Microsoft

winhec

Taipei 2015

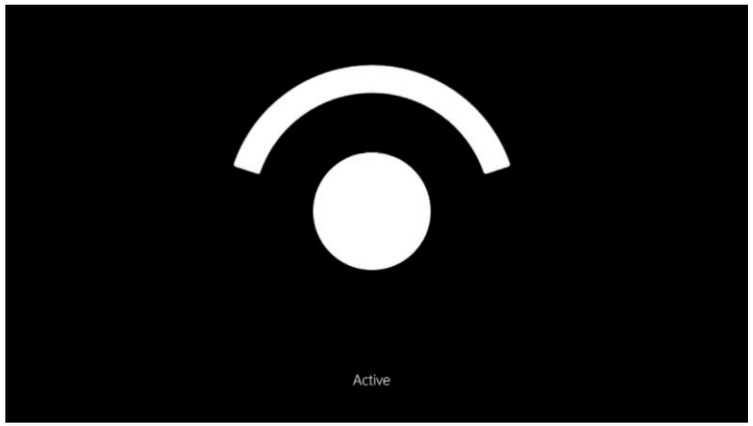
Microsoft

How to Implement Face Authentication in Windows 10

Sam Chang
Senior Program Manager
Microsoft Corporation

Introducing Windows Hello

- Windows 10 supports biometric:
  - Fingerprint
  - Face
- Both are recommended features on devices with supporting hardware
- Integrated with Windows Biometric Framework
- Use Windows end to end experiences and scenarios
  - share the same design language for enrollment and usage

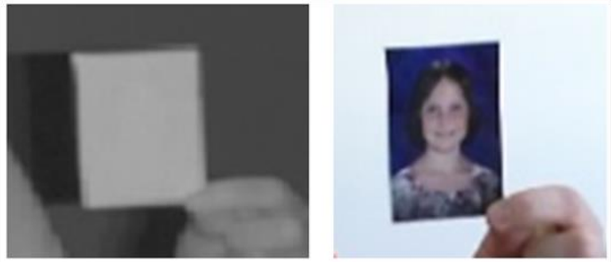


Windows Hello: Sensor Support

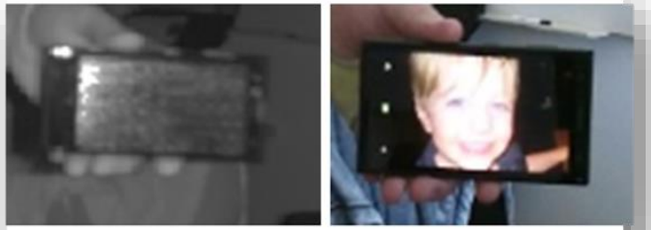
- Fingerprint
  - All current fingerprint capable devices are supported
- Face
  - All devices that include an IR sensor that meets Microsoft sensor spec

Windows Hello face authentication: Enterprise-grade Security

- Meets enterprise-grade security:
  - Demonstrates False Acceptance Rate (FAR): 1/100,000
  - True Accept Rate: 95%
  - Includes anti-spoofing counter measures
  - Recognition takes less than 1.5 seconds



School Portrait



Lumia 1020

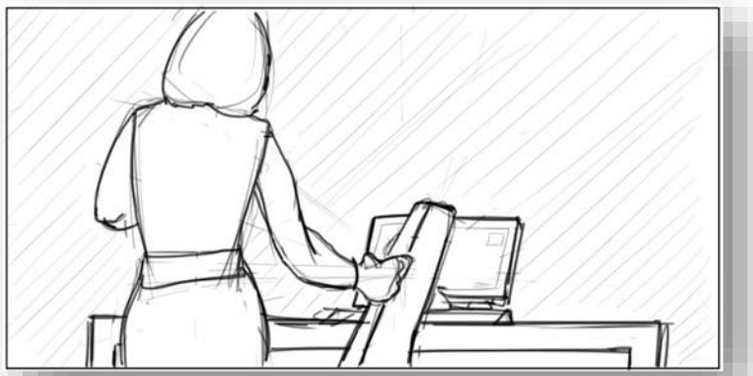
Surface Pro 3

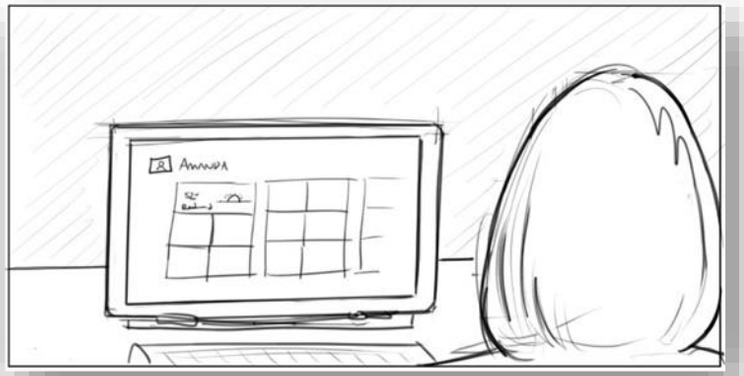
https://msdn.microsoft.com/en-us/library/windows/hardware/mt587095(v=vs.85).aspx

Face Authentication

Features

- Microsoft Face Authentication in Windows 10 is an enterprise grade identity verification mechanism that integrates into the Windows Biometric Framework (WBF) as a core windows component.
- Face Authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock Windows devices as well as unlock your Microsoft Passport.
- By building on Microsoft Passport and advanced camera technology, Windows will utilize a variety of factors to ensure your data stays secure.





Key Benefits and Capabilities

- Facial recognition across all Windows 10 devices and platforms with compatible hardware (near IR sensor)
- A user friendly interface that provides a single sign-in form of verification to unlock your Microsoft Passport
- Enterprise grade authentication and access to Microsoft Passport supported content, including network resources, websites, and payment instruments
- The ability to provide a consistent image (via IR) in diverse lighting conditions that also allows for subtle changes in appearance including facial hair, cosmetic makeup, etc.

Use Cases

Scenario:	Authentication to Login or Unlock
Average Duration:	< 1.5 seconds
Expected Frequency:	High
Description:	Applies each and every time a user wants to authenticate to their desktop and move past the lock screen.

Scenario:	Authentication to Verify
Average Duration:	< 1.5 seconds
Expected Frequency:	Low
Description:	Applies any time an application requires the user to re-authenticate during high value transactions such as online payments, etc..

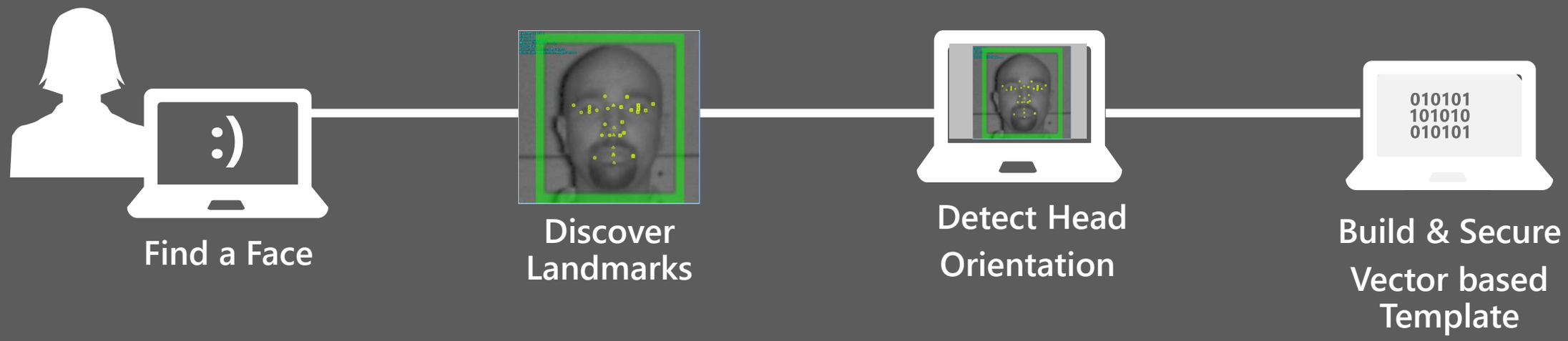
DEMO – WINDOWS HELLO

How It Works

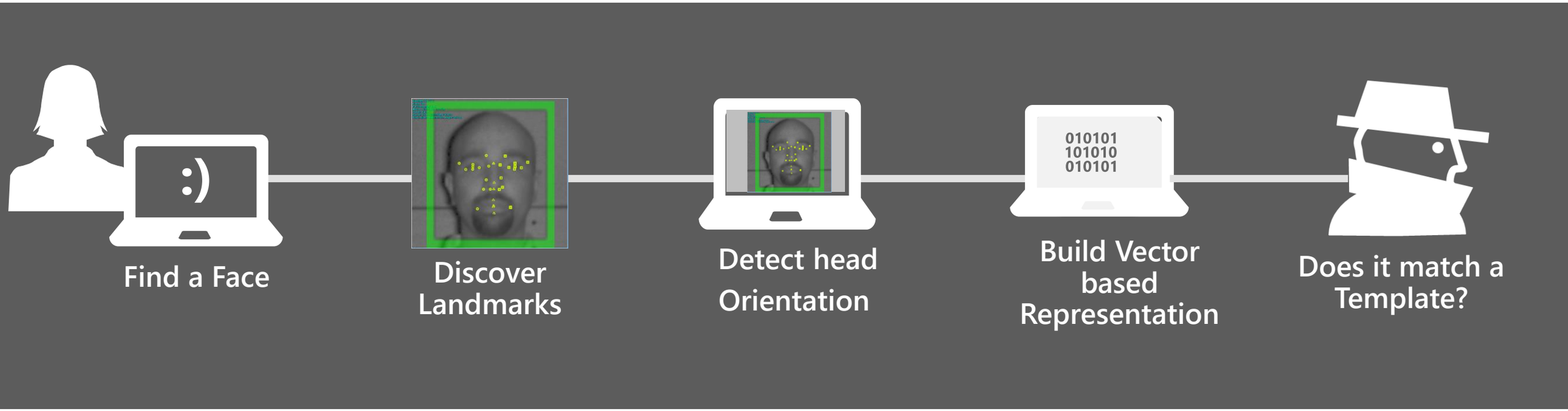
The Microsoft Face Recognition engine consists of four distinct steps that allow Windows to understand who is in front of the sensor.

1. Find face & discover landmarks
   The algorithm detects the user's face and then locates facial landmark points (also known as alignment points), which correspond to eyes, nose, mouth, etc.
2. Head orientation
   The algorithm ensures the user is mostly facing towards the device +/- 15 degrees.
3. Representation vector
   Using the landmark locations as anchor points, the algorithm takes thousands of samples from different areas of the face to build a representation. No image of the face is ever stored – it is only the representation.
4. Decision engine
   It's compared to the enrolled users on physical device.

Enrollment


:)
Find a Face
Discover Landmarks
Detect Head Orientation
010101
101010
010101
Build & Secure Vector based Template

Usage


:)
Find a Face
Discover Landmarks
Detect head Orientation
010101
101010
010101
Build Vector based Representation
Does it match a Template?

Clean Infrared as a Sensor

Clean IR is ideal as a data source for identity scenarios as it provides:

- Clean and consistent image regardless of ambient lighting and weather conditions, including complete darkness
- High tolerance for changes in physical appearance such as facial hair and cosmetic makeup
- Multiple enrollments not needed
- High True Positive rate
- High user satisfaction -> just works!
- Users won’t disable it in frustration

Benefits of Near Infrared

scenario	Color Image from integrated Camera	IR Image from Microsoft Reference Sensor
Low light representative of watching TV or giving a PowerPoint presentation		
Side lighting when sitting near a window or desk lamp		

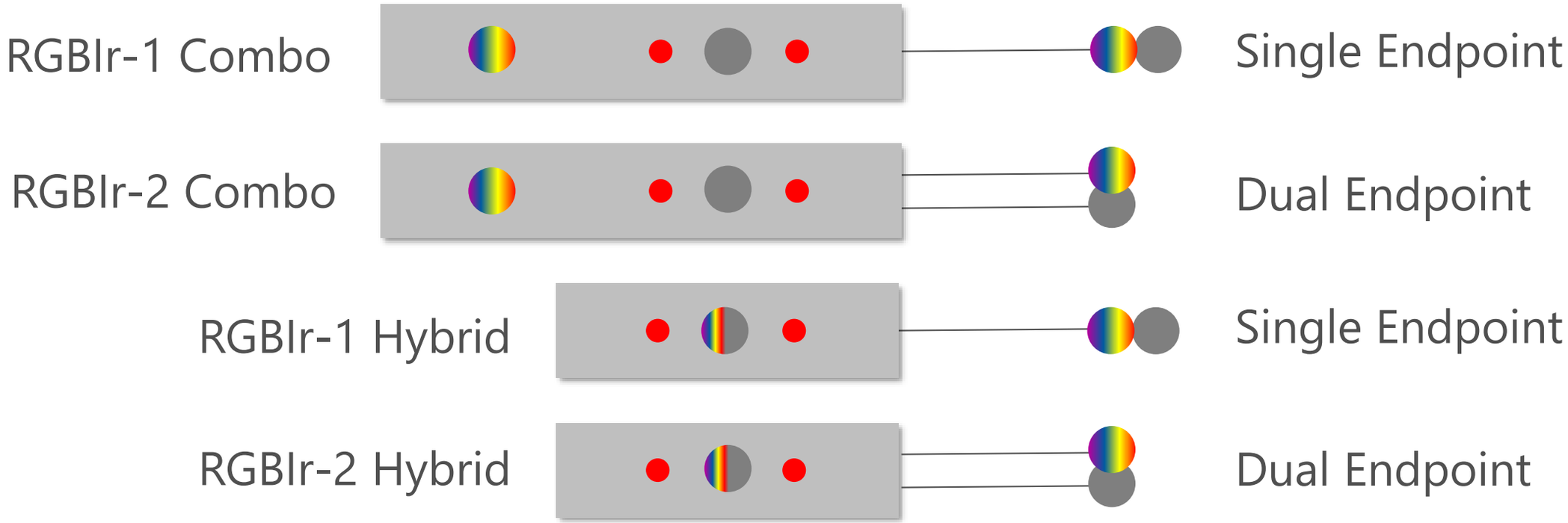
Hardware Implementation

Hardware and Driver Implementation

- The Face Authentication feature is a 2D based solution that has the following primary technology dependencies:
  - Hardware sensor components
  - Driver and IFrameProvider interface
  - Specific hardware requirements that define the capabilities and fidelity of the camera

- Hardware Components
  - 640x480 monochrome webcam (MIPI, USB)
  - IR capable lens
  - IR illuminator
  - IR band pass filter
  - Controller (SoC, ISP)
  - RGB webcam (MIPI, USB)*

Camera Module Types



If a device is capable of providing simultaneous RGB data in addition to IR, Windows will use the data to supplement the integrated anti-spoofing countermeasures.

Face Authentication Specification V1.51

Item	Minimum	Maximum	Description
Sensor type	Global Shutter (Recommended) Rolling Shutter	-	Both Rolling Shutter and Global shutter are supported sensor types. Please see HW section 4 below for further details.
Resolution	60 horizontal IR pixels across a 15 cm object @ max range	-	Represents the average head size and how many pixels across the face are required.
Image Size	340x340	1920x1080	The minimum and maximum image size supported by the IFrameProvider independent of sensor resolution
Field of View	>= 40 degrees horizontal >= 45 degrees vertical	-	The field of view required to provide an optimal user experience. Note: >=60 is recommended for the best user experience.
Near Range	Notebook/Tablet: 30cm Desktop:30cm Mobile (Phone) :20cm	Form Factor specific	The minimum distance between the user's face and the sensor for the listed form factor. MTF and SNR will need to be verified throughout the device range.
Far Range	Notebook/Tablet: 75cm Desktop: 100cm Mobile (Phone): 45cm	Form factor specific	The recommended maximum distance between the user's face and the sensor for the listed form factor. MTF and SNR will need to be verified throughout the device range.
Clean IR	Alternating Illuminated and unilluminated	Alternating Illuminated and unilluminated	IR illuminated frame and ambient frame must be provided in order for Microsoft to do ambient light subtraction
Sensor Frame Rate	Global Shutter: 30fps Rolling Shutter: 60fps	-	Minimum framerate required for Windows Hello. See section 3 below for further details.
Frame Pair Rate	15fps Illuminated 15fps Ambient	-	Minimum ambient and illuminate frame rate in order for Microsoft to achieve performance metrics with Clean IR.
Image Processing	None	Very minimal	Heavy image processing should not be applied to sharpen or smooth images.
Distortion	-	+/- 5.5% error	Lens distortion that is acceptable across entire field of view.
Modulation Transfer Function (MTF)	.25 @ 50%	.35 @ 50%	Camera should be focused for optimal MTF at the midpoint of the operating range. MTF should be measured at the near and far points of the operating range.
MTF Overshoot	-	5%	No sharpening or smoothing that will increase Overshoot beyond 5%
MTF Undershoot	-	3%	No sharpening or smoothing that will increase Undershoot beyond 3%
Signal to Noise Ratio	30dB over FOV	-	Signal to noise ratio over the entire field of view of the image. SNR needs to be evaluated in two ways: 1. With the illuminated frame alone; 2. With Illuminated minus Ambient frame (i.e. ambient subtraction).
Dynamic Range	No Saturation		Allowed Image saturated at the minimum distance for the device.
Gamma	1.0 (Linear Gamma)	1.0 (Linear Gamma)	A linear curve to ensure information across face is not lost
Startup Time	-	500ms	The time it takes to complete face authentication initiation as measured from the time IFrameProvider entering Face Authentication Mode to the first frame delivered.
Filter	840nm	870nm	Band-pass filter used to eliminate frequencies of IR not provided exclusively by the illuminator (e.g. sun, lights, etc.). < 2% Optical transmission for wavelengths outside of the filter bandwidth.
Uniformity of Illumination	-	65%	Illumination light shall be distributed so the Relative illumination on the sensor does not fall below 65% of the Peak Value. Note: Cropping can be applied to assist in achieving target results as long as minimum resolution and FOV is maintained.
Illumination Wavelength	840nm	870nm	The required specific range to assist with Anti-Spoofing features.
Safety	Met	Met	Local and regional safety standards met for the class of device.
Timestamp Precision	1 millisecond precision		The device or driver must be able to provide a timestamp corresponding to when the frame was captured. This timestamp must be monotonically increasing over frames captured from the device. The timestamp should be exposed in units of hundreds of nanoseconds. If this timestamp is computed at the driver level, the guidance is to use the GetSystemTimePreciseAsFileTime API.
Color + IR	Simultaneous Access	-	Simultaneous access to both the Color & IR frames are recommended for enhanced anti-spoofing scenarios on enterprise class machines.
Mount Location	Top or bottom Middle	-	Optimal location for sensor and illumination to be mounted.
Ambient Light Levels	5	1000	The required light source for this test is a broad-spectrum Incandescent with a strong IR component.

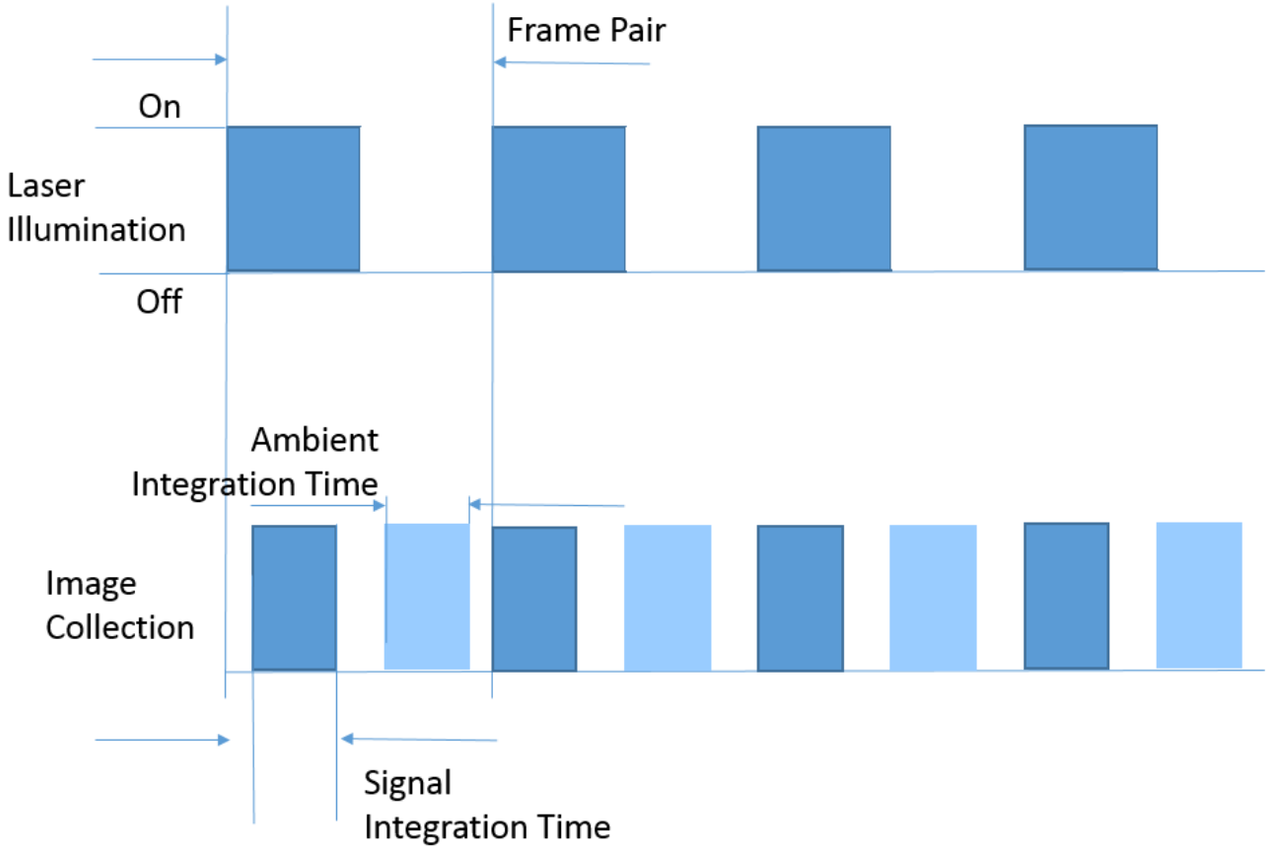
Clean IR

- To reduce the effects of ambient light sources of 840nm-870nm near IR light, the device should be Clean IR capable.
  - Provide frame pair
- Microsoft will subtract frame pairs and create clean IR
  - Enhance motion detection
  - Enhance clean IR quality
  - Outdoor mode switch

Frame Pairing

- Removes the ambient IR from the image and helps ensure recognition is not impacted by other outside sources of infrared light

840-870nm NIR



≥15 frame pairs

Rolling Shutter vs. Global Shutter

- Global Shutter solutions are recommended

- Rolling shutter solutions are more complex
  - Ensure frames (either illuminated or ambient) are not partially illuminated by a light source
  - Bad frames have to be discarded

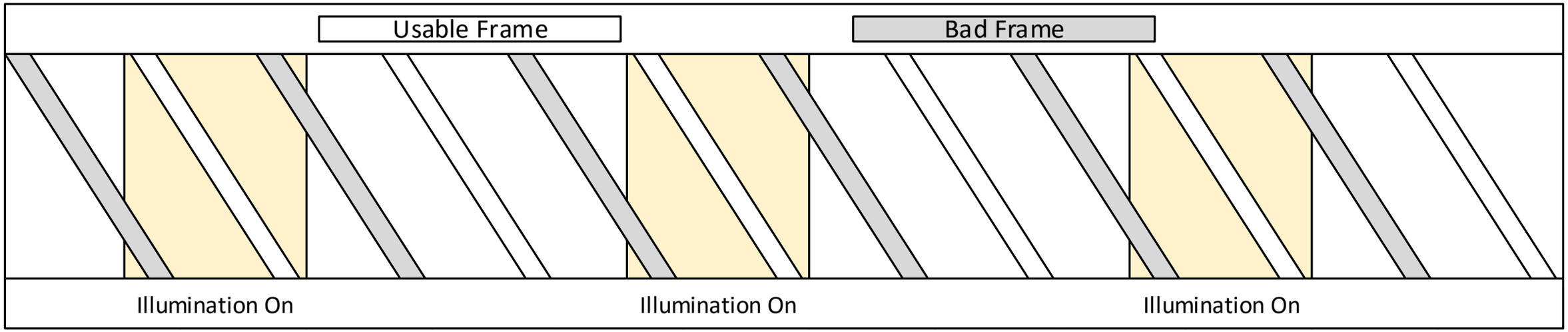
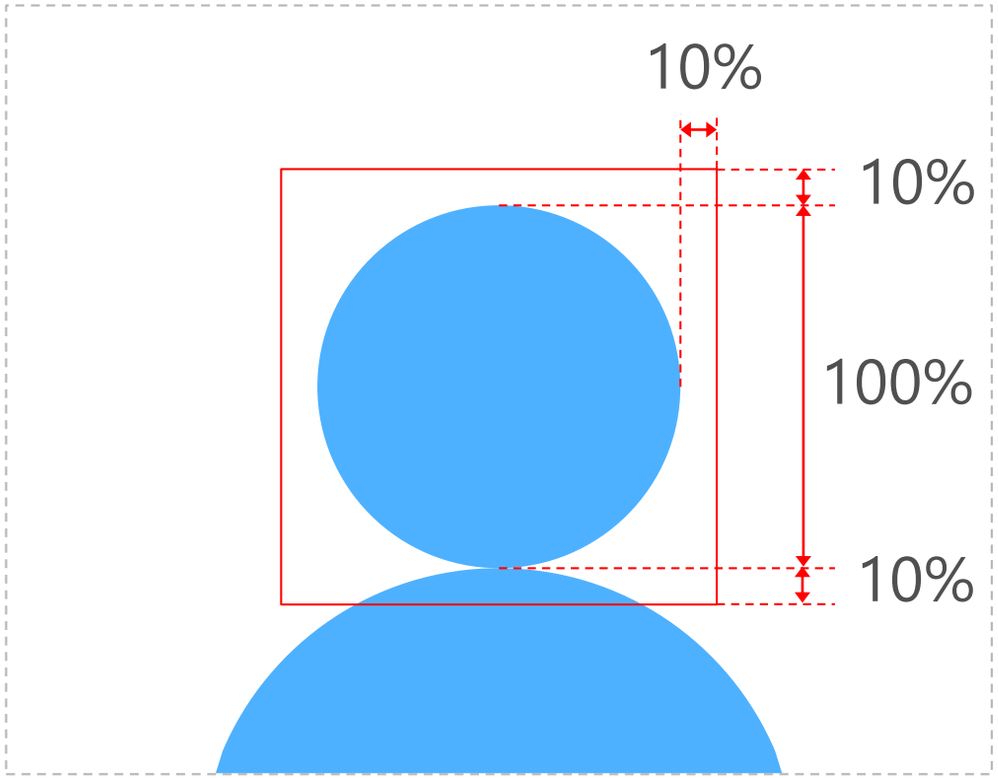


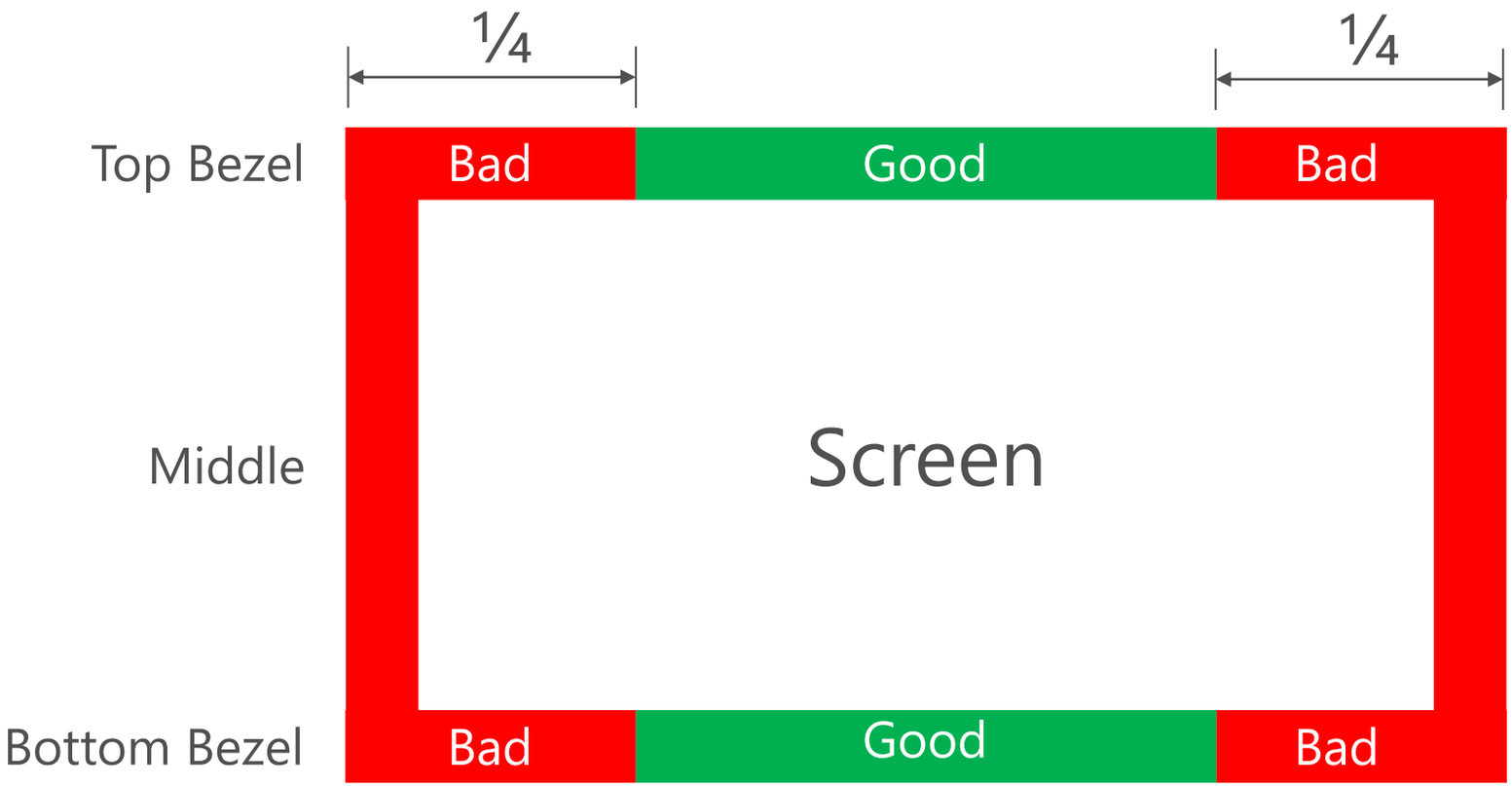
Image Size and Position

- Resolution
  - Minimum: 340 x 340
  - Maximum: 1920 x 1080
- Pixel
  - 15cm object >= 60 pixels
- Distance
  - Significant distance of face from the edge
- Angle
  - User's face is +/- 15 degrees from facing the sensor



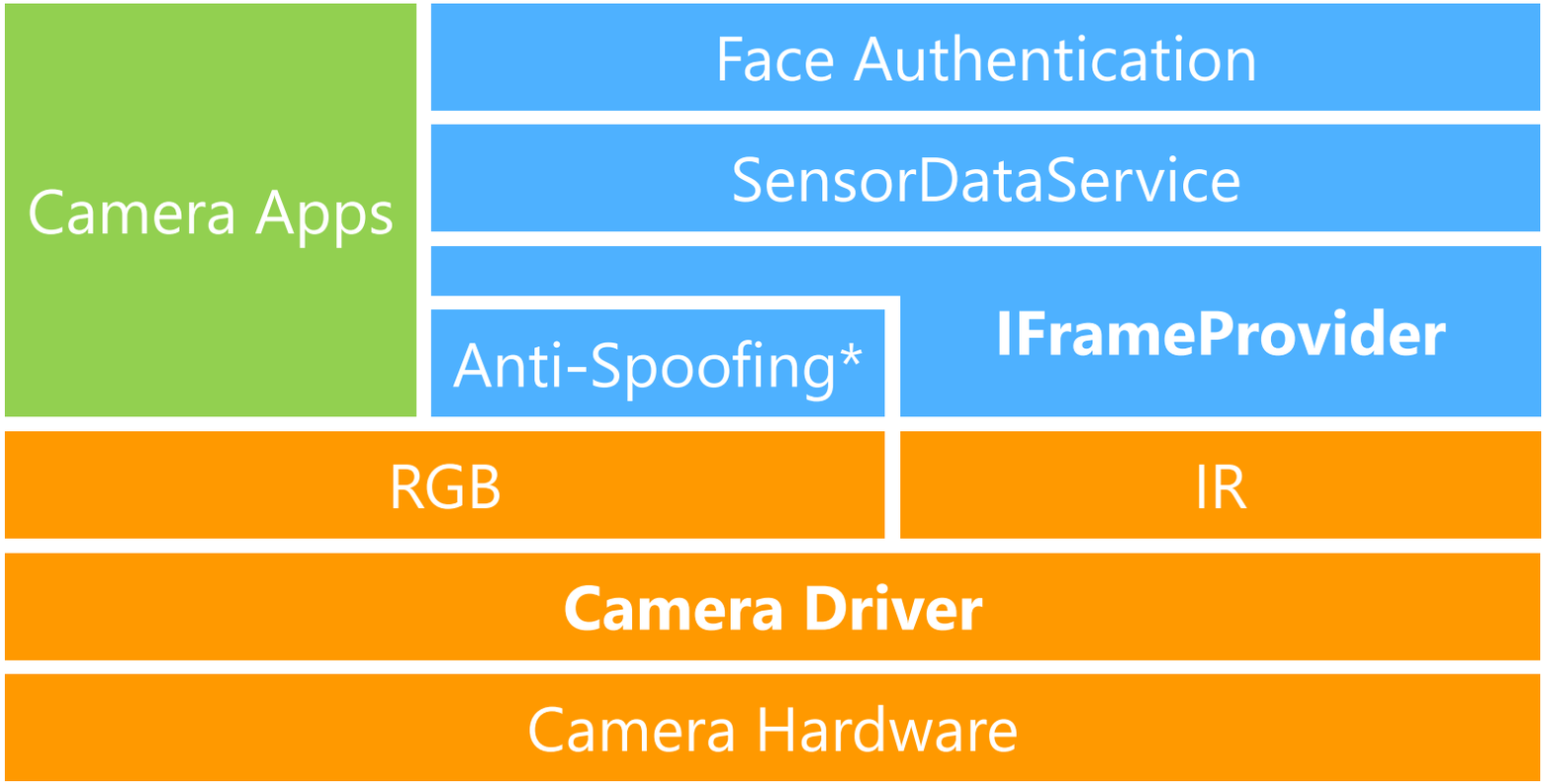
Mounting Requirements

- Face Authentication in Windows 10 will account for the sensor being placed in a variety of locations across the top or bottom bezel of the device.



Software Implementation

Driver and Provider



* Simultaneous RGB data in addition to IR to supplement the integrated anti-spoofing countermeasures.

IFrameProvider

- IFrameProvider is the user mode interface between sensors and the SeneorDataService in Windows
  - The interface provides a collection of sources associated with one or more physical sensors
  - Independent hardware vendors (IHVs) implement this interface in order to deliver media frames to the SensorDataService
  - All source providers must be registered with the service, from which they will be activated
  - It requires data to be delivered in a lossless format, at 8-bit intensity value

Hide IR Device from Applications

- IR Cameras have to be hidden from applications to avoid user confusion
  - IR Cameras be hidden from applications such as Skype or Camera to avoid user confusion
- Specify imaging device in .inf
  - **KSCATEGORY_SENSOR_CAMERA** instead of KSCATEGORY_VIDEO_CAMERA
- Enumerate KSCATEGORY_SENSOR_CAMERA

```
HSTRING MF_VIDEO_CAPTURE_IR_PROFILE_ID = MAKE_STRING(L"F2DF2908-F781-4F7D-9817-E58B69E92148")

HRESULT CreateWmcForIRCamera()
{
    HRESULT                 hr = S_OK;
    ComPtr<IMFAttributes>   spAttributes;
    UINT32                  cActivates = 0;
    IMFActivate**           ppActivates = NULL;
    ComPtr<IMFActivate>     spVideoDeviceActivate;

    //
    // Enumerate IR camera
    //
    VERIFY_SUCCEEDED(MFCreateAttributes(&spAttributes, 1));
    VERIFY_SUCCEEDED(spAttributes->SetGUID(MF_DEVSOURCE_ATTRIBUTE_SOURCE_TYPE, MF_DEVSOURCE_ATTRIBUTE_SOURCE_TYPE_VIDCAP_GUID));
    VERIFY_SUCCEEDED(spAttributes->SetGUID(MF_DEVSOURCE_ATTRIBUTE_SOURCE_TYPE_VIDCAP_CATEGORY, KSCATEGORY_VIDEO_CAMERA_DEPTH));
    VERIFY_SUCCEEDED(MFEnumDeviceSources(spAttributes.Get(), &ppActivates, &cActivates));

  int i = 0;  // use your logic to find the correct IR device to activate.
  ComPtr<IMFActivate>                             spVideoDeviceActivate = ppActivates[i];
  ComPtr<IMediaCaptureInitializationSettings>     spInitializationSettings;
  HSTRING                                         hstrCameraId;
  PWSTR                                           pwzCameraId = nullptr;
  UINT32                                          cchCameraId = 0;

  VERIFY_IS_NOT_NULL(spVideoDeviceActivate);
  VERIFY_SUCCEEDED(spVideoDeviceActivate->GetAllocatedString(MF_DEVSOURCE_ATTRIBUTE_SOURCE_TYPE_VIDCAP_SYMBOLIC_LINK, &pwzCameraId,
&cchCameraId));
  VERIFY_SUCCEEDED(WindowsCreateString(pwzCameraId, cchCameraId, &hstrCameraId));

  ComPtr<IMediaCapture> spMediaCaptureServer;
  ComPtr<Windows::Media::Capture::IInitializeOperation> spInitializeOperation;
  VERIFY_SUCCEEDED(MediaCaptureInitializationSettingsServer::Make(
      nullptr,
      hstrCameraId.Get(),
      StreamingCaptureMode::StreamingCaptureMode_Video,
      PhotoCaptureSource::PhotoCaptureSource_Auto,
      MediaCategory::MediaCategory_Other,
      AudioProcessing::AudioProcessing_Default,
      spInitializationSettings.ReleaseAndGetAddressOf()));

  // initialize media capture server object
  VERIFY_SUCCEEDED(spMediaCaptureServer->InitializeWithSettingsAsync(spInitializationSettings.Get(),
spInitializeOperation.ReleaseAndGetAddressOf()));

    //
    // Cleanup
    //
    for (UINT32 i = 0; i < cActivates; i++)
    {
        ppActivates[i]->Release();
        ppActivates[i] = nullptr;
    }
    CoTaskMemFree(ppActivates);
}
```

Windows Update

- The device firmware and IFrameProvider (including any additional needed drivers), must be compatible and serviceable via Windows Update.

Call to Action

- Design-in secure biometric sensors into system designs
- Engage your Microsoft Ecosystem representatives
- Send your Windows biometric authentication questions to askmpcdevices@microsoft.com