和服务的密码，而不是使用容易被忘记、被破解或随手写下的一串随机排列的字母或数字。

Windows Hello 要求硬件方面的支持，通过硬件加软件的方式实现生物特征的识别和鉴权，对于虹膜、指纹需要扫描器等常规硬件，对于脸部生物特征的目前支持RealSense 摄像头设备。

## Microsoft Passport

Microsoft Passport用来为用户提供一个安全的登录方式。通过它，您可以安全地登录到系统、应用、网站和网络。Windows10可以帮助用户在不使用密码的前提下安全地为系统、应用、网站和网络授权。

Microsoft Passport可使用户对Microsoft账户、Active Directory账户、Microsoft Azure Active Directory(AD)账户或支持Fast ID Online(FIDO)身份验证的非Microsoft 服务进行身份验证。

Microsoft Passport的优点：

* 便利性。用户提供凭据（例如账户和密码，或其他凭据），然后系统将指导他设置Microsoft Passport和Windows Hello。设置成功后，用户既可以通过生物特征来登录访问资源，而不使用易被盗取和破解的凭据。
* 安全性。Microsoft Passport有助于保护用户身份和用户凭据。由于不使用任何密码，它有助于避开网络钓鱼和暴力攻击。除此之外，他还有助于防止服务器功能损坏，因为Microsoft Passport凭据是不对称的密钥对，这有助于在受信任平台模块（TPM）的隔离环境内生成这些密钥时阻止重播攻击。

## Windows Hello 与 Microsoft Passport的关系

在Windows10中,Windows Hello和Microsoft Passport结合在一起为,Microsoft Passport将用户的鉴权信息通过系统加密保存起来，用于系统级别的安全认证。

简单的来讲，Microsoft Passport用来加密、存储用户的鉴权信息。Windows Hello用来识别用户的生物特征。我们可以使用Windows Hello读取用户的生物特征，将用户的鉴权信息保存在Passport里面，并且建立生物特征与用户鉴权信息的关联。在用户登录时，用户通过生物特征即可查找对应的密码完成鉴权登录。

**工作原理：**

Passport凭据是不对称的密钥对，它是在系统受信的隔离环境内生成的。而Windows Hello是系统通过设备采集的生物特征，采集成功后，会返回一个唯一的用户ID。系统将用户ID与Passport的密钥存储在系统隔离区内，在用户登录时，如果生物特征识别成功，系统会根据用户ID来查找密钥并验证授权登录。

## 动手实验

Windows 10 SDK为开发者提供了Windows Hello的API。开发人员通过这些API，可以构建自己的安全策略，将自己的鉴权系统与Windows Hello相结合，开发更炫酷的应用。

## 通过示例您将学会

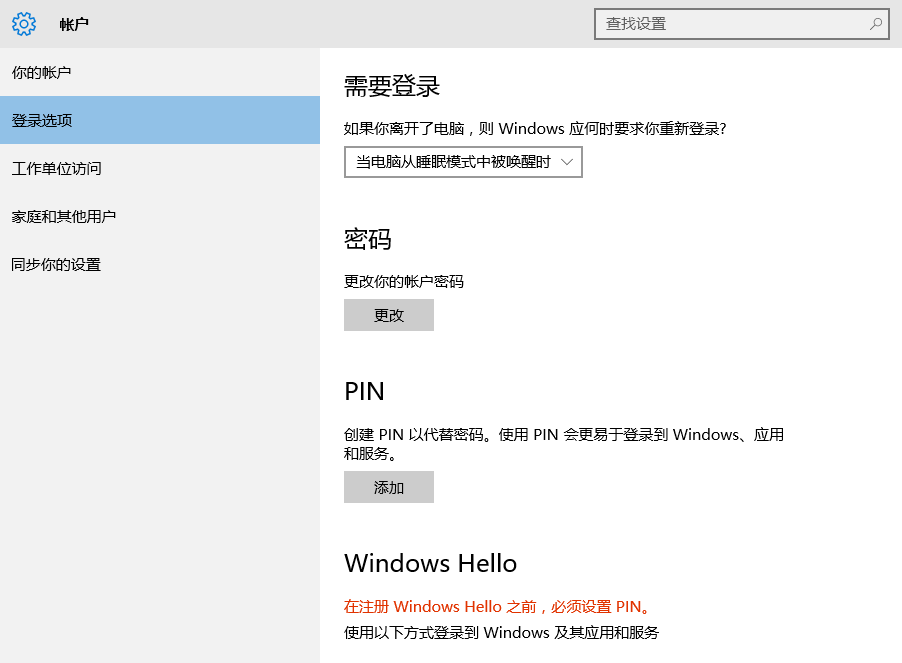
* 本地密码凭据管理。凭据创建、凭据获取。
* Windows Hello启用。PIN码使用。

## 准备工作

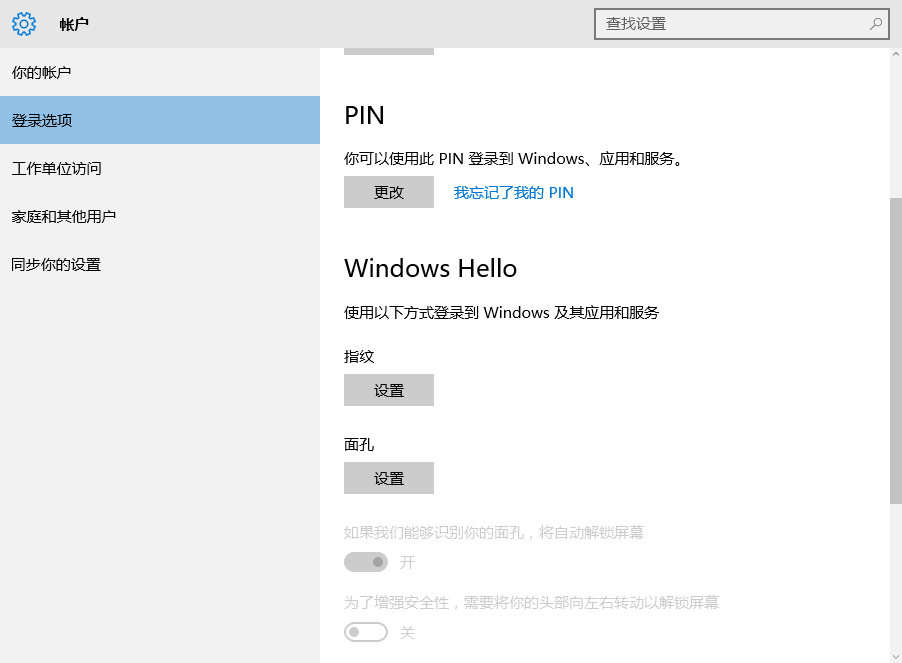
Windows 10 要求必须在包含生物特征传感器的设备上启用PIN码，才能使用Windows Hello来管理登录凭据。下面，我们来演示如何启用PIN码。（如果您的已启用PIN码，请忽略这个段落的内容）

**设置PIN码**

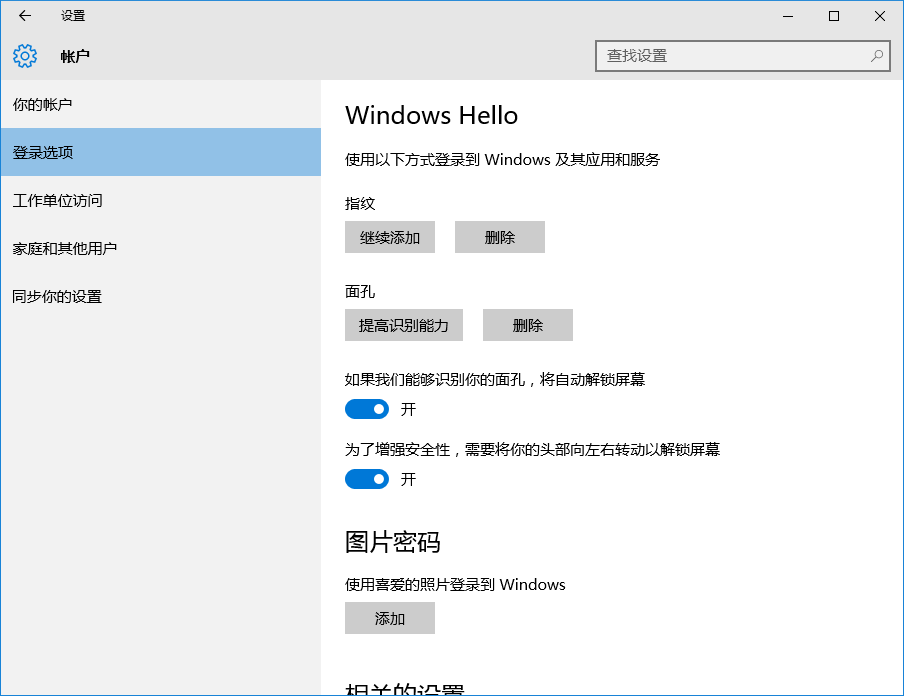
打开“开始”菜单，点击设置-登录选项。



在“登录选项”面板下，添加一个PIN码后，即可开启Windows Hello。



在Windows Hello 选项下面，我们可以设置指纹、面孔，通过设备的传感器来采集我们的生物特征。



## 挑战

我们将使用Visual Studio 2015 打开SimpleHello项目，来学习Windows Hello相关API。

— 打开SimpleHello项目。

## 创建场景

### 场景描述

在这个场景里面，主要演示了如何使用Windows Hello API来管理账户凭据，该场景演示了一个银行账户的登录过程。用户在首次登录时，应用程序会检测当前设备是否支持Windows Hello。如果设备支持，应用程序会使用将当前账户凭据，来创建本地的密码凭据。用户在下次登录时，可以通过传感器设备来验证生物特征，同时读取并验证本地凭据，当凭据验证成功后，用户可以直接登录并看到银行账户的详细情况。

## Windows Hello的登录过程，用户可以选择脸部特征识别、虹膜识别、指纹识别三种方式来认证，指纹识别需要指纹输入设备，虹膜识别在需要虹膜识别摄像头，脸部特征识别则需要人脸识别摄像头，目前支持的硬件有Intel RealSense F200设备。 Intel RealSense（F200）3D摄像头简介：

Windows Hello支持Intel RealSense(F200) 3D摄像头，用于人脸识别。RealSense 3D是一套实感计算解决方案，它配有深度传感器和全1080p彩色镜头，能够精确识别手势动作、面部特征、前景和背景，进而让设备理解人的动作和情感，该设备还可以对物体实现三维扫描。

Intel RealSense的驱动及SDK下载地址：<https://software.intel.com/zh-cn/intel-realsense-sdk/download>

**注意：RealSense 驱动需要安装intel\_rs\_dcm\_f200\_1.4.27.41944 及以上版本。RealSense需要USB3.0的支持，在脸部特征识别过程中需要保证USB对RealSense设备供电。有些电脑硬件对RS F200不识别，则无法安装驱动，也无法实现Windows Hello中的人脸识别。**

### 知识点

Windows Hello 密钥凭据管理是使用Windows.Security.Credentials命名空间下的KeyCredentialManager类。

**KeyCredentialManager类，该类用于本地秘钥凭据的管理。主要方法如下：**

**RequestCreateAsync(System.String name, KeyCredentialCreationOption option)**：用于创建本地凭据，该方法返回密码凭据的一个检索结果类KeyCredentialRetrievalResult。（该方法会调用Windows Hello，通过本地生物特征识别来返回生物特征验证结果）

**KeyCredentialCreationOption**参数：是一个创建操作枚举，主要有ReplaceExisting(密码凭据存在则替换)、FailIfExists(密码凭据存在，返回错误)两个选项。

**OpenAsync(System.String name)**：根据密码凭据用户名打开本地密码凭据，该方法返回密码凭据的一个检索结果类KeyCredentialRetrievalResult。（该方法会调用Windows Hello，通过本地生物特征识别来返回生物特征验证结果）

**IsSupportedAsync()**：该方法返回一个布尔类型，用于判断当前设备是否支持Windows Hello。

**KeyCredentialRetrievalResult**：该类用于保存密码凭据的检索结果。它包含KeyCredential、KeyCredentialStatus两个属性。

**KeyCredentialStatus**：是一个枚举类，定义了密钥凭据的检索结果。

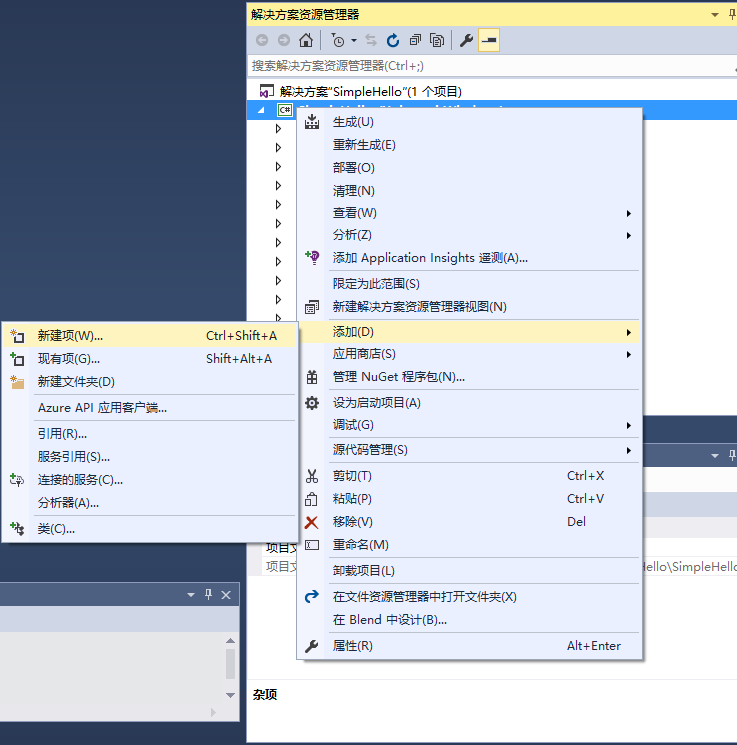
**KeyCredential**：该类用于保存秘钥凭据信息，主要方法如下：

**GetAttestationAsync()**：该方法返回一个鉴权认证结果。

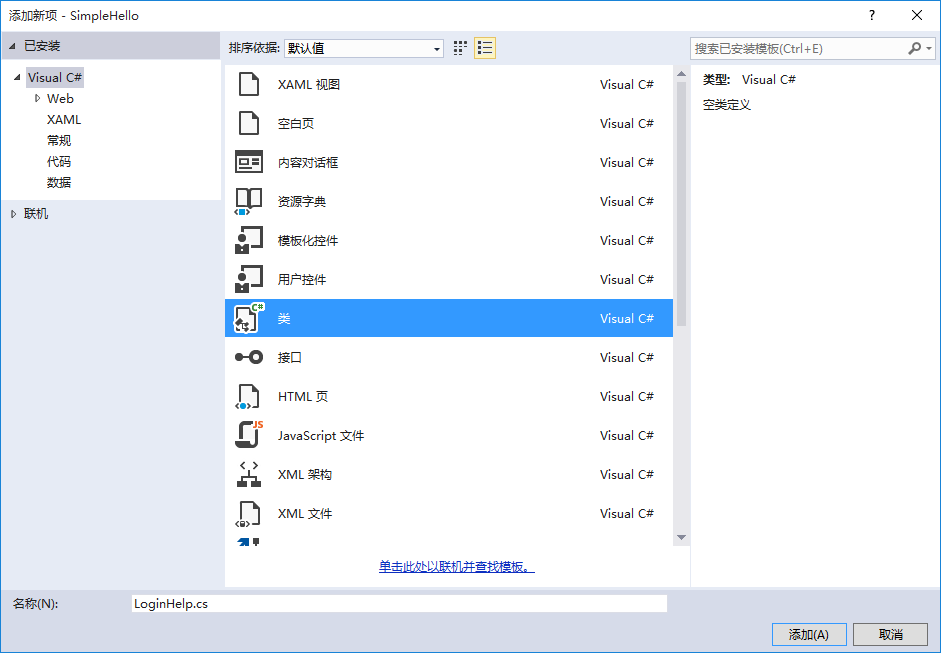
**RequestSignAsync(IBuffer data)**：该方法返回一个密码凭证验证结果。

### 创建登录辅助类

在“解决方案资源管理器”中，右键单击该项目SimpleHello。从“添加”菜单中，选择“新建项”



在左侧Visual C# 模板中，可以选择文件类型，我们添加一个“类”用来实现密钥的管理。基于我们的场景，我们建议的命名是LoginHelp.cs。它主要用于示例的登录辅助功能。



打开LoginHelp.cs 文件，添加密钥管理及登录相关方法，代码如下：

|  |
| --- |
| using System;  using System.Collections.Generic;  using System.Linq;  using System.Text;  using System.Threading.Tasks;  using Windows.Security.Credentials;  using Windows.Security.Cryptography;  using Windows.Storage.Streams;  namespace SimpleHello  {  public class LoginHelp  {  private Account activeAccount;  public LoginHelp(Account account)  {  this.activeAccount = account;  }  /// <summary>  /// The function called when the user wants to sign in with Passport but from  /// the username/password dialog.  ///  /// First we check if they already use Passport as their primary login method  ///  /// Otherwise we authenticate their username/password and then begin the Passport  /// enrollment process which consists of creating a Passport key and then sending that to  /// the authentication server.  /// </summary>  public async Task<bool> SignInPassport()  {  if (await AuthenticatePassport() == true)  {  SuccessfulSignIn(false);  return true;  }  else  {  return false;  }  }  /// <summary>  /// Username and password authentication  /// </summary>  /// <param name="isnewAccount">true:new user,false:old user</param>  /// <returns></returns>  public async Task<bool> SignInPassword(bool isnewAccount)  {  try  {  bool signedIn = await AuthenticatePasswordCredentials();  if (signedIn == false)  {  return false;  }  else  {  if(isnewAccount)  SuccessfulSignIn(true);  return true;  }  }  catch (Exception e)  {  return false;  }  }  /// <summary>  /// Authenticate user credentials with server and return result.  /// </summary>  /// <returns>Boolean representing if authenticating the user credentials with the server succeeded</returns>  private async Task<bool> AuthenticatePasswordCredentials()  {  // TODO: Authenticate with server once that part is done for the sample.  return true;  }  /// <summary>  /// Function to be called when we need to register our public key with  /// the server for Microsoft Passport  /// </summary>  /// <returns>Boolean representing if adding the Passport login method to this account on the server succeeded</returns>  public async Task<bool> AddPassportToAccountOnServer()  {  // TODO: Add Passport signing info to server when that part is done for the sample  return true;  }  /// <summary>  /// Attempts to get the authentication message from the Passport key for this account.  ///  /// This will bring up the Passport PIN dialog and prompt the user for their PIN.  ///  /// The authentication message will be null if signing fails.  /// </summary>  /// <returns>Boolean representing if authenticating Passport succeeded</returns>  private async Task<bool> AuthenticatePassport()  {  IBuffer message = CryptographicBuffer.ConvertStringToBinary("LoginAuth", BinaryStringEncoding.Utf8);  IBuffer authMessage = await GetPassportAuthenticationMessage(message, this.activeAccount.Email);  if (authMessage != null)  {  return true;  }  return false;  }  /// <summary>  /// Handles user saving for our list of users if this is a new user  /// </summary>  private void SuccessfulSignIn(bool isAdd)  {  // If this is an already existing account, replace the old  // version of this account in the account list.  if (isAdd == false)  {  foreach (Account a in UserSelect.accountList)  {  if (a.Email == this.activeAccount.Email)  {  UserSelect.accountList.Remove(a);  break;  }  }  }  UserSelect.accountList.Add(this.activeAccount);  AccountsHelper.SaveAccountList(UserSelect.accountList);  }  /// <summary>  /// Attempts to sign a message using the Passport key on the system for the accountId passed.  /// </summary>  /// <param name="message">The message to be signed</param>  /// <param name="accountId">The account id for the Passport key we are using to sign</param>  /// <returns>Boolean representing if creating the Passport authentication message succeeded</returns>  private async Task<IBuffer> GetPassportAuthenticationMessage(IBuffer message, string accountId)  {  KeyCredentialRetrievalResult openKeyResult = await KeyCredentialManager.OpenAsync(accountId);  if (openKeyResult.Status == KeyCredentialStatus.Success)  {  KeyCredential userKey = openKeyResult.Credential;  IBuffer publicKey = userKey.RetrievePublicKey();  KeyCredentialOperationResult signResult = await userKey.RequestSignAsync(message);  if (signResult.Status == KeyCredentialStatus.Success)  {  return signResult.Result;  }  else if (signResult.Status == KeyCredentialStatus.UserCanceled)  {  // User cancelled the Passport PIN entry.  //  // We will return null below this and the username/password  // sign in form will show.  }  else if (signResult.Status == KeyCredentialStatus.NotFound)  {  // Must recreate Passport key  }  else if (signResult.Status == KeyCredentialStatus.SecurityDeviceLocked)  {  // Can't use Passport right now, remember that hardware failed and suggest restart  }  else if (signResult.Status == KeyCredentialStatus.UnknownError)  {  // Can't use Passport right now, try again later  }  return null;  }  else if (openKeyResult.Status == KeyCredentialStatus.NotFound)  {  // Passport key lost, need to recreate it  }  else  {  // Can't use Passport right now, try again later  }  return null;  }  /// <summary>  /// Creates a Passport key on the machine using the account id passed.  /// Then returns a boolean based on whether we were able to create a Passport key or not.  ///  /// Will also attempt to create an attestation that this key is backed by hardware on the device, but is not a requirement  /// for a working key in this scenario. It is possible to not accept a key that is software-based only.  /// </summary>  /// <param name="accountId">The account id associated with the account that we are enrolling into Passport</param>  /// <returns>Boolean representing if creating the Passport key succeeded</returns>  public async Task<bool> CreatePassportKey(string accountId)  {  KeyCredentialRetrievalResult keyCreationResult = await KeyCredentialManager.RequestCreateAsync(accountId, KeyCredentialCreationOption.ReplaceExisting);  if (keyCreationResult.Status == KeyCredentialStatus.Success)  {  KeyCredential userKey = keyCreationResult.Credential;  IBuffer publicKey = userKey.RetrievePublicKey();  KeyCredentialAttestationResult keyAttestationResult = await userKey.GetAttestationAsync();  if (keyAttestationResult.Status == KeyCredentialAttestationStatus.Success)  {  //keyAttestation Included.  //TODO:read keyAttestationResult.AttestationBuffer and keyAttestationResult.CertificateChainBuffer  }  else if (keyAttestationResult.Status == KeyCredentialAttestationStatus.TemporaryFailure)  {  //keyAttestation CanBeRetrievedLater  }  else if (keyAttestationResult.Status == KeyCredentialAttestationStatus.NotSupported)  {  //keyAttestation is not supported  }  // Package public key, keyAttesation if available,  // certificate chain for attestation endorsement key if available,  // status code of key attestation result: keyAttestationIncluded or  // keyAttestationCanBeRetrievedLater and keyAttestationRetryType  // and send it to application server to register the user.  bool serverAddedPassportToAccount = await AddPassportToAccountOnServer();  if (serverAddedPassportToAccount == true)  {  return true;  }  }  else if (keyCreationResult.Status == KeyCredentialStatus.UserCanceled)  {  // User cancelled the Passport enrollment process  }  else if (keyCreationResult.Status == KeyCredentialStatus.NotFound)  {  // User needs to create PIN  return false;  }  return false;  }  }  } |

* **public async Task<bool> SignInPassport():**该方法用于Passport登录，如果成功设置PIN码，调用该方法会调用Windows Hello API来进行用户身份鉴权。
* **public async Task<bool> SignInPassword(bool isnewAccount)**：该方法用于用户输入用户名、密码鉴权登录，如果验证成功，我们会将用户名缓存在本地文件中。为用户的下一次登录提供用户列表选择。

**isnewAccount 参数：**当前用户是否新用户。（如果从用户列表选择用户登录为false，如果用户第一次登录为True）

* **private async Task<bool> AuthenticatePasswordCredentials()：**该方法用于服务器用户身份鉴权。（我们可以构建自己的鉴权服务，通过扩展该方法来完成APP与服务器的数据交互,用于用户的身份鉴权）。
* **public async Task<bool> AddPassportToAccountOnServer()：**该方法用于上传Passport信息到我们自己的服务器，用作服务器鉴权。（通过扩展该方法我们可以上传Passport信息）
* **private async Task<bool> AuthenticatePassport()：**该方法用于调用Windows Hello API来完成本地身份鉴权。
* **private void SuccessfulSignIn(bool isAdd)：**该方法用于用户登录信息的持久化。
* **private async Task<IBuffer> GetPassportAuthenticationMessage(IBuffer message, string accountId)：**该方法用于本地用户身份鉴权。

**message 参数：**本地数据二进制流。

**accountId参数：**登录用户唯一标识。（通常为用户的邮箱，在这里我们使用用户名）

* **public async Task<bool> CreatePassportKey(string accountId):**该方法通过调用Windows Hello API 来创建本地鉴权数据。

**accountId 参数：**用户唯一标识。（通常为用户的邮箱，在这里我们使用用户名）

## Windows Hello常见问题问答

* **Windows 10 什么版本可以使用Windows Hello？**

在Windows 10 Build 10125 及以后的版本已经包含了Windows Hello功能。

* **是否必须使用Windows Hello 才可以登录到Windows10?**

否。 如果不使用 Windows Hello，可以使用密码或 PIN 进行登录。 如果你决定使用 Windows Hello 并且稍后想改变决定，可以在“设置”中将它关闭。

* Windows Hello的常见使用场景?

1.鉴权登陆和授权解锁；2.购买或者支付的二次授权；3.身份识别

* **哪些数据将用于识别我并且那些数据是如何存储的？**

设置期间，Windows 将从人脸或虹膜感应器或指纹读取器采集数据，然后创建身份特征，将其加密并保存在你的设备上。 （这不是一幅图像，而更像是一张图表。） 你的身份特征保留在你的设备上。 Windows 绝不会将你的人脸、虹膜或指纹的照片或图像存储在你的设备上或其他任何地方。

* **英特尔实感摄像头在线资源:**

[**https://software.intel.com/zh-cn/articles/intel-realsense-sdk-faq-for-front-facing-camera-f200?utm\_source=CSDN.com&utm\_medium=Text+Link&utm\_campaign=RS\_PRC\_Q215\_CSDN**](https://software.intel.com/zh-cn/articles/intel-realsense-sdk-faq-for-front-facing-camera-f200?utm_source=CSDN.com&utm_medium=Text+Link&utm_campaign=RS_PRC_Q215_CSDN)