black hat® BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Windows Hell No for Business

Dr Baptiste David   Tillmann Oßwald

bdavid@ernw.de   tosswald@ernw.de

“Windows Dissected”

- Funded by the German Federal Office for IT Security, carried out by ERNW
- *“Various in-depth security analyses of security-critical components and functions in Windows…”*
- Started in 2024, planned to end in spring 2026
- Various work packages including
  - Windows Hello for Business
  - eXtended Control Flow Guard – state of the art and limitations
  - Code Integrity – caching and known bypasses
  - Group Policy Objects – processing flow

ERNW
providing security.

Bundesamt
für Sicherheit in der
Informationstechnik

Who am I?

- Tillmann Osswald
- **ERNW Enno Rey Netzwerke GmbH**
  - Security researcher and Windows System Analyst
  - Since 2015
  - "Make the world a safer place"
- Master degree in IT security from the University of Applied Sciences Darmstadt.
- 💖Reverse engineering Windows components.

Who am I?

- Dr David Baptiste
- I am 🇫🇷 and I work in 🇩🇪
- **ERNW Enno Rey Netzwerke GmbH**
  - Computer security service in Heidelberg, Germany
  - “Make the World a Safer Place!”
- Did many conferences
  - Black Hat USA, DefCon, EICAR, Recon, …
  - And also, one called TROOPERS 😃
- I like good food and good wine 😏

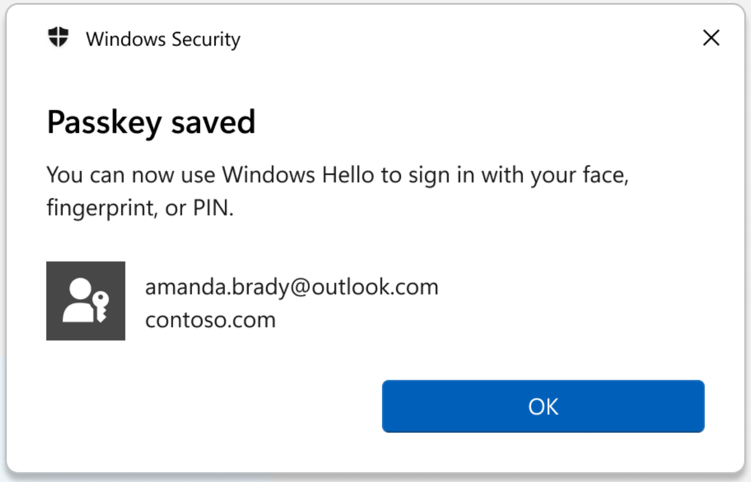
Windows Hello for Business

As a whole

Say Hello to Windows Hello

What is Windows Hello for Business?

- Windows Hello for Business is Microsoft’s passwordless flagship
  - Windows Recall, Passkey, ...
- Build on two key principals
  - Identification -> Windows Hello ...
  - Authentication -> ... for Business

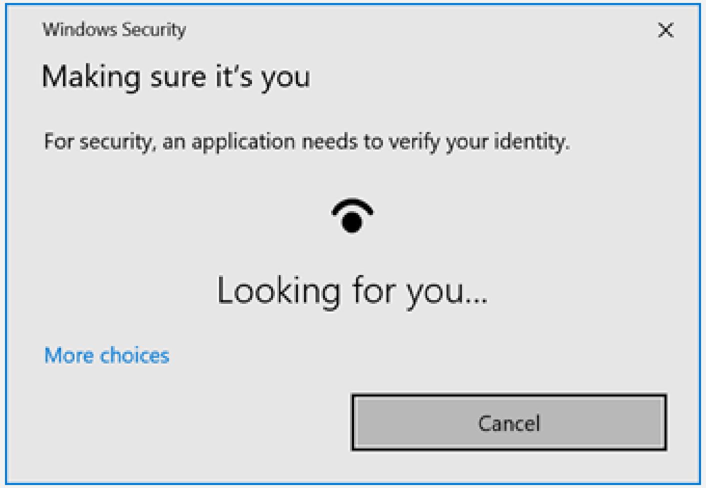


Windows Security

Passkey saved

You can now use Windows Hello to sign in with your face, fingerprint, or PIN.

amanda.brady@outlook.com
contoso.com

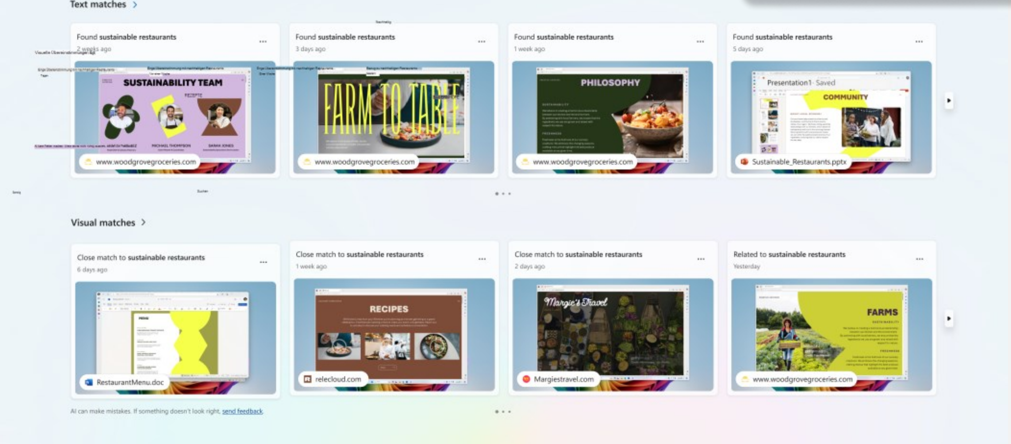


Windows Security

Making sure it’s you

For security, an application needs to verify your identity.

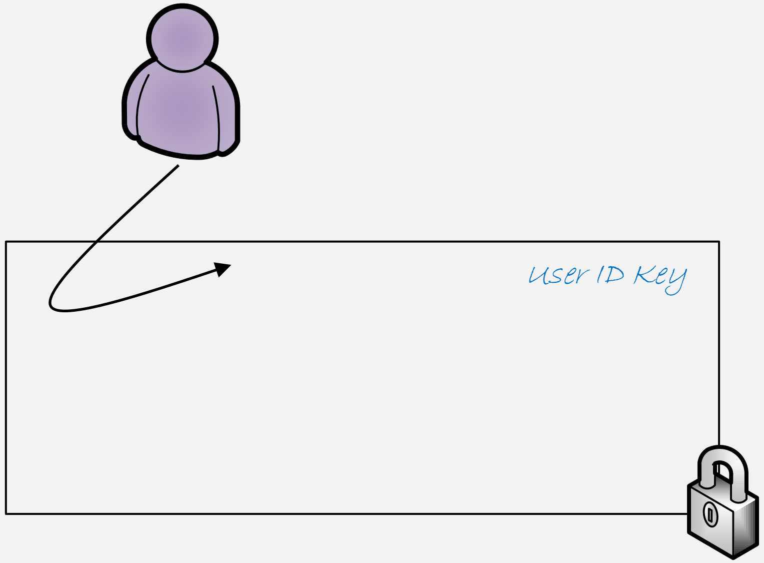
Looking for you...



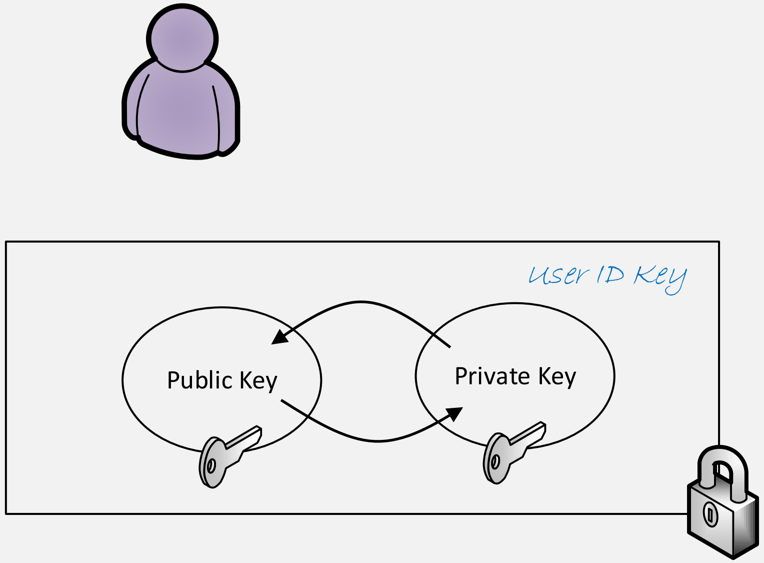
Text matches
Found sustainable restaurants
SUSTAINABILITY TEAM
FARM TO TABLE
PHILOSOPHY
COMMUNITY
www.woodgrovegroceries.com
Sustainable_Restaurants.pptx
Visual matches
Close match to sustainable restaurants
Related to sustainable restaurants
RECIPES
Margie's Travel
FARMS
RestaurantMenu.doc
relecloud.com
Margiestravel.com

Windows Hello for Business – Enrollment

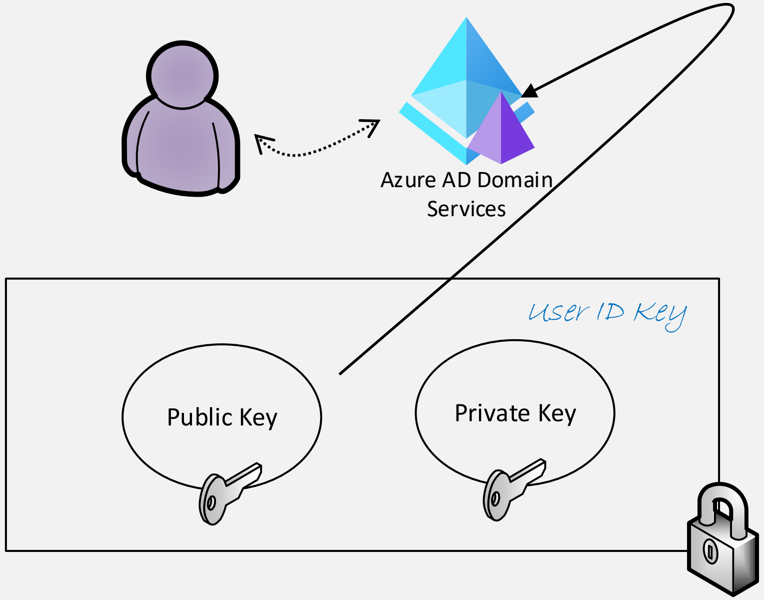
Windows Hello for Business – Enrollment



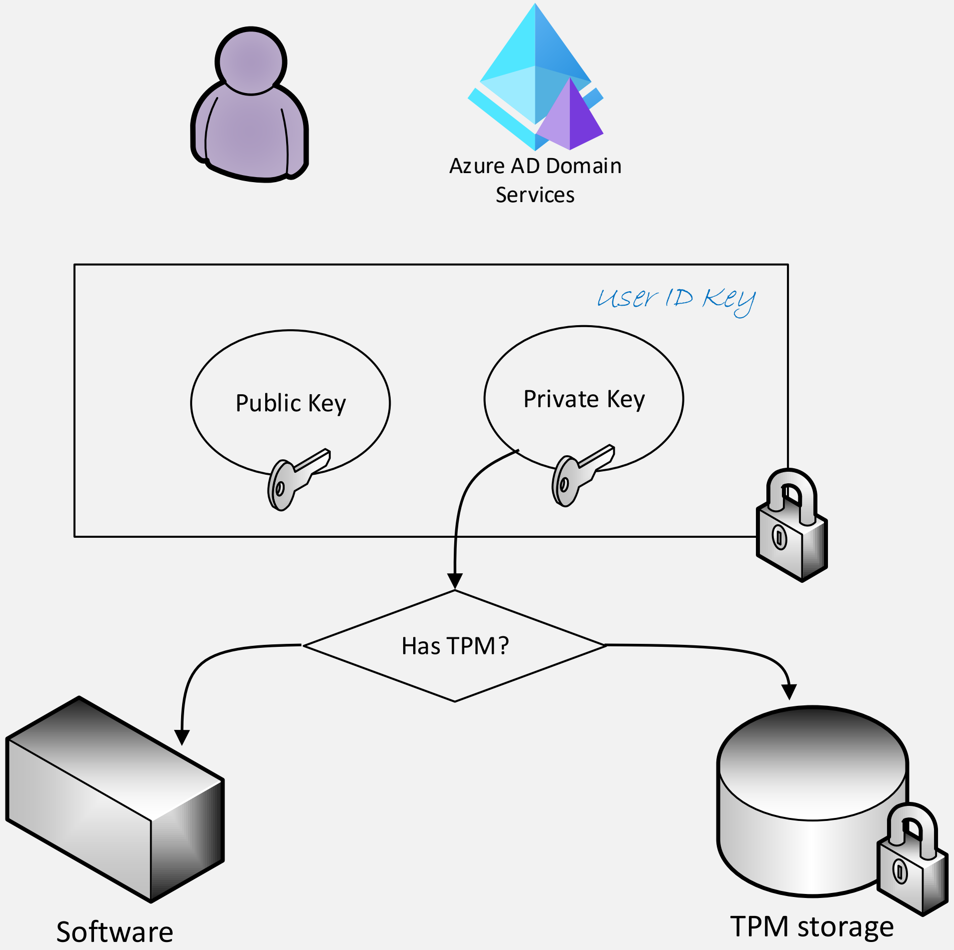
Windows Hello for Business – Enrollment



Windows Hello for Business – Enrollment

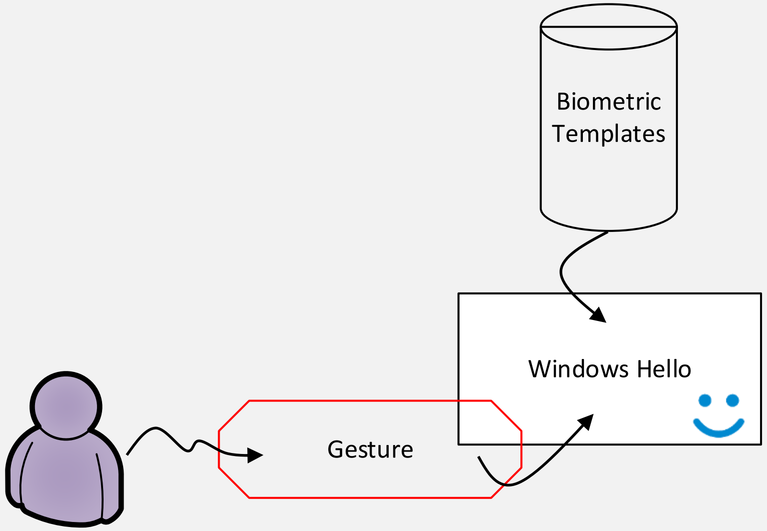


Windows Hello for Business – Enrollment

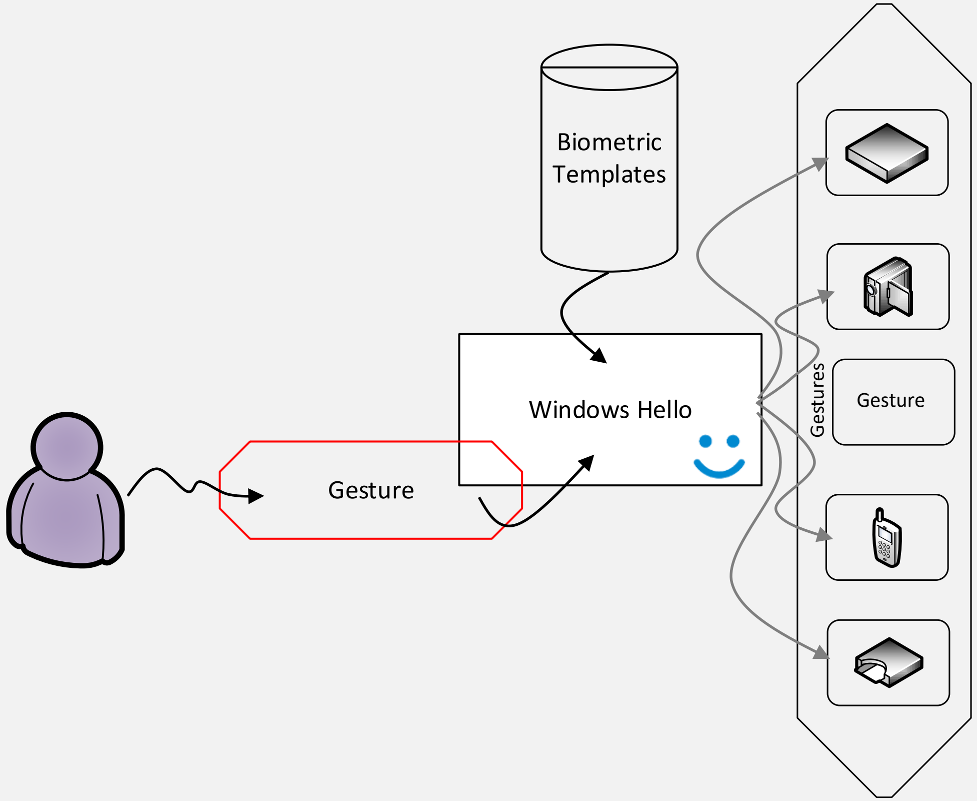


Windows Hello for Business

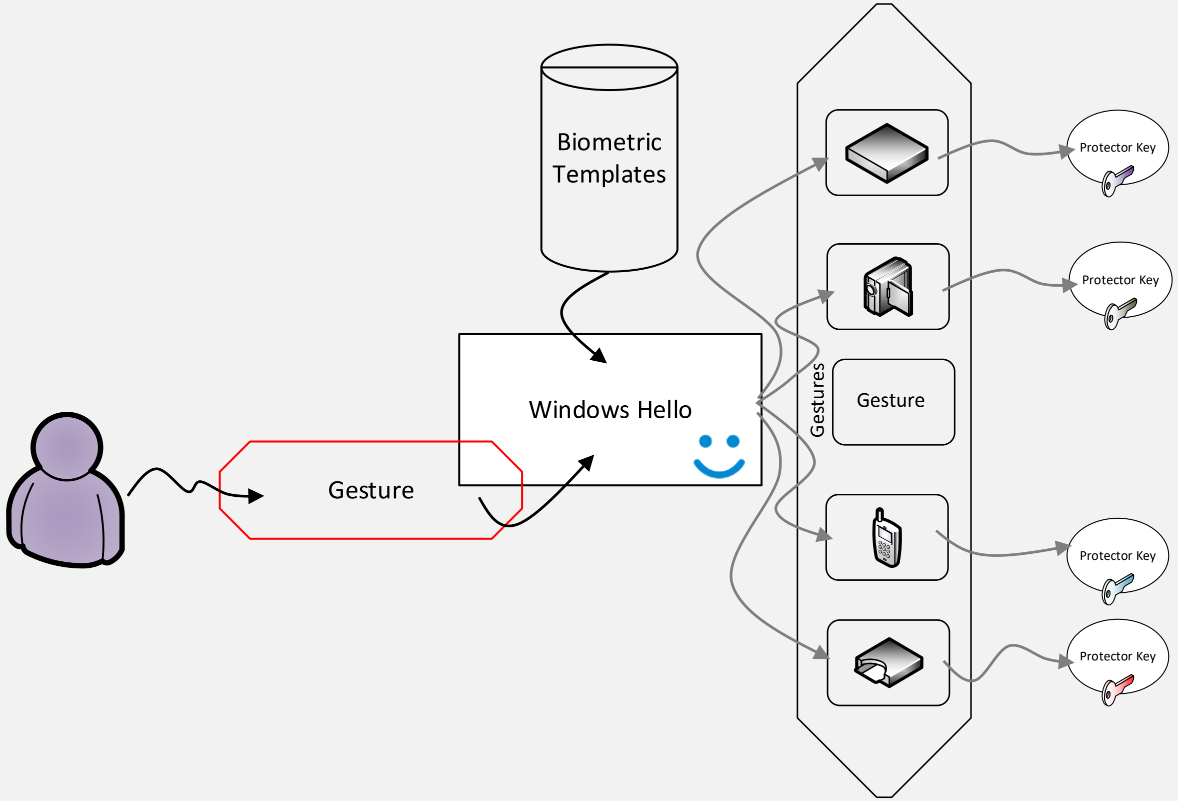
Windows Hello for Business



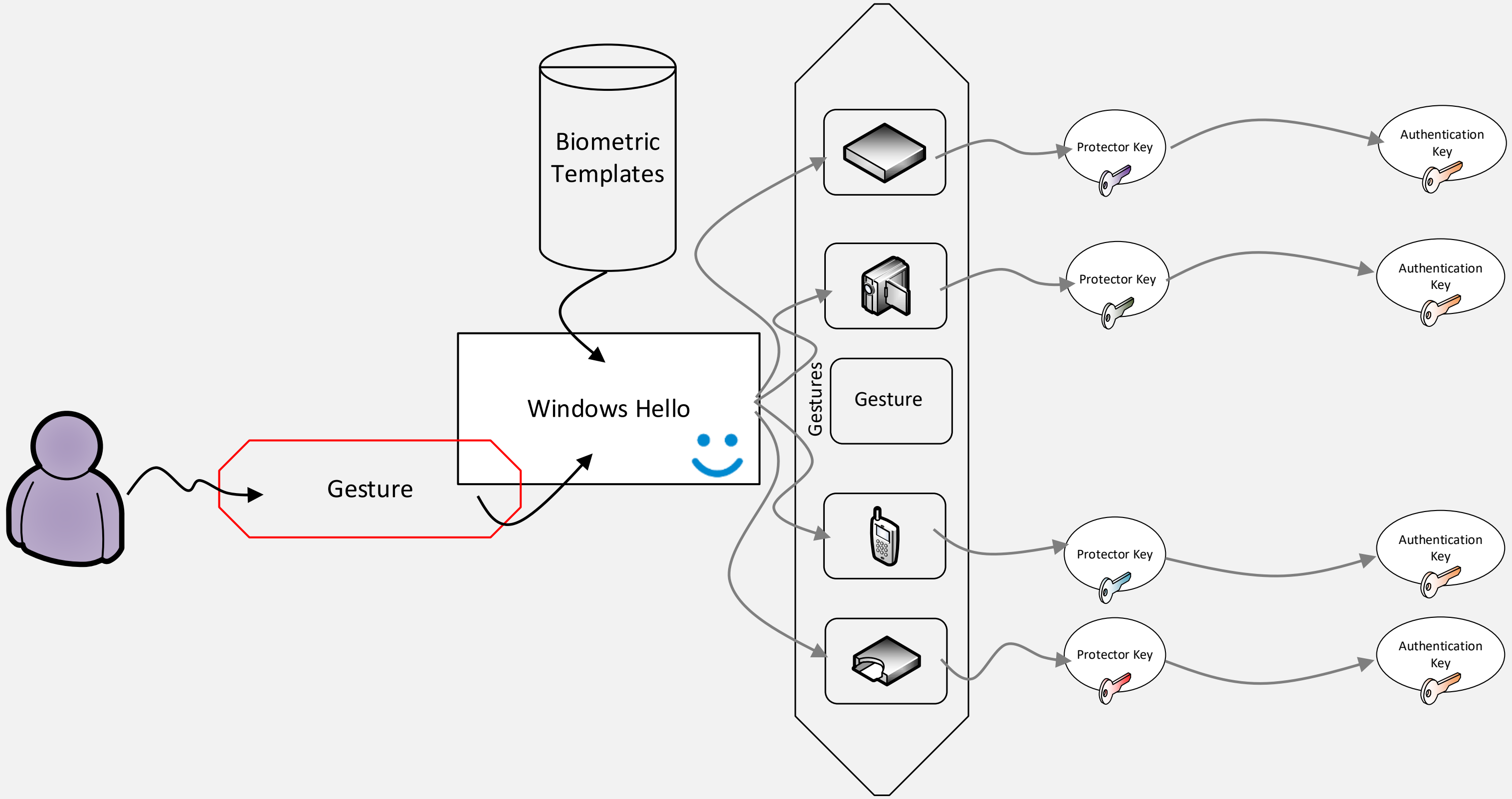
Windows Hello for Business



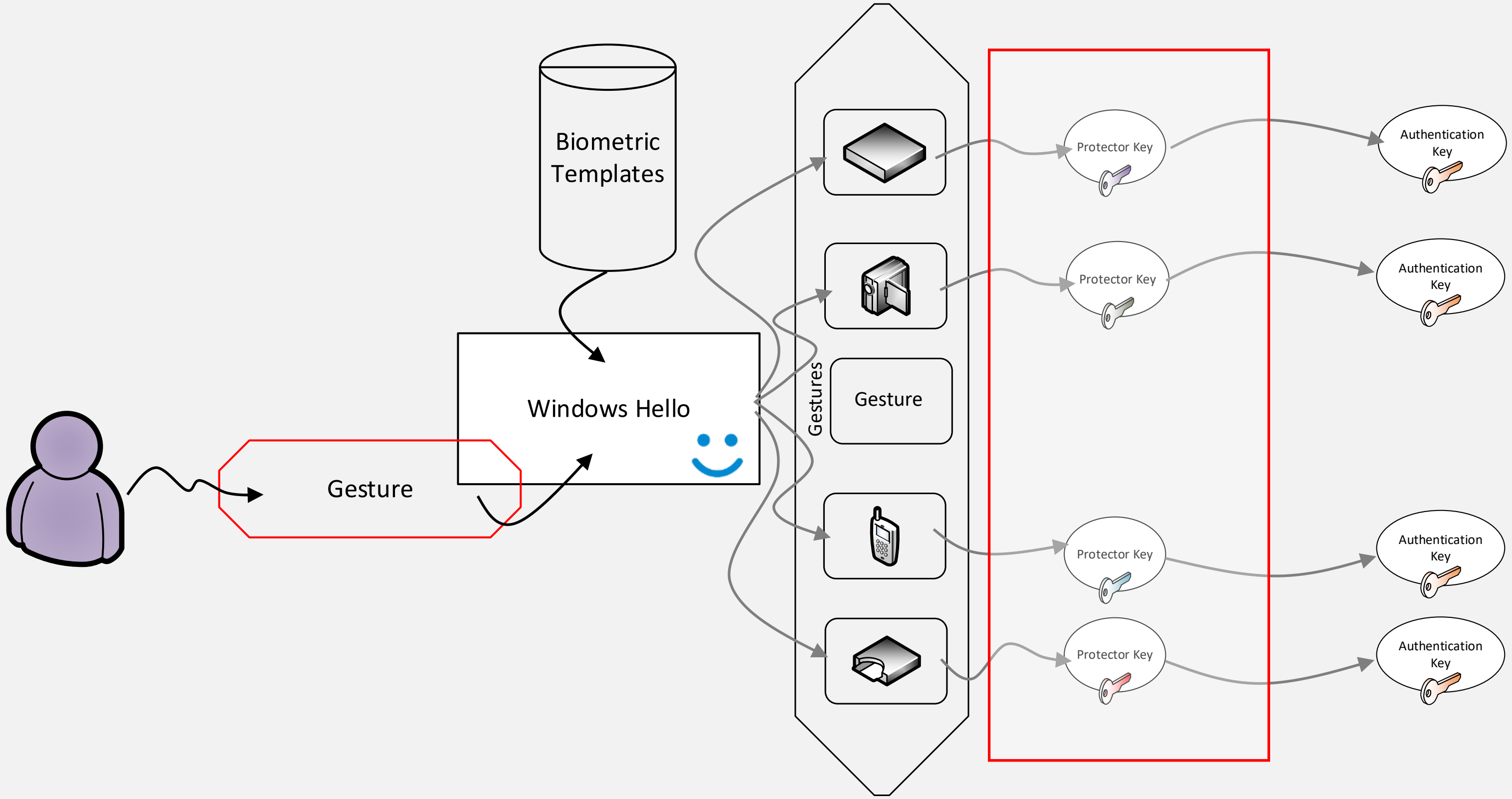
Windows Hello for Business



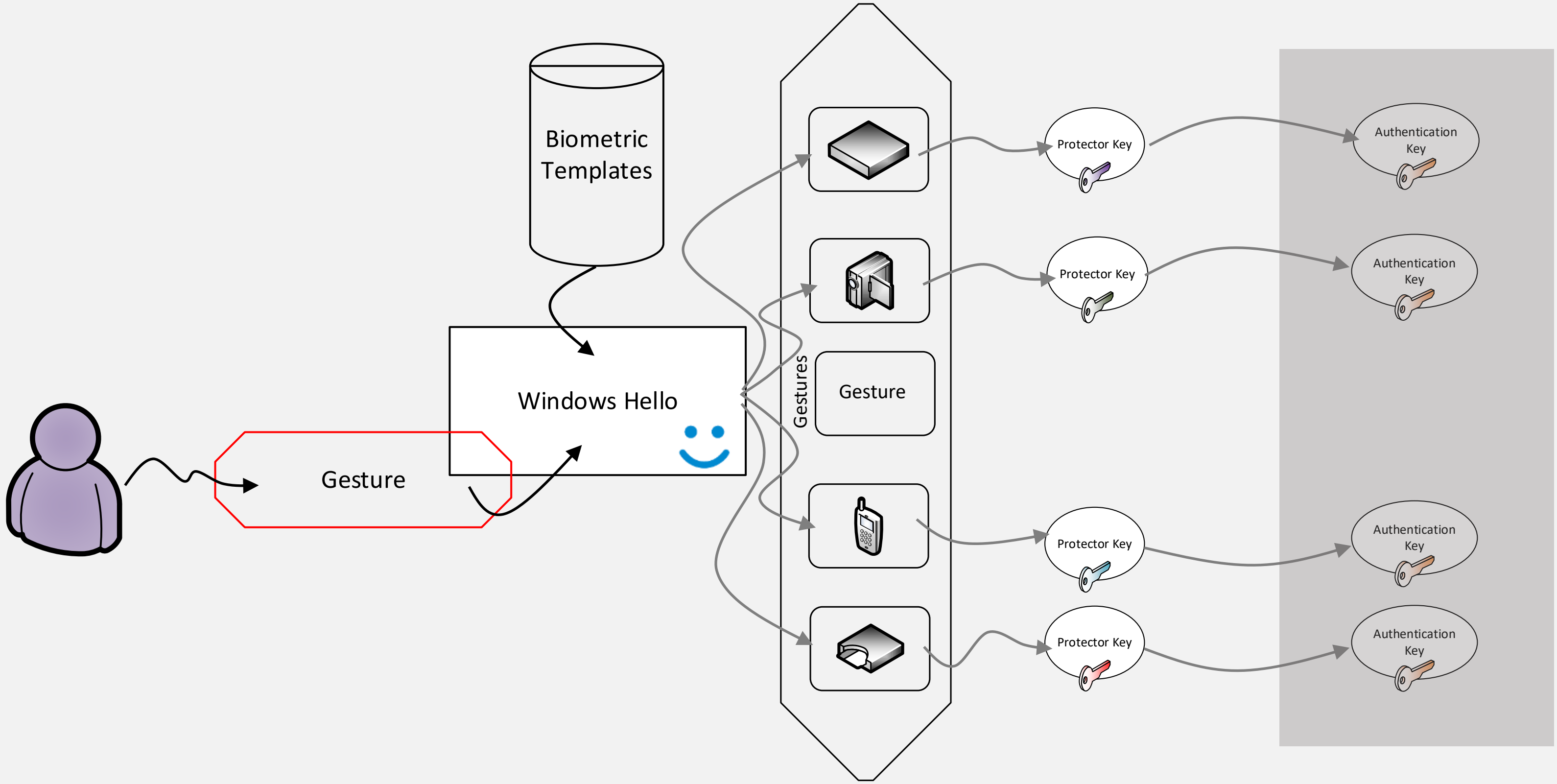
Windows Hello for Business



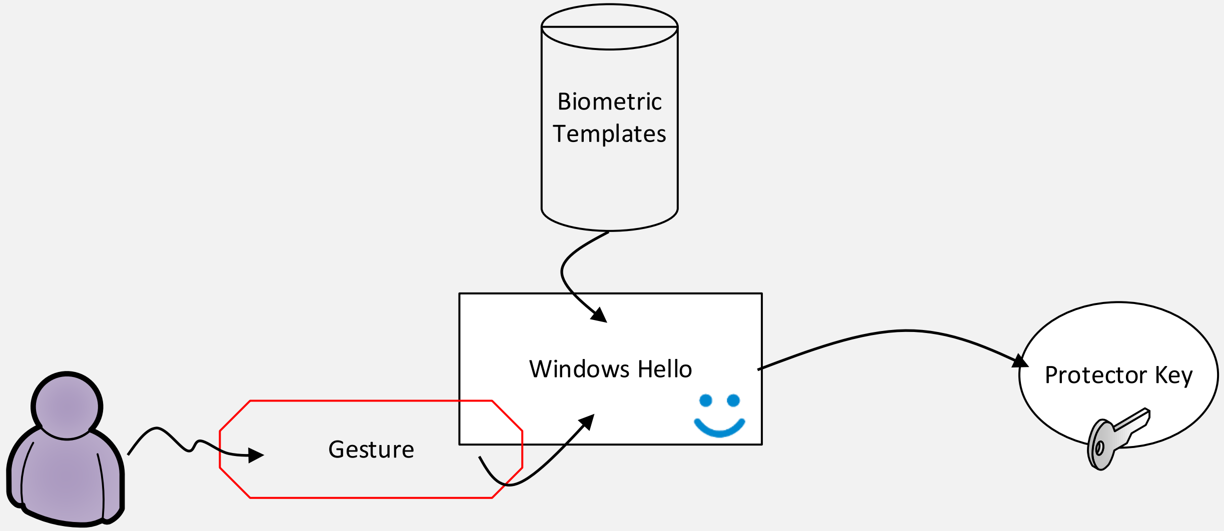
Windows Hello for Business



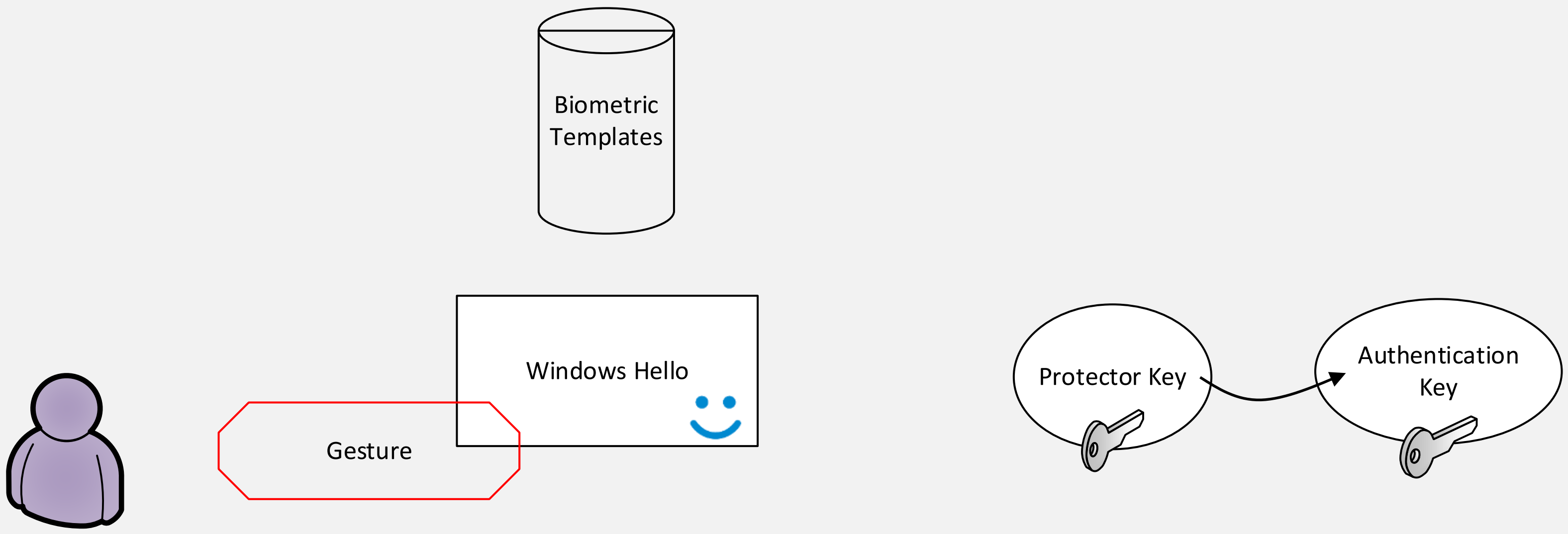
Windows Hello for Business



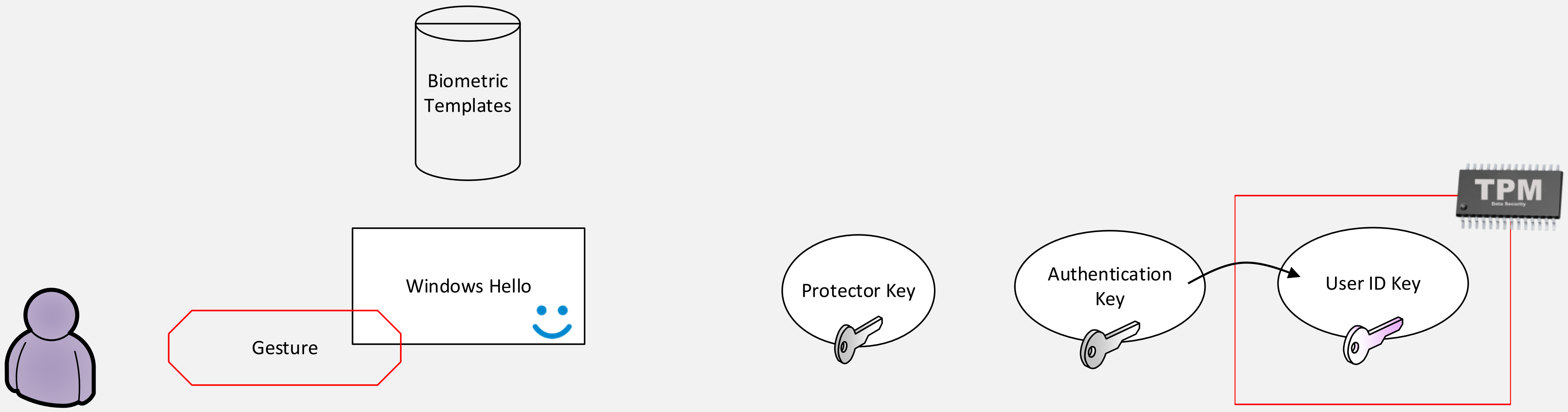
Windows Hello for Business



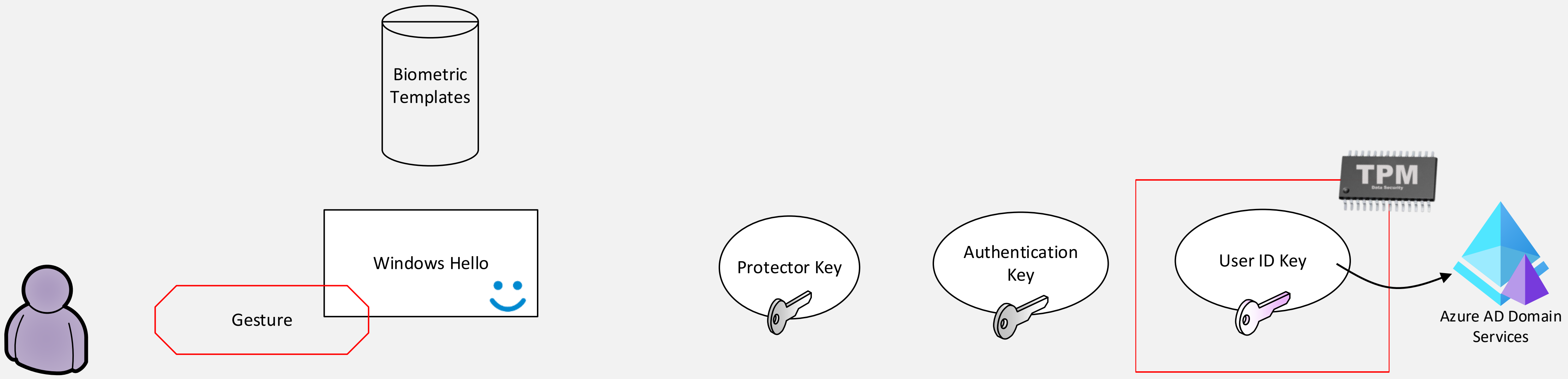
Windows Hello for Business



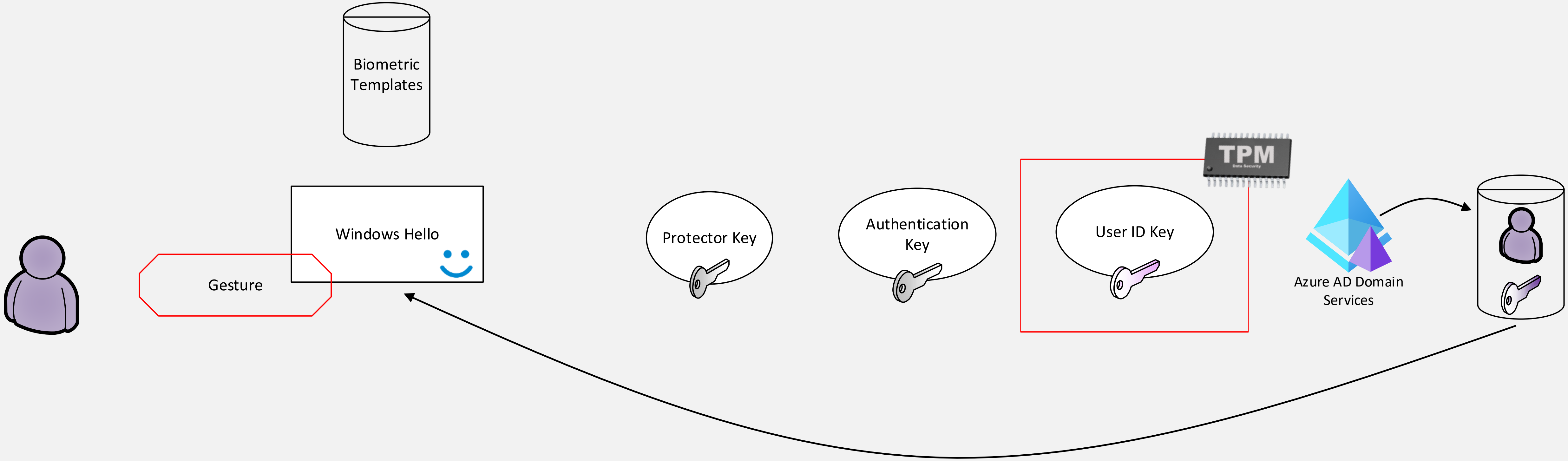
Windows Hello for Business



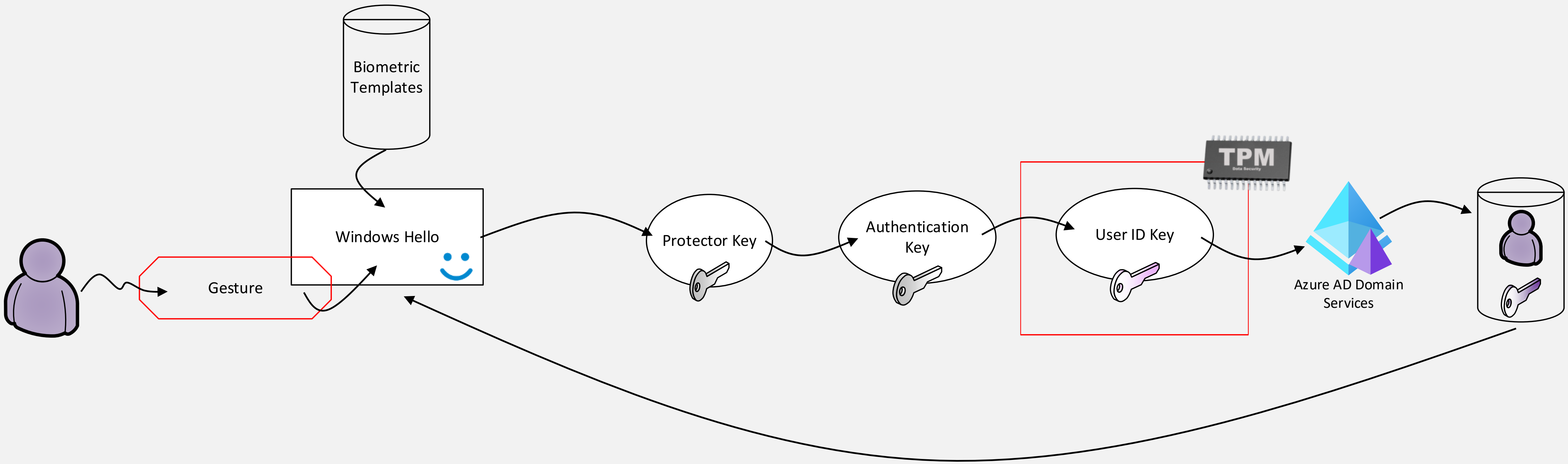
Windows Hello for Business



Windows Hello for Business



Windows Hello for Business

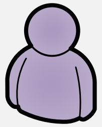


Windows Hello for Business

Internals

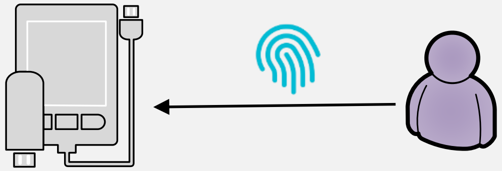
Windows Hello

- Simplified view



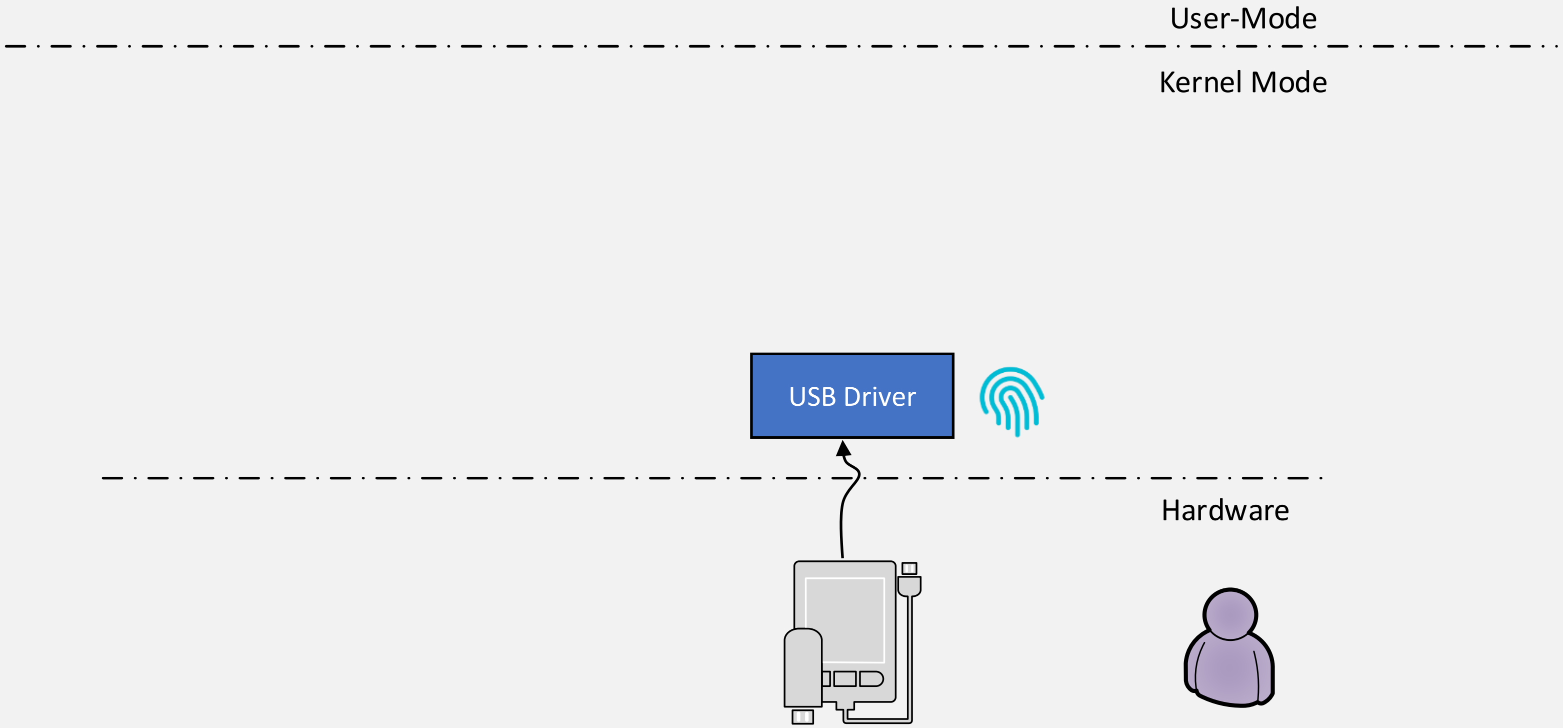
Windows Hello

- Simplified view



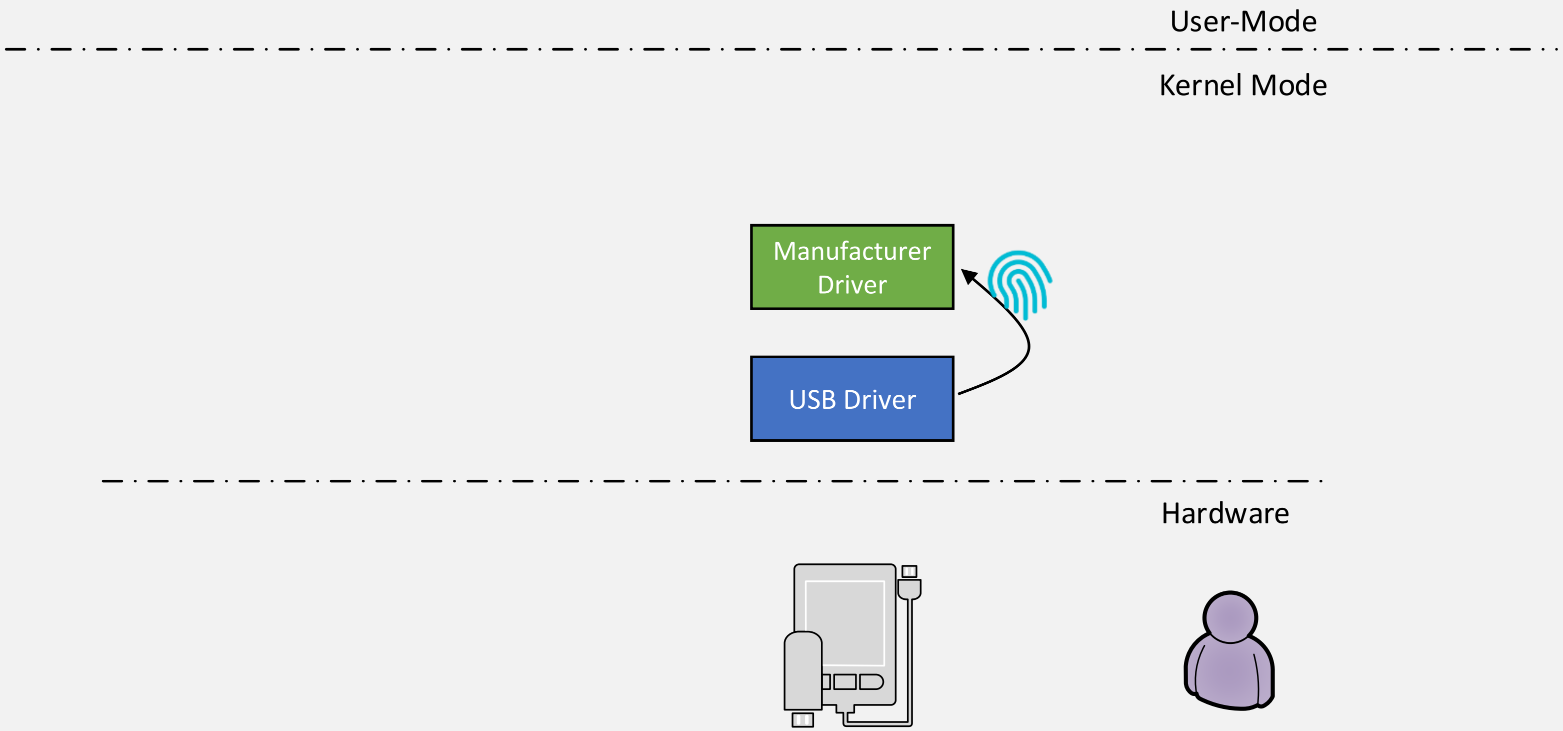
Windows Hello

- Simplified view



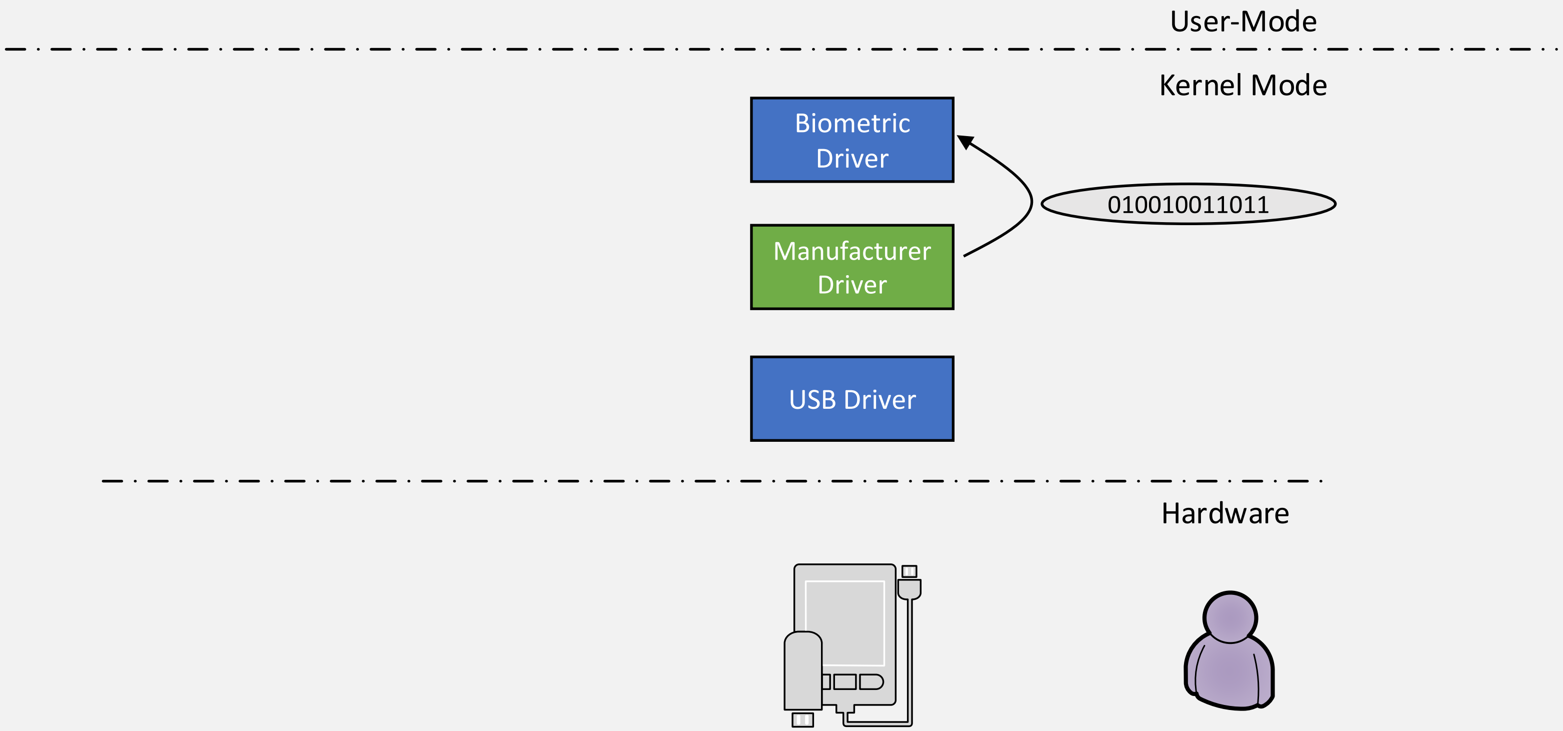
Windows Hello

- Simplified view



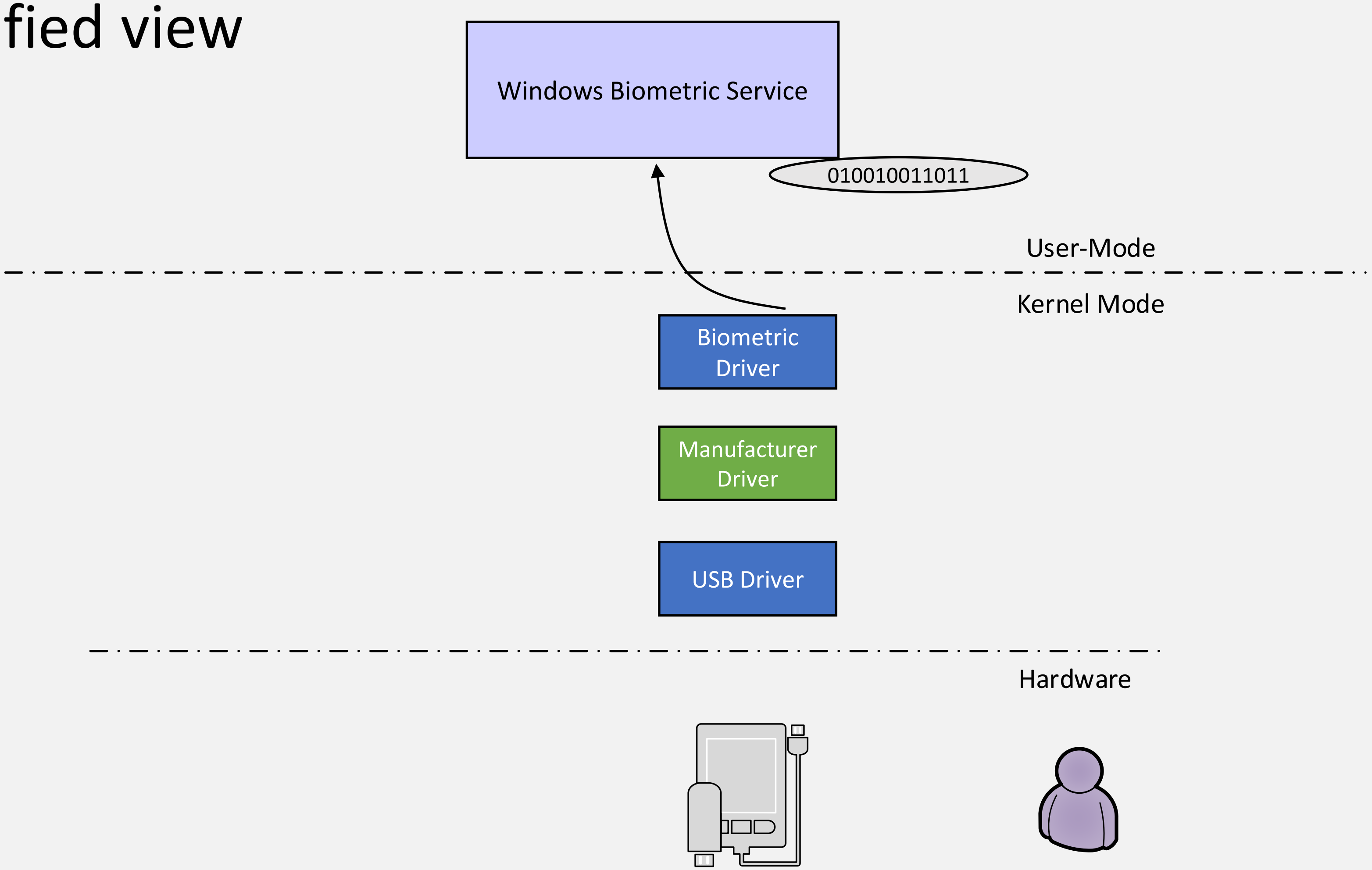
Windows Hello

- Simplified view



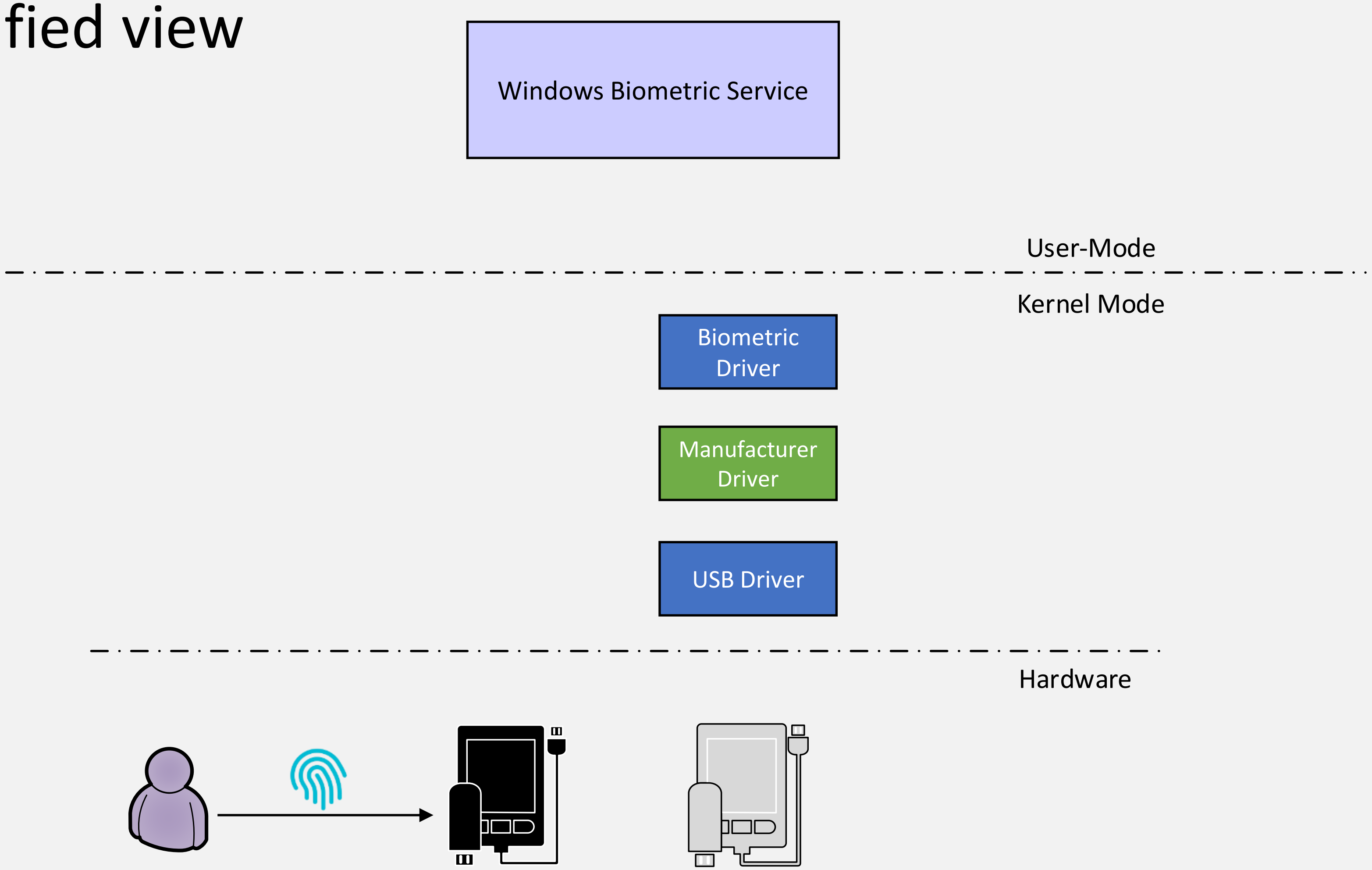
Windows Hello

- Simplified view



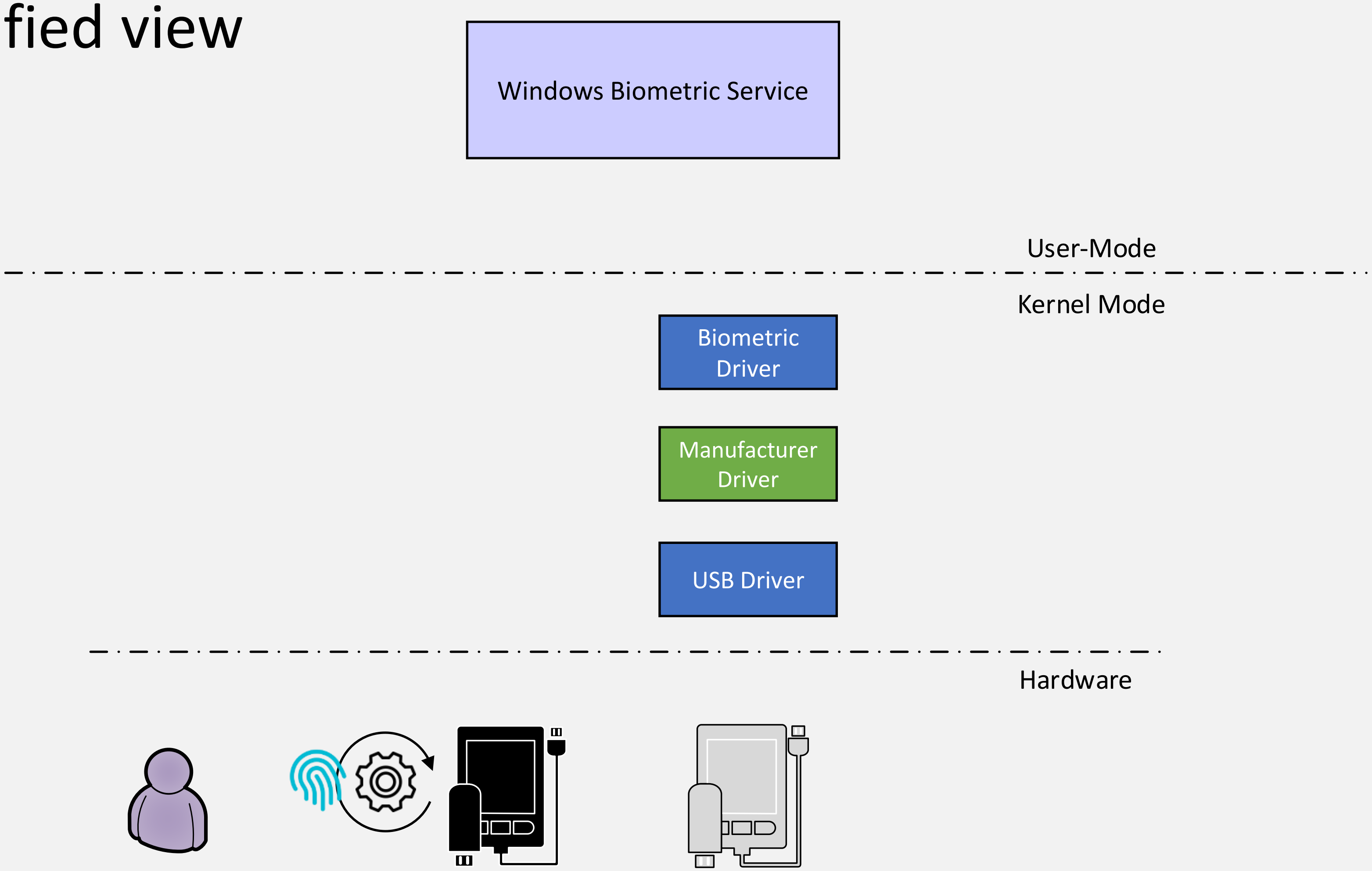
Windows Hello

- Simplified view



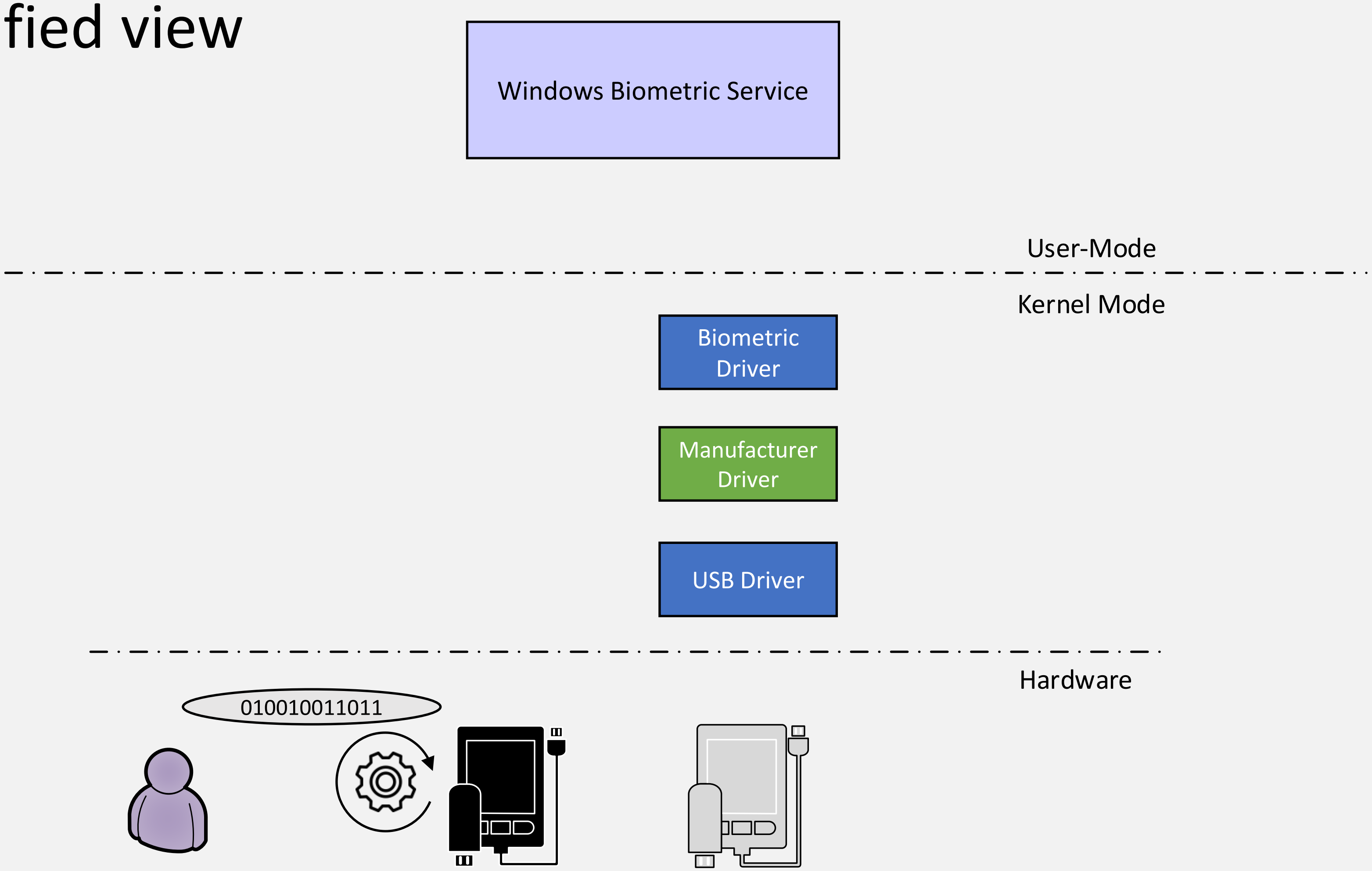
Windows Hello

- Simplified view



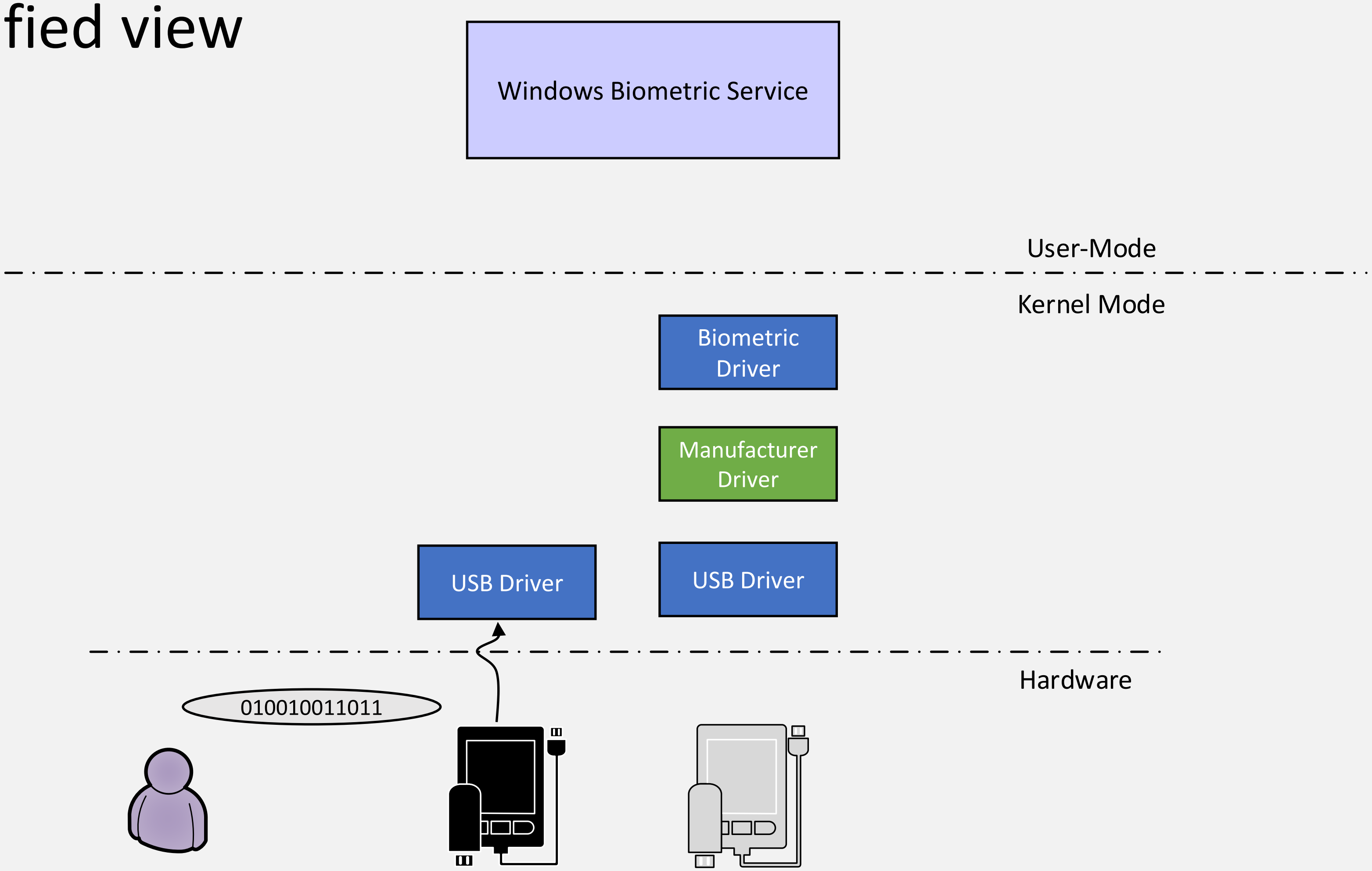
Windows Hello

- Simplified view



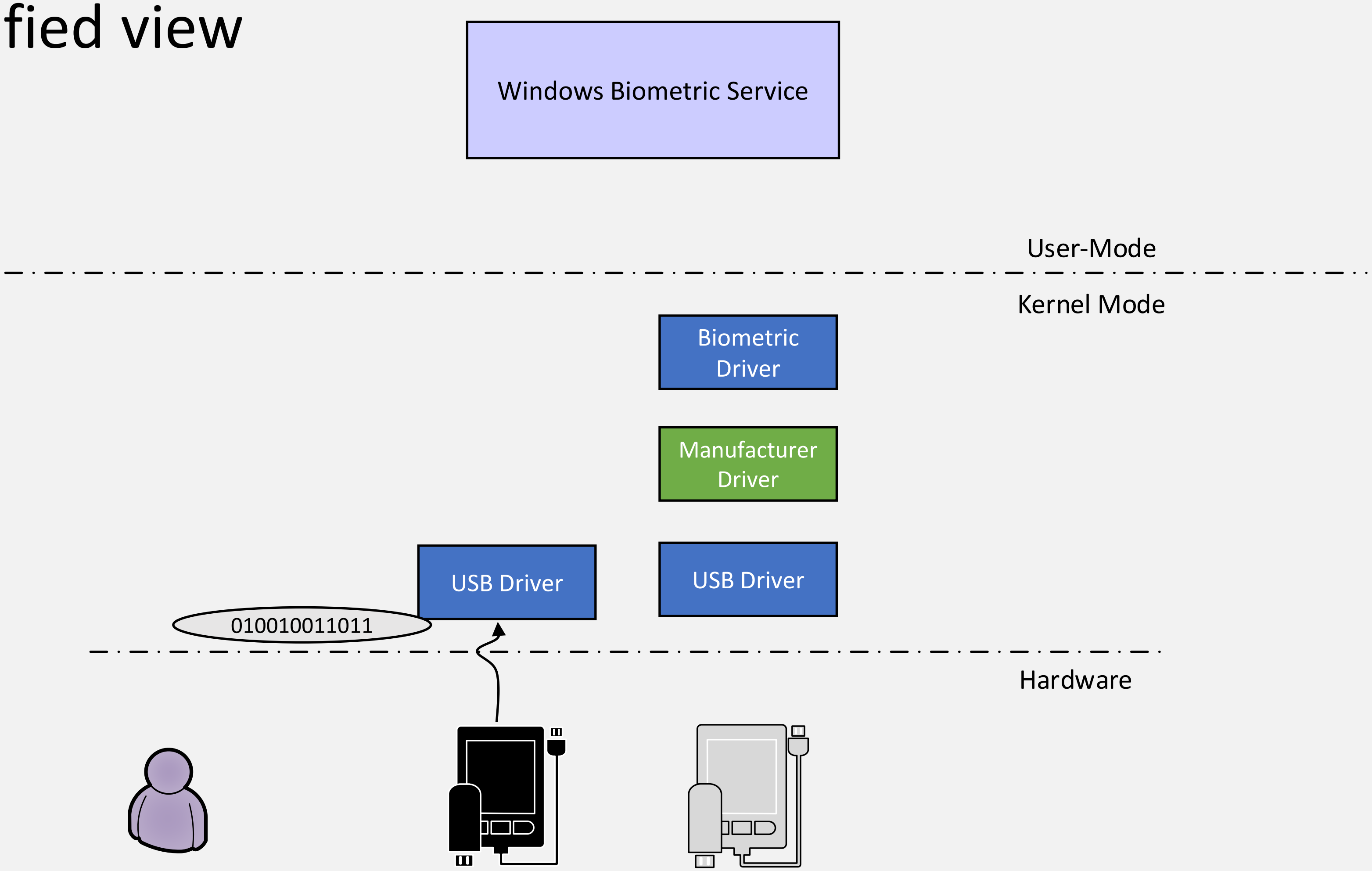
Windows Hello

- Simplified view



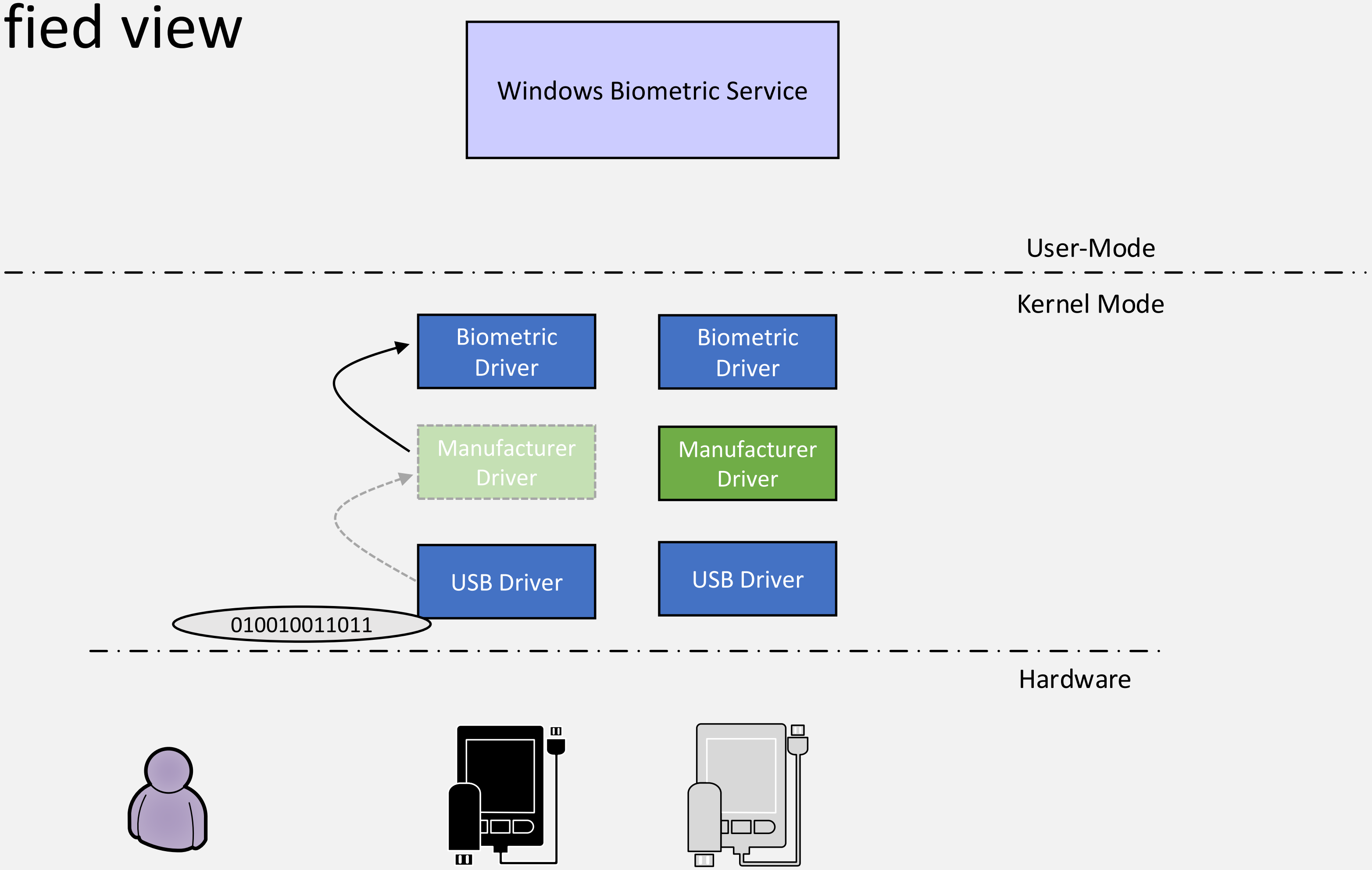
Windows Hello

- Simplified view



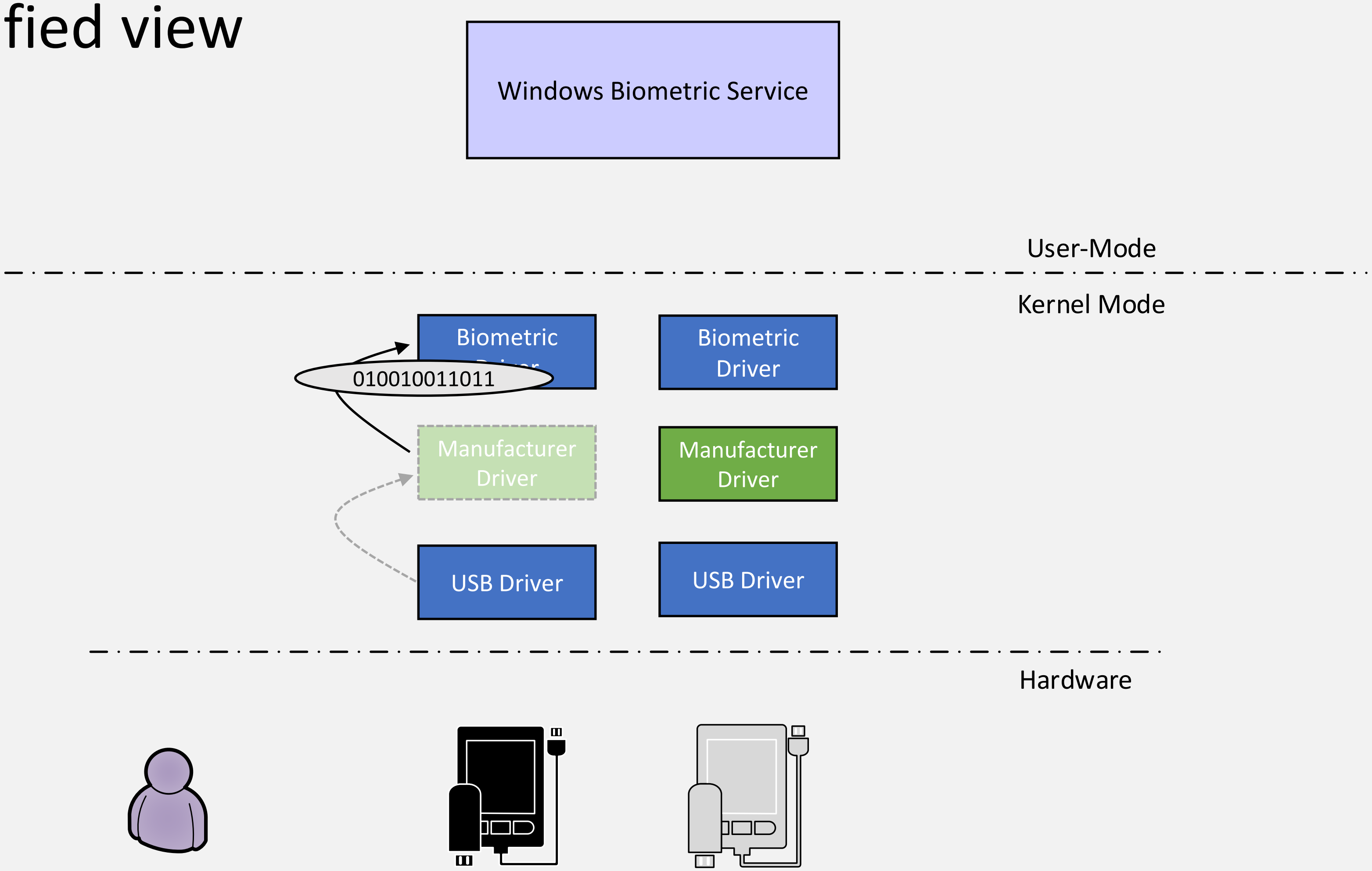
Windows Hello

- Simplified view



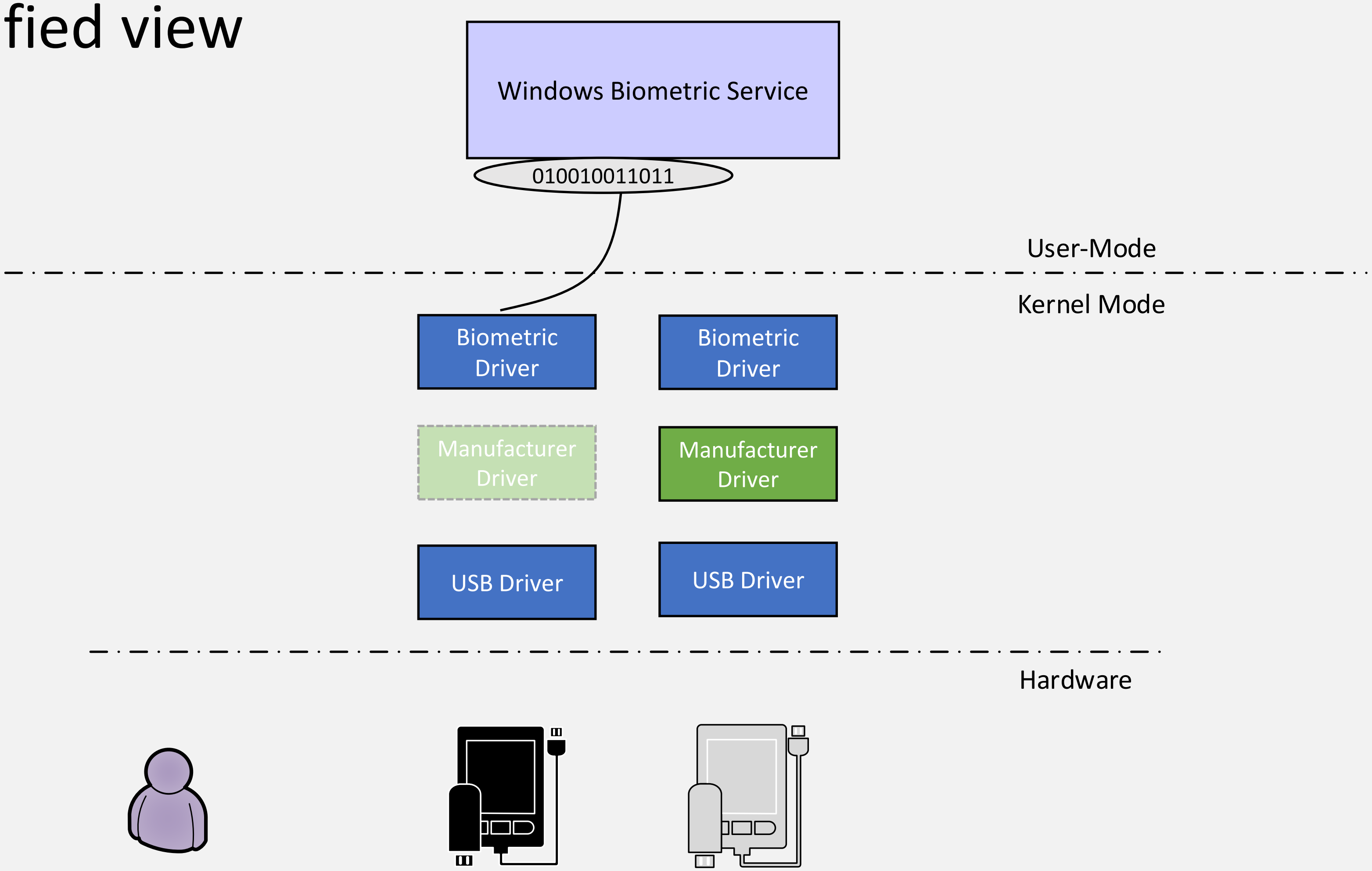
Windows Hello

- Simplified view



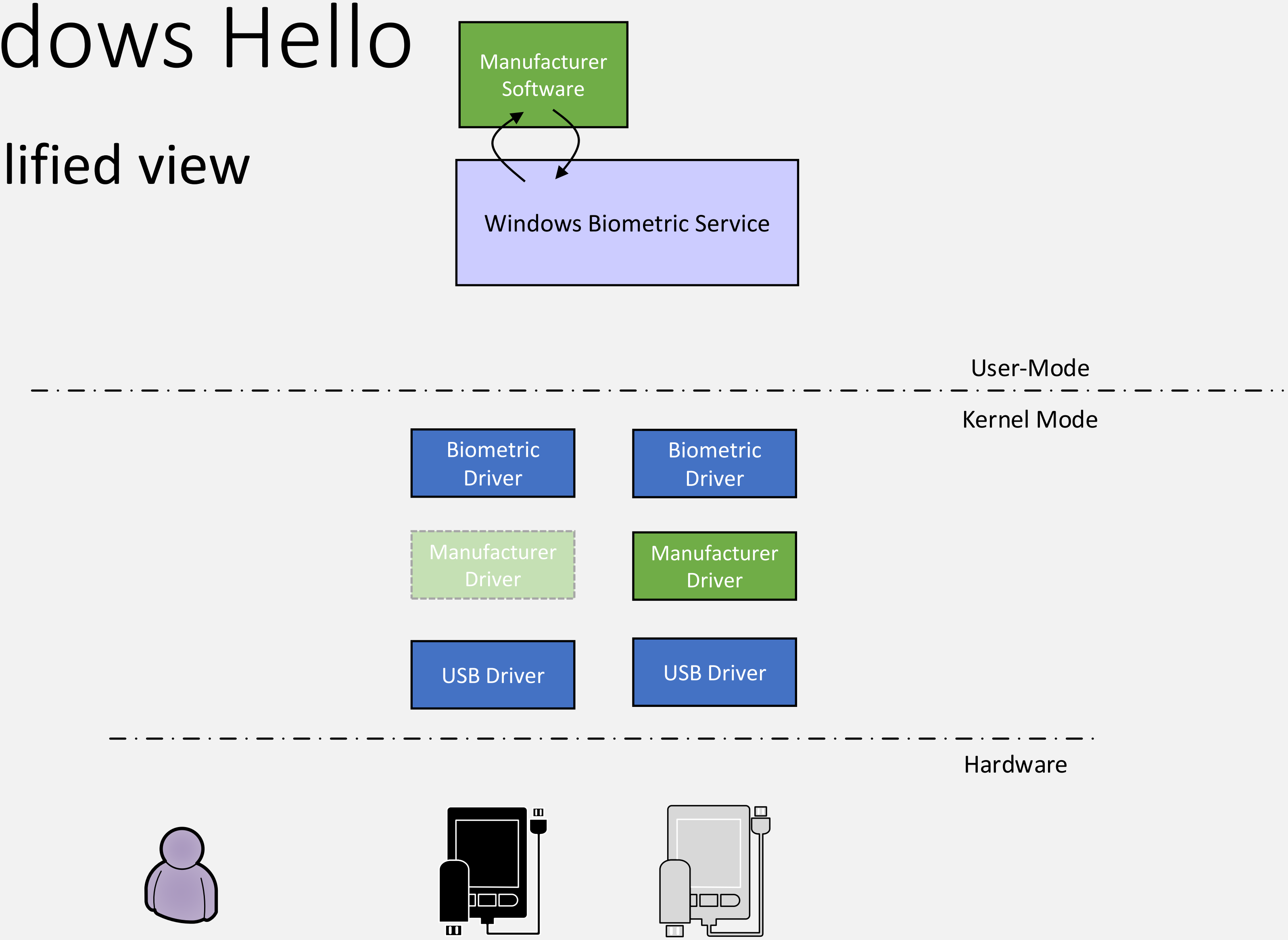
Windows Hello

- Simplified view



Windows Hello

- Simplified view



Manufacturer Software

Windows Biometric Service

User-Mode

Kernel Mode

Biometric Driver

Biometric Driver

Manufacturer Driver

Manufacturer Driver

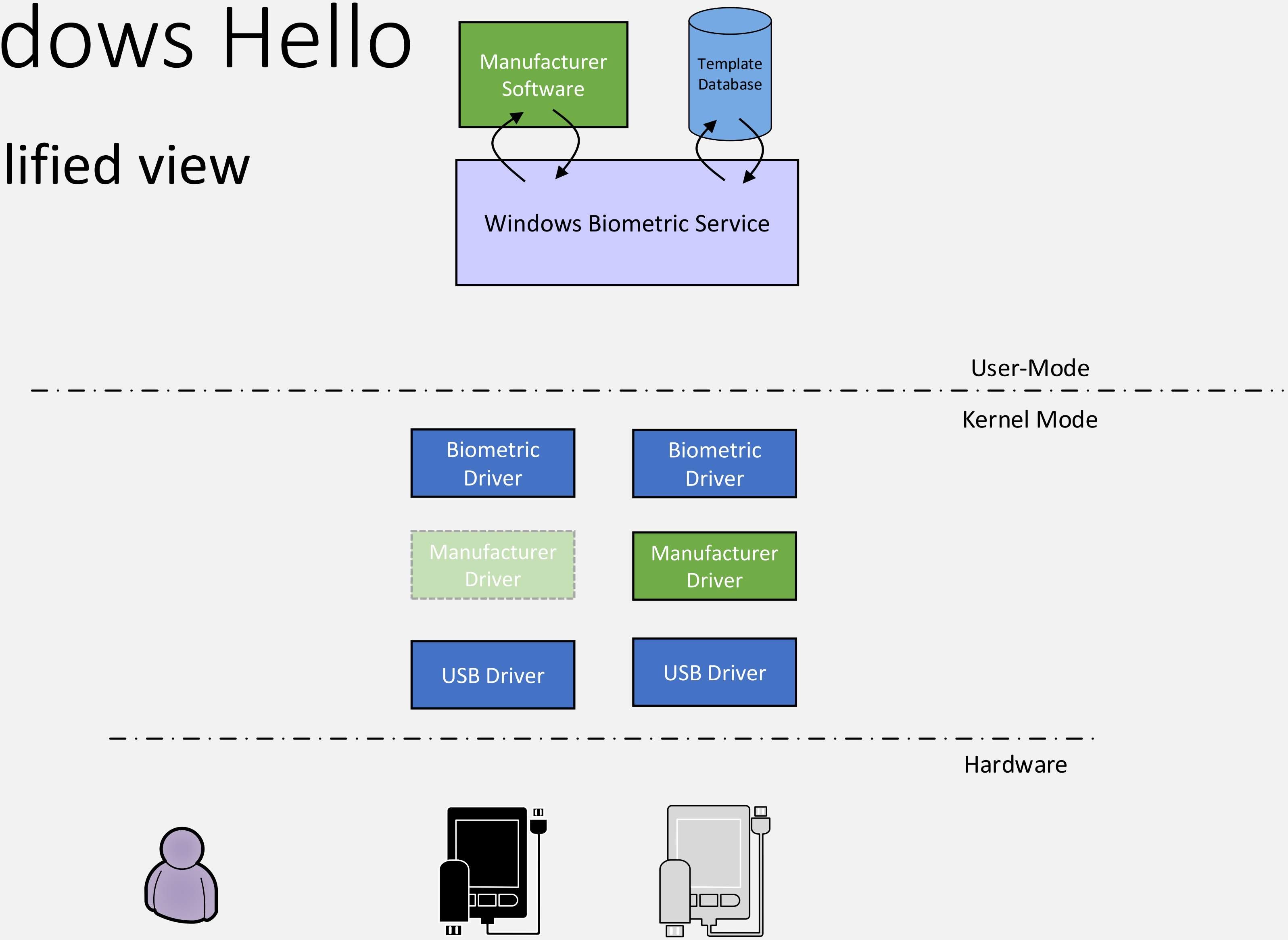
USB Driver

USB Driver

Hardware

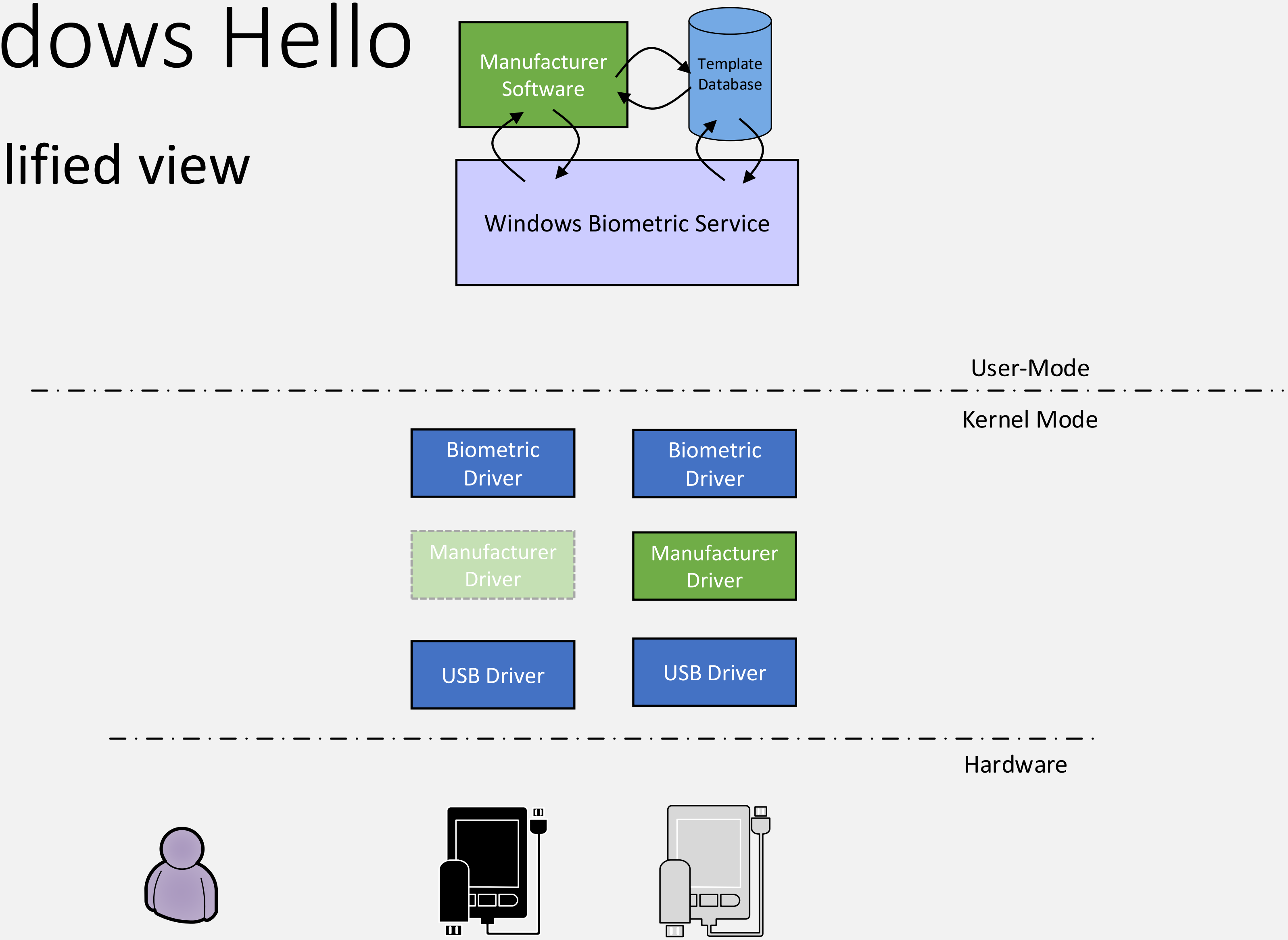
Windows Hello

- Simplified view



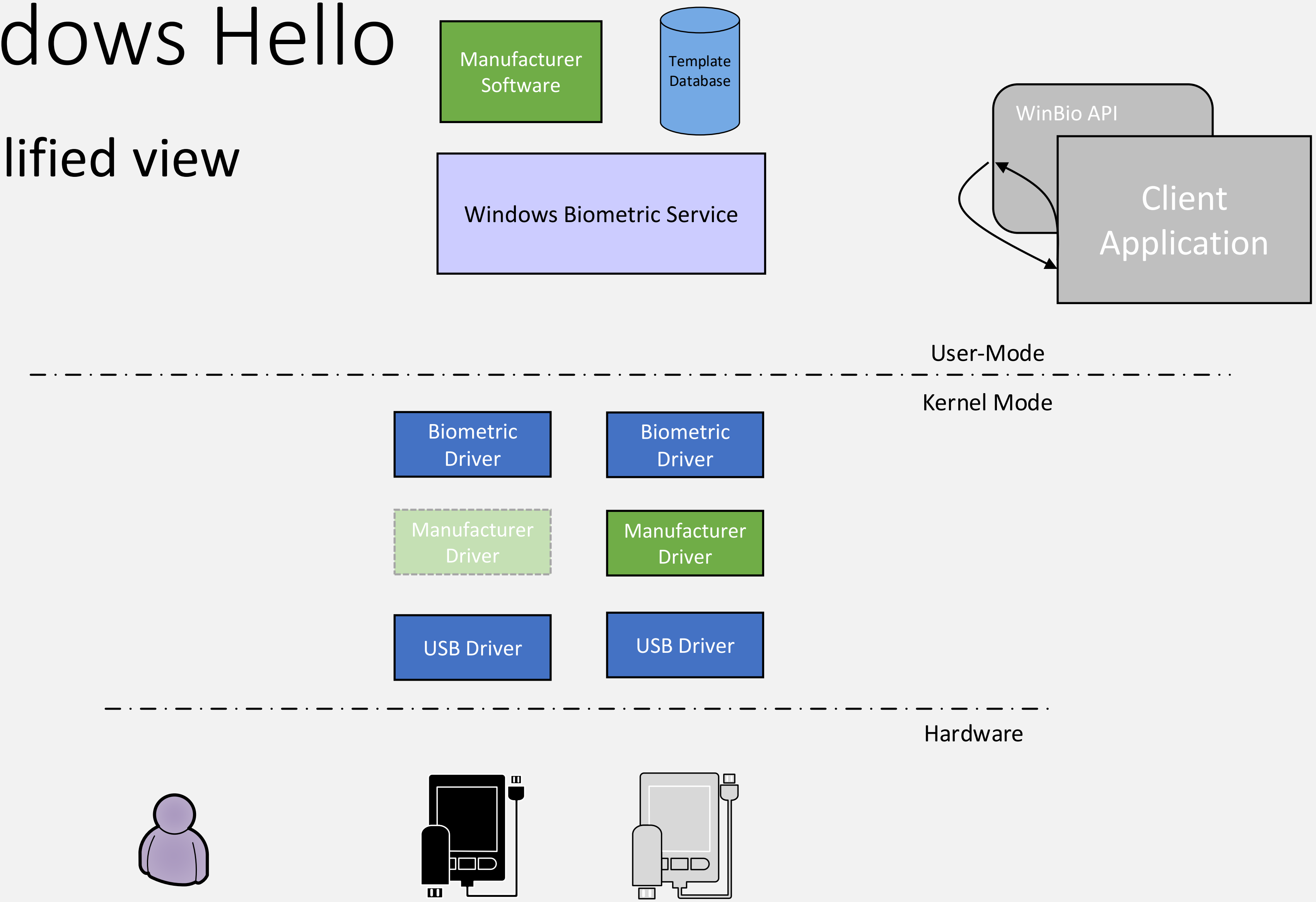
Windows Hello

- Simplified view



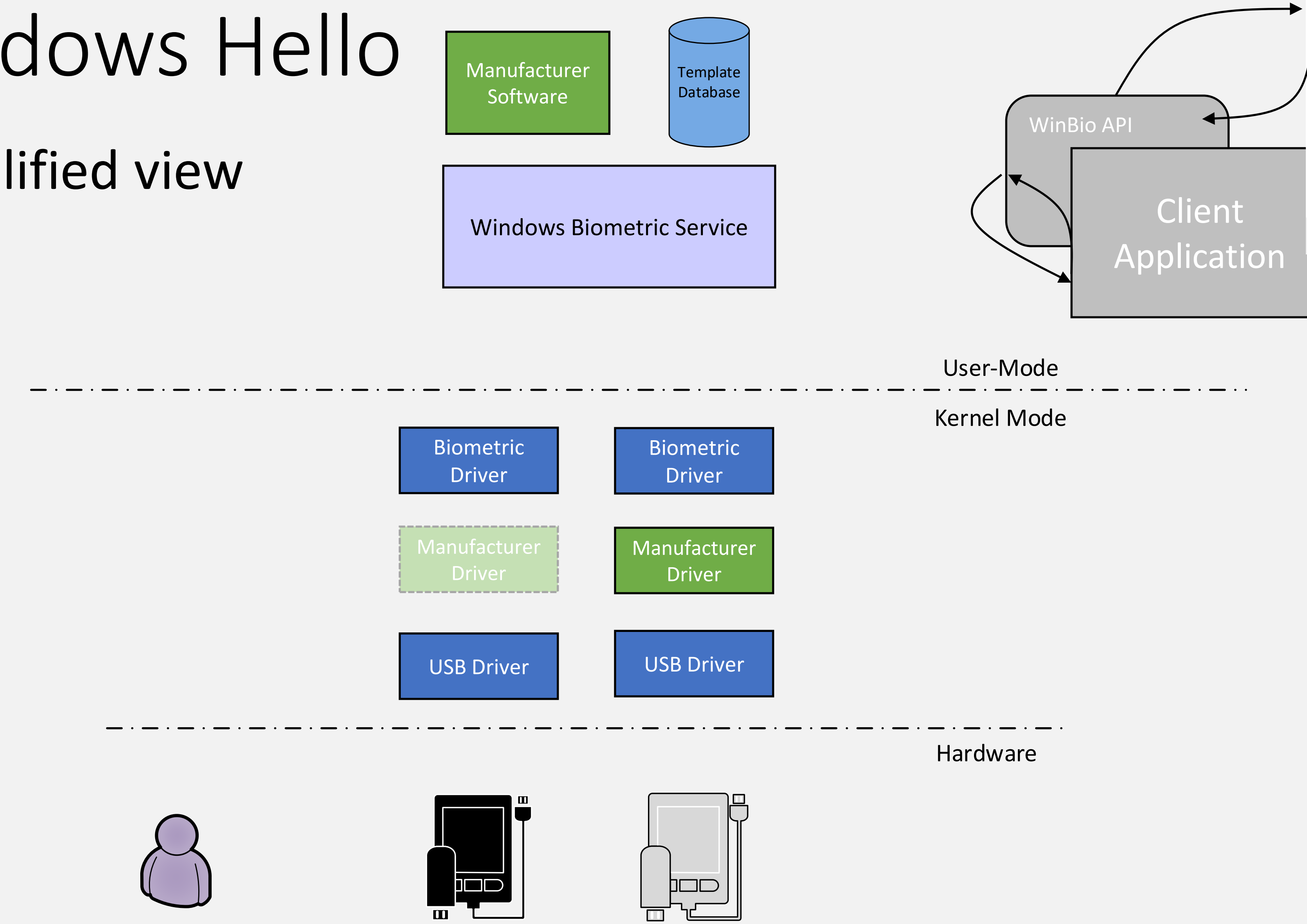
Windows Hello

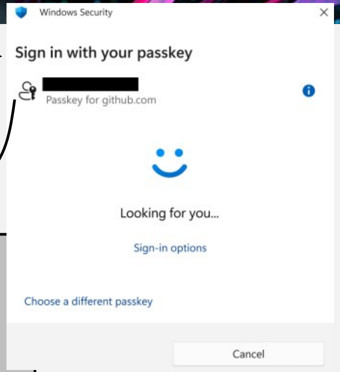
- Simplified view



Windows Hello

- Simplified view





Windows Security

Sign in with your passkey

[redacted]
Passkey for github.com

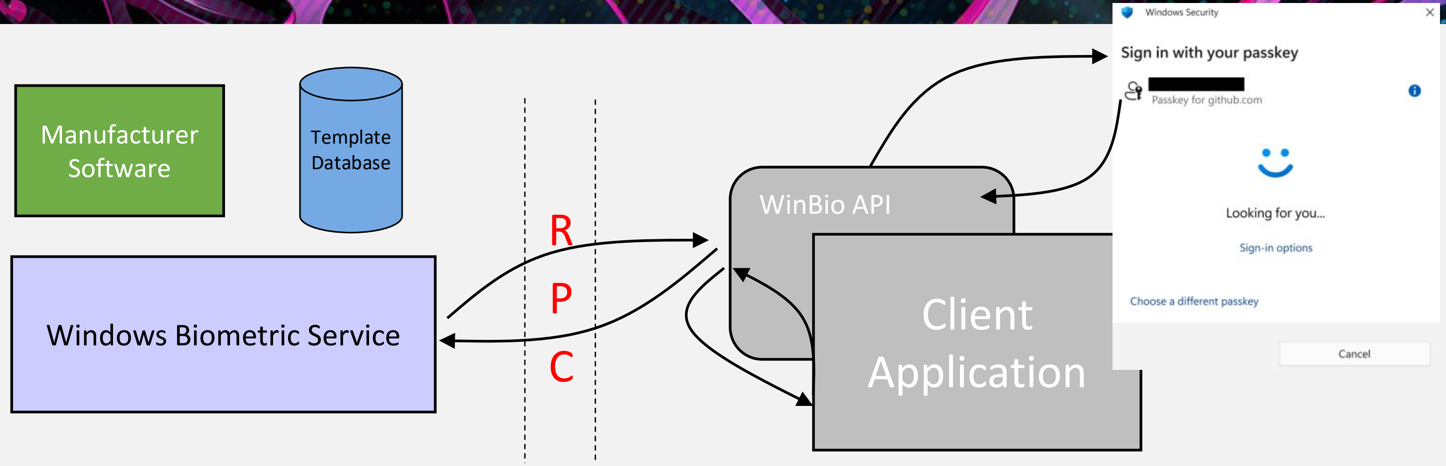
Looking for you...

Sign-in options

Choose a different passkey

Windows Hello

- Simplified view



Windows Security

Sign in with your passkey

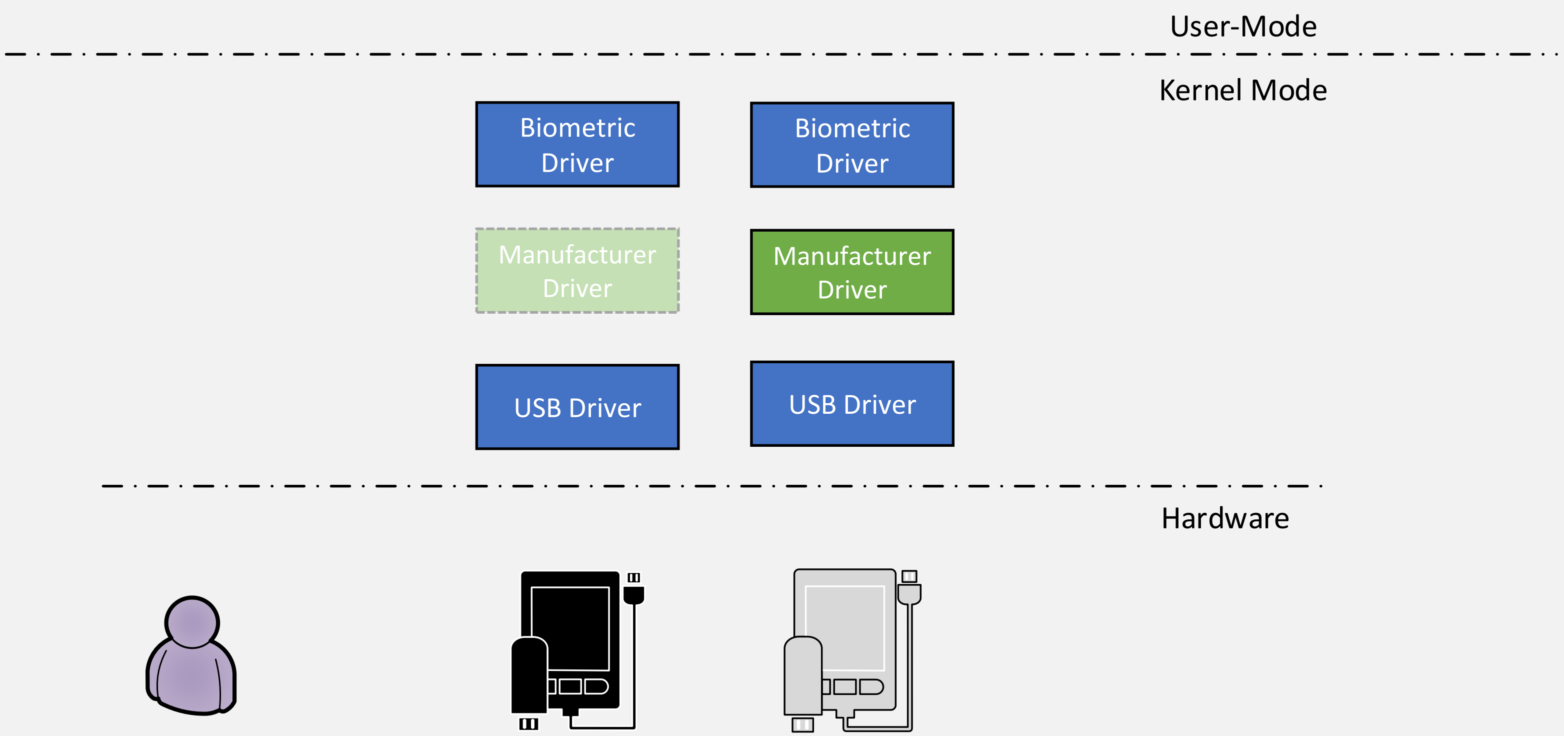
[redacted]
Passkey for github.com

Looking for you...

Sign-in options

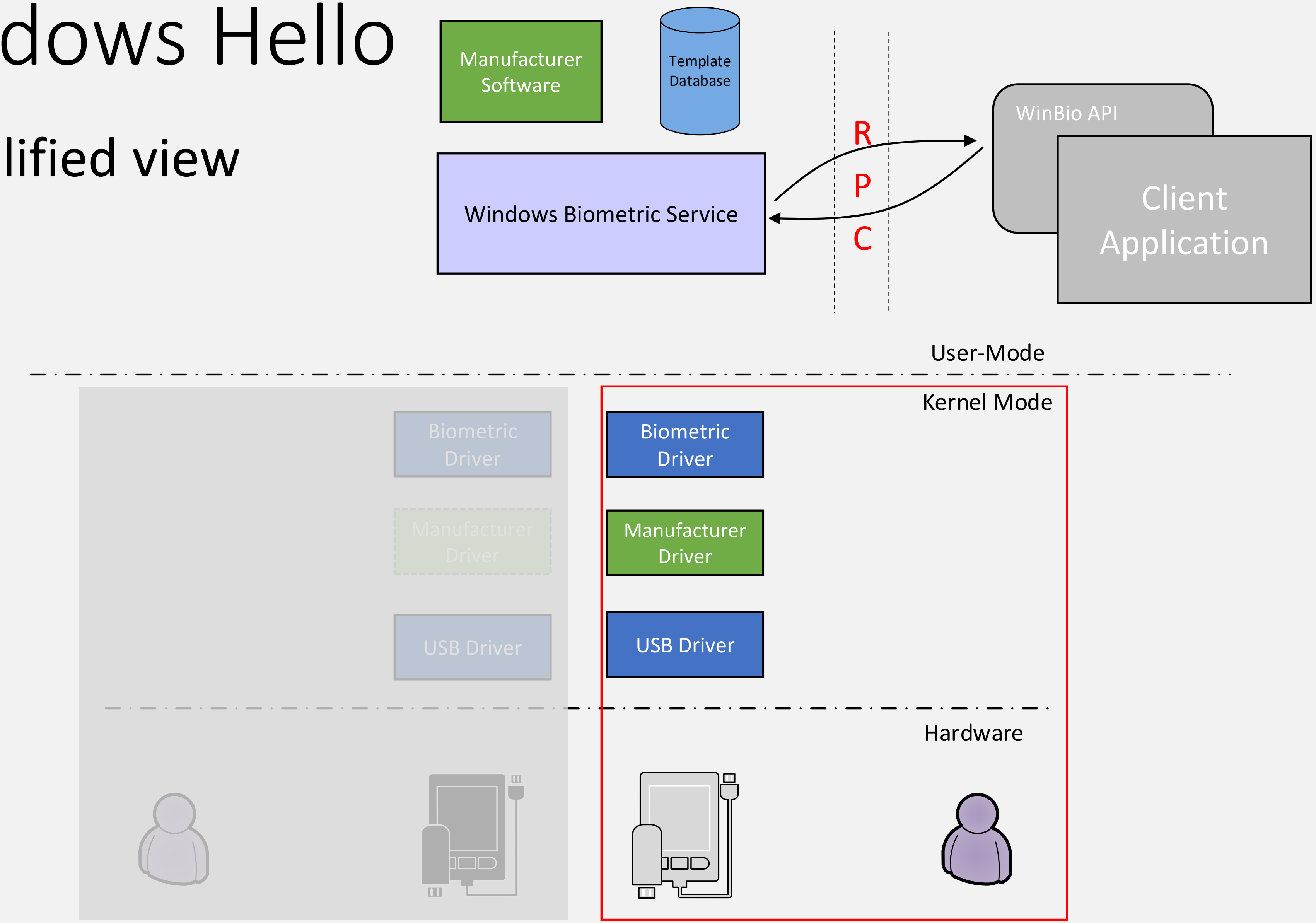
Choose a different passkey

Cancel



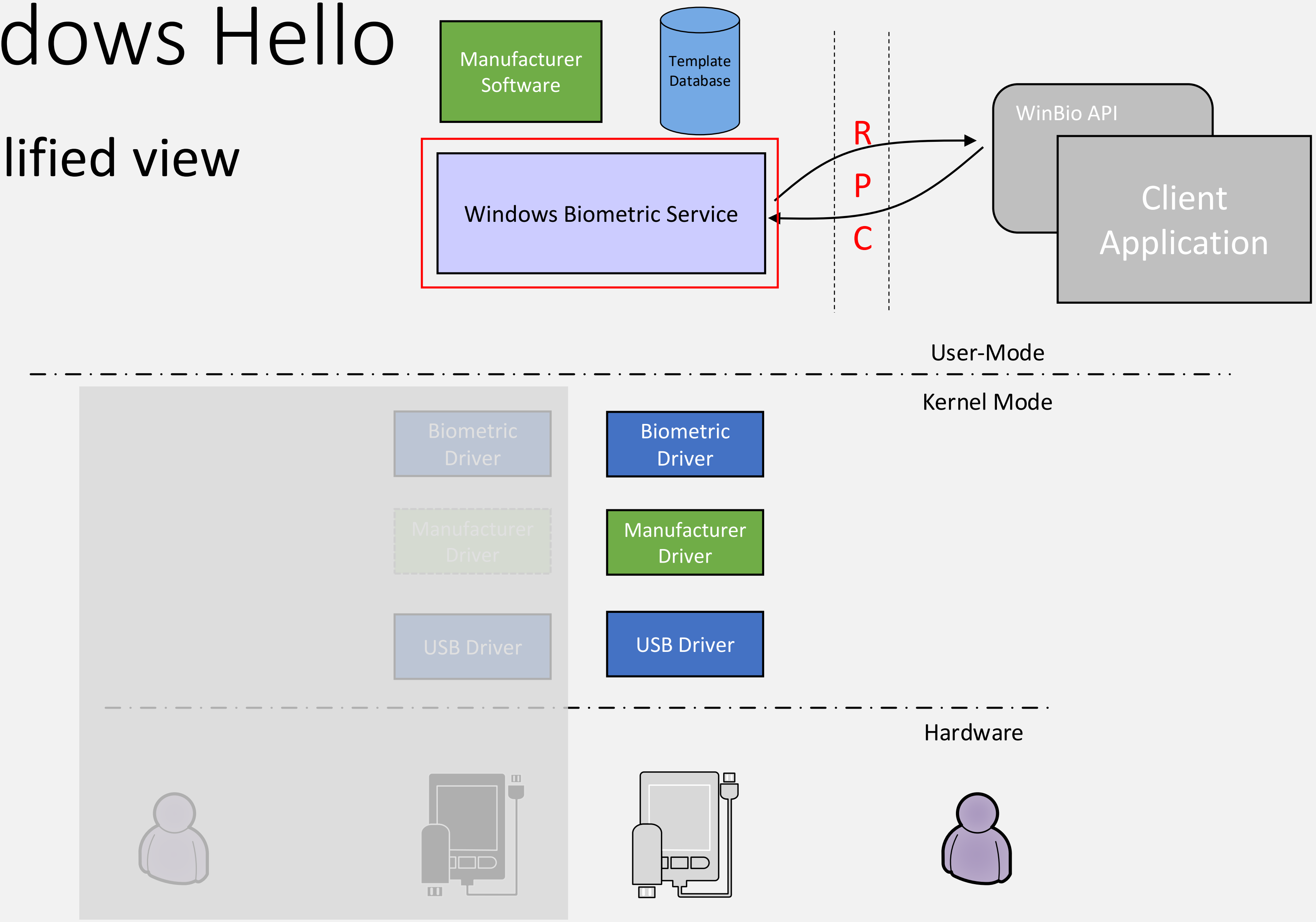
Windows Hello

- Simplified view



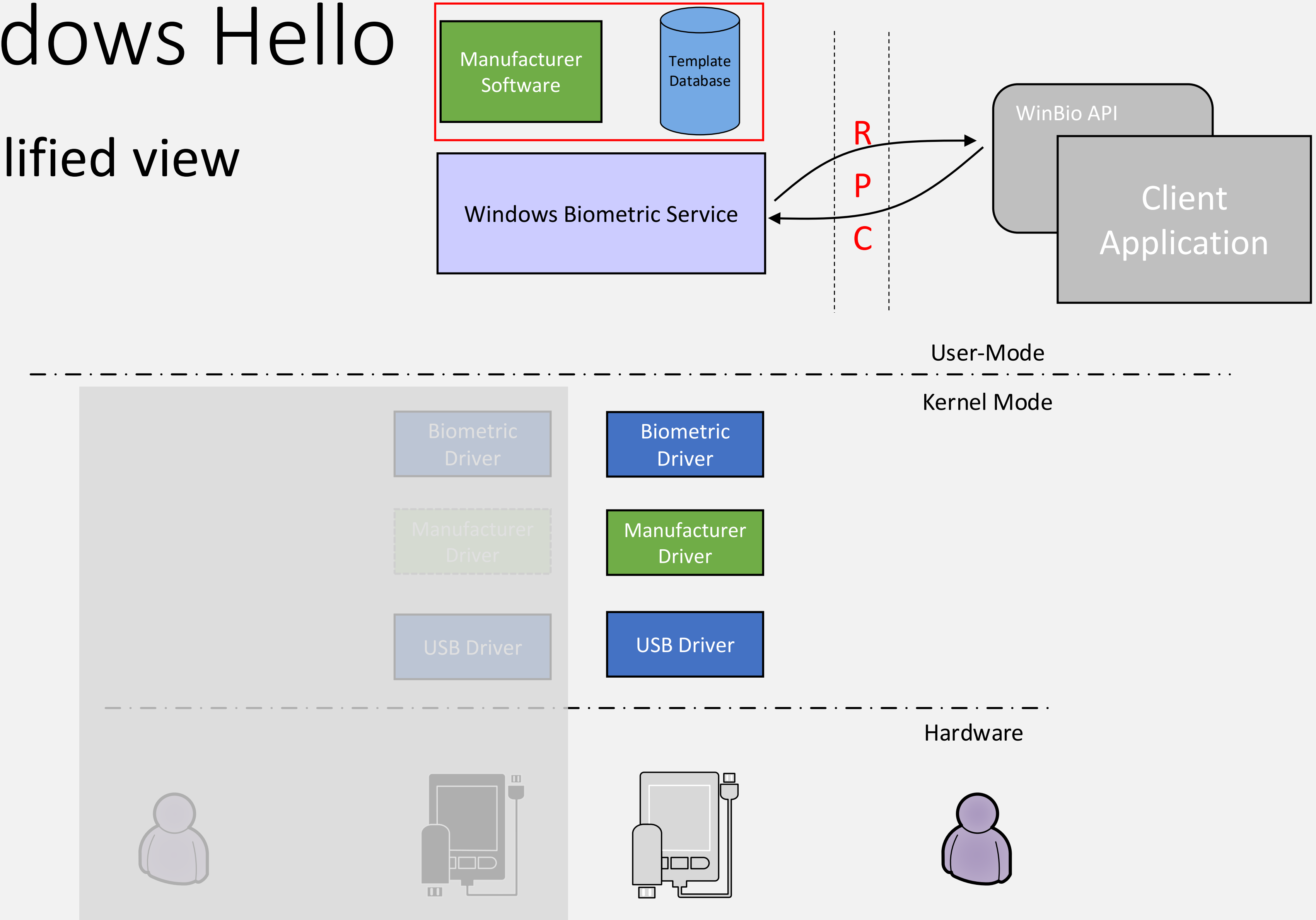
Windows Hello

- Simplified view

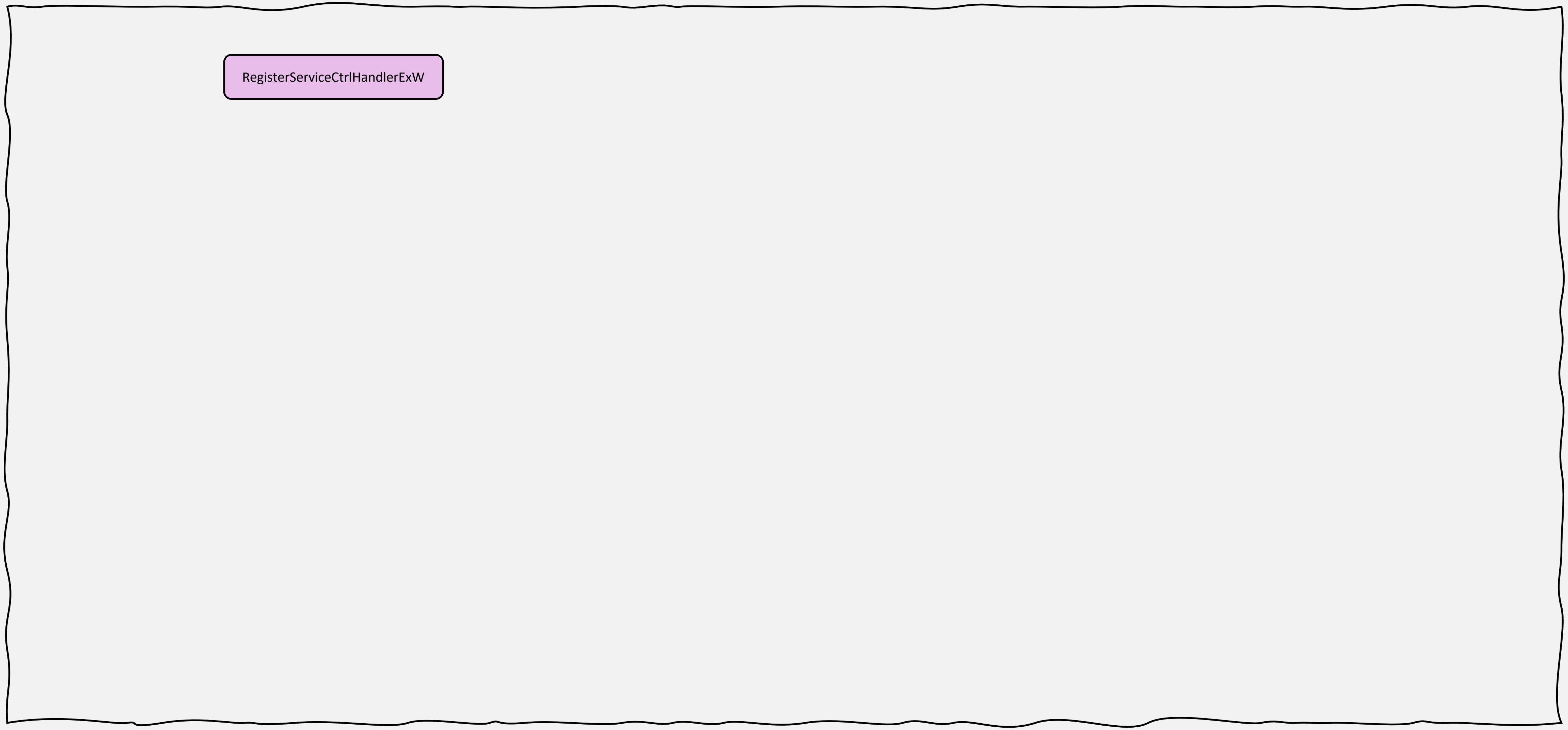


Windows Hello

- Simplified view

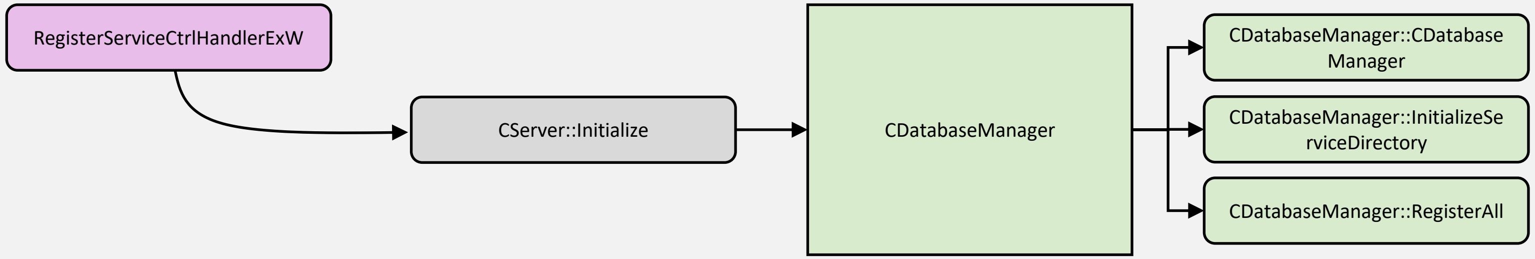


Windows Biometric Service – Initialization

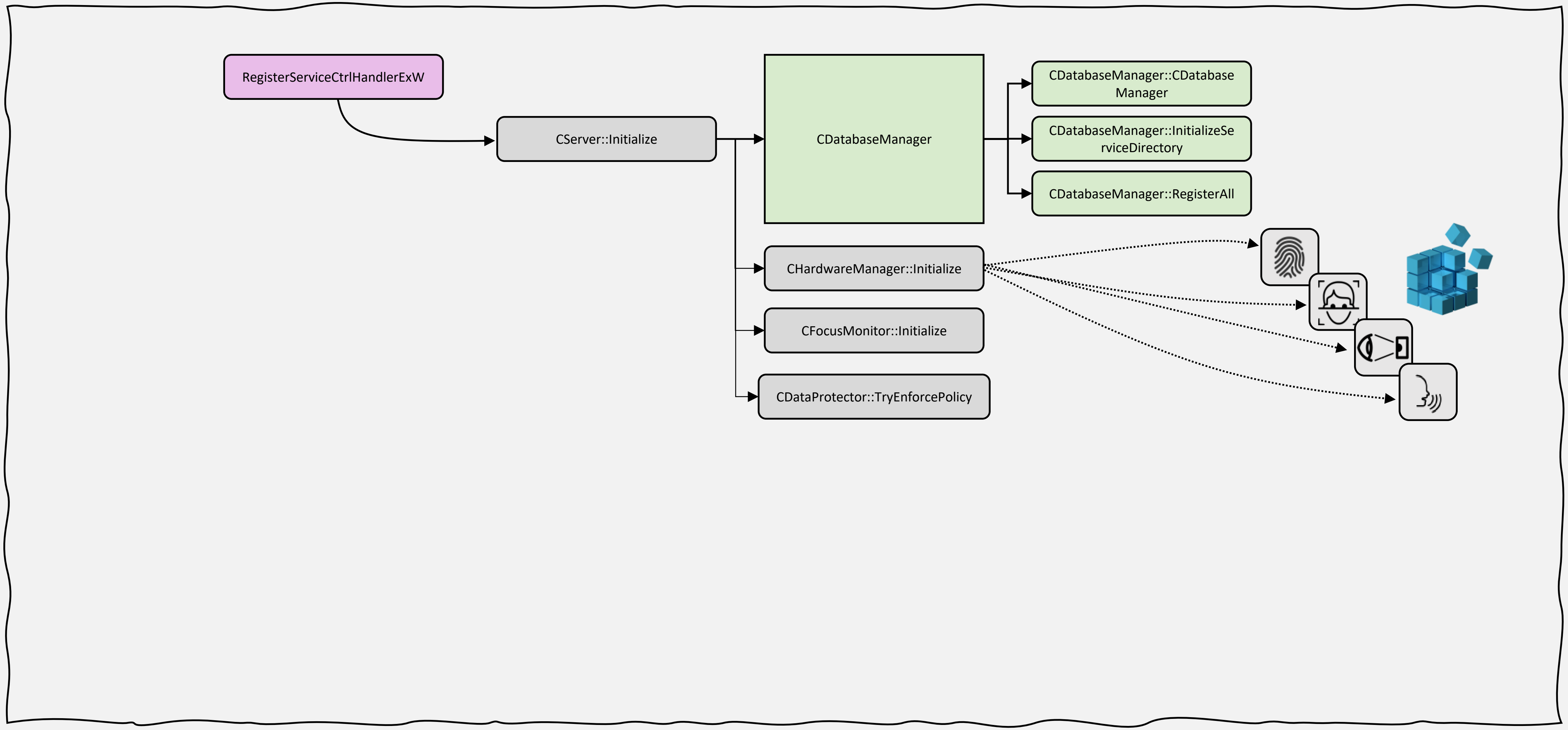


RegisterServiceCtrlHandlerExW

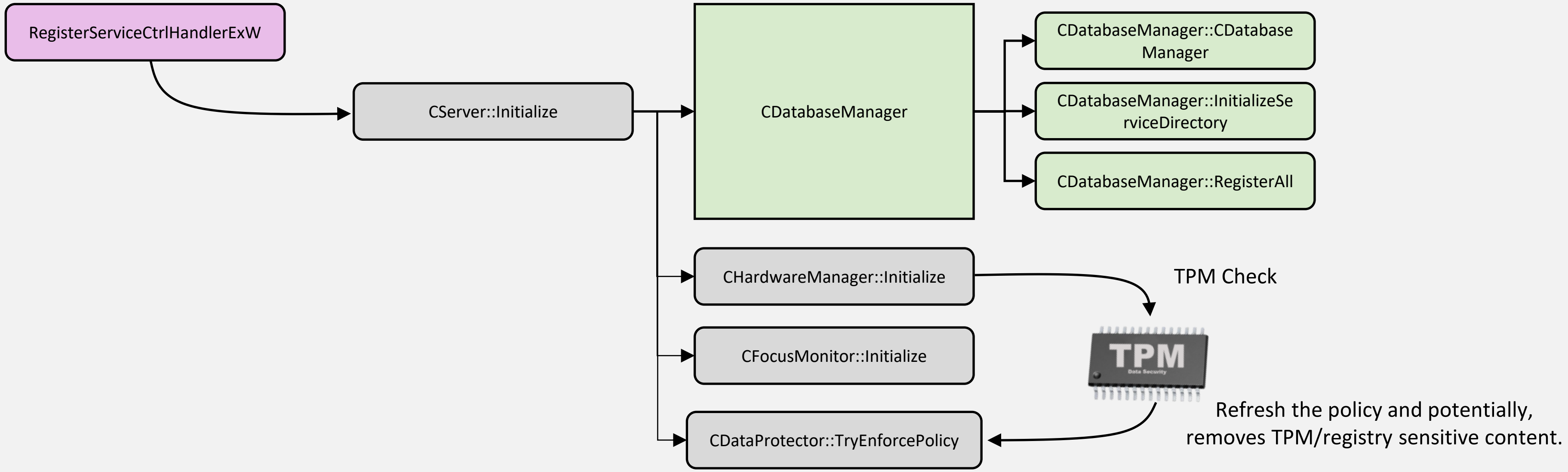
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll

Windows Biometric Service – Initialization

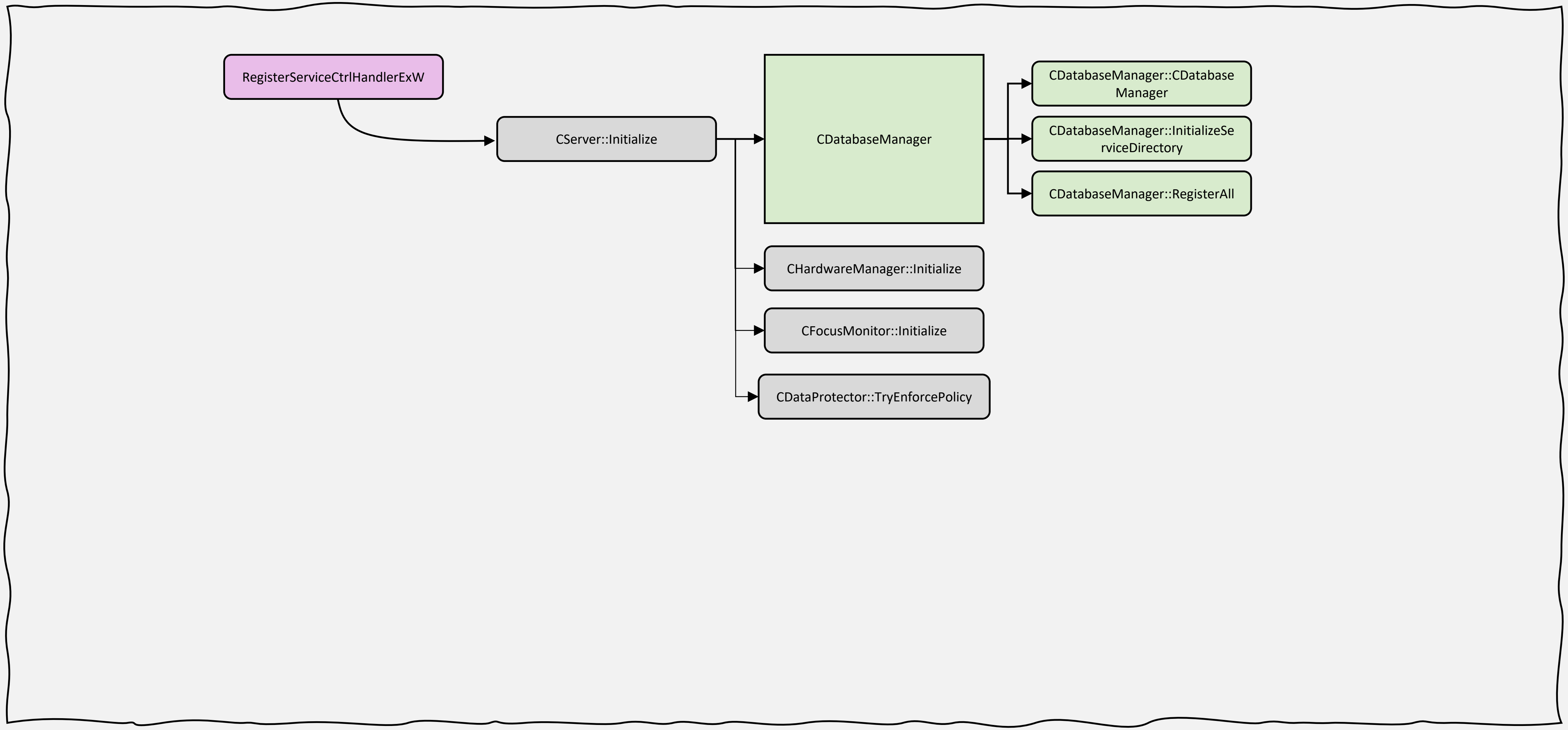

RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy

Windows Biometric Service – Initialization

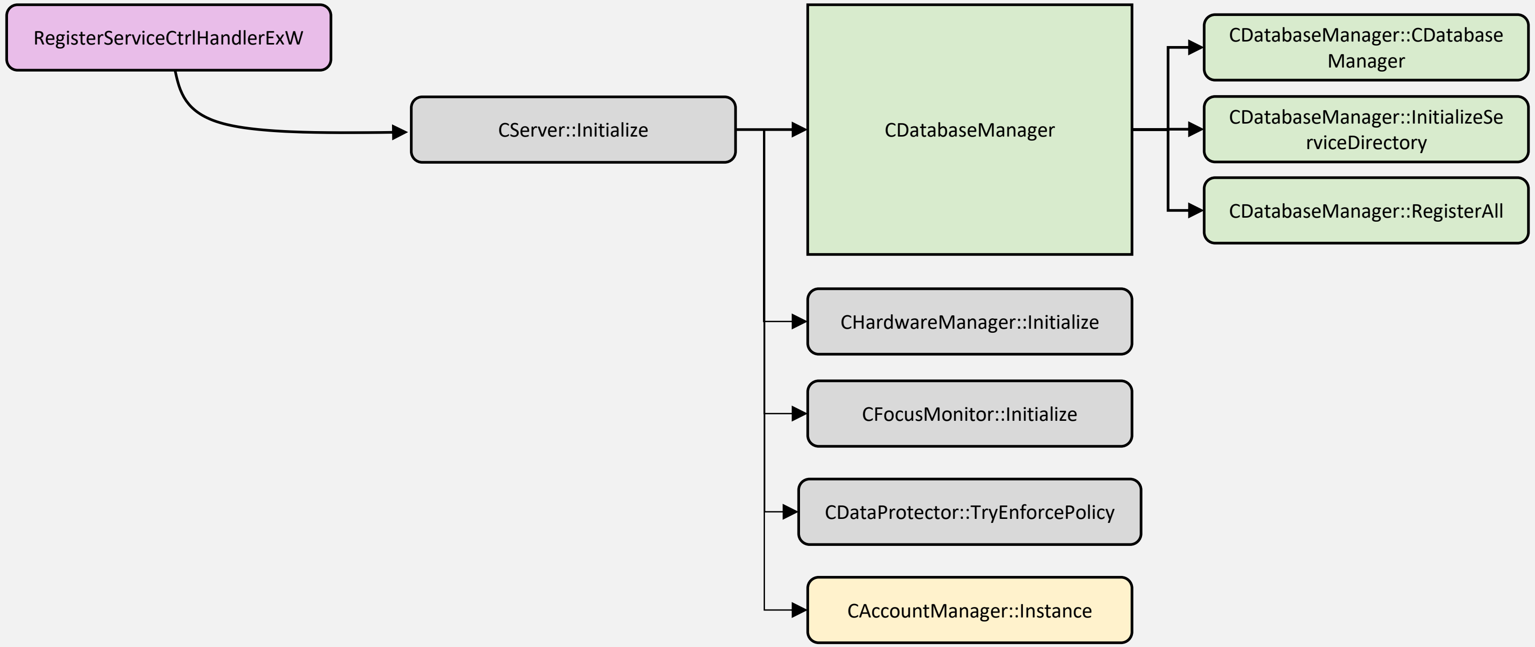

RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
TPM Check
TPM
Data Security

Refresh the policy and potentially, removes TPM/registry sensitive content.

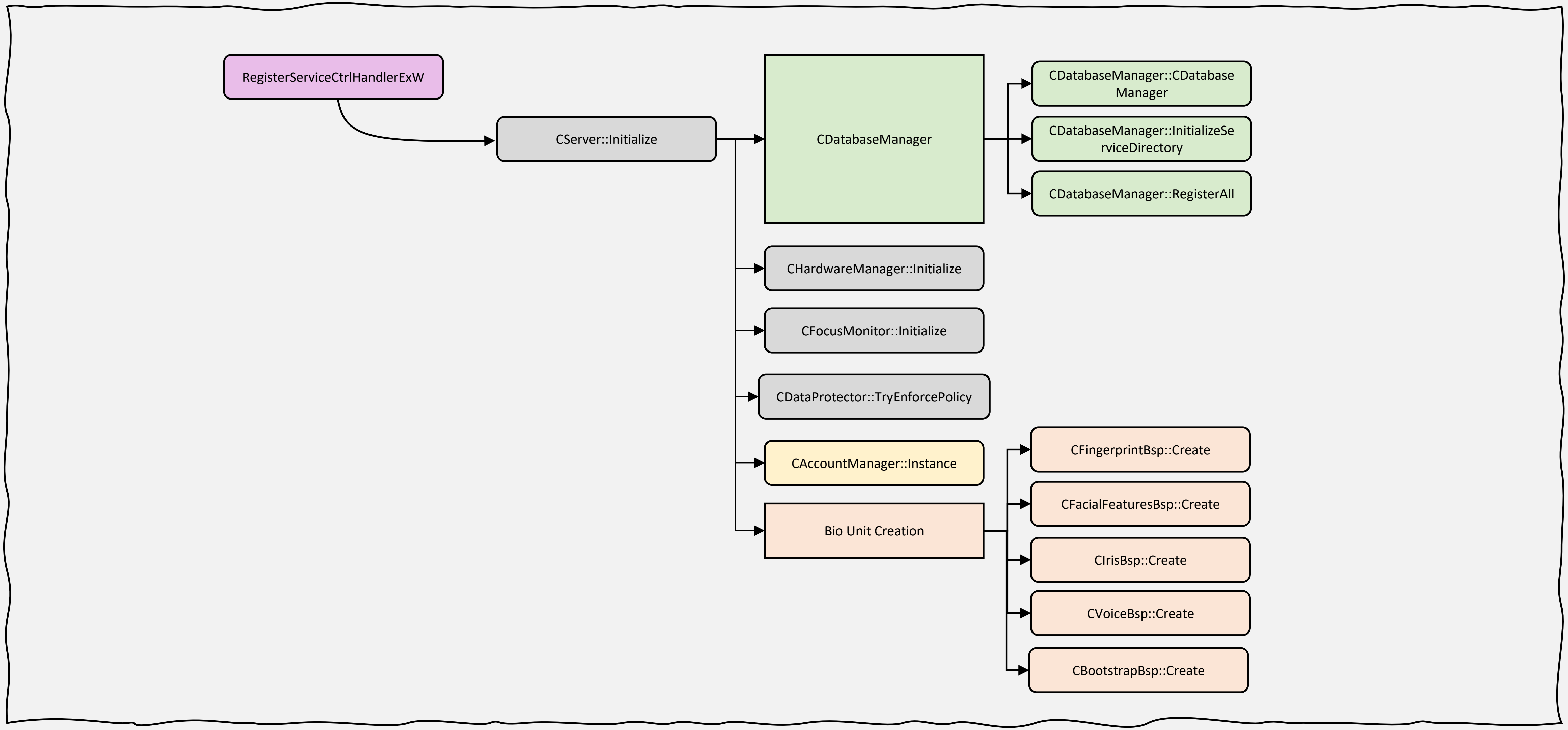
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy

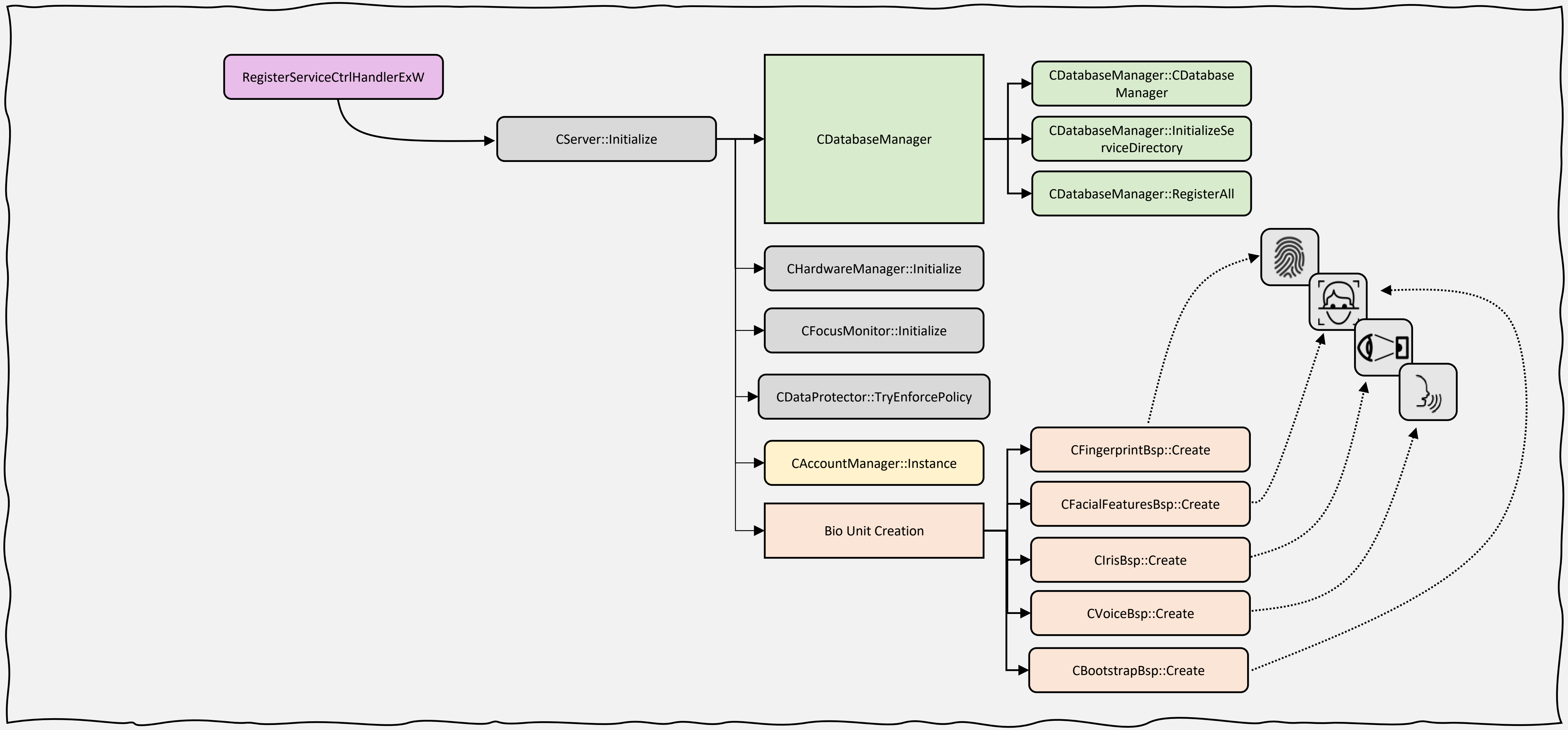
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance

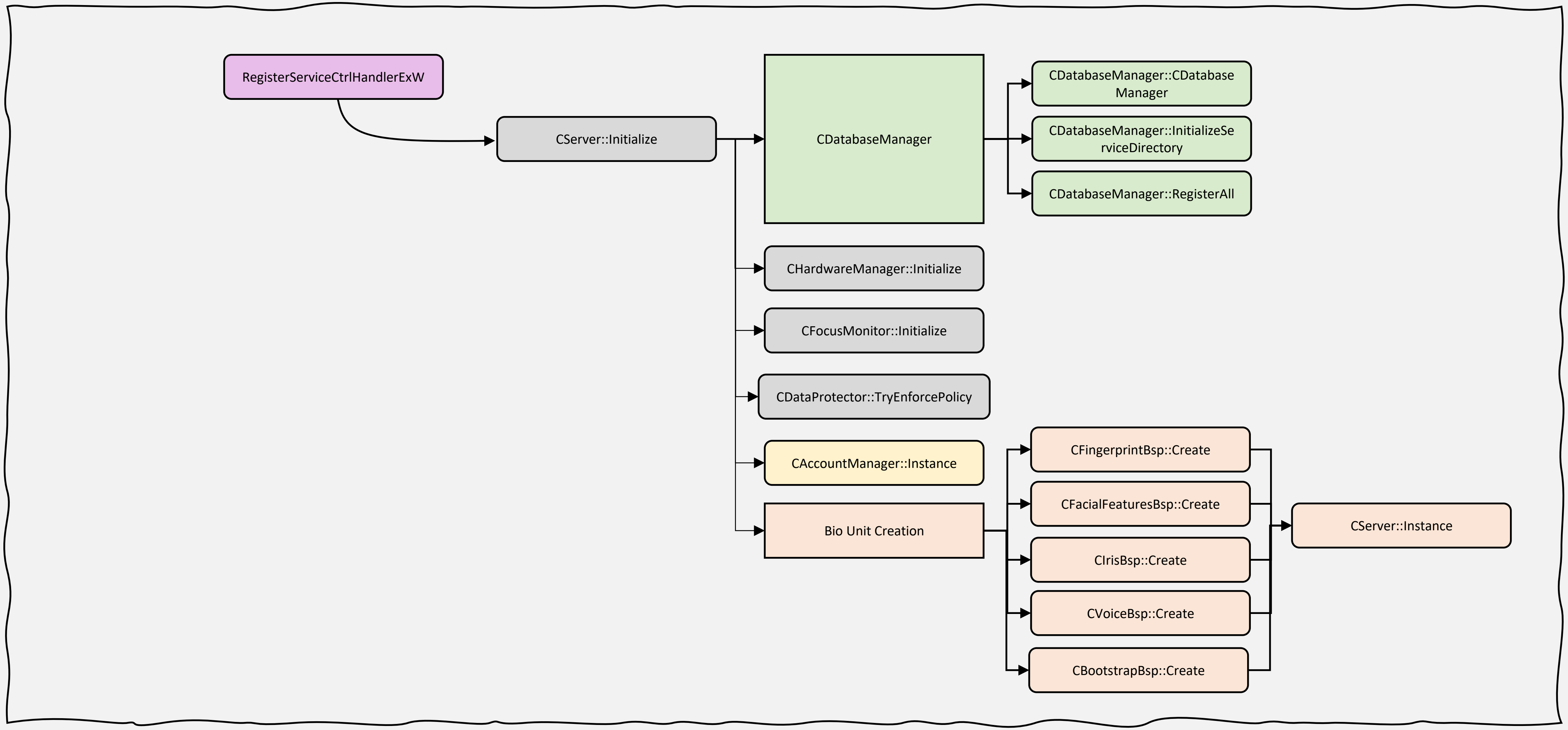
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create

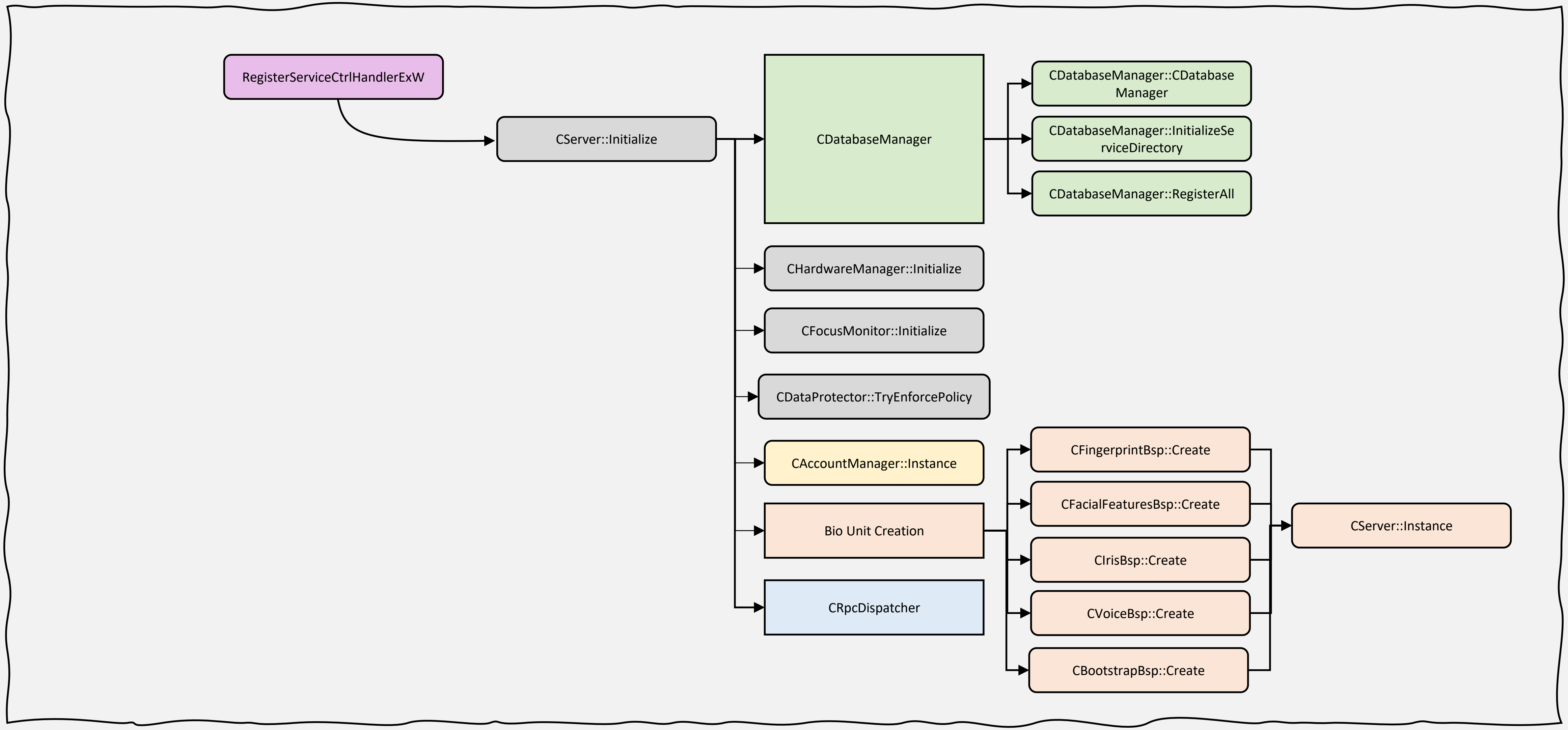
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create

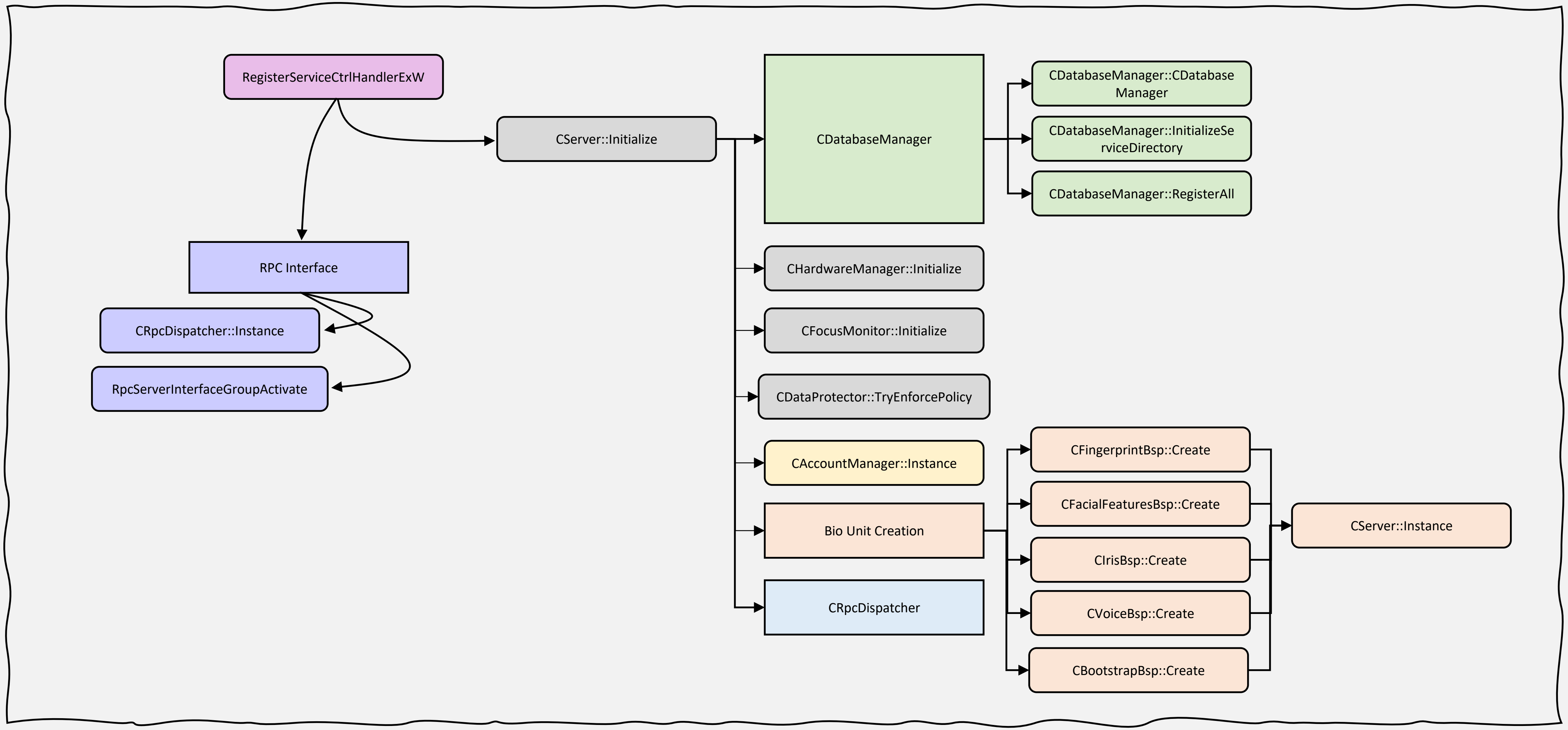
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create
CServer::Instance

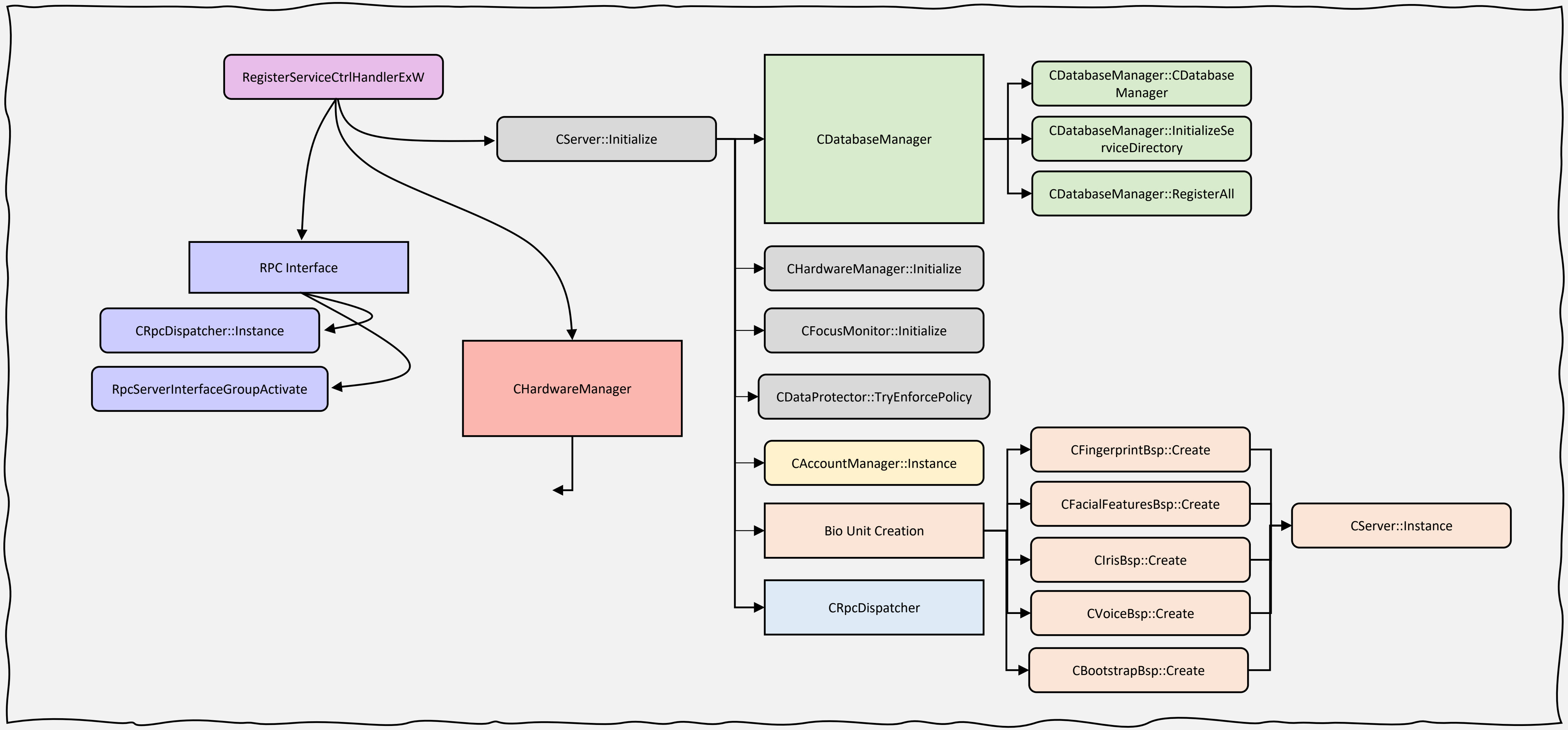
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeSe rviceDirectory
CDatabaseManager::RegisterAll
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CRpcDispatcher
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create
CServer::Instance

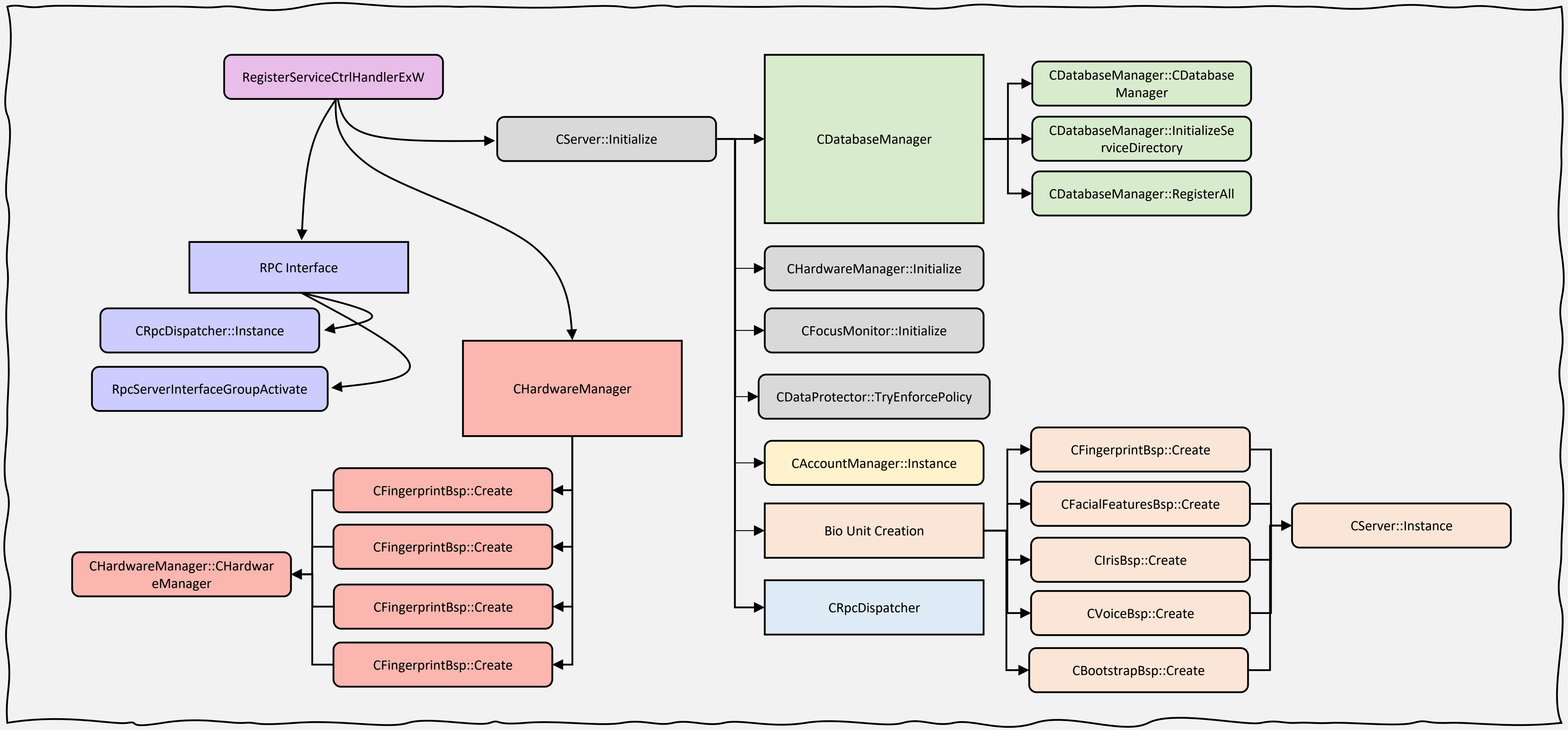
Windows Biometric Service – Initialization


RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
RPC Interface
CRpcDispatcher::Instance
RpcServerInterfaceGroupActivate
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CRpcDispatcher
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create
CServer::Instance

Windows Biometric Service – Initialization

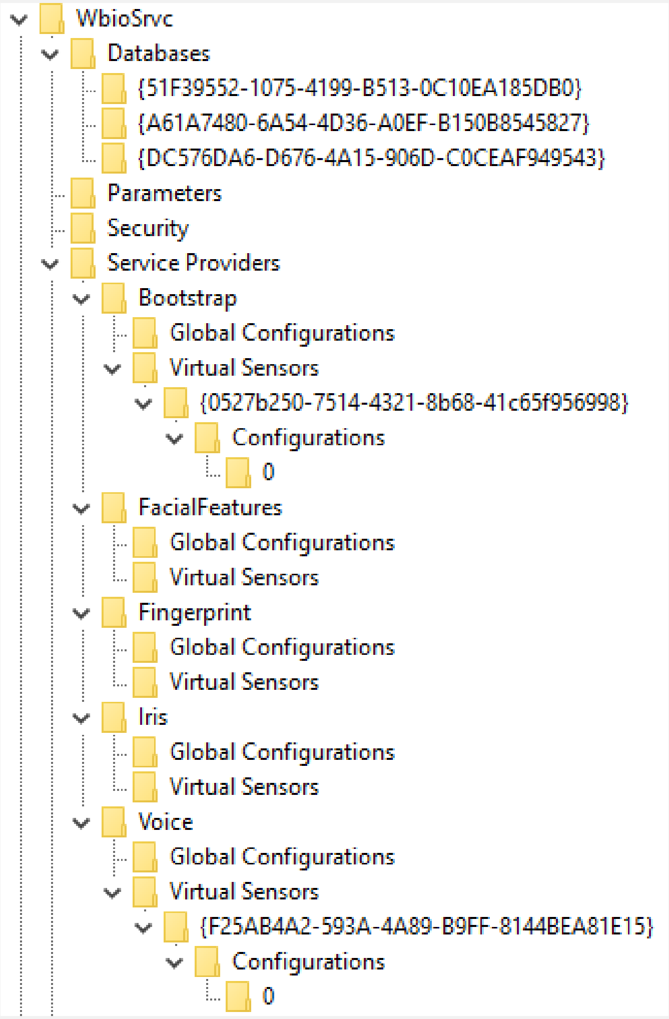

RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
RPC Interface
CRpcDispatcher::Instance
RpcServerInterfaceGroupActivate
CHardwareManager
CHardwareManager::Initialize
CFocusMonitor::Initialize
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
Bio Unit Creation
CRpcDispatcher
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CIrisBsp::Create
CVoiceBsp::Create
CBootstrapBsp::Create
CServer::Instance

Windows Biometric Service – Initialization



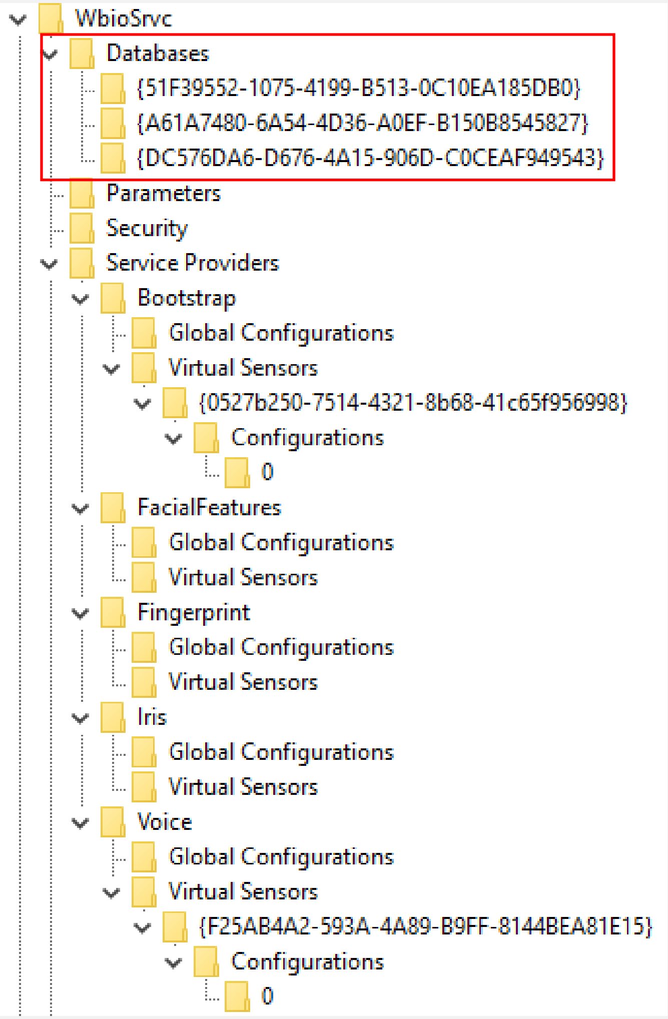
RegisterServiceCtrlHandlerExW
CServer::Initialize
CDatabaseManager
CDatabaseManager::CDatabase Manager
CDatabaseManager::InitializeServiceDirectory
CDatabaseManager::RegisterAll
RPC Interface
CRpcDispatcher::Instance
RpcServerInterfaceGroupActivate
CHardwareManager::Initialize
CFocusMonitor::Initialize
CHardwareManager
CDataProtector::TryEnforcePolicy
CAccountManager::Instance
CFingerprintBsp::Create
CFingerprintBsp::Create
CFacialFeaturesBsp::Create
CFingerprintBsp::Create
Bio Unit Creation
CServer::Instance
CHardwareManager::CHardwareManager
CIrisBsp::Create
CFingerprintBsp::Create
CRpcDispatcher
CVoiceBsp::Create
CFingerprintBsp::Create
CBootstrapBsp::Create

Windows Biometric Service – Configuration

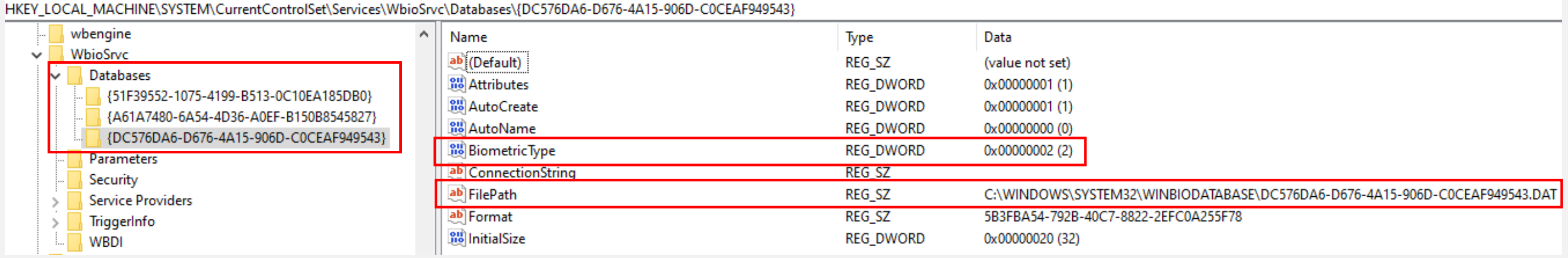


```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```

Windows Biometric Service – Configuration



```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```

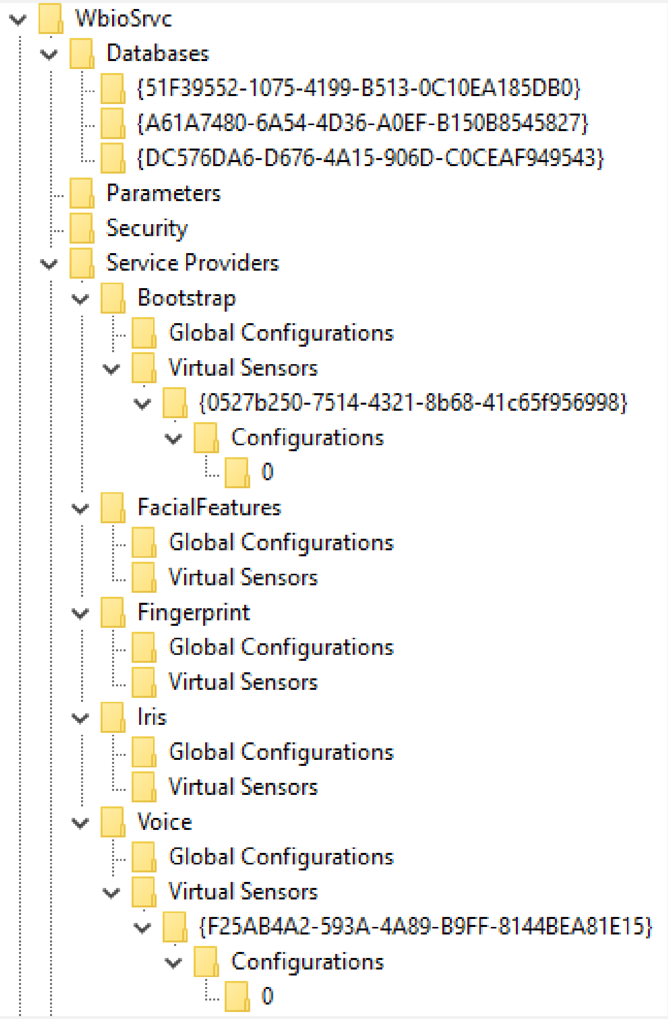


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

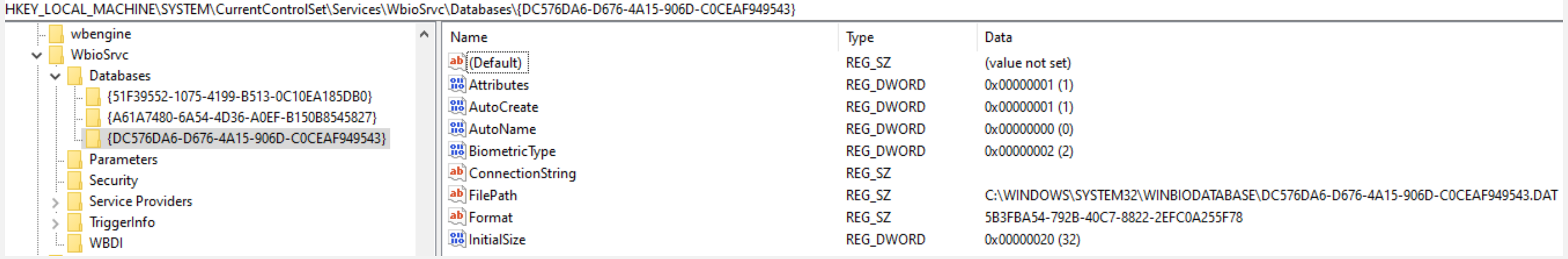
```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

Windows Biometric Service – Configuration



```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```

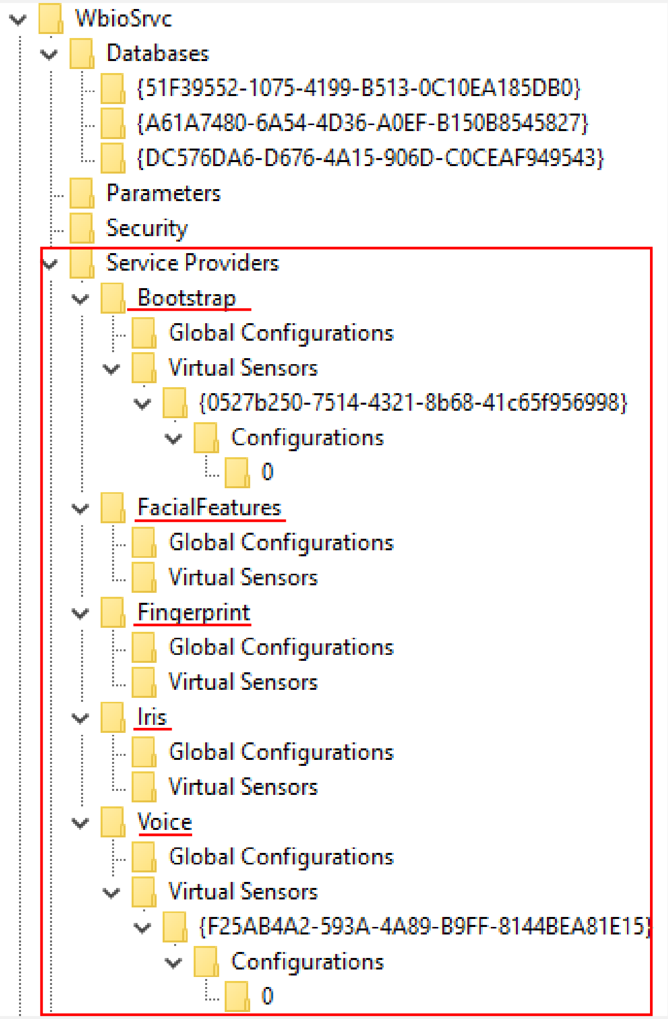


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

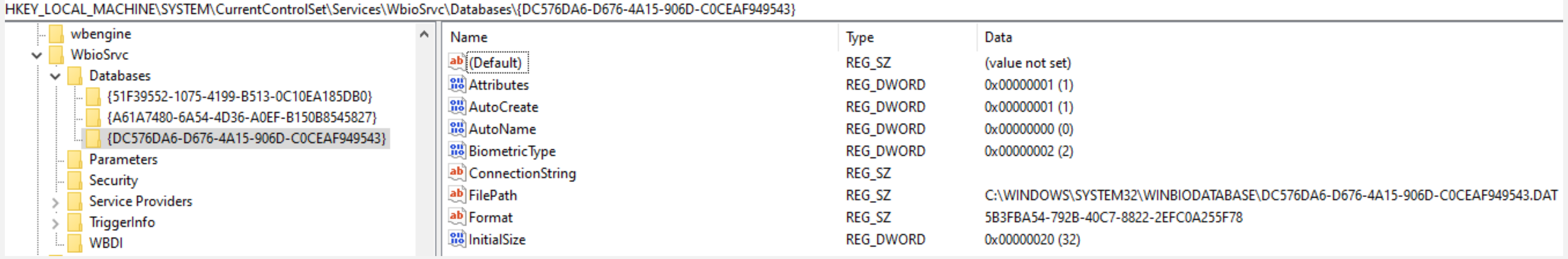
```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

Windows Biometric Service – Configuration



```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```

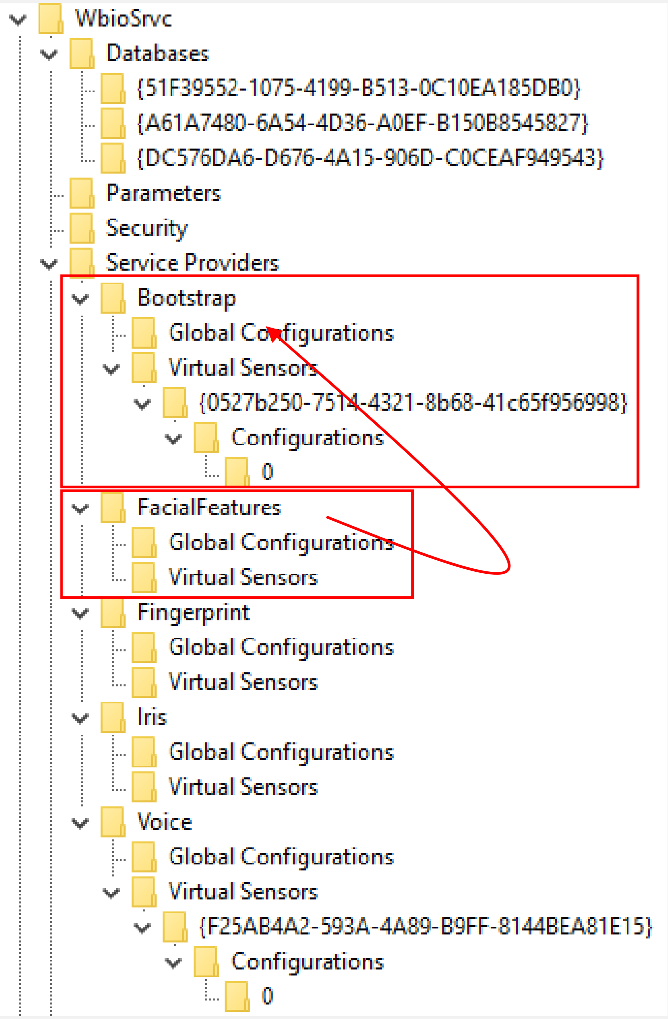


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

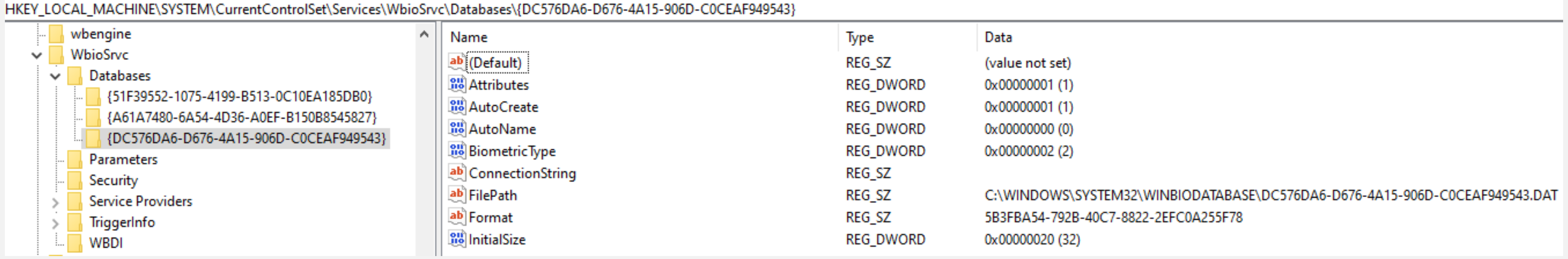
```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

Windows Biometric Service – Configuration



```
WbioSrvc
    Databases
        {51F39552-1075-4199-B513-0C10EA185DB0}
        {A61A7480-6A54-4D36-A0EF-B150B8545827}
        {DC576DA6-D676-4A15-906D-C0CEAF949543}
    Parameters
    Security
    Service Providers
        Bootstrap
            Global Configurations
            Virtual Sensors
                {0527b250-7514-4321-8b68-41c65f956998}
                    Configurations
                        0
        FacialFeatures
            Global Configurations
            Virtual Sensors
        Fingerprint
            Global Configurations
            Virtual Sensors
        Iris
            Global Configurations
            Virtual Sensors
        Voice
            Global Configurations
            Virtual Sensors
                {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
                    Configurations
                        0
```

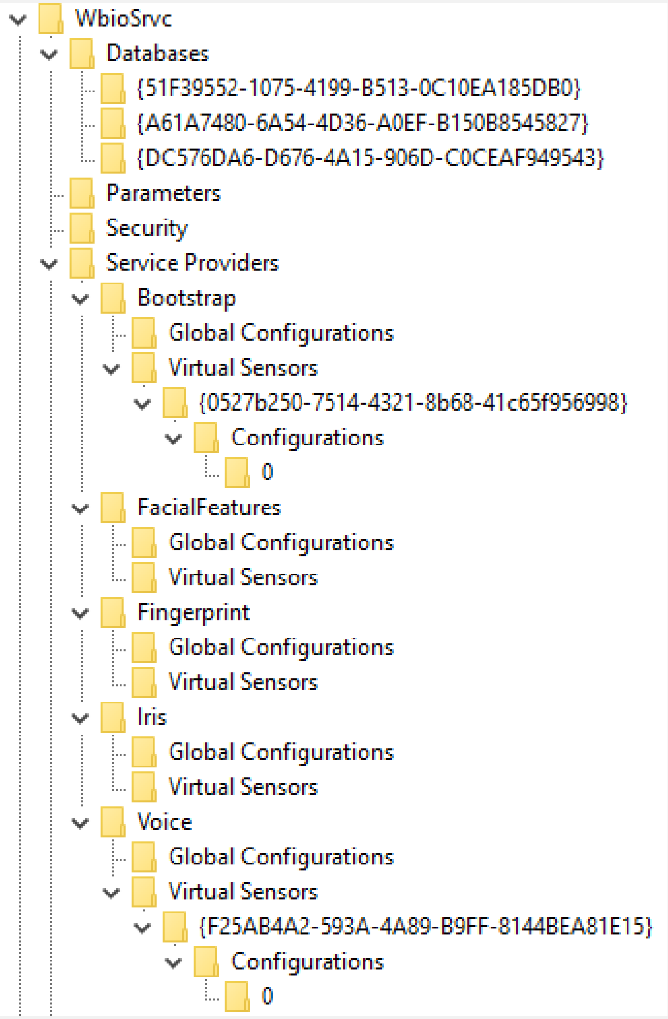


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

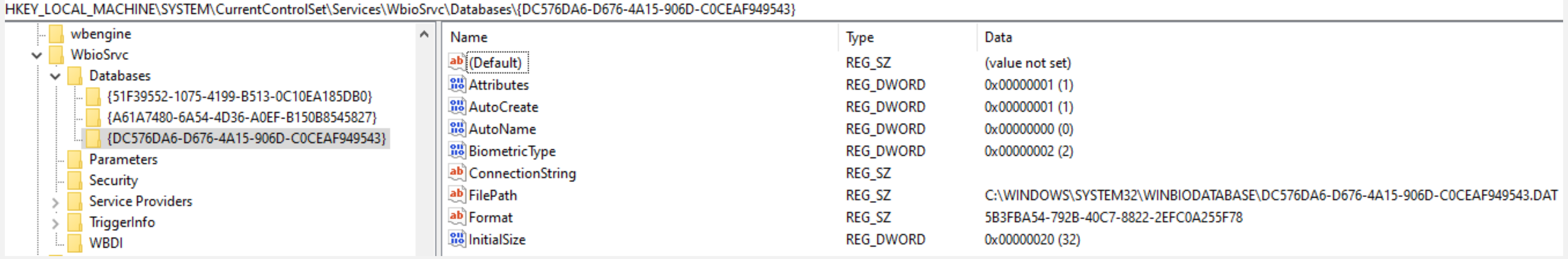
```
wbengine
WbioSrvc
    Databases
        {51F39552-1075-4199-B513-0C10EA185DB0}
        {A61A7480-6A54-4D36-A0EF-B150B8545827}
        {DC576DA6-D676-4A15-906D-C0CEAF949543}
    Parameters
    Security
    Service Providers
    TriggerInfo
    WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

Windows Biometric Service – Configuration



```
WbioSrvc
    Databases
        {51F39552-1075-4199-B513-0C10EA185DB0}
        {A61A7480-6A54-4D36-A0EF-B150B8545827}
        {DC576DA6-D676-4A15-906D-C0CEAF949543}
    Parameters
    Security
    Service Providers
        Bootstrap
            Global Configurations
            Virtual Sensors
                {0527b250-7514-4321-8b68-41c65f956998}
                    Configurations
                        0
        FacialFeatures
            Global Configurations
            Virtual Sensors
        Fingerprint
            Global Configurations
            Virtual Sensors
        Iris
            Global Configurations
            Virtual Sensors
        Voice
            Global Configurations
            Virtual Sensors
                {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
                    Configurations
                        0
```

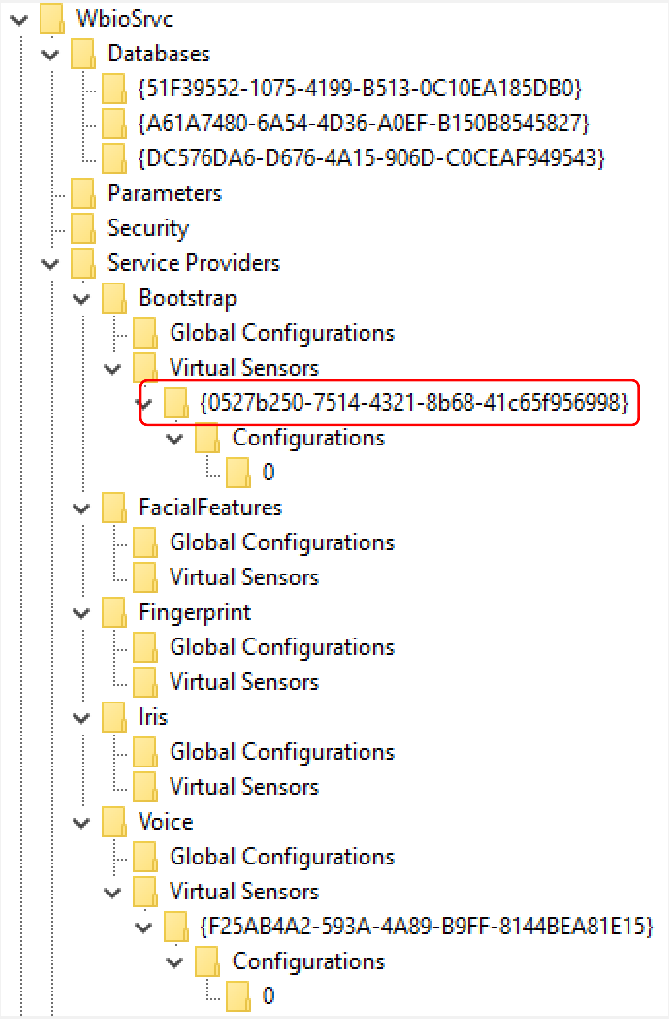


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

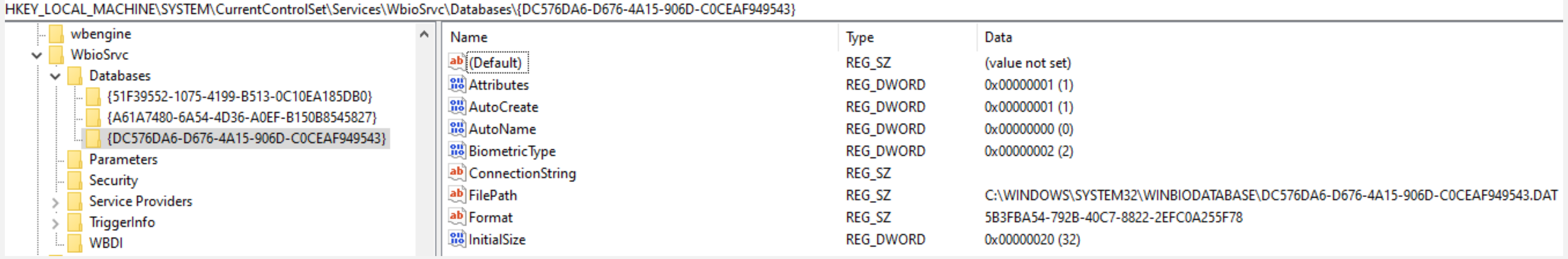
```
    wbengine
    WbioSrvc
        Databases
            {51F39552-1075-4199-B513-0C10EA185DB0}
            {A61A7480-6A54-4D36-A0EF-B150B8545827}
            {DC576DA6-D676-4A15-906D-C0CEAF949543}
        Parameters
        Security
        Service Providers
        TriggerInfo
        WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

Windows Biometric Service – Configuration



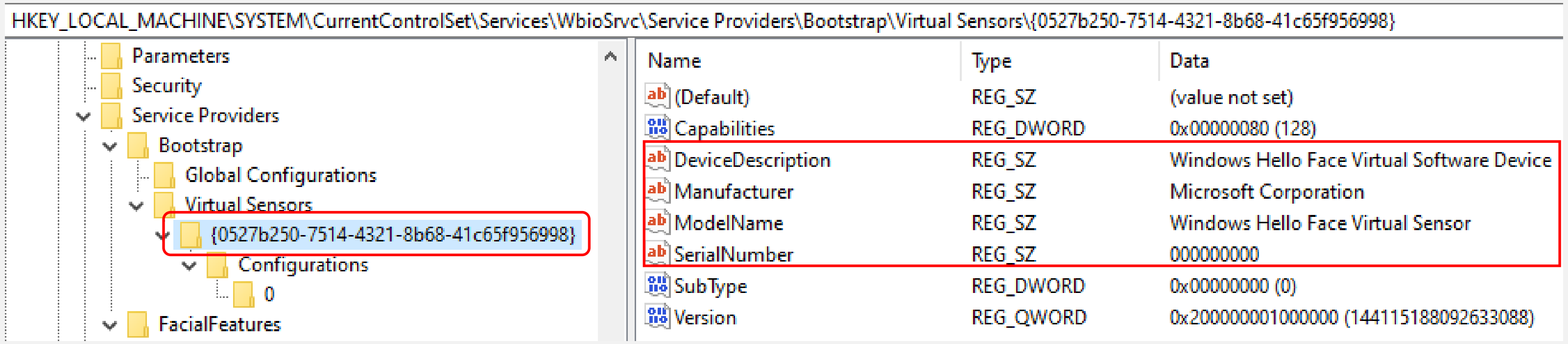
```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)

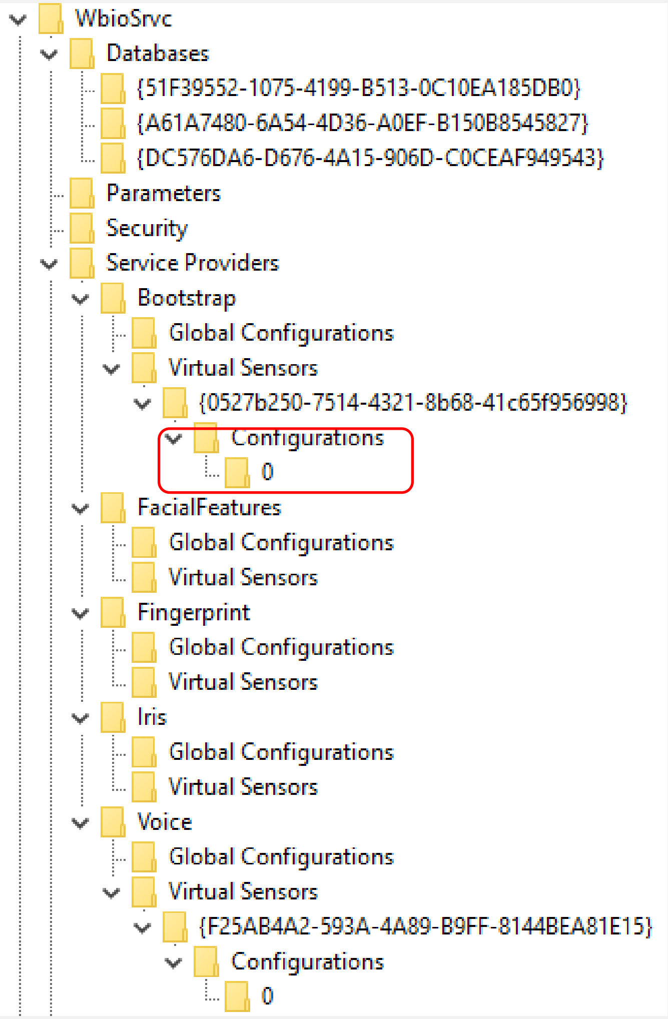


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Service Providers\Bootstrap\Virtual Sensors\{0527b250-7514-4321-8b68-41c65f956998}

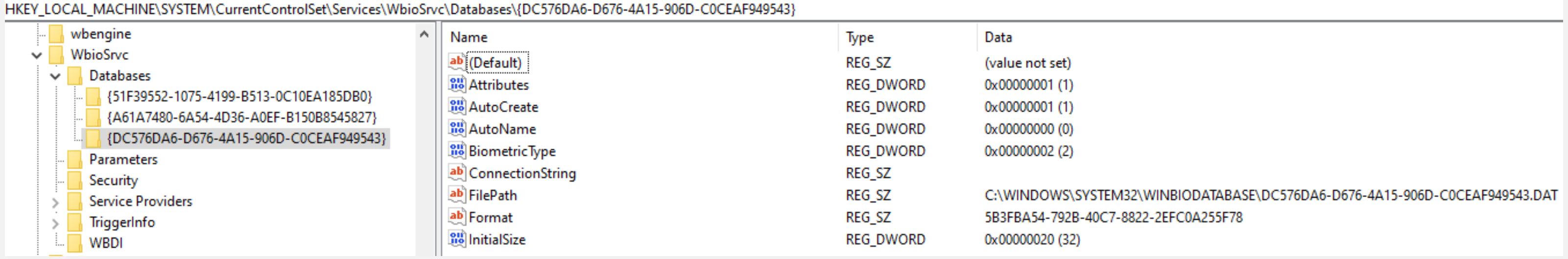
```
Parameters
Security
Service Providers
  Bootstrap
    Global Configurations
    Virtual Sensors
      {0527b250-7514-4321-8b68-41c65f956998}
        Configurations
          0
  FacialFeatures
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000080 (128)
DeviceDescription	REG_SZ	Windows Hello Face Virtual Software Device
Manufacturer	REG_SZ	Microsoft Corporation
ModelName	REG_SZ	Windows Hello Face Virtual Sensor
SerialNumber	REG_SZ	000000000
SubType	REG_DWORD	0x00000000 (0)
Version	REG_QWORD	0x200000001000000 (144115188092633088)

Windows Biometric Service – Configuration



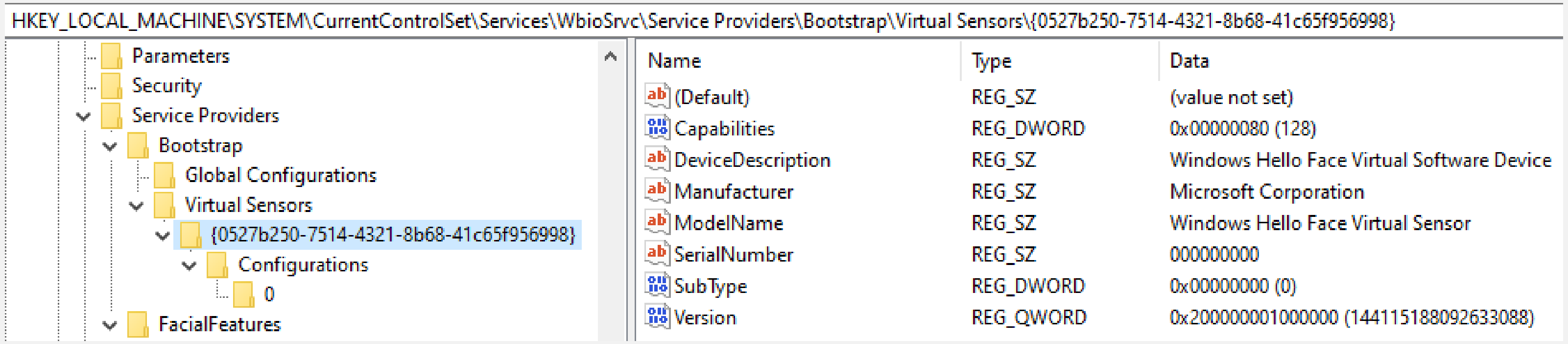
```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

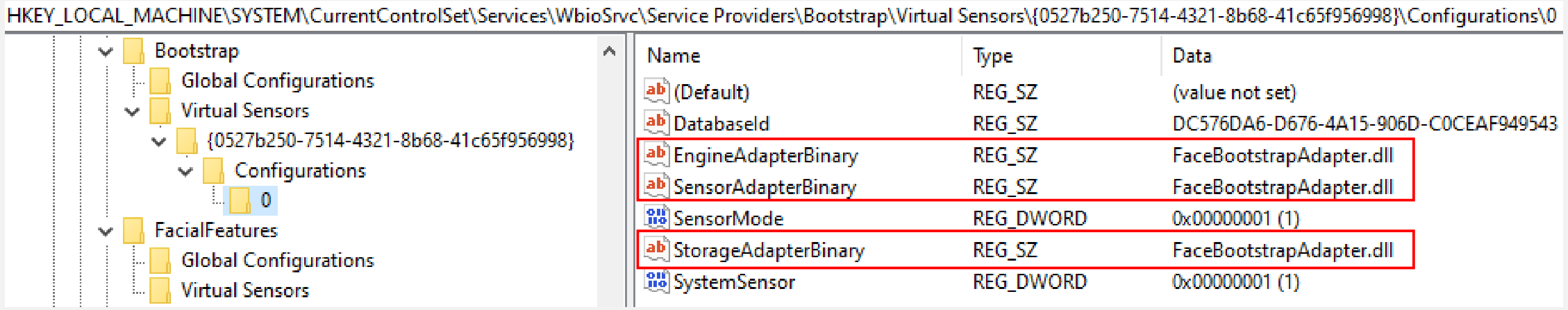
Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Service Providers\Bootstrap\Virtual Sensors\{0527b250-7514-4321-8b68-41c65f956998}

```
Parameters
Security
Service Providers
  Bootstrap
    Global Configurations
    Virtual Sensors
      {0527b250-7514-4321-8b68-41c65f956998}
        Configurations
          0
  FacialFeatures
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000080 (128)
DeviceDescription	REG_SZ	Windows Hello Face Virtual Software Device
Manufacturer	REG_SZ	Microsoft Corporation
ModelName	REG_SZ	Windows Hello Face Virtual Sensor
SerialNumber	REG_SZ	000000000
SubType	REG_DWORD	0x00000000 (0)
Version	REG_QWORD	0x200000001000000 (144115188092633088)

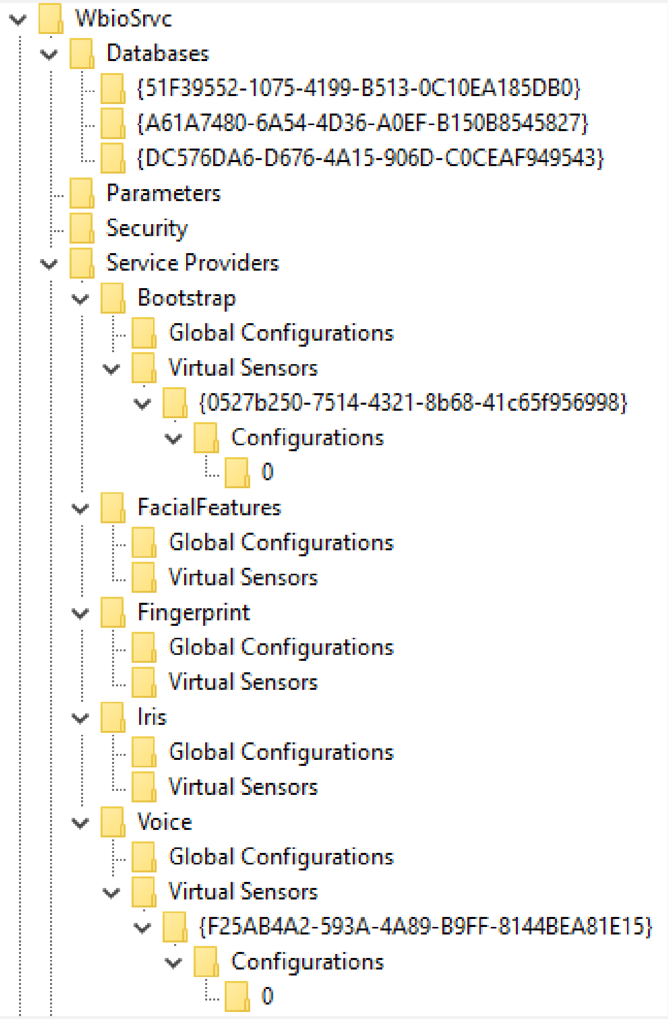


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Service Providers\Bootstrap\Virtual Sensors\{0527b250-7514-4321-8b68-41c65f956998}\Configurations\0

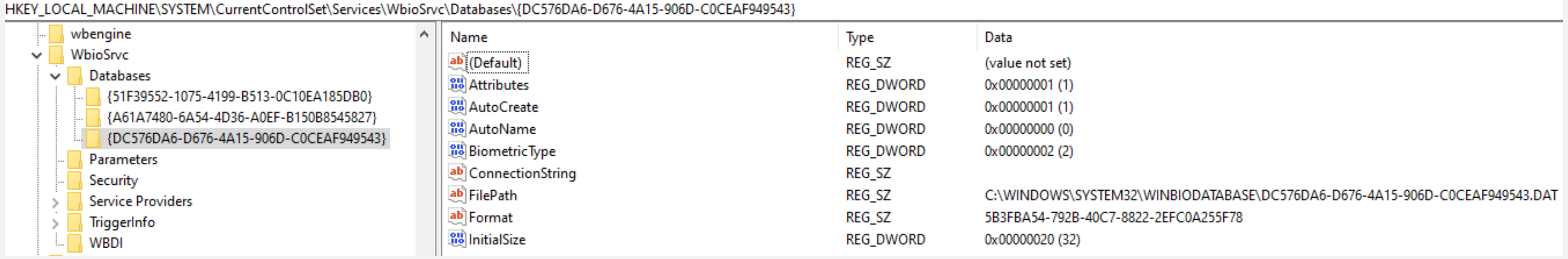
```
Bootstrap
  Global Configurations
  Virtual Sensors
    {0527b250-7514-4321-8b68-41c65f956998}
      Configurations
        0
FacialFeatures
  Global Configurations
  Virtual Sensors
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
DatabaseId	REG_SZ	DC576DA6-D676-4A15-906D-C0CEAF949543
EngineAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SensorAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SensorMode	REG_DWORD	0x00000001 (1)
StorageAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SystemSensor	REG_DWORD	0x00000001 (1)

Windows Biometric Service – Configuration



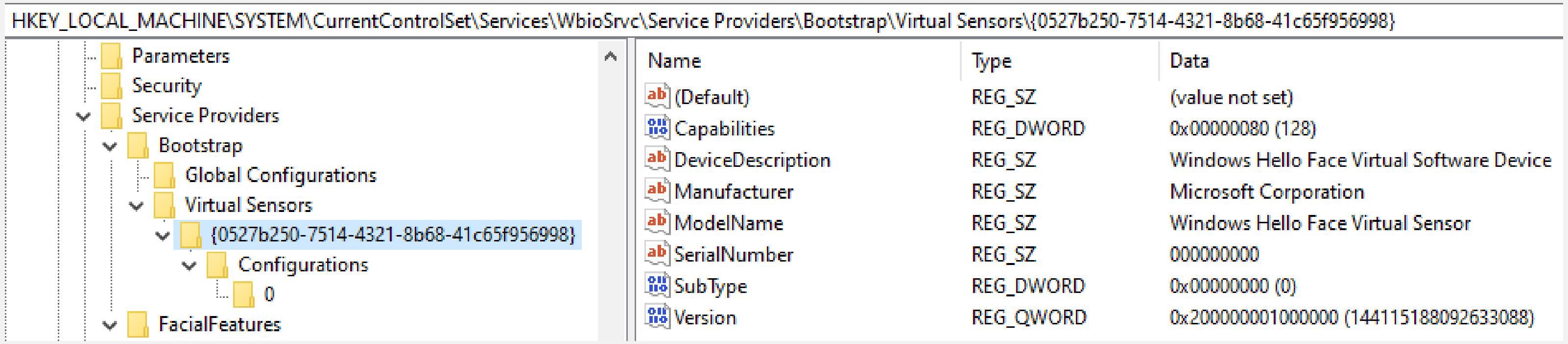
```
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
    Bootstrap
      Global Configurations
      Virtual Sensors
        {0527b250-7514-4321-8b68-41c65f956998}
          Configurations
            0
    FacialFeatures
      Global Configurations
      Virtual Sensors
    Fingerprint
      Global Configurations
      Virtual Sensors
    Iris
      Global Configurations
      Virtual Sensors
    Voice
      Global Configurations
      Virtual Sensors
        {F25AB4A2-593A-4A89-B9FF-8144BEA81E15}
          Configurations
            0
```



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Databases\{DC576DA6-D676-4A15-906D-C0CEAF949543}

```
wbengine
WbioSrvc
  Databases
    {51F39552-1075-4199-B513-0C10EA185DB0}
    {A61A7480-6A54-4D36-A0EF-B150B8545827}
    {DC576DA6-D676-4A15-906D-C0CEAF949543}
  Parameters
  Security
  Service Providers
  TriggerInfo
  WBDI
```

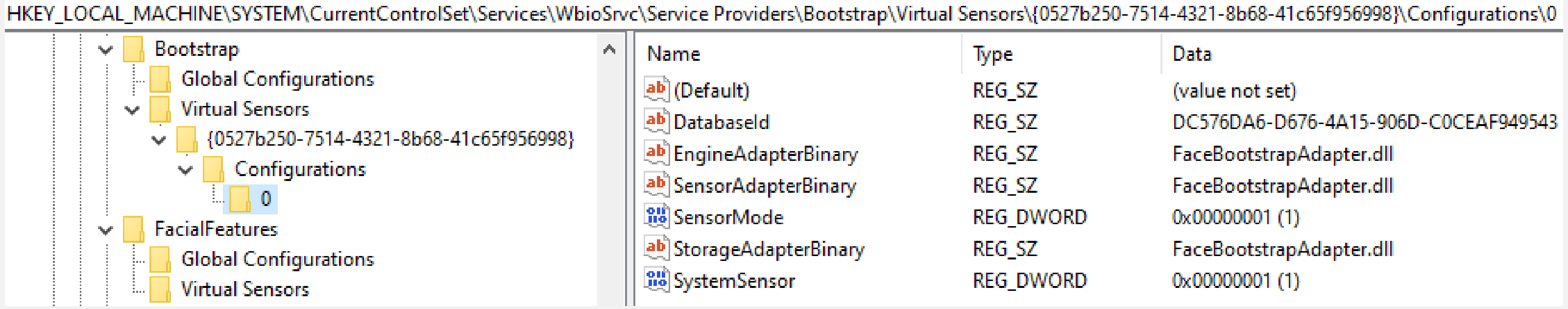
Name	Type	Data
(Default)	REG_SZ	(value not set)
Attributes	REG_DWORD	0x00000001 (1)
AutoCreate	REG_DWORD	0x00000001 (1)
AutoName	REG_DWORD	0x00000000 (0)
BiometricType	REG_DWORD	0x00000002 (2)
ConnectionString	REG_SZ	
FilePath	REG_SZ	C:\WINDOWS\SYSTEM32\WINBIODATABASE\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Format	REG_SZ	5B3FBA54-792B-40C7-8822-2EFC0A255F78
InitialSize	REG_DWORD	0x00000020 (32)



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Service Providers\Bootstrap\Virtual Sensors\{0527b250-7514-4321-8b68-41c65f956998}

```
Parameters
Security
Service Providers
  Bootstrap
    Global Configurations
    Virtual Sensors
      {0527b250-7514-4321-8b68-41c65f956998}
        Configurations
          0
  FacialFeatures
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000080 (128)
DeviceDescription	REG_SZ	Windows Hello Face Virtual Software Device
Manufacturer	REG_SZ	Microsoft Corporation
ModelName	REG_SZ	Windows Hello Face Virtual Sensor
SerialNumber	REG_SZ	000000000
SubType	REG_DWORD	0x00000000 (0)
Version	REG_QWORD	0x200000001000000 (144115188092633088)

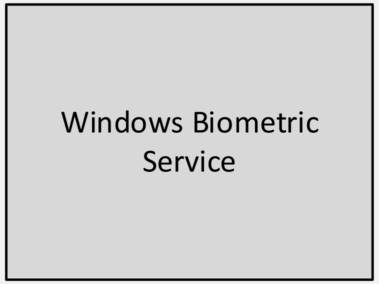


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WbioSrvc\Service Providers\Bootstrap\Virtual Sensors\{0527b250-7514-4321-8b68-41c65f956998}\Configurations\0

```
Bootstrap
  Global Configurations
  Virtual Sensors
    {0527b250-7514-4321-8b68-41c65f956998}
      Configurations
        0
FacialFeatures
  Global Configurations
  Virtual Sensors
```

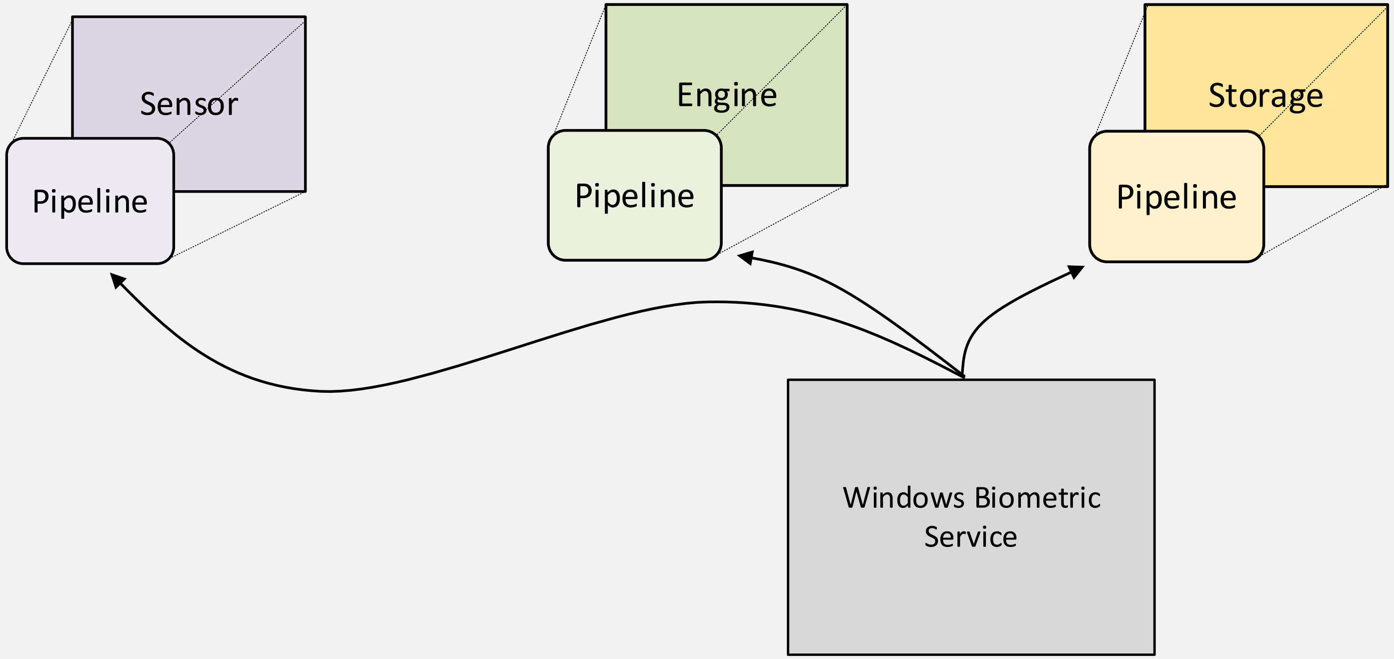
Name	Type	Data
(Default)	REG_SZ	(value not set)
DatabaseId	REG_SZ	DC576DA6-D676-4A15-906D-C0CEAF949543
EngineAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SensorAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SensorMode	REG_DWORD	0x00000001 (1)
StorageAdapterBinary	REG_SZ	FaceBootstrapAdapter.dll
SystemSensor	REG_DWORD	0x00000001 (1)

Biometric Unit

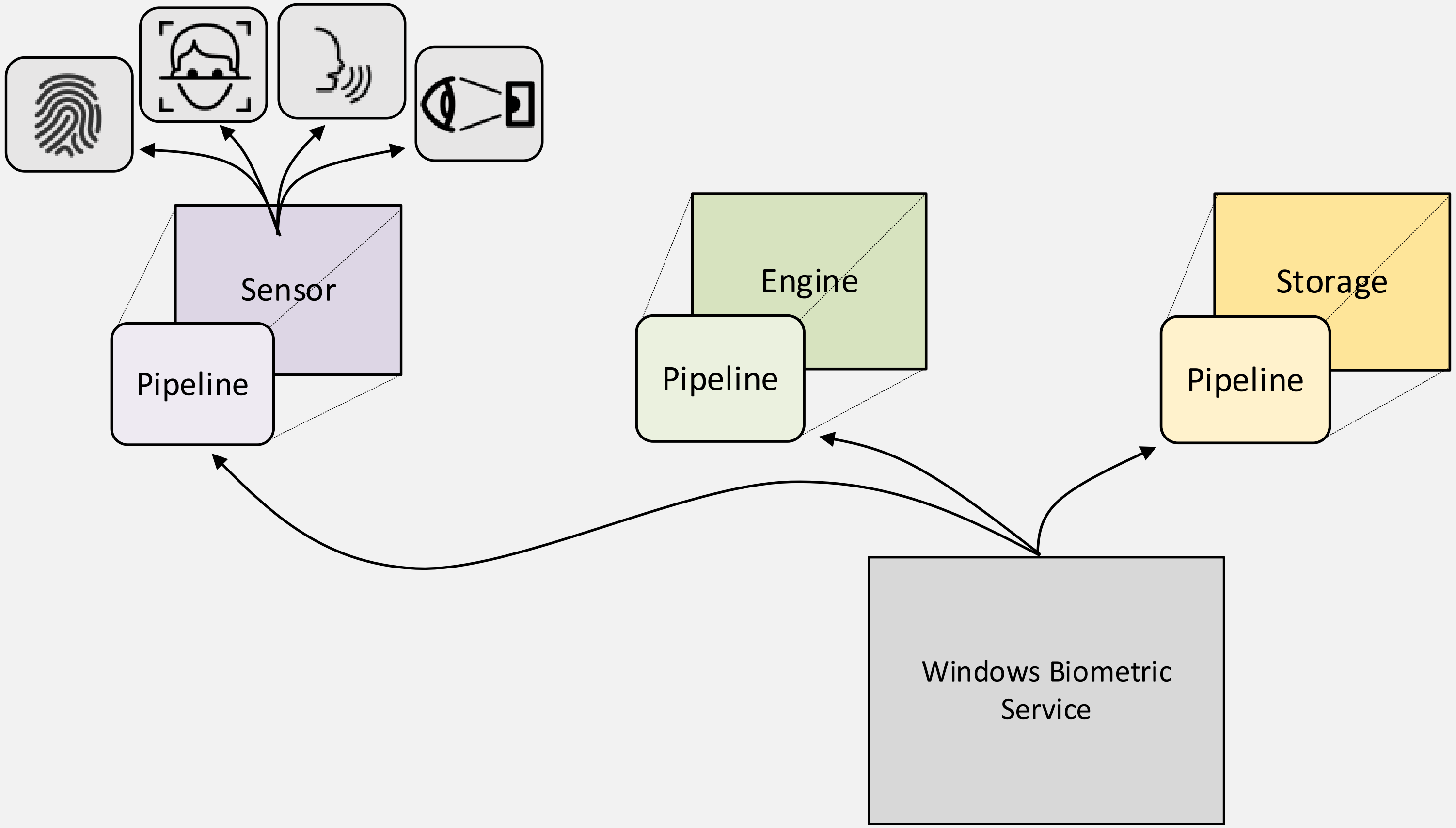


Windows Biometric Service

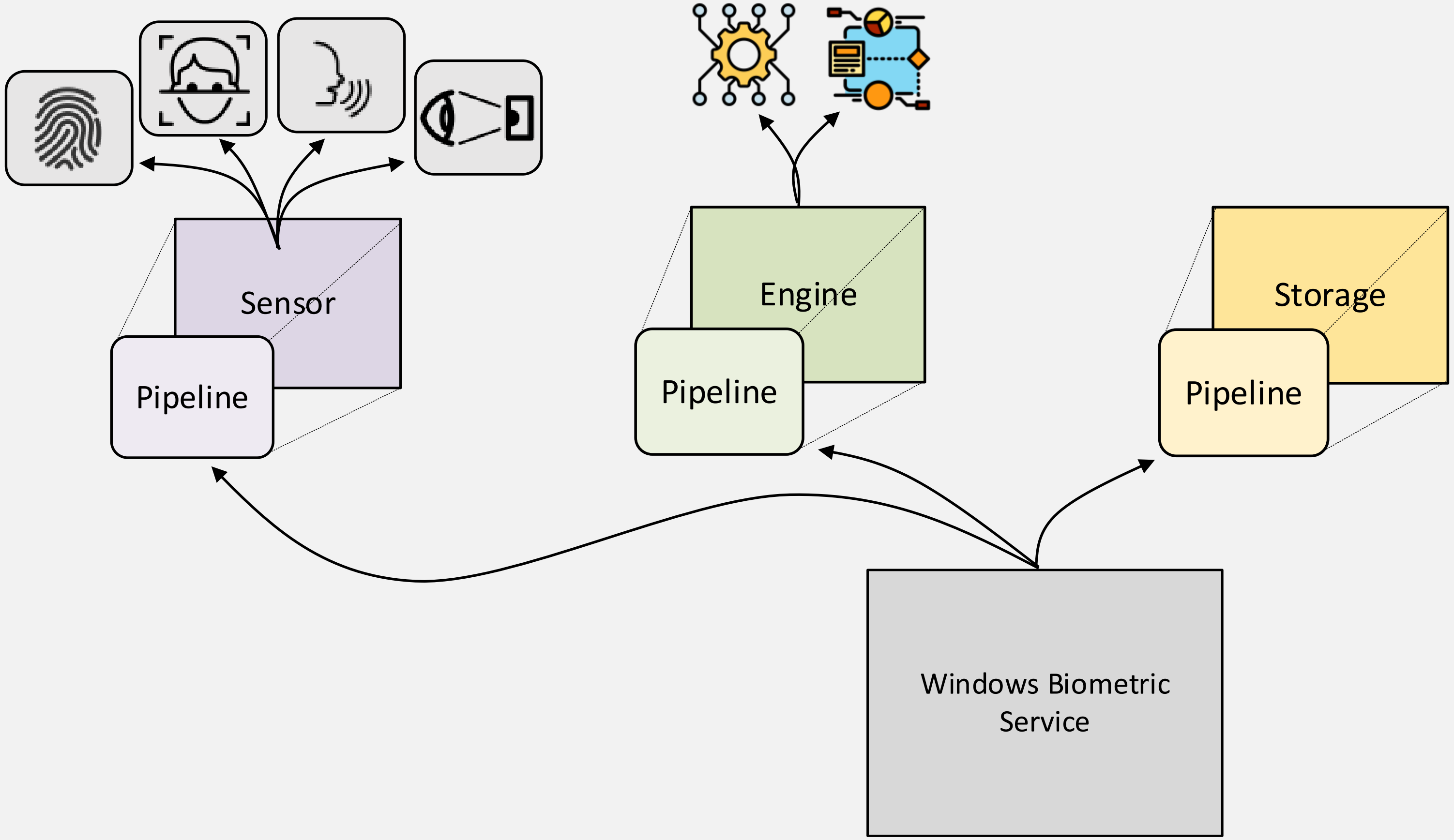
Biometric Unit



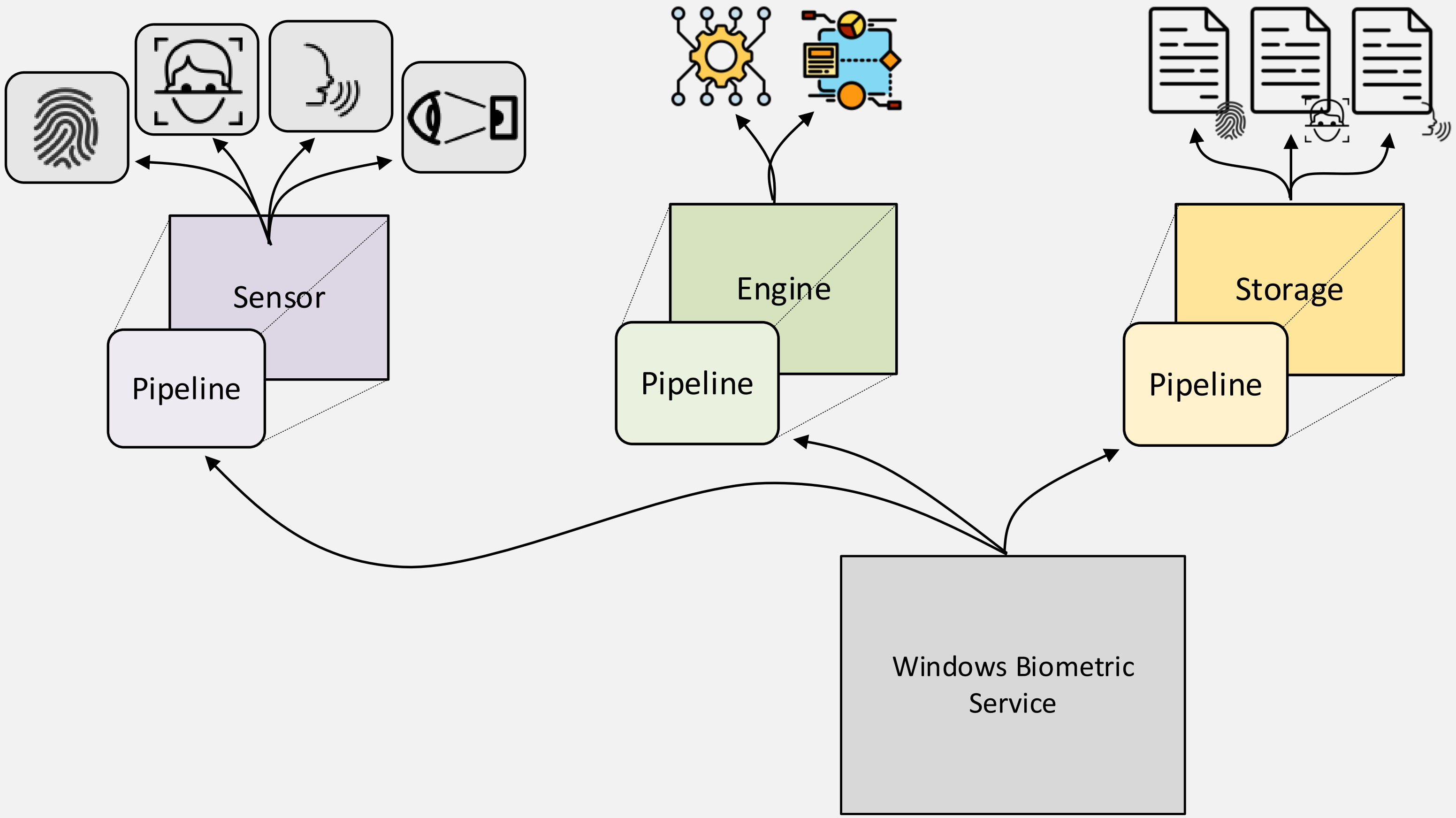
Biometric Unit



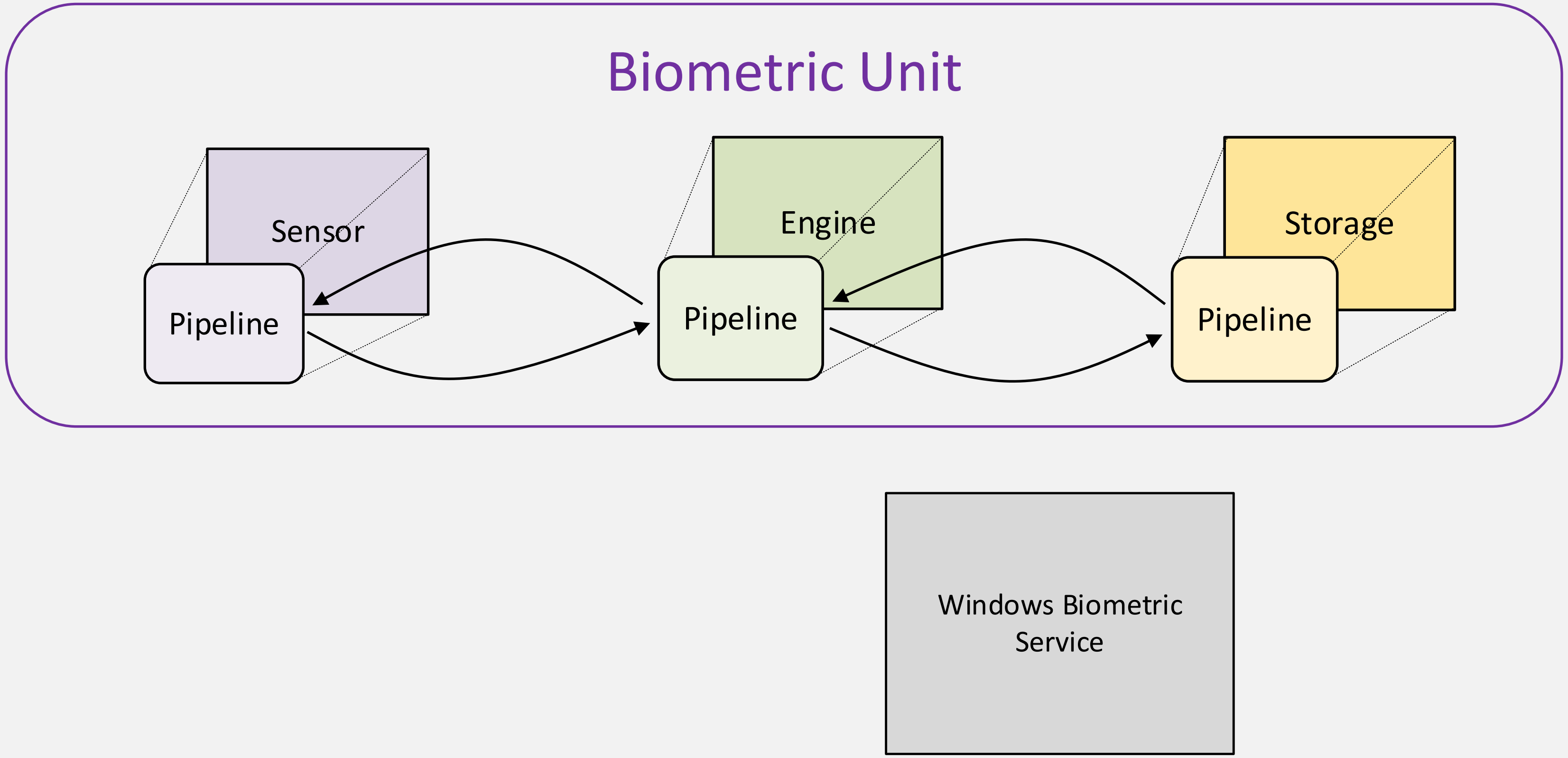
Biometric Unit



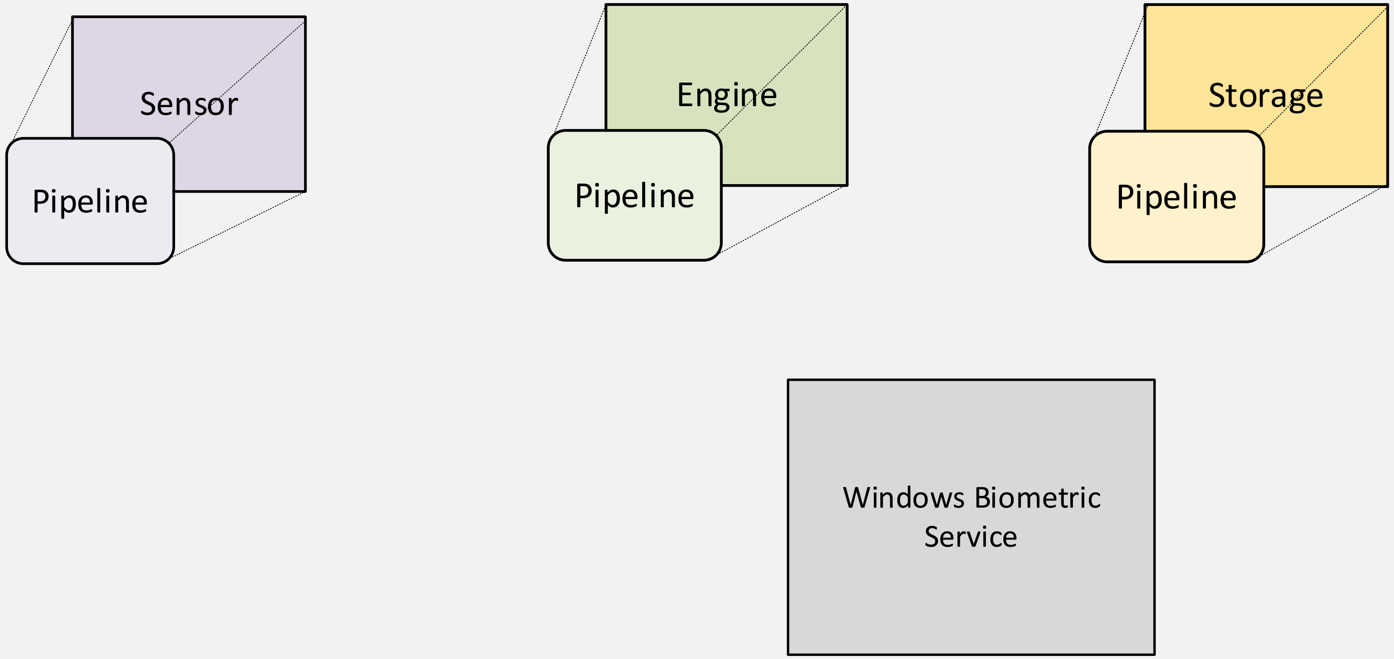
Biometric Unit



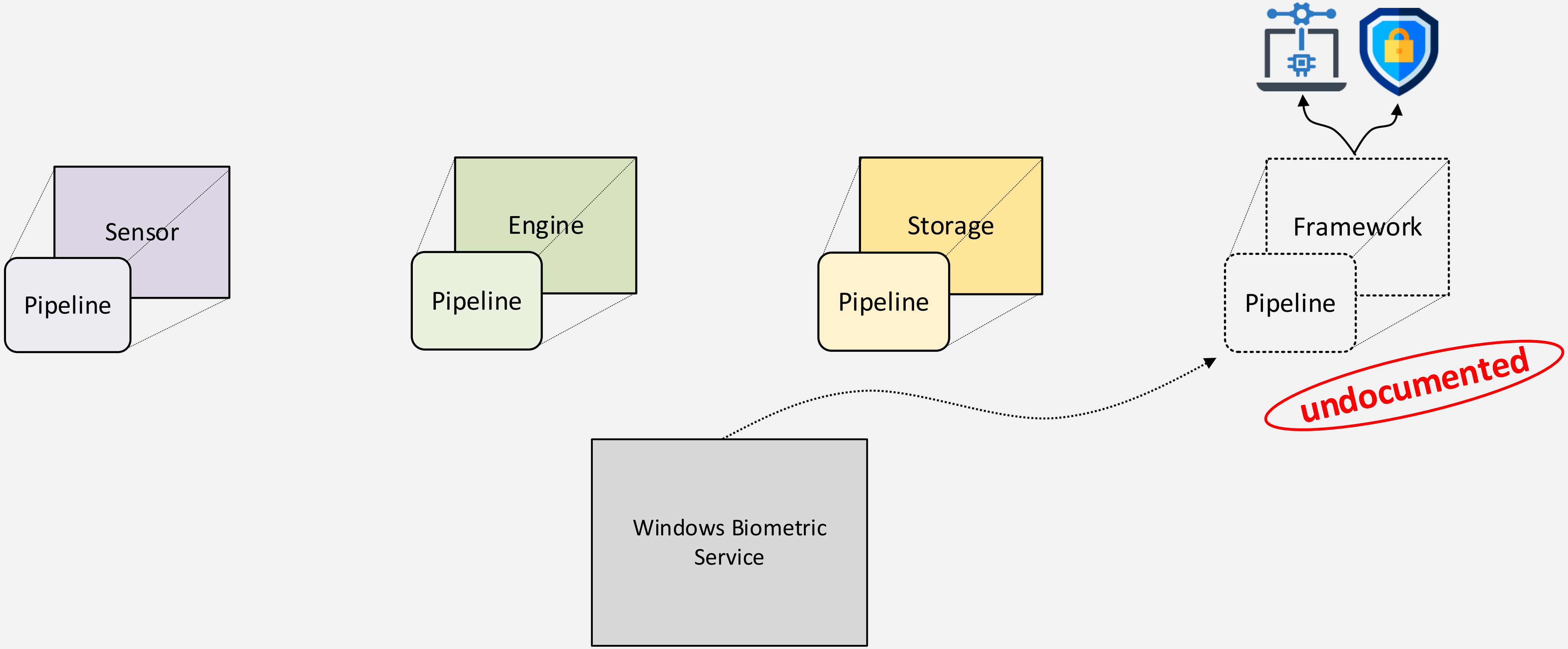
Biometric Unit



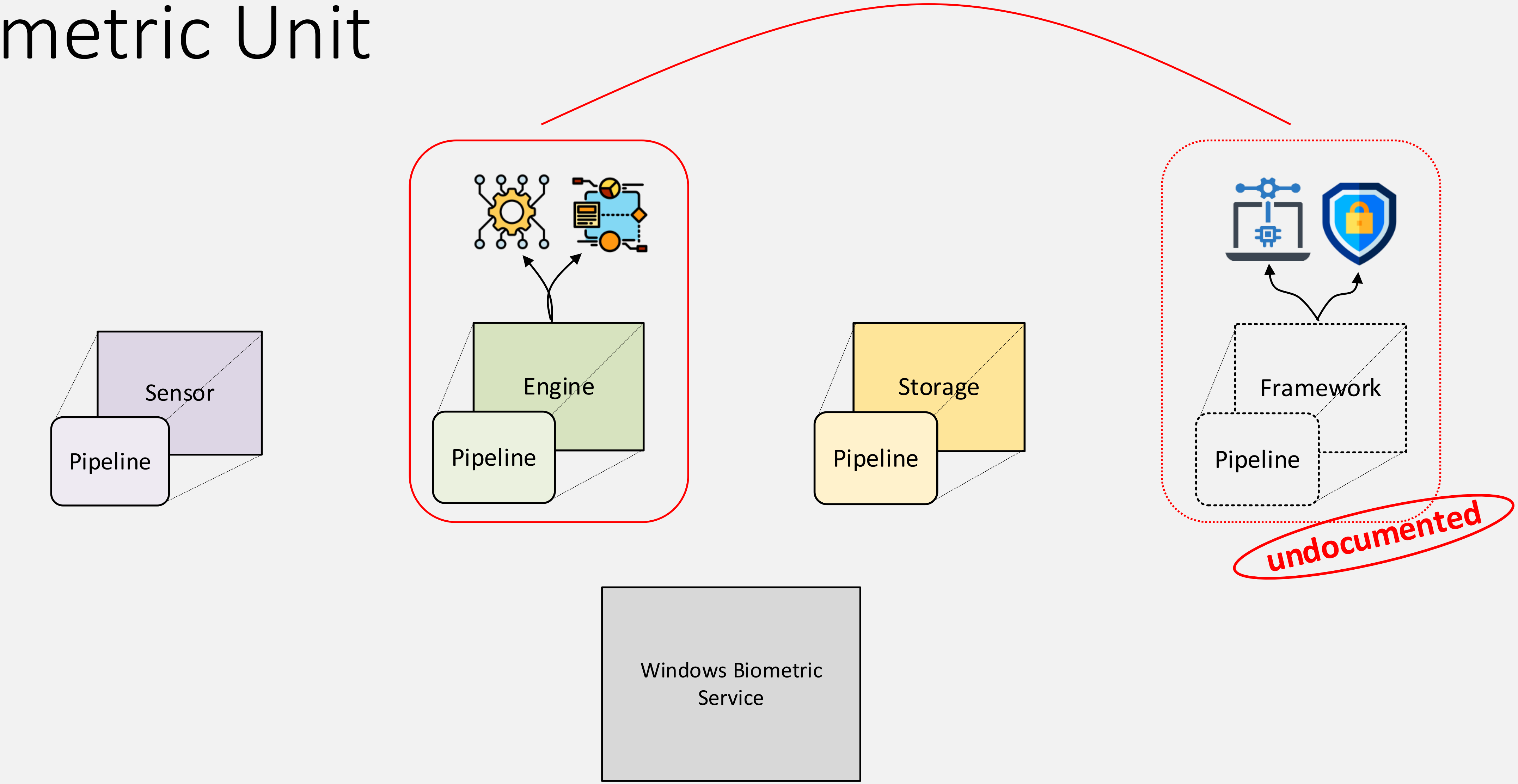
Biometric Unit



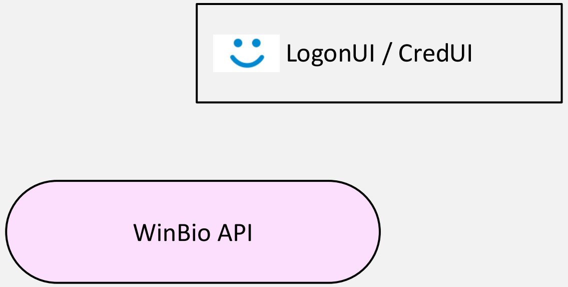
Biometric Unit



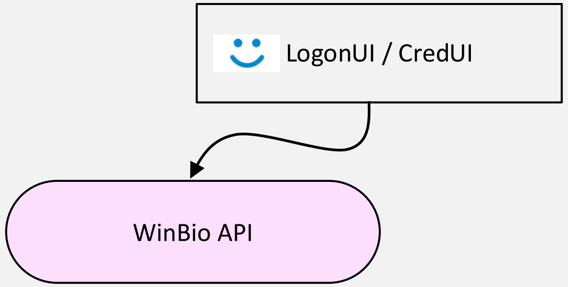
Biometric Unit



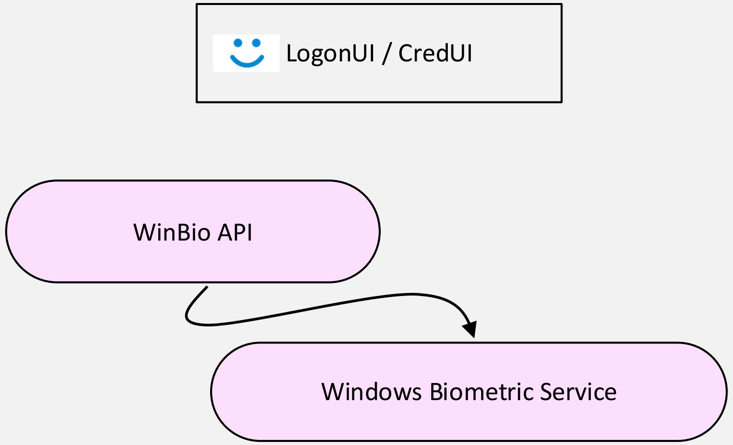
Enhanced Sign-in Security (ESS)



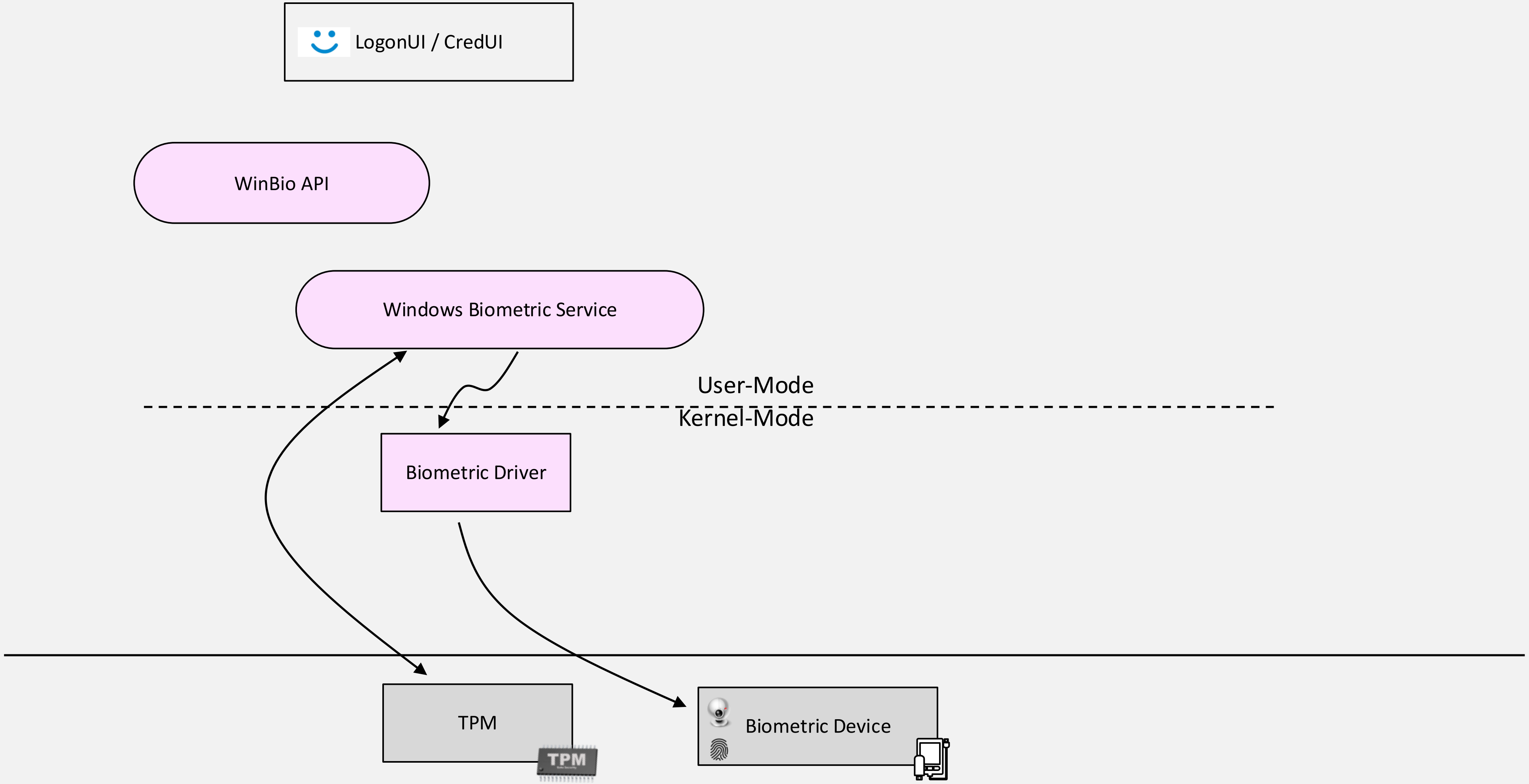
Enhanced Sign-in Security (ESS)



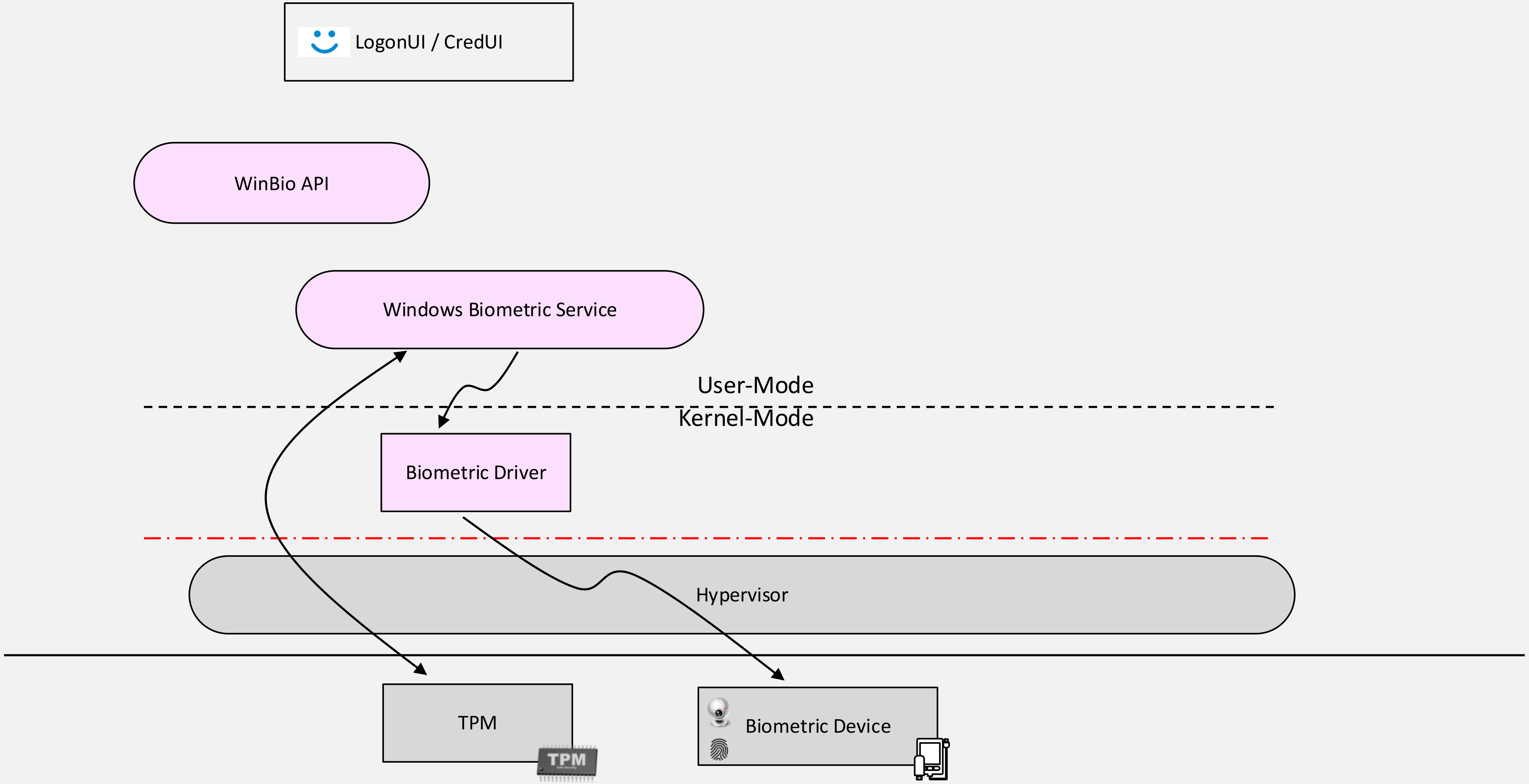
Enhanced Sign-in Security (ESS)



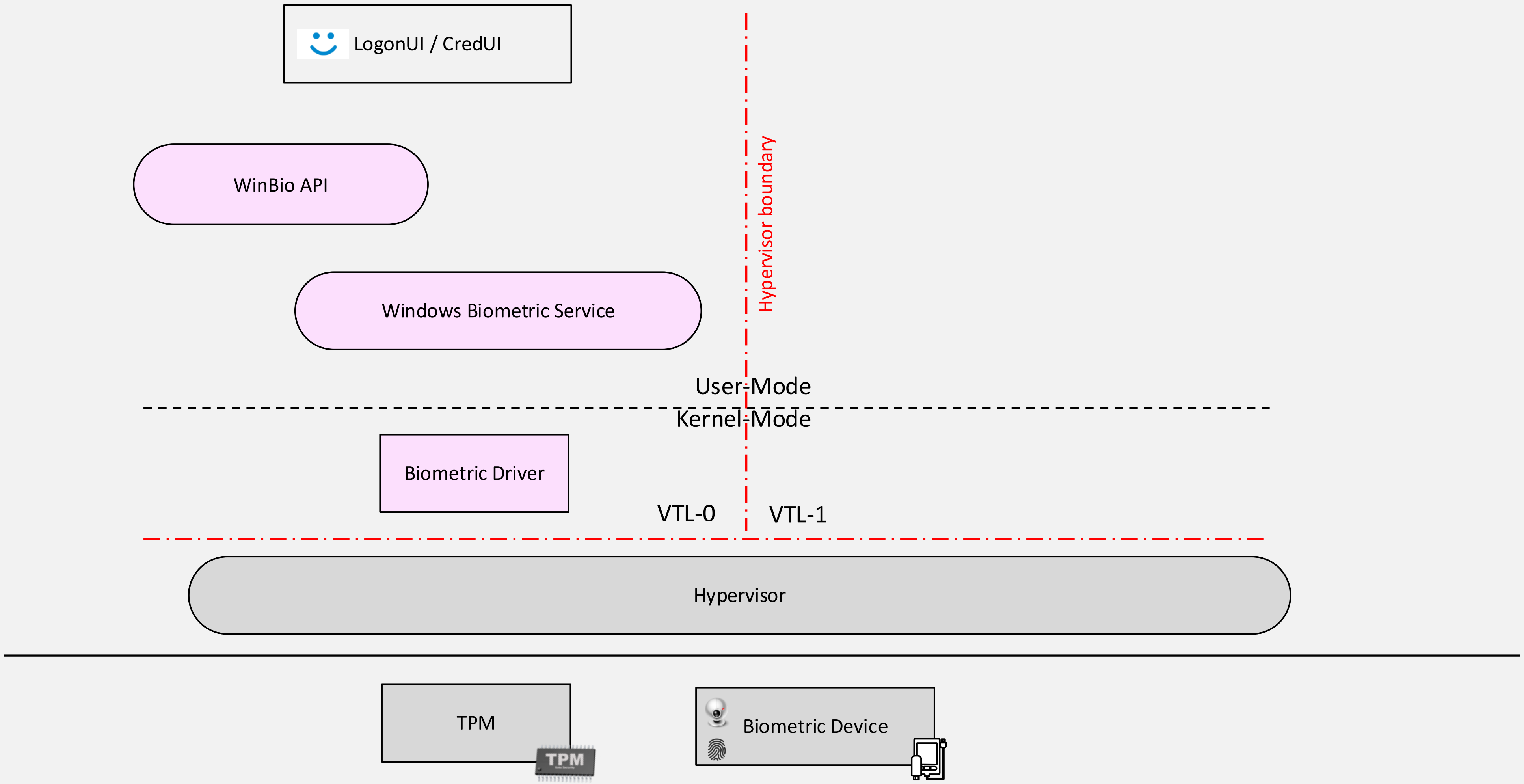
Enhanced Sign-in Security (ESS)



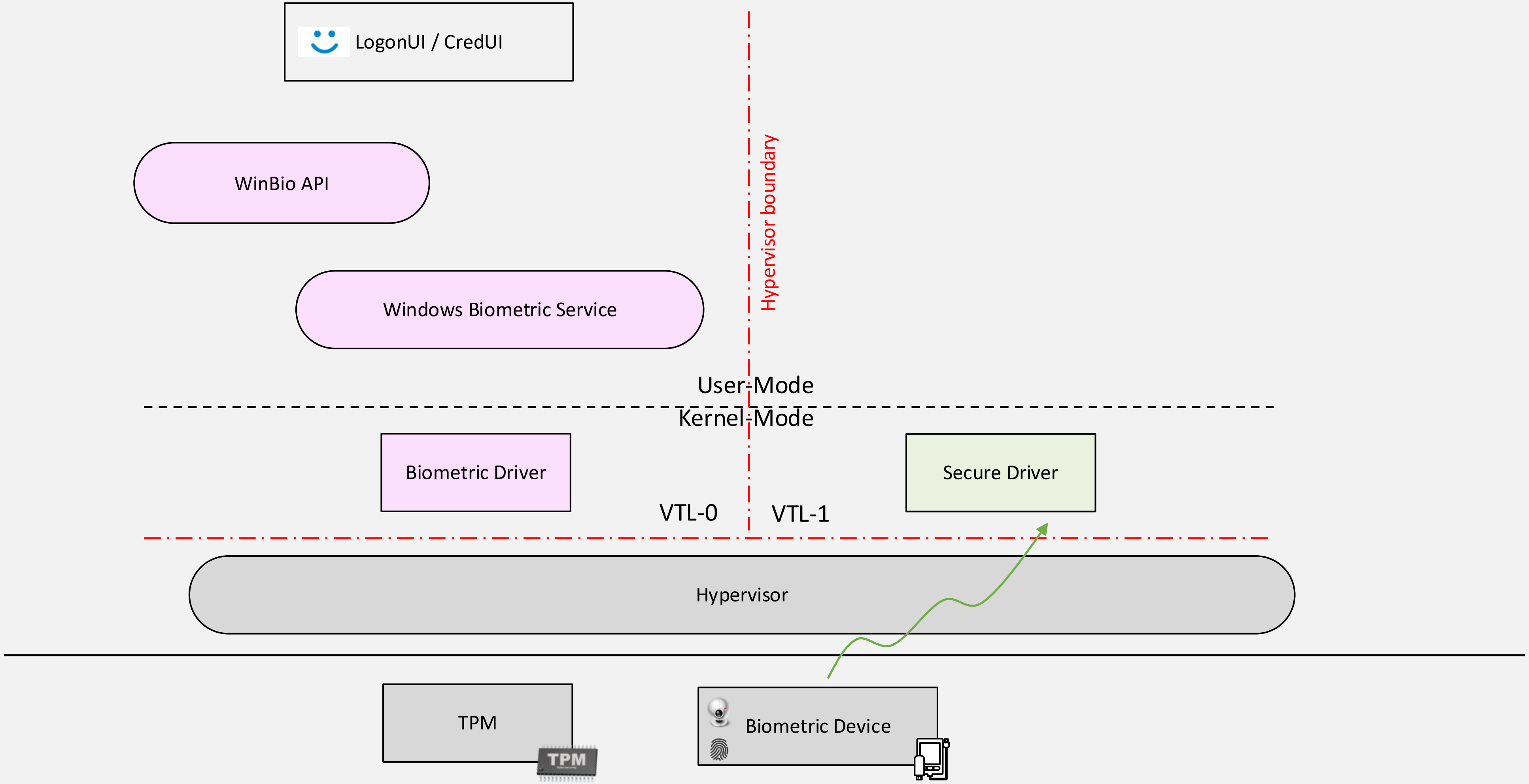
Enhanced Sign-in Security (ESS)



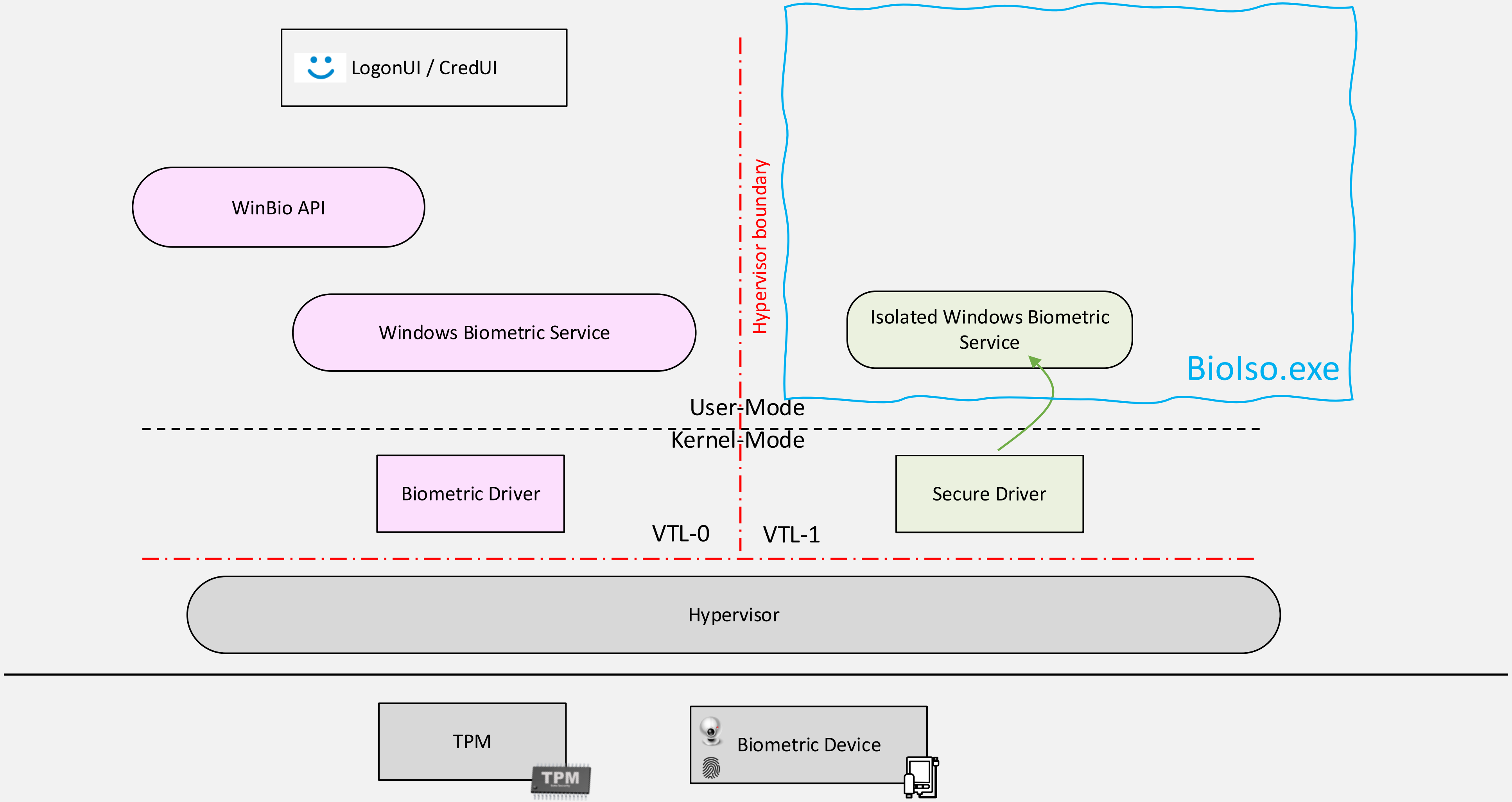
Enhanced Sign-in Security (ESS)



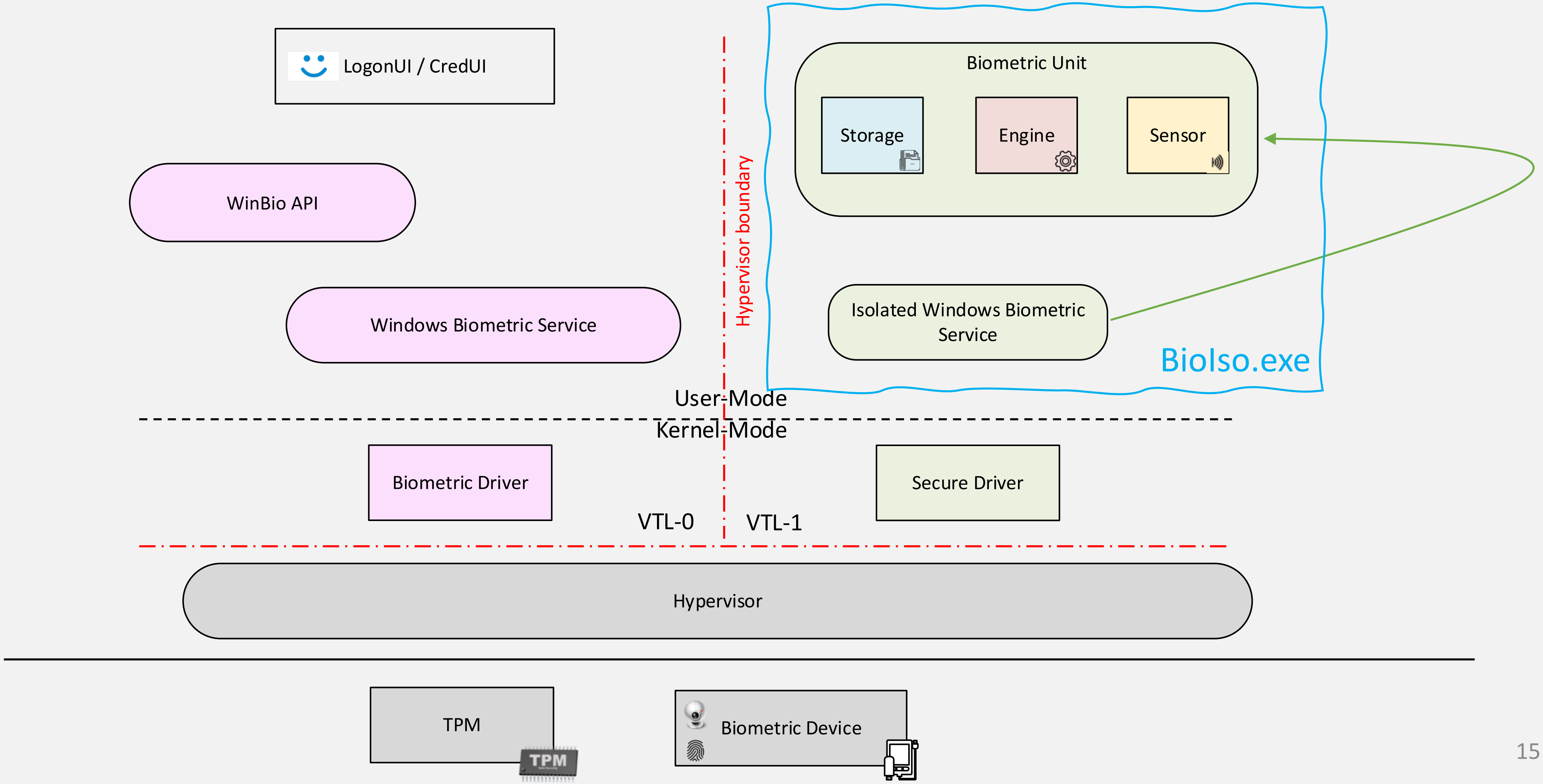
Enhanced Sign-in Security (ESS)



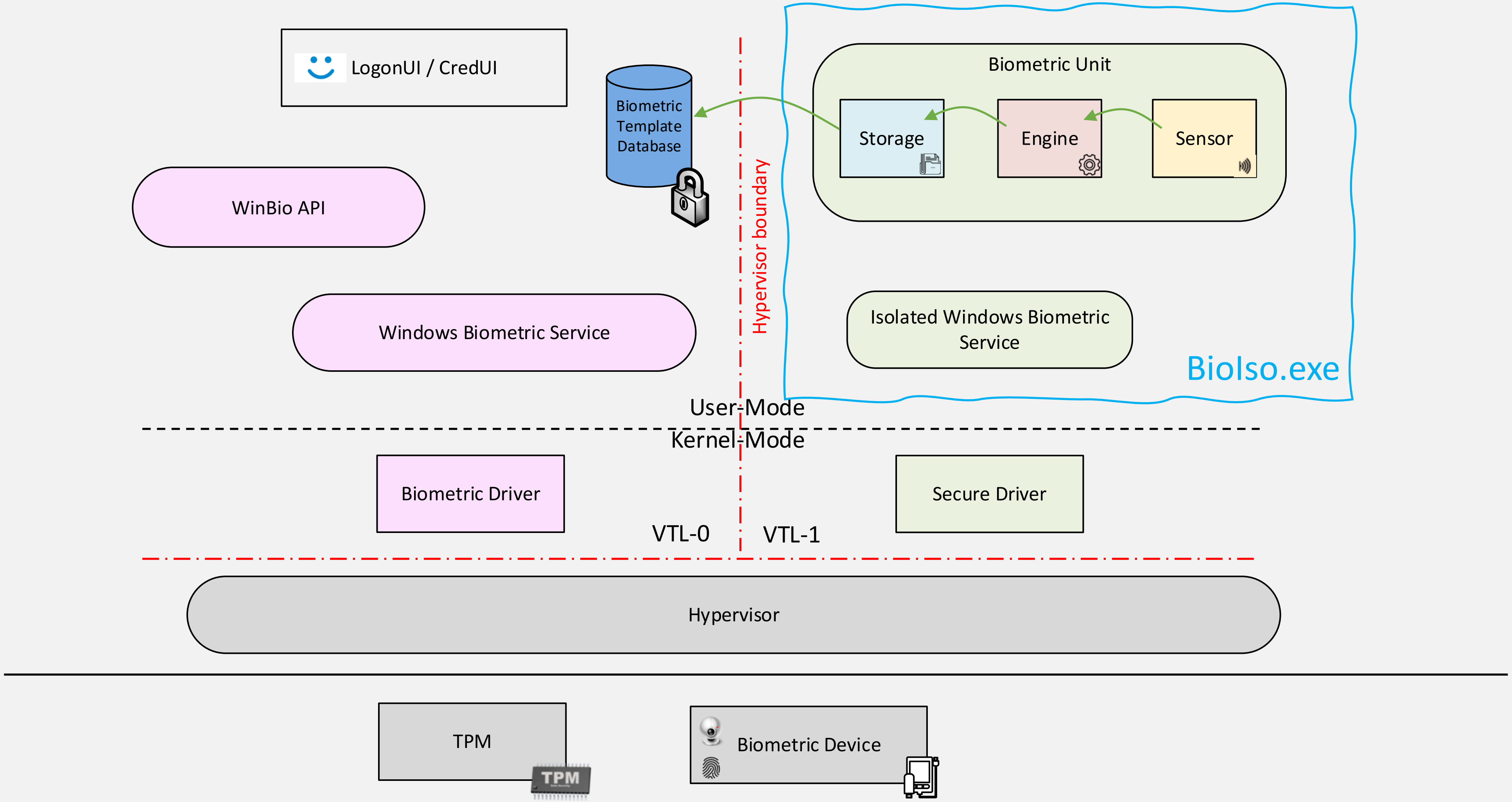
Enhanced Sign-in Security (ESS)



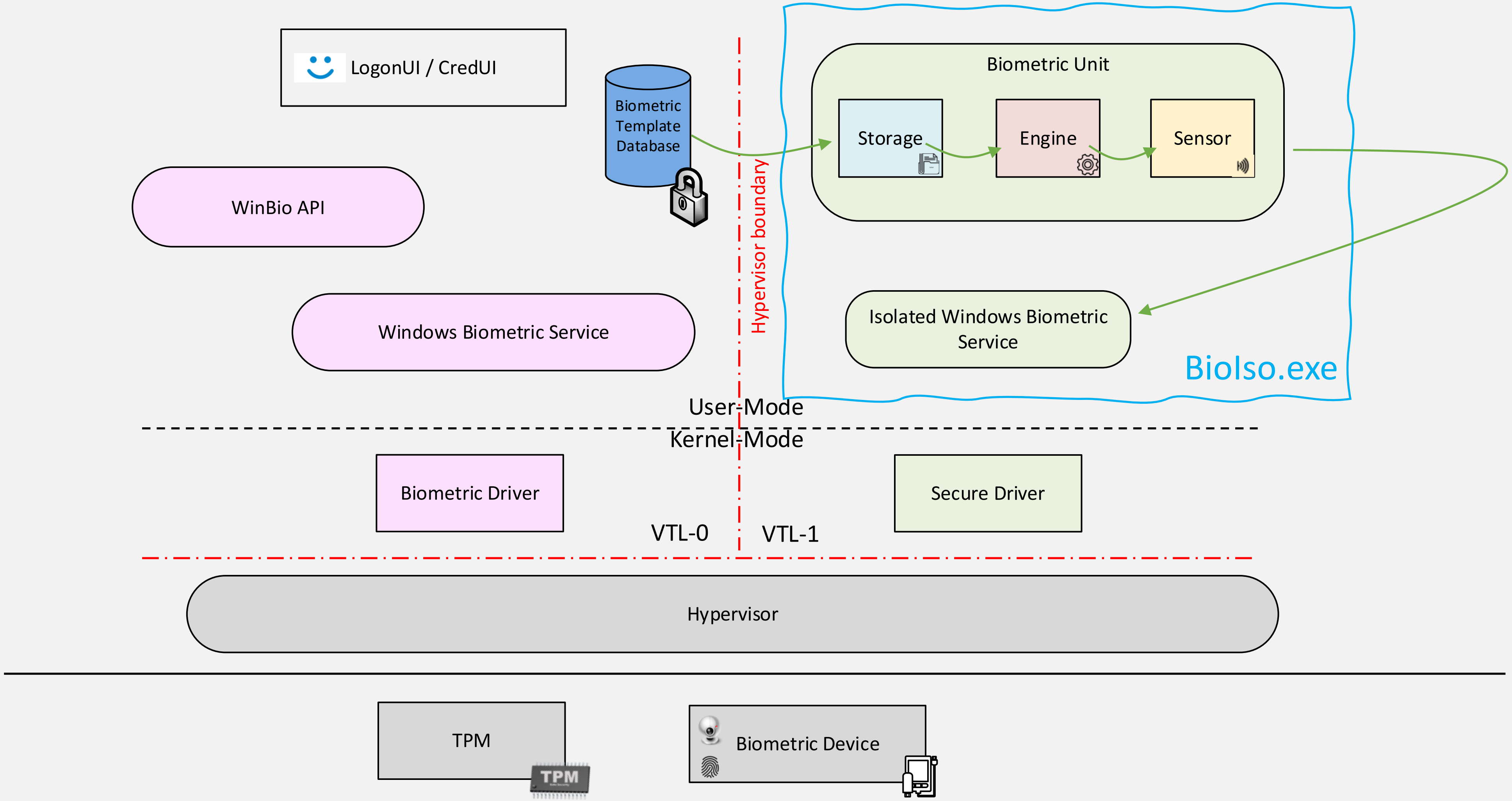
Enhanced Sign-in Security (ESS)



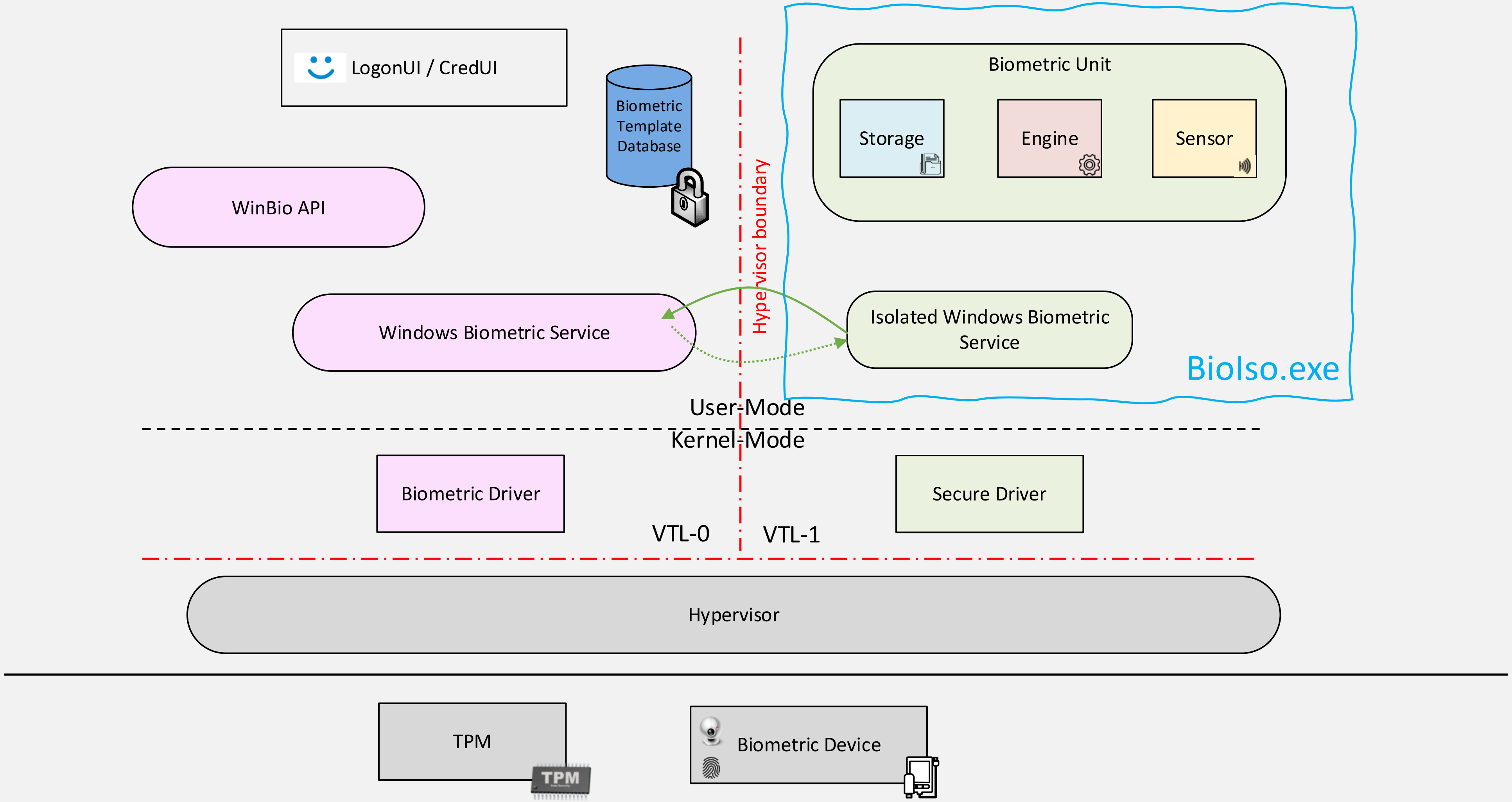
Enhanced Sign-in Security (ESS)



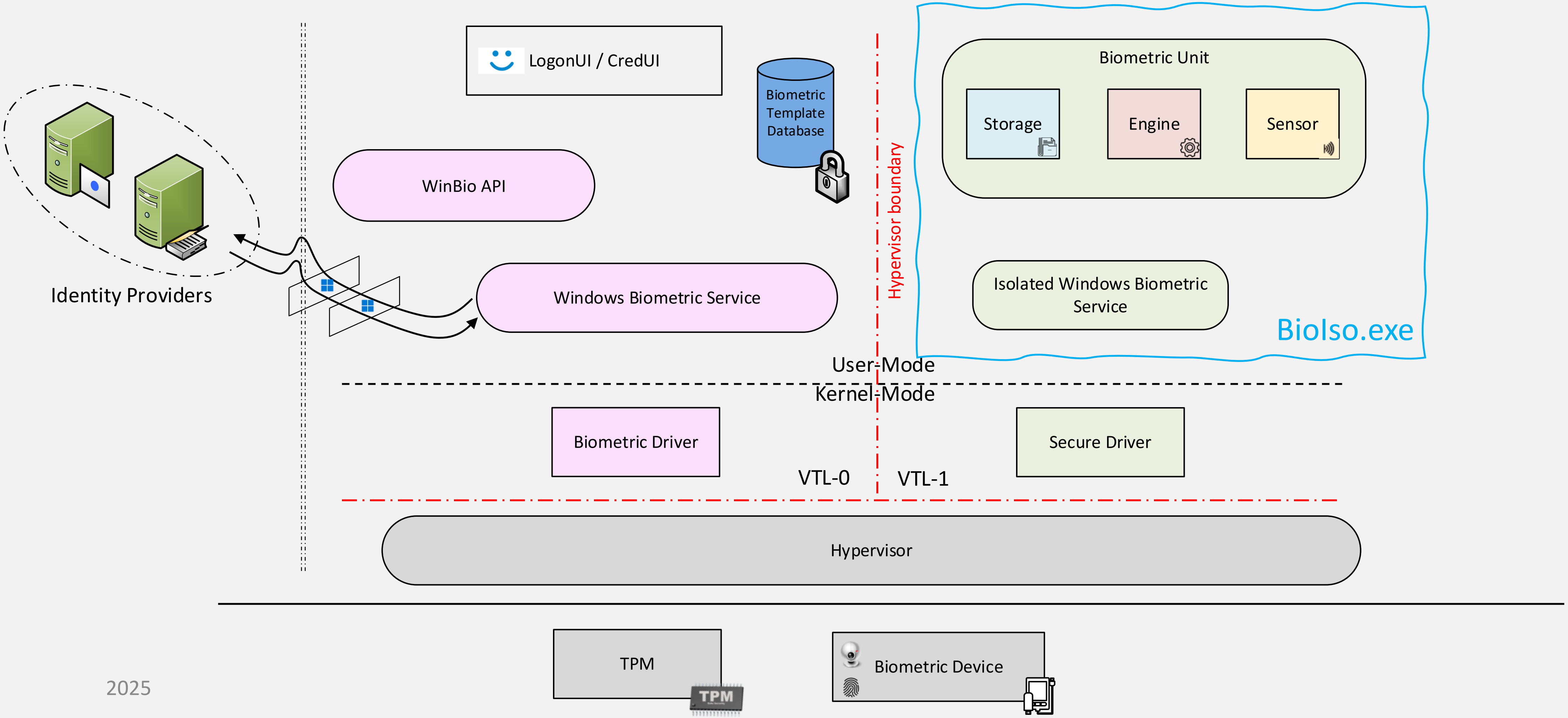
Enhanced Sign-in Security (ESS)



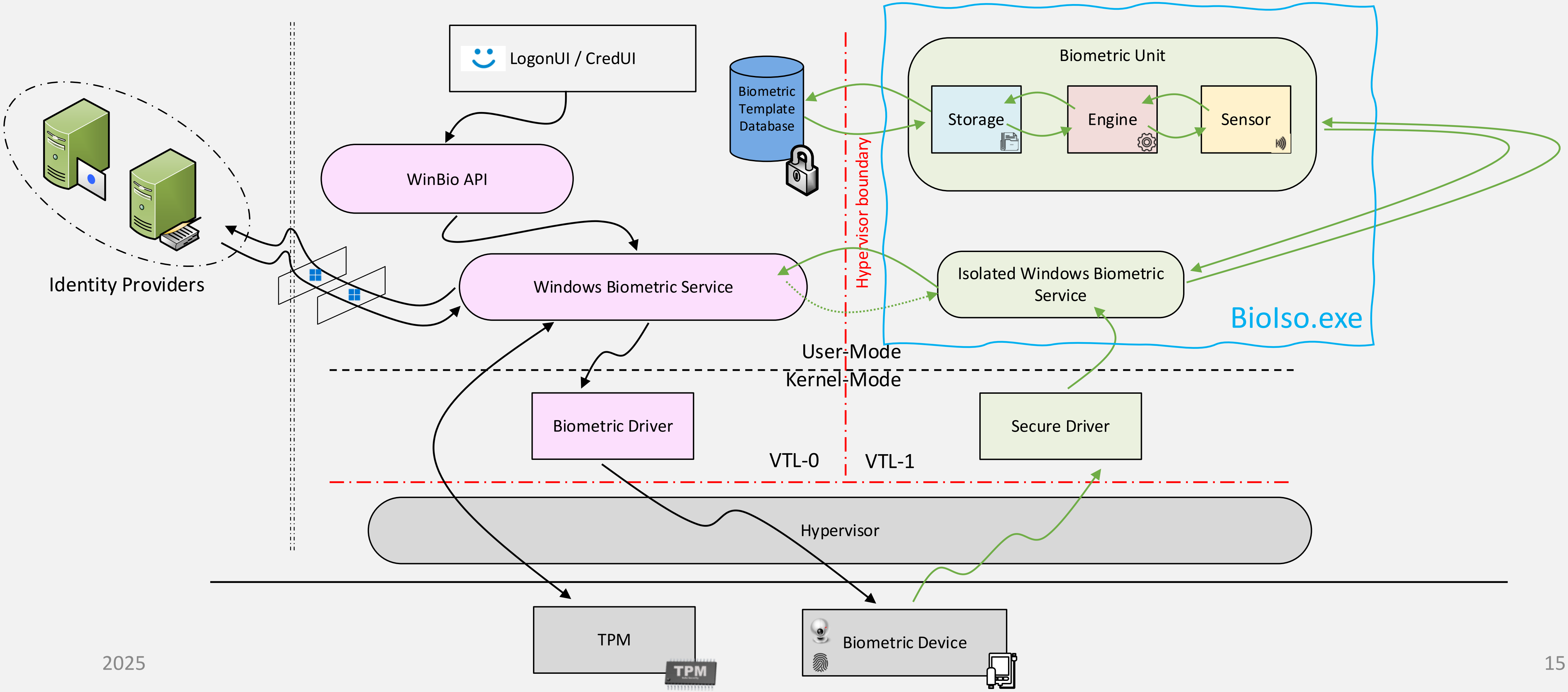
Enhanced Sign-in Security (ESS)



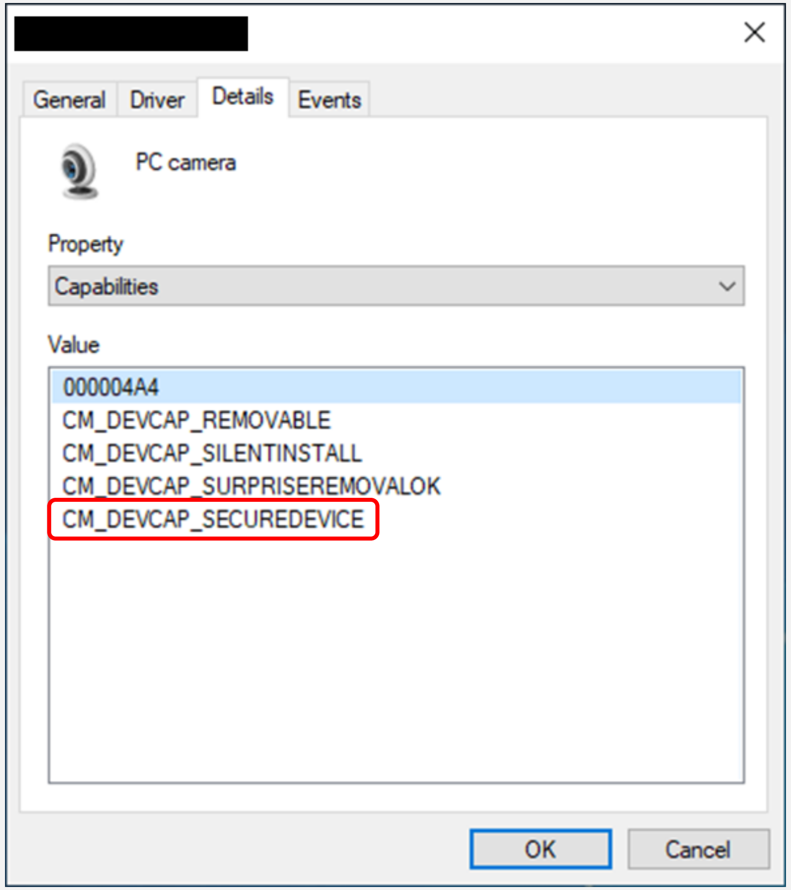
Enhanced Sign-in Security (ESS)



Enhanced Sign-in Security (ESS)



Enhanced Sign-in Security (ESS)



[redacted]

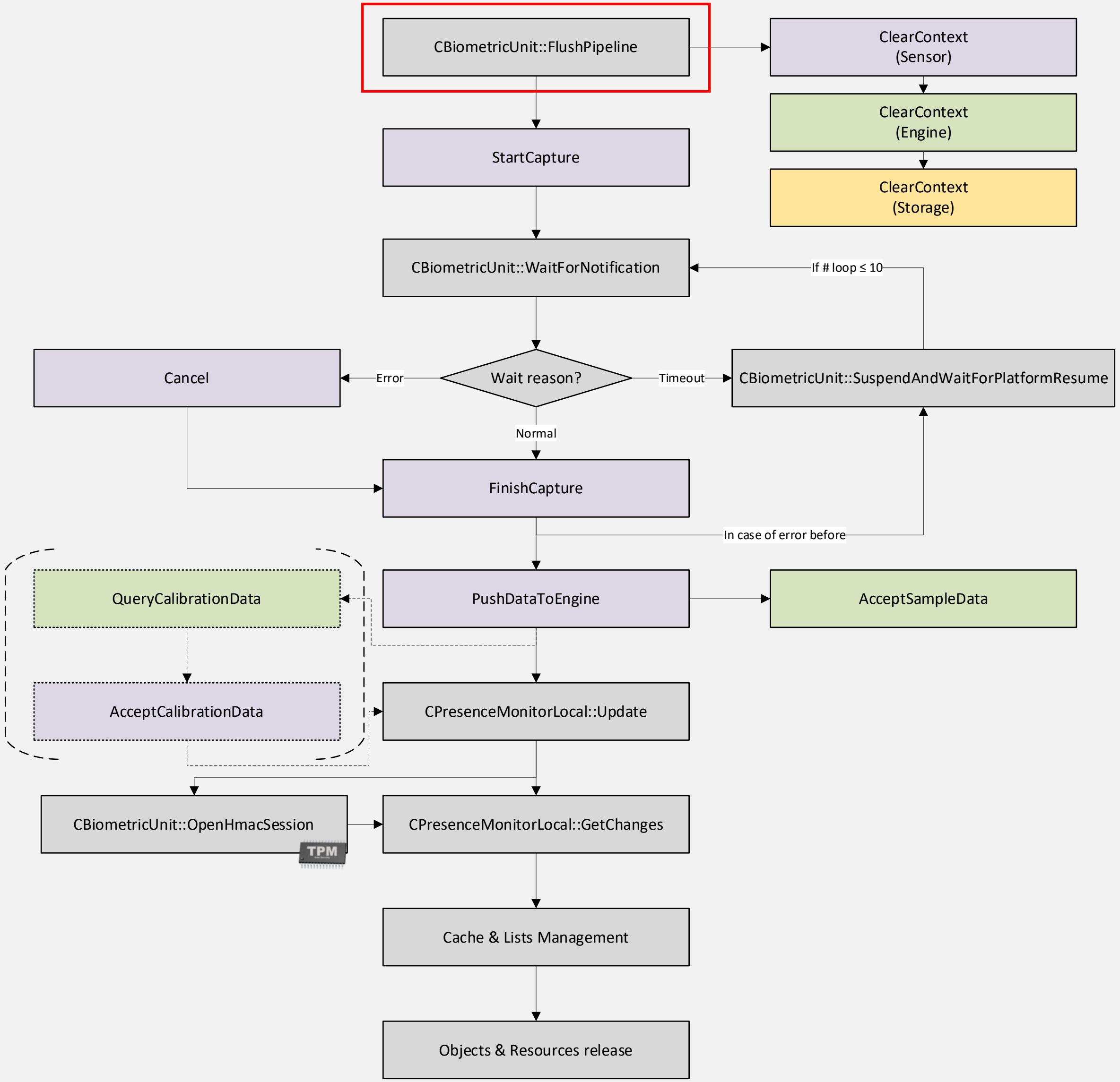
PC camera

Property: Capabilities

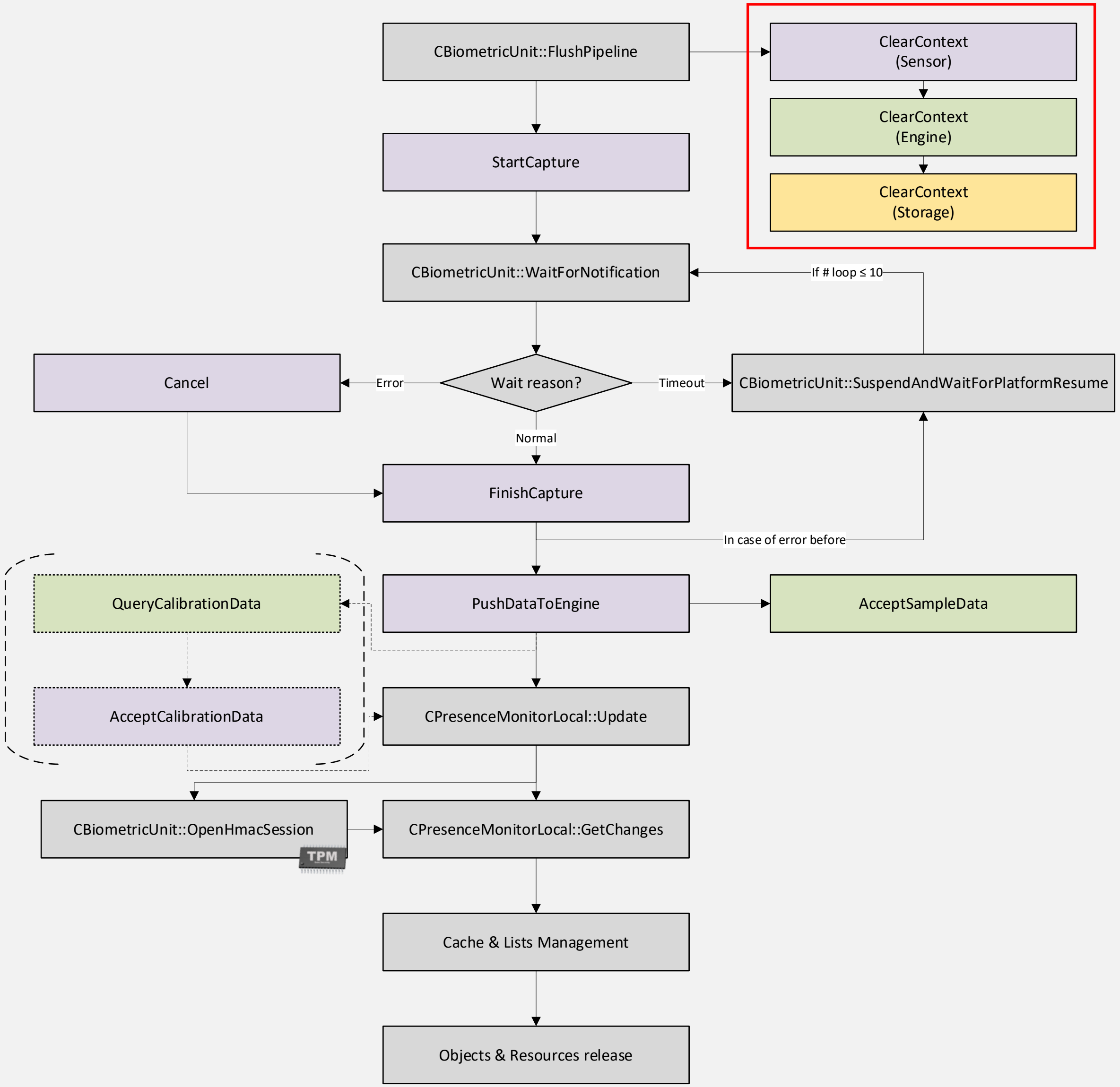
Value:

```
000004A4
CM_DEVCAP_REMOVABLE
CM_DEVCAP_SILENTINSTALL
CM_DEVCAP_SURPRISEREMOVALOK
CM_DEVCAP_SECUREDEVICE
```

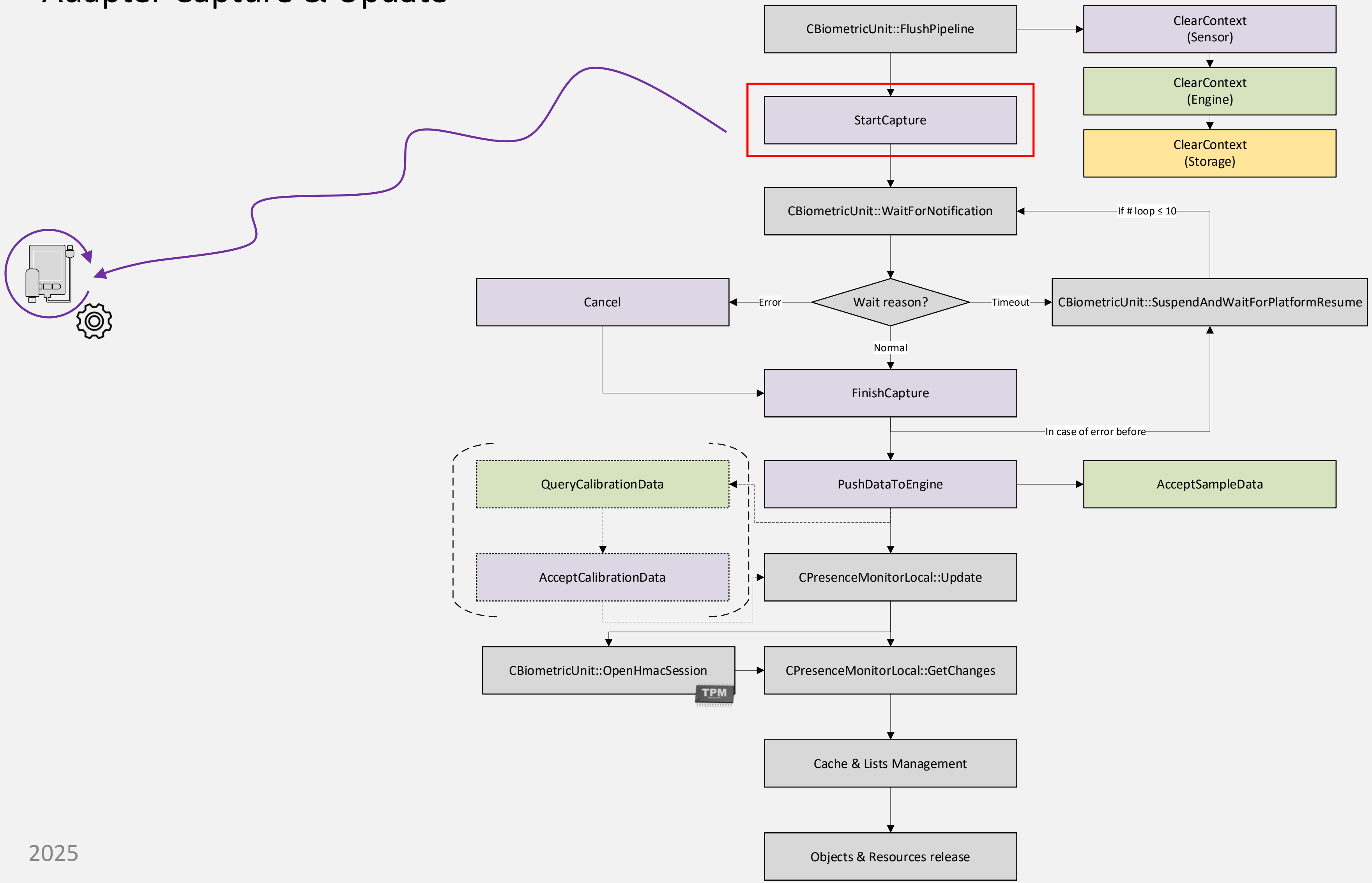
- Adapter Capture & Update



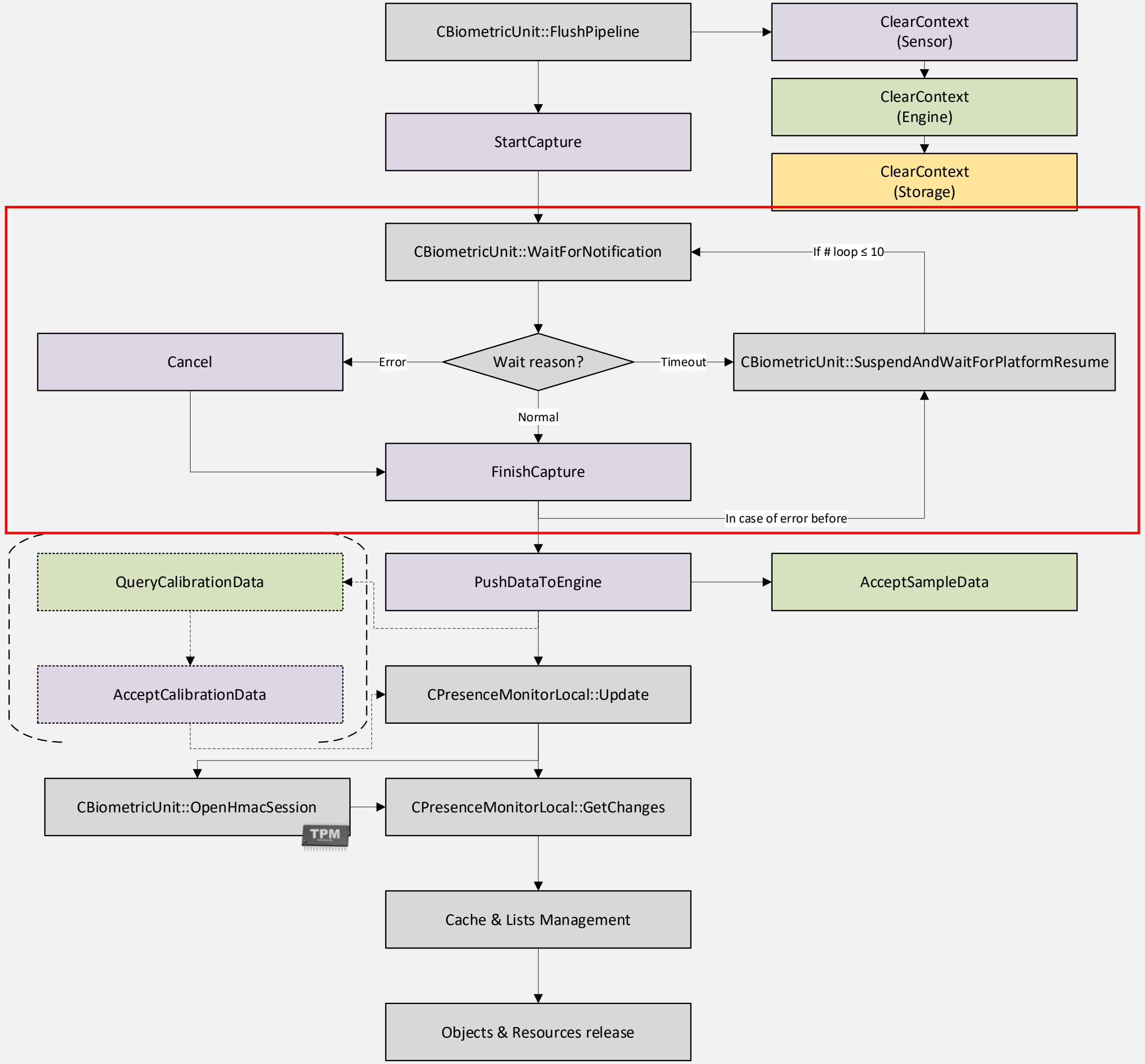
- Adapter Capture & Update



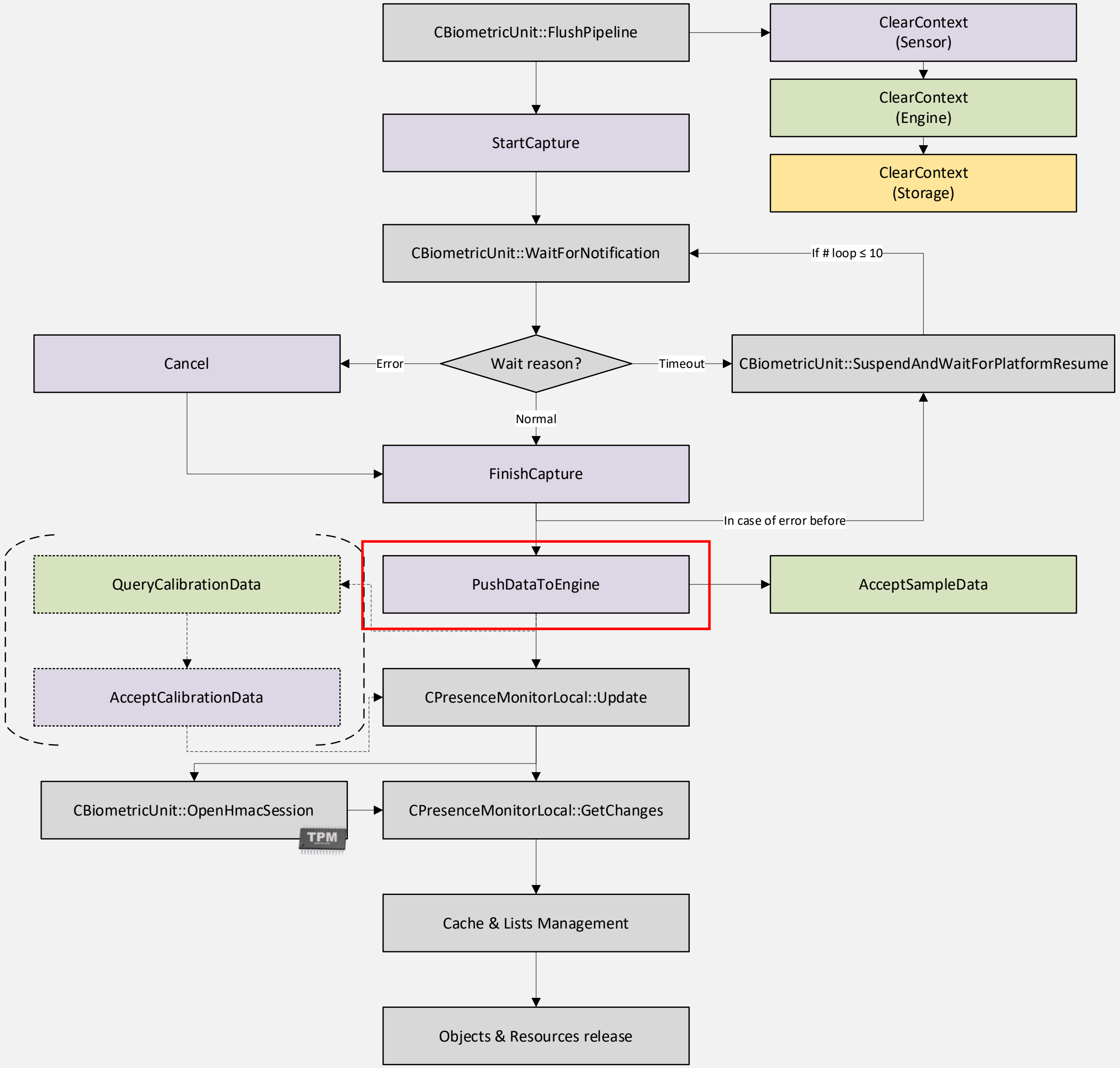
- Adapter Capture & Update



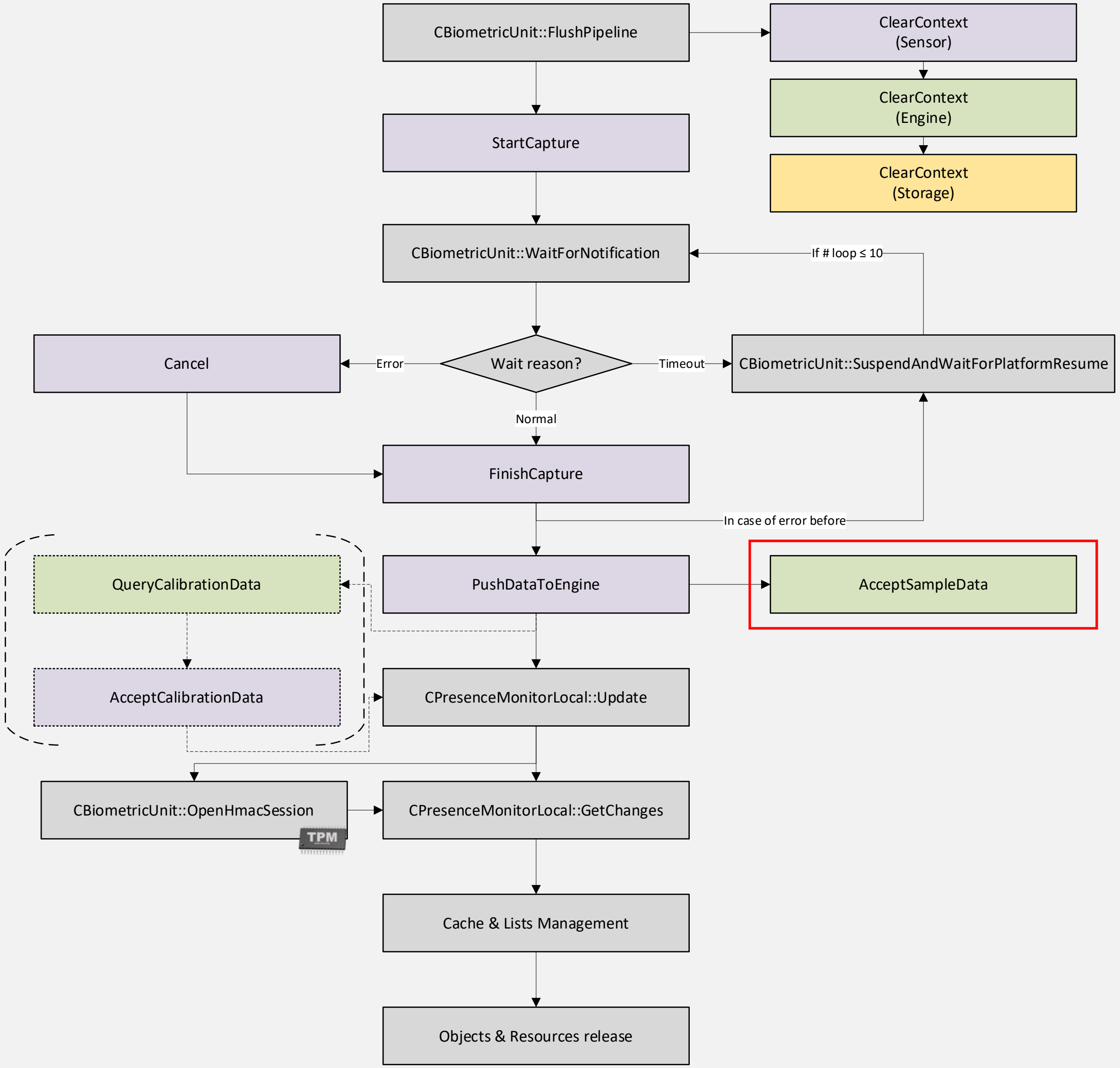
- Adapter Capture & Update



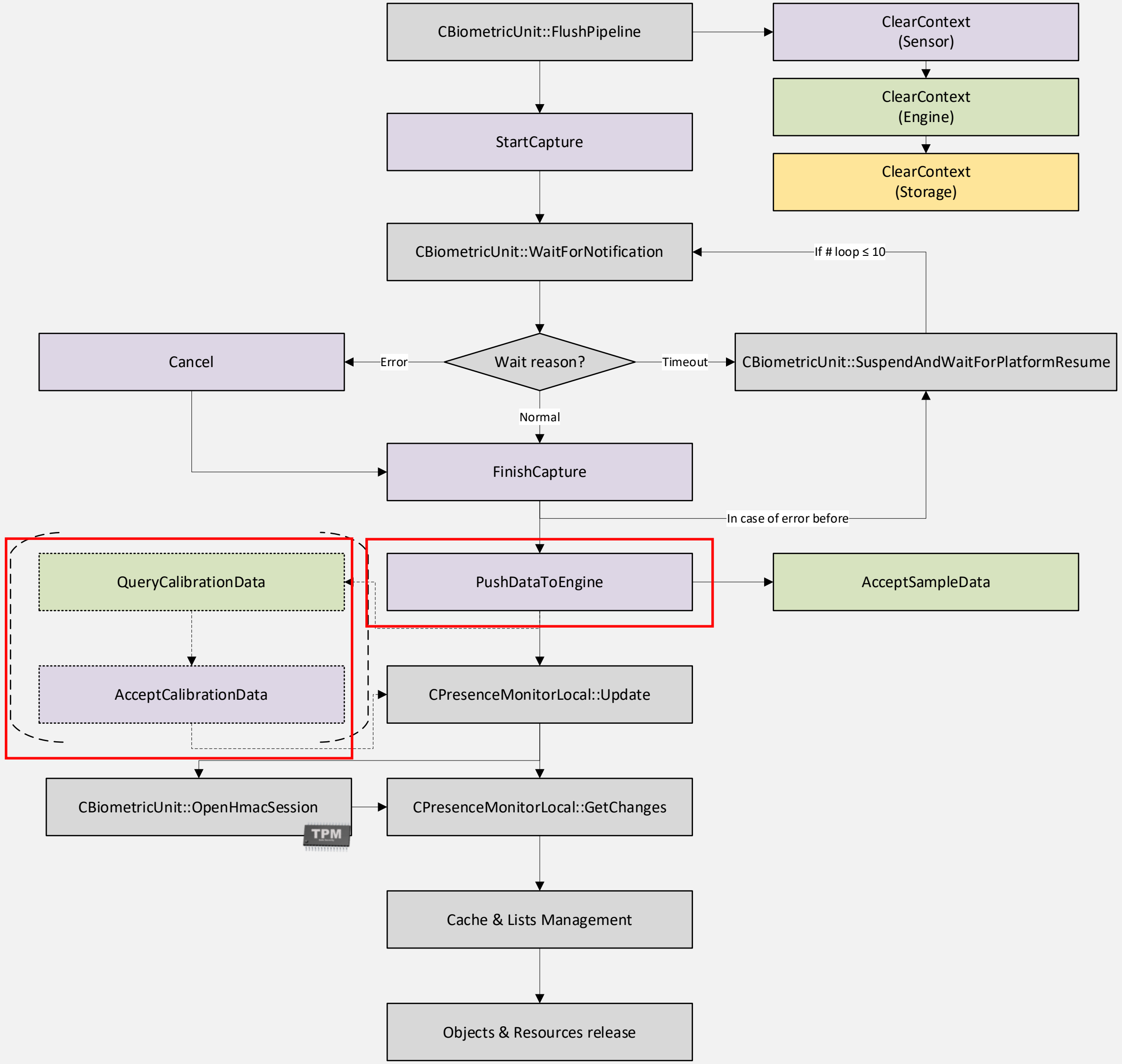
- Adapter Capture & Update



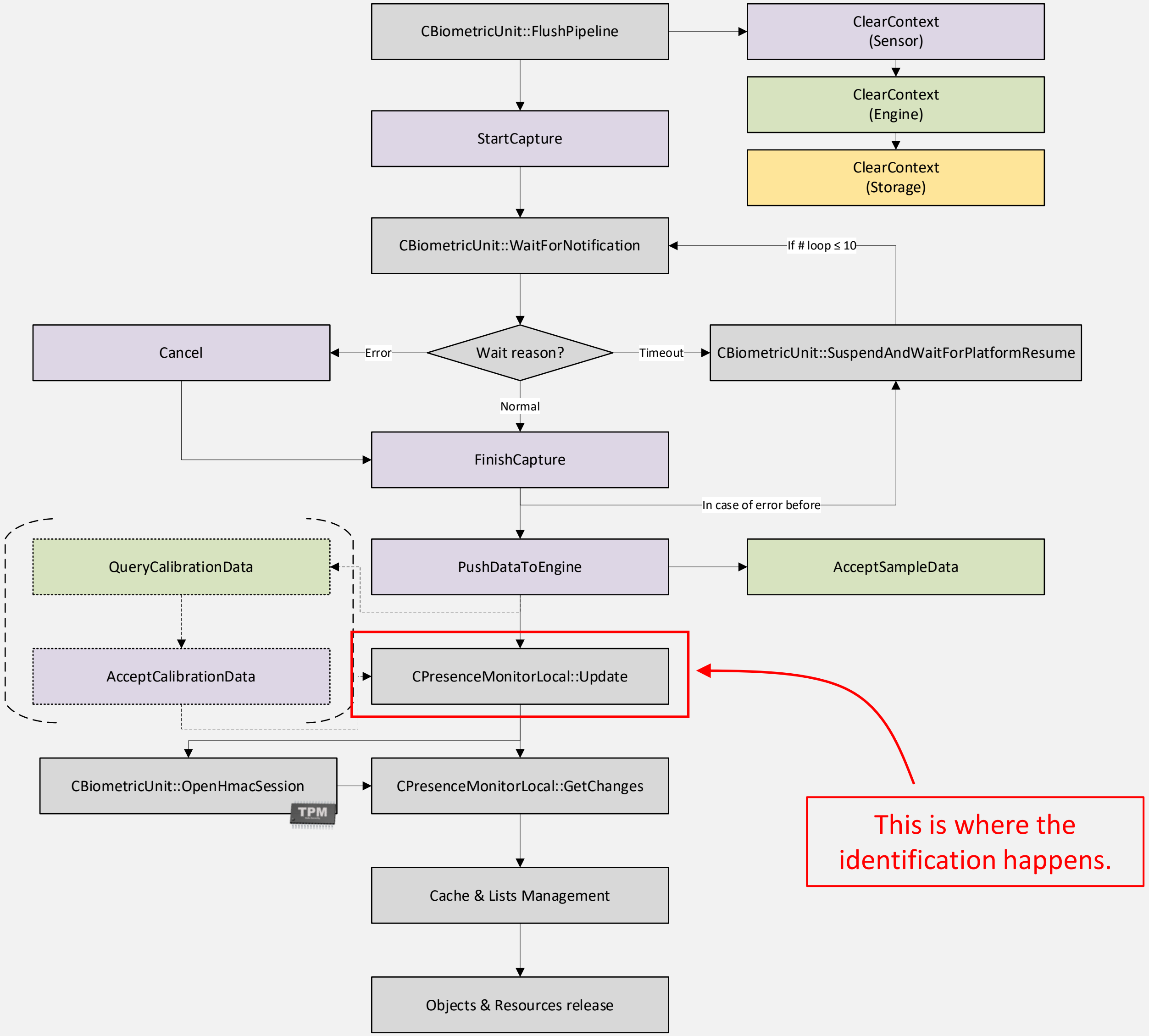
- Adapter Capture & Update



- Adapter Capture & Update

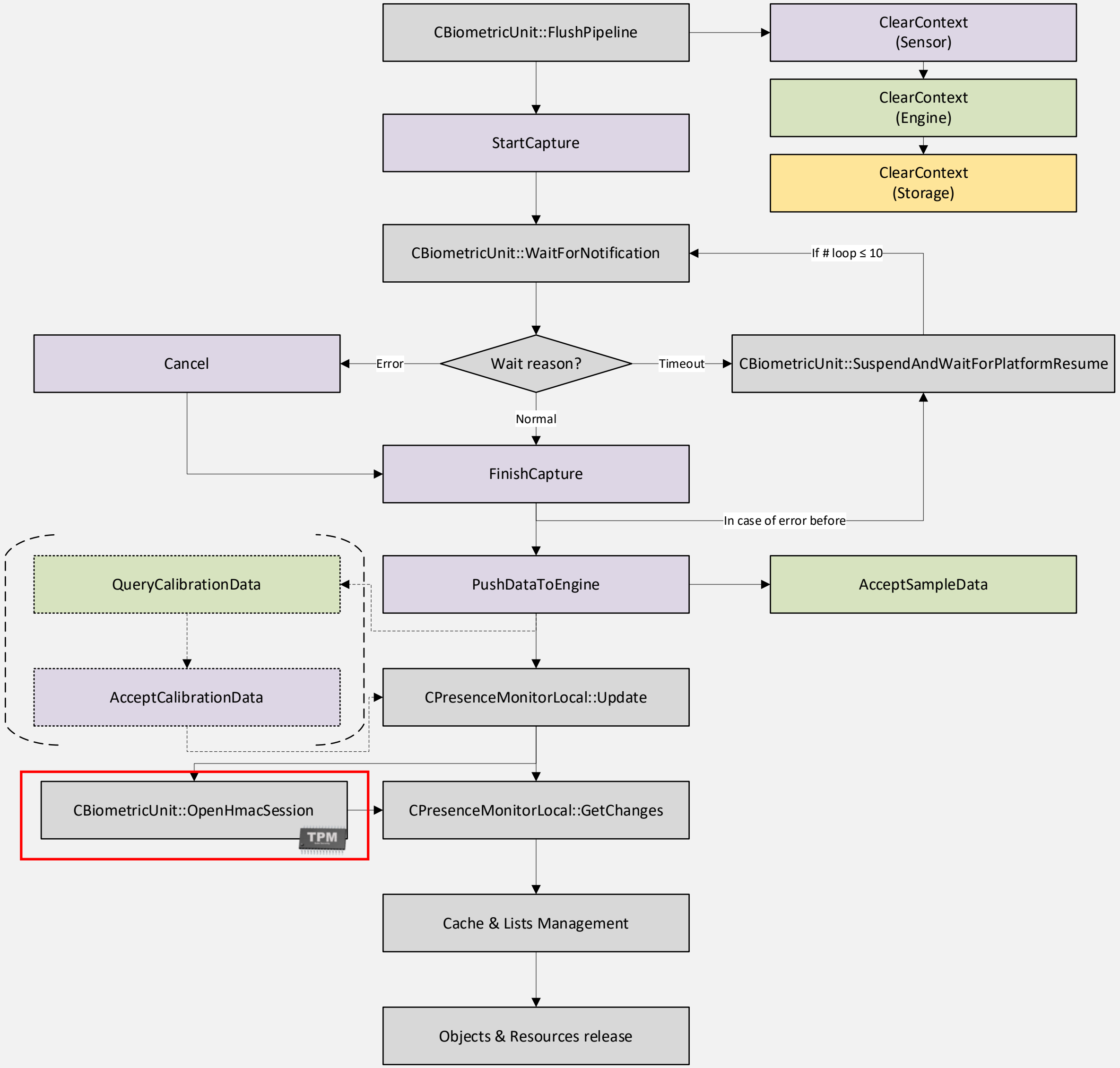


- Adapter Capture & Update

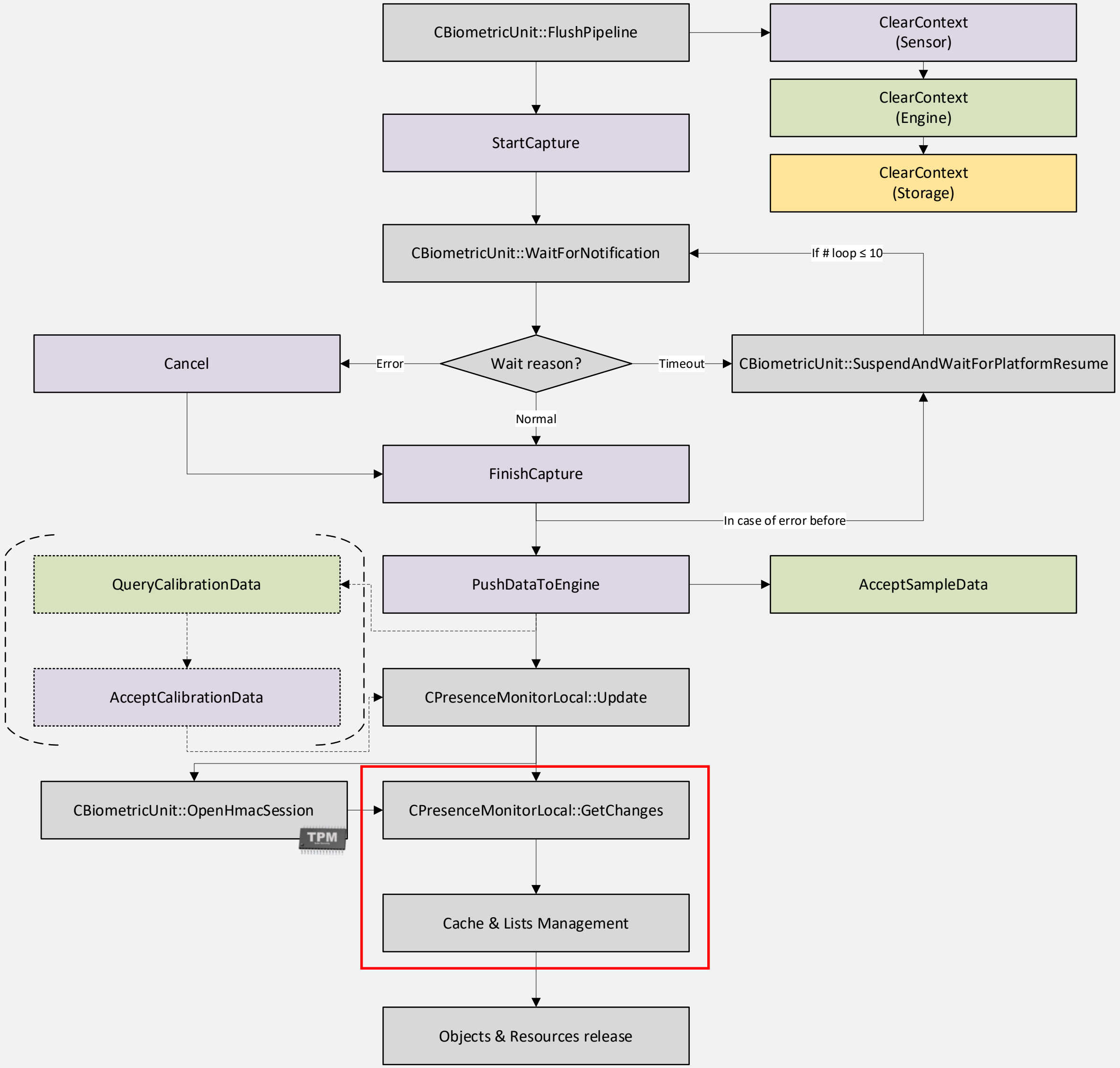


This is where the identification happens.

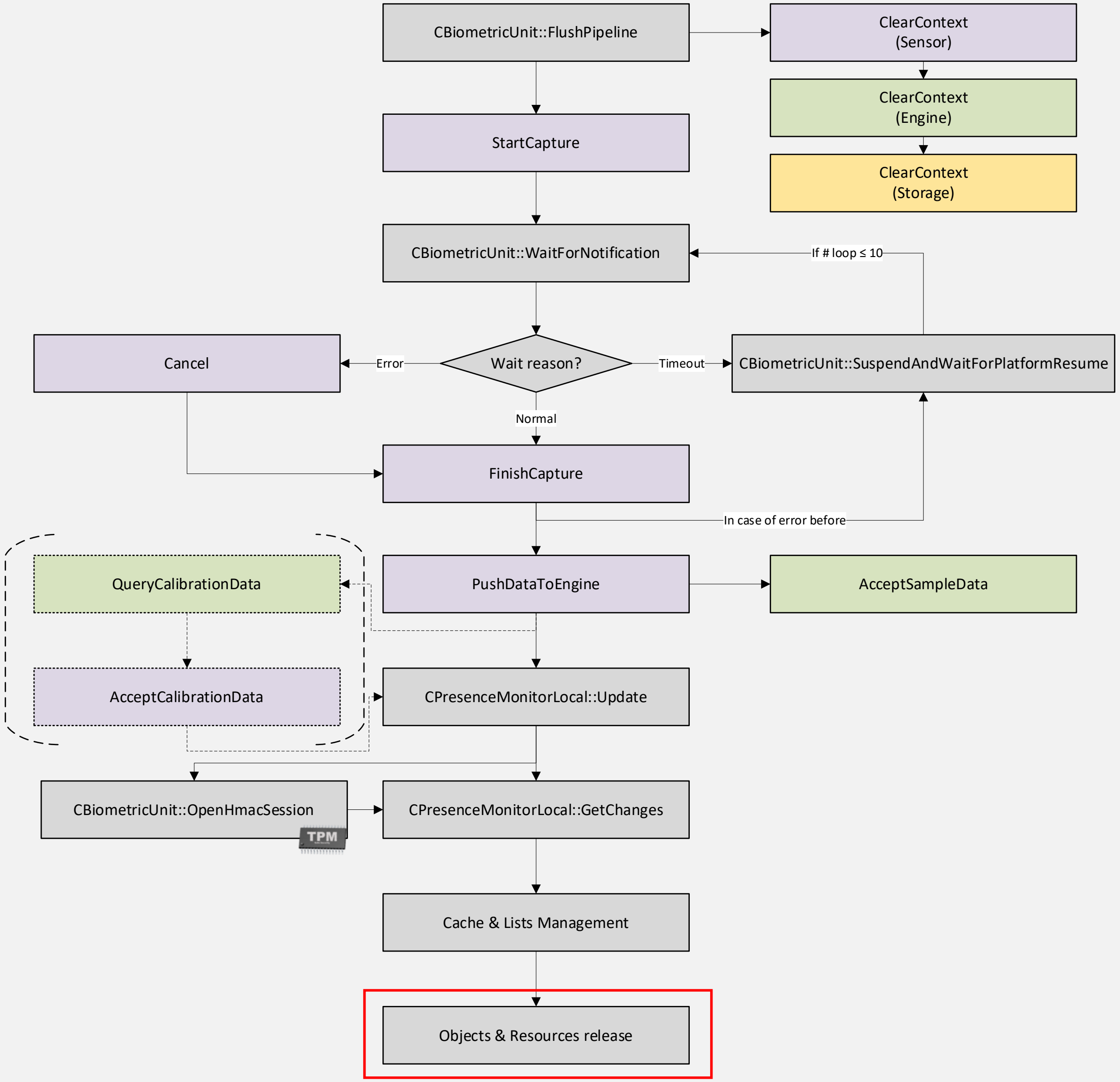
- Adapter Capture & Update



- Adapter Capture & Update

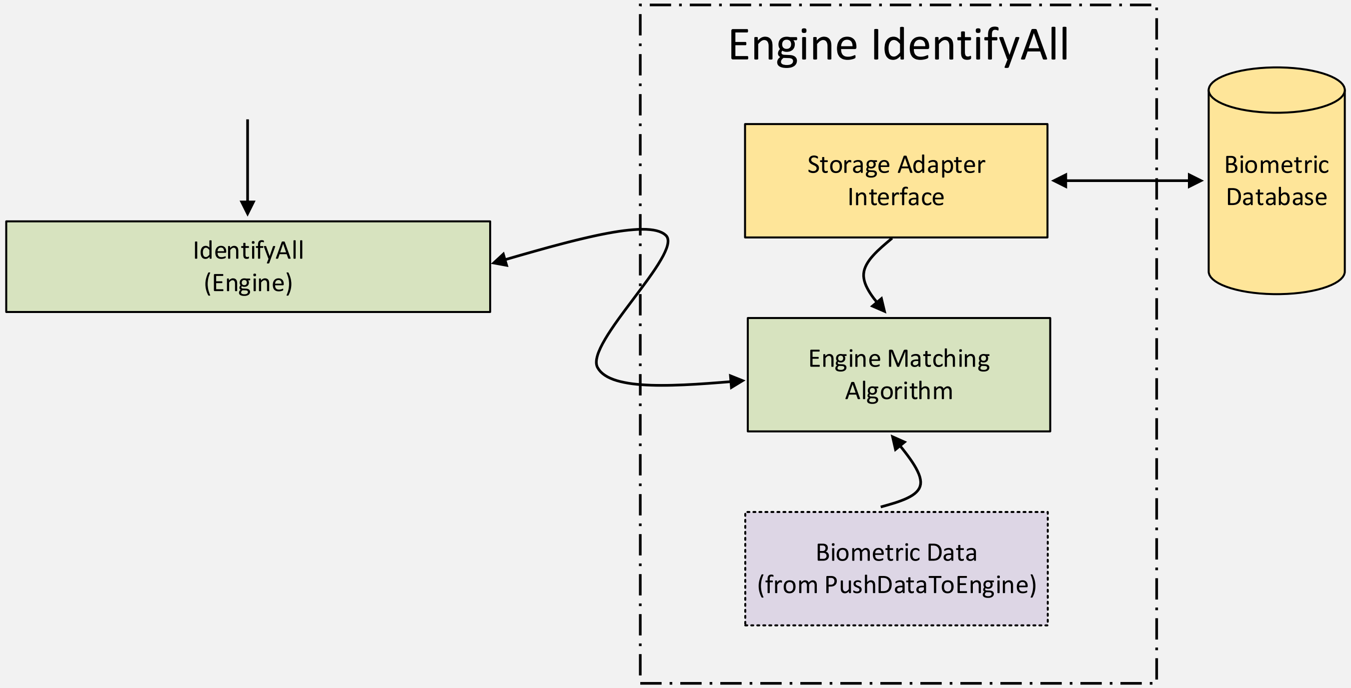


- Adapter Capture & Update

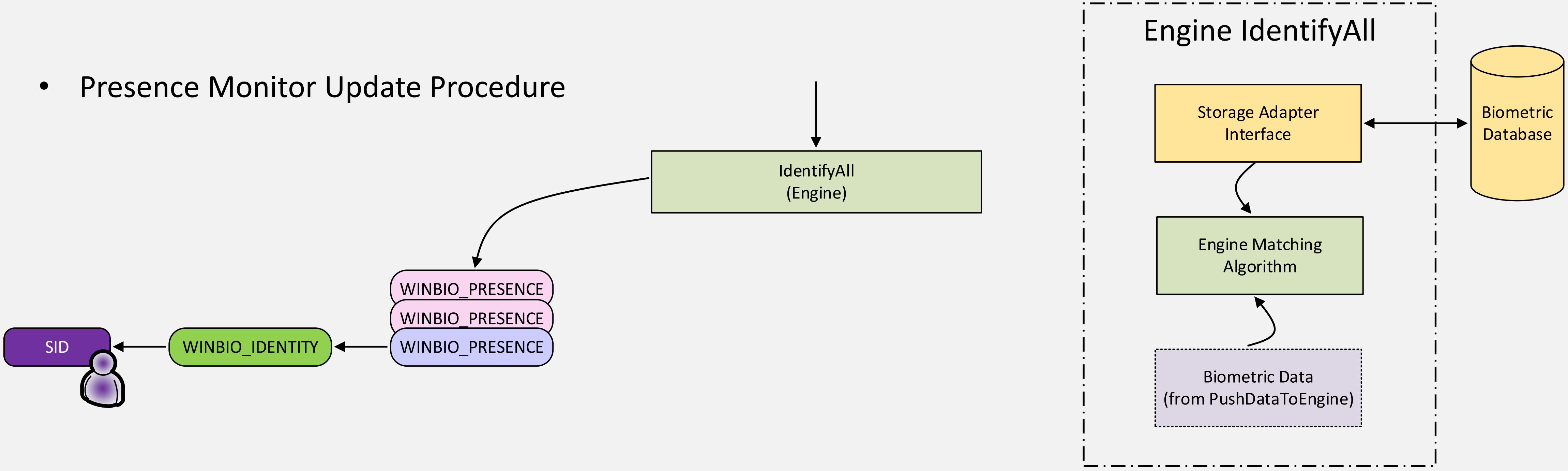


- Presence Monitor Update Procedure

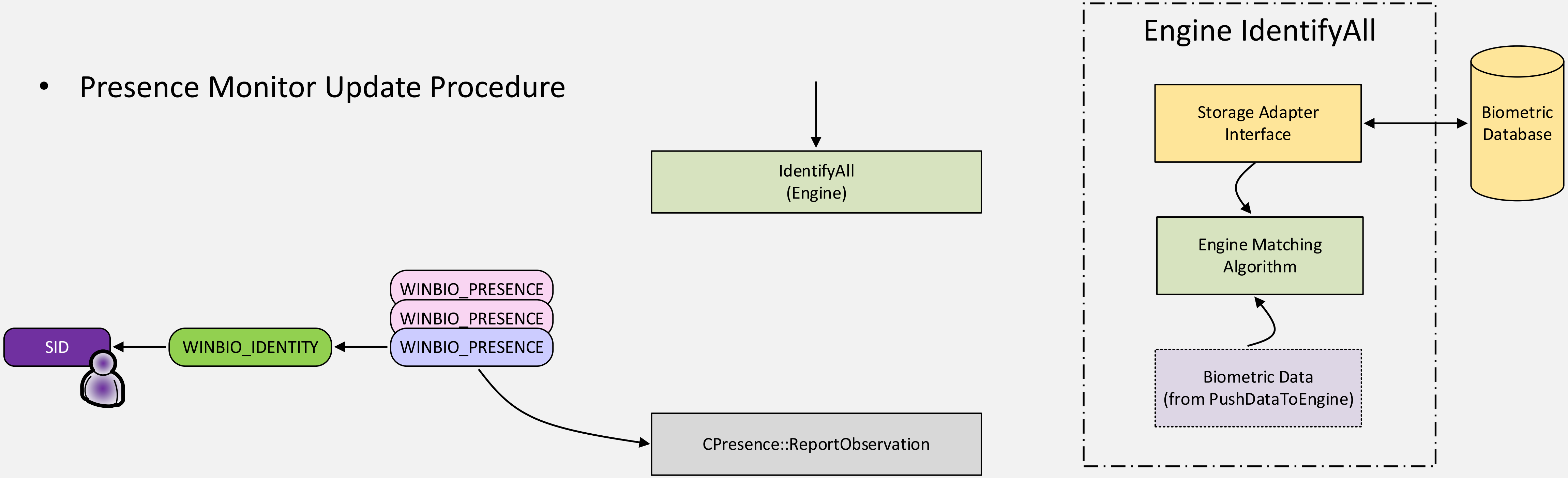
- Presence Monitor Update Procedure


Engine IdentifyAll
Storage Adapter Interface
Biometric Database
IdentifyAll (Engine)
Engine Matching Algorithm
Biometric Data (from PushDataToEngine)

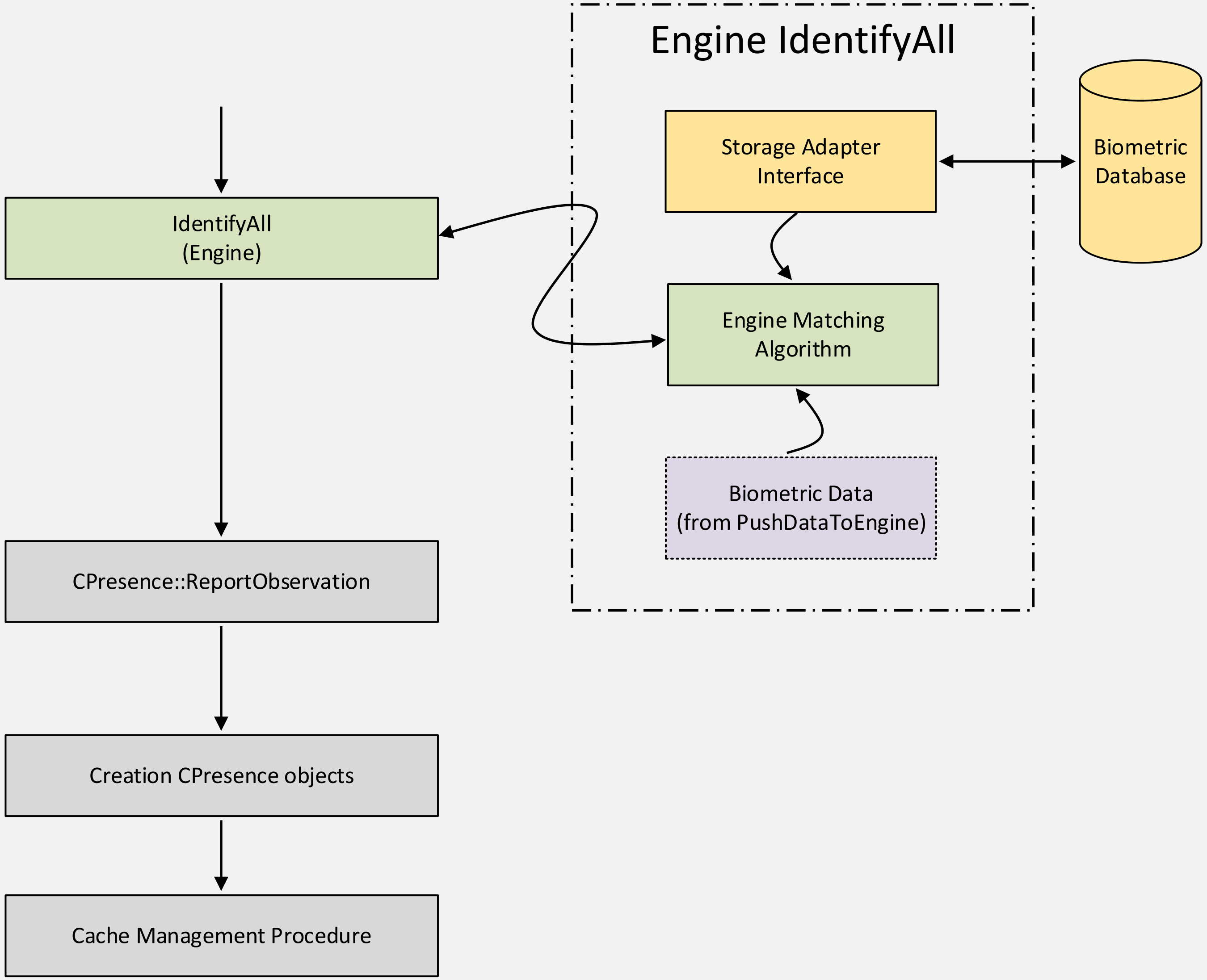
- Presence Monitor Update Procedure



- Presence Monitor Update Procedure



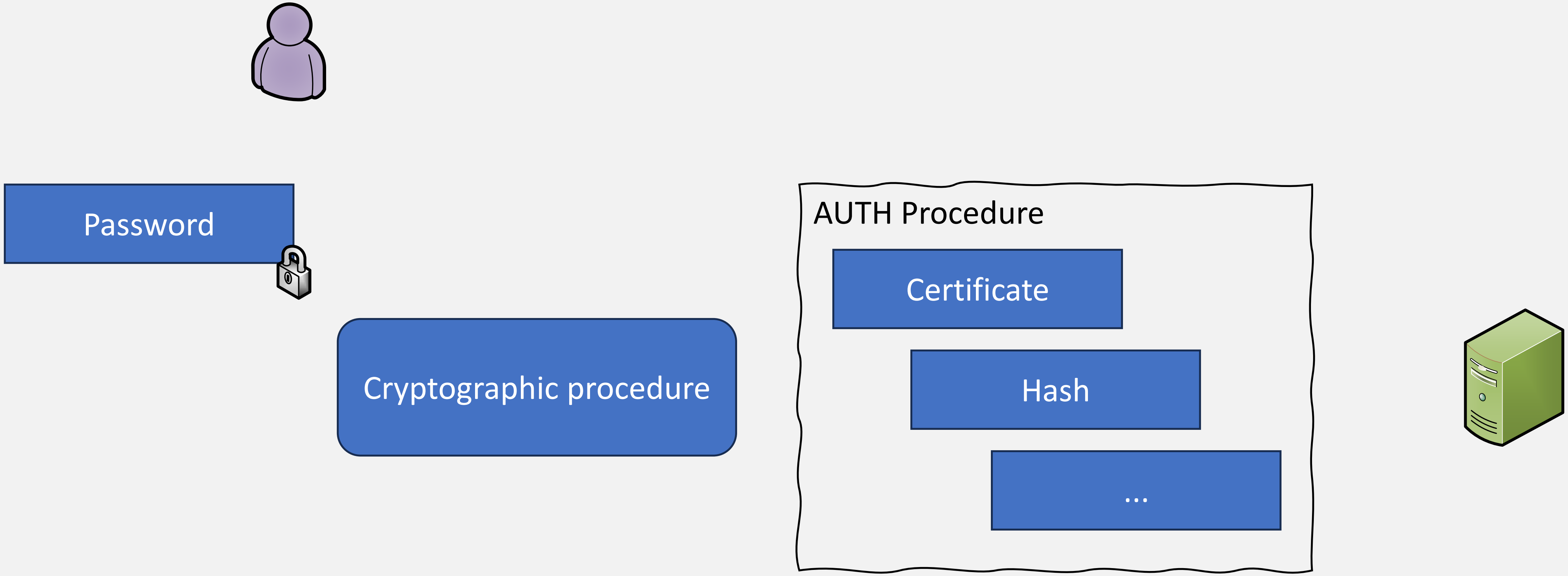
- Presence Monitor Update Procedure


Engine IdentifyAll
Storage Adapter Interface
Biometric Database
IdentifyAll (Engine)
Engine Matching Algorithm
Biometric Data (from PushDataToEngine)
CPresence::ReportObservation
Creation CPresence objects
Cache Management Procedure

Authentication procedure

Once the identification happened

Traditional Auth management



Password

Cryptographic procedure

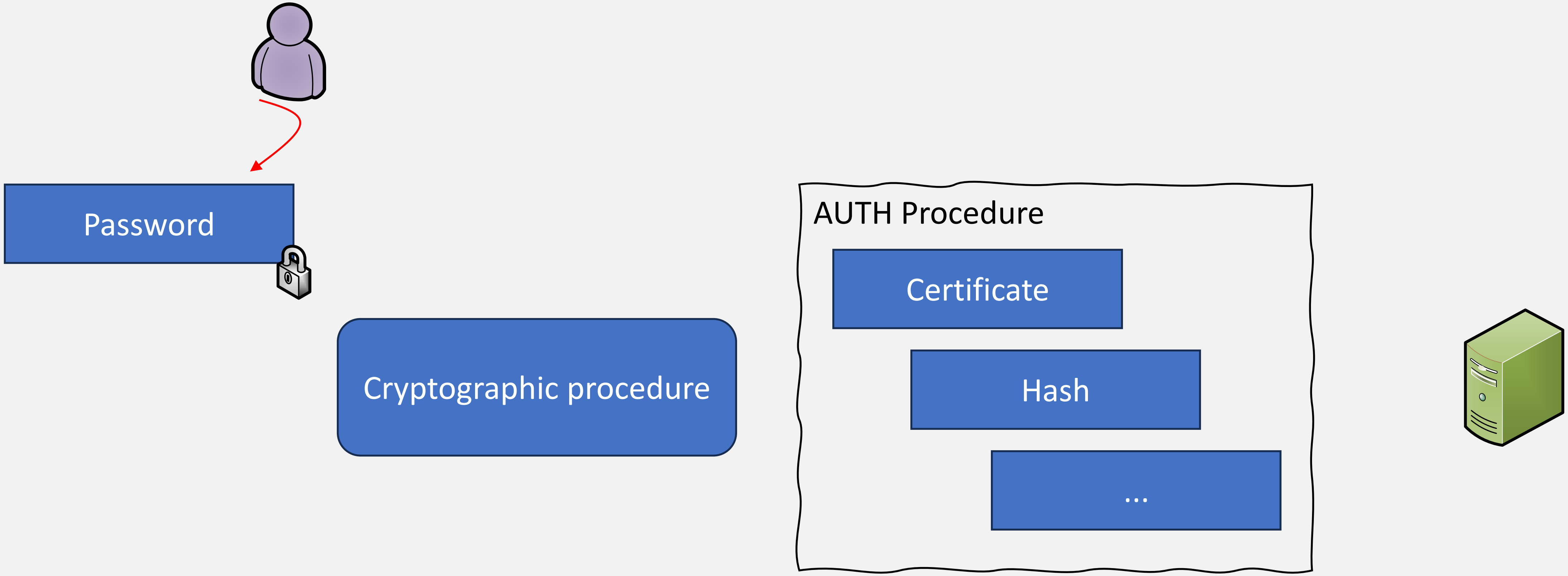
AUTH Procedure

Certificate

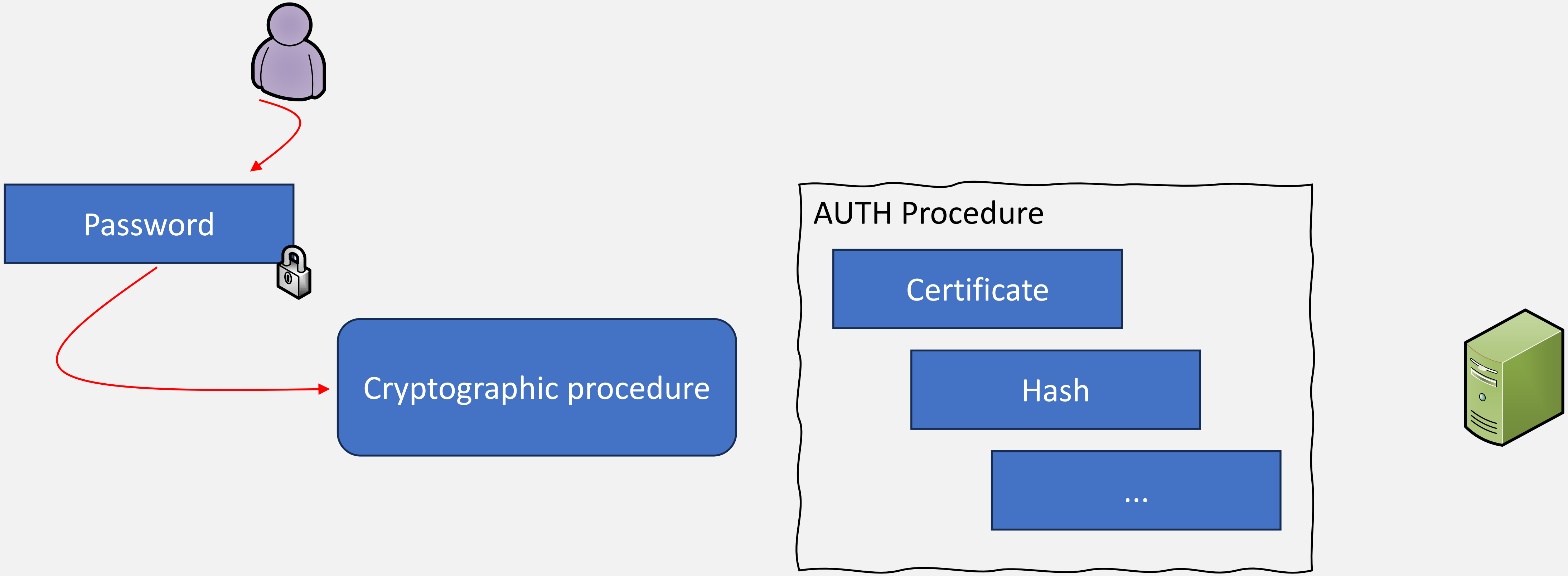
Hash

...

Traditional Auth management



Traditional Auth management



Password

Cryptographic procedure

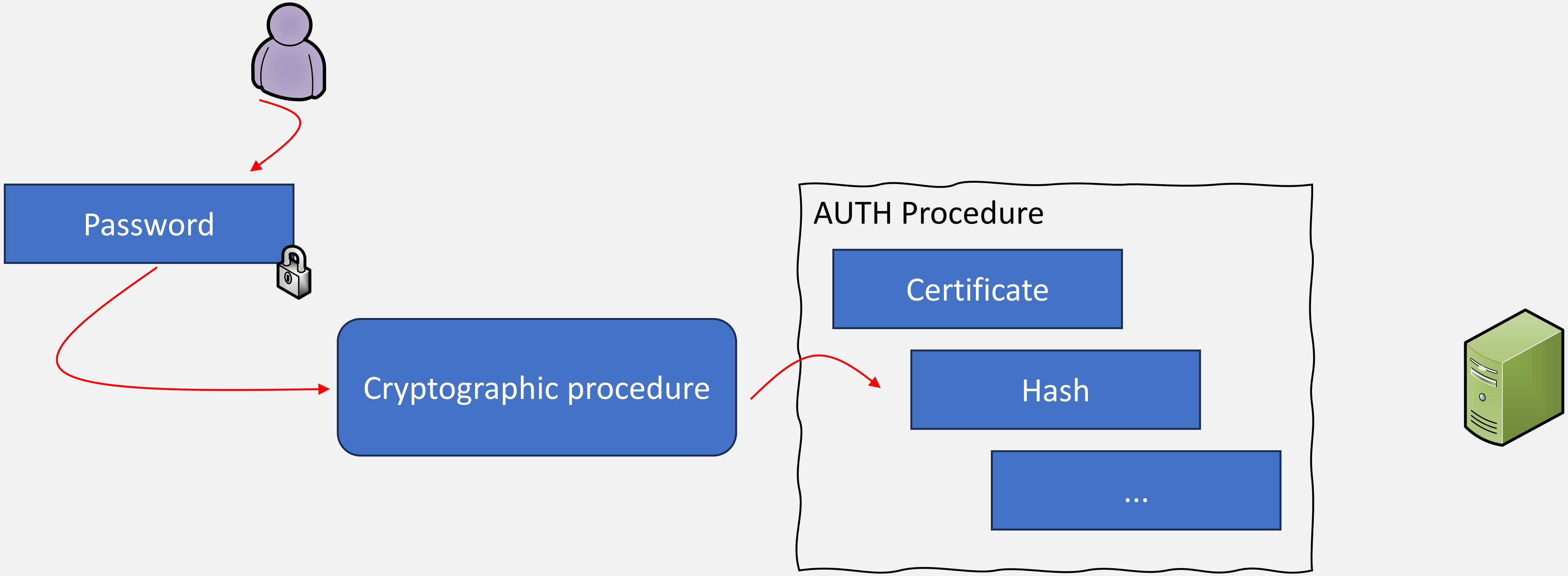
AUTH Procedure

Certificate

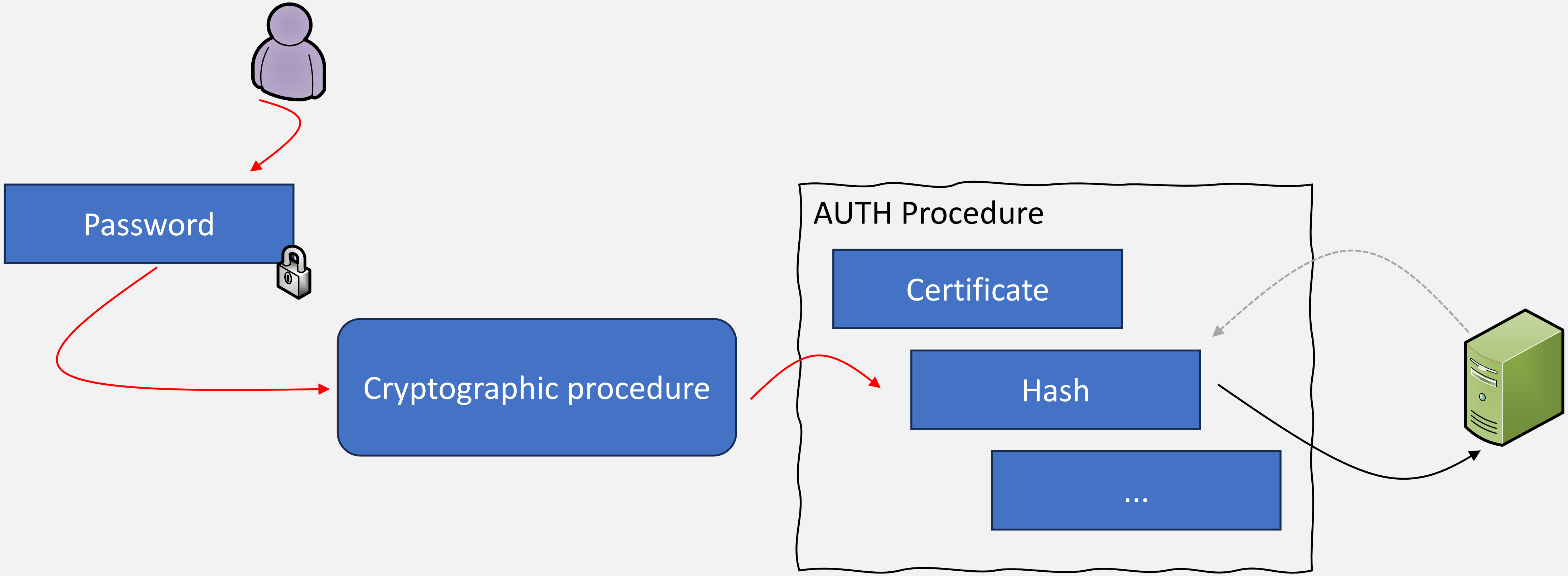
Hash

...

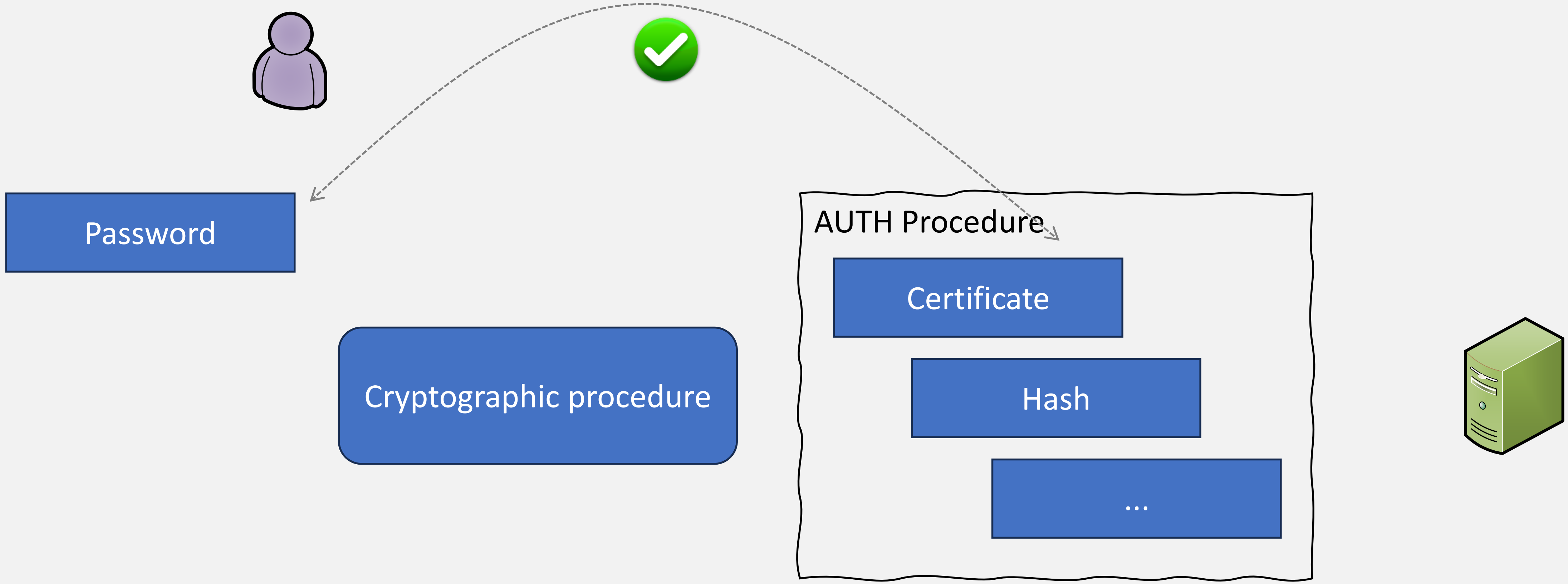
Traditional Auth management



Traditional Auth management



Traditional Auth management



Password

Cryptographic procedure

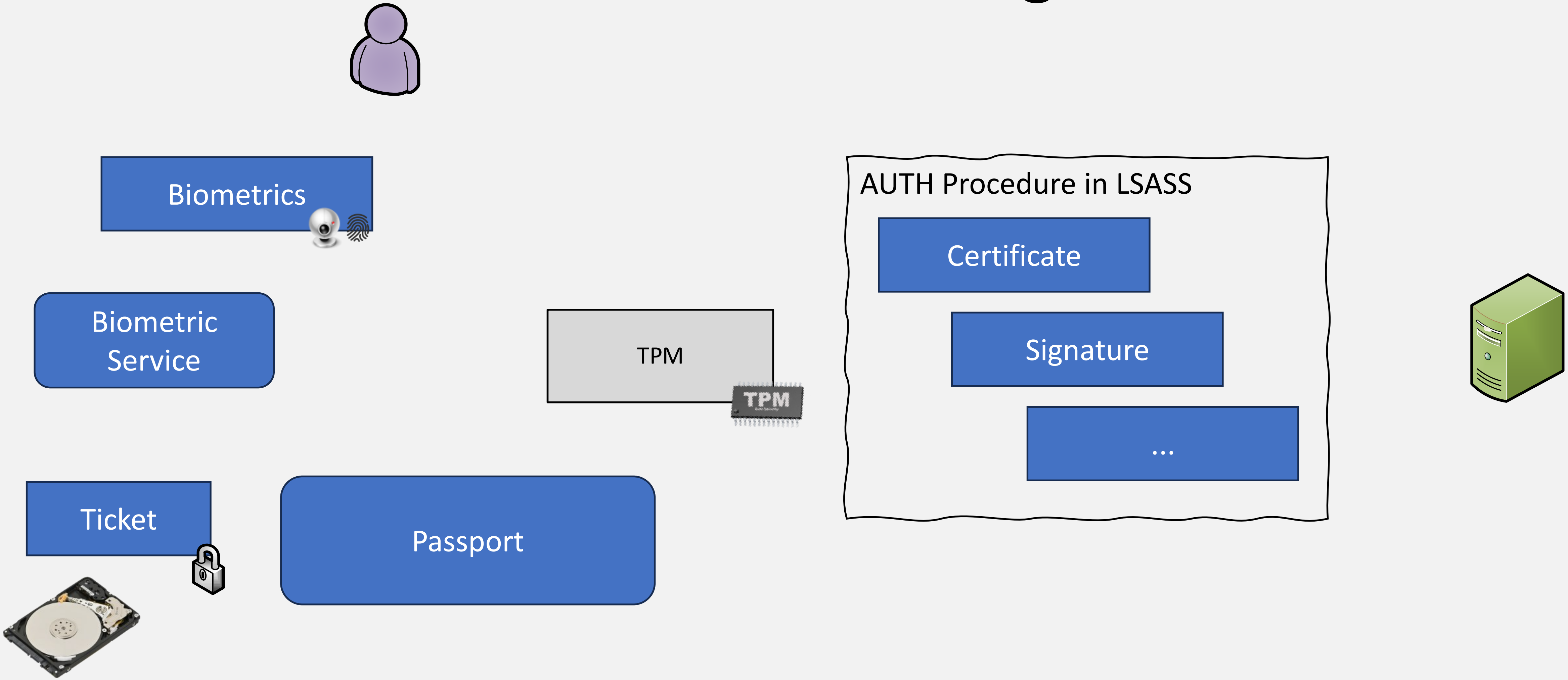
AUTH Procedure

Certificate

Hash

...

Windows Biometric Auth management



Biometrics

Biometric Service

Ticket

Passport

TPM

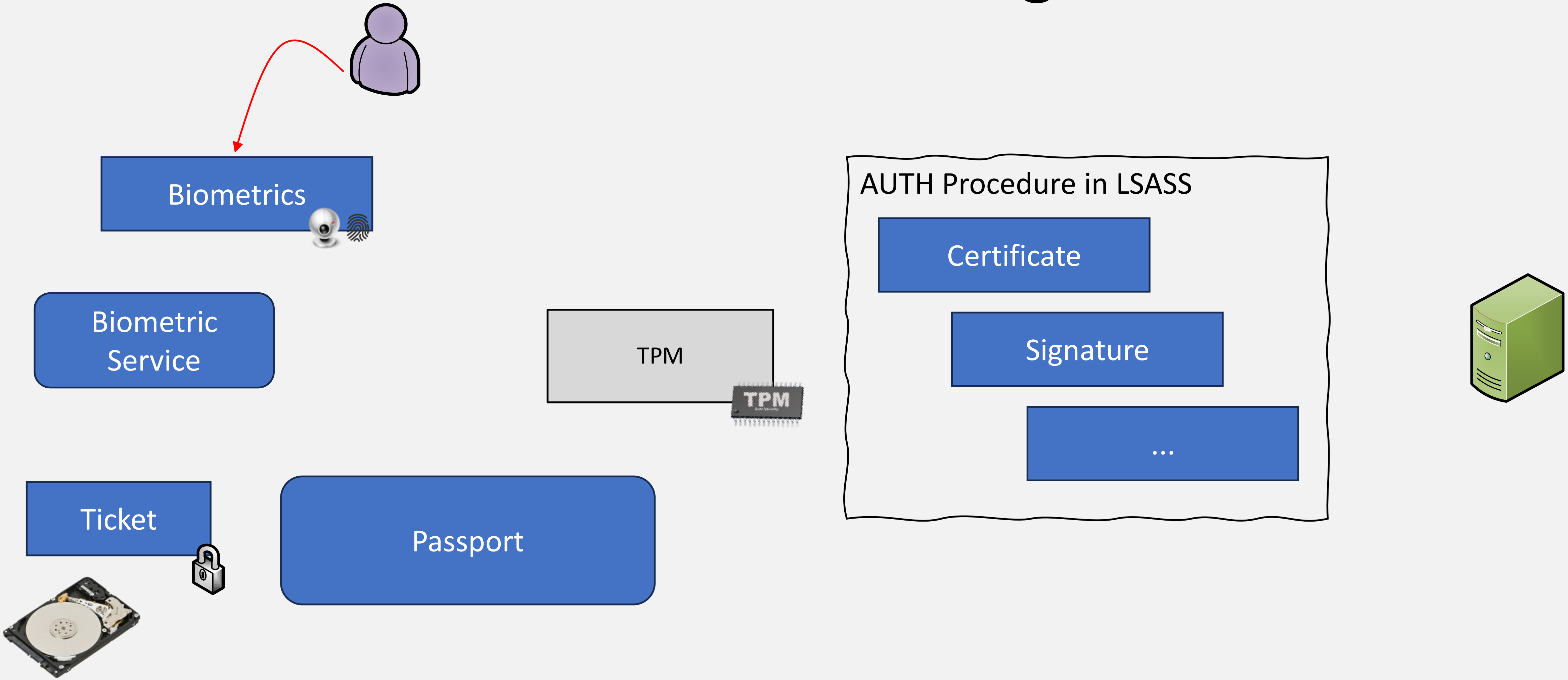
AUTH Procedure in LSASS

Certificate

Signature

...

Windows Biometric Auth management



Biometrics

Biometric Service

TPM

Ticket

Passport

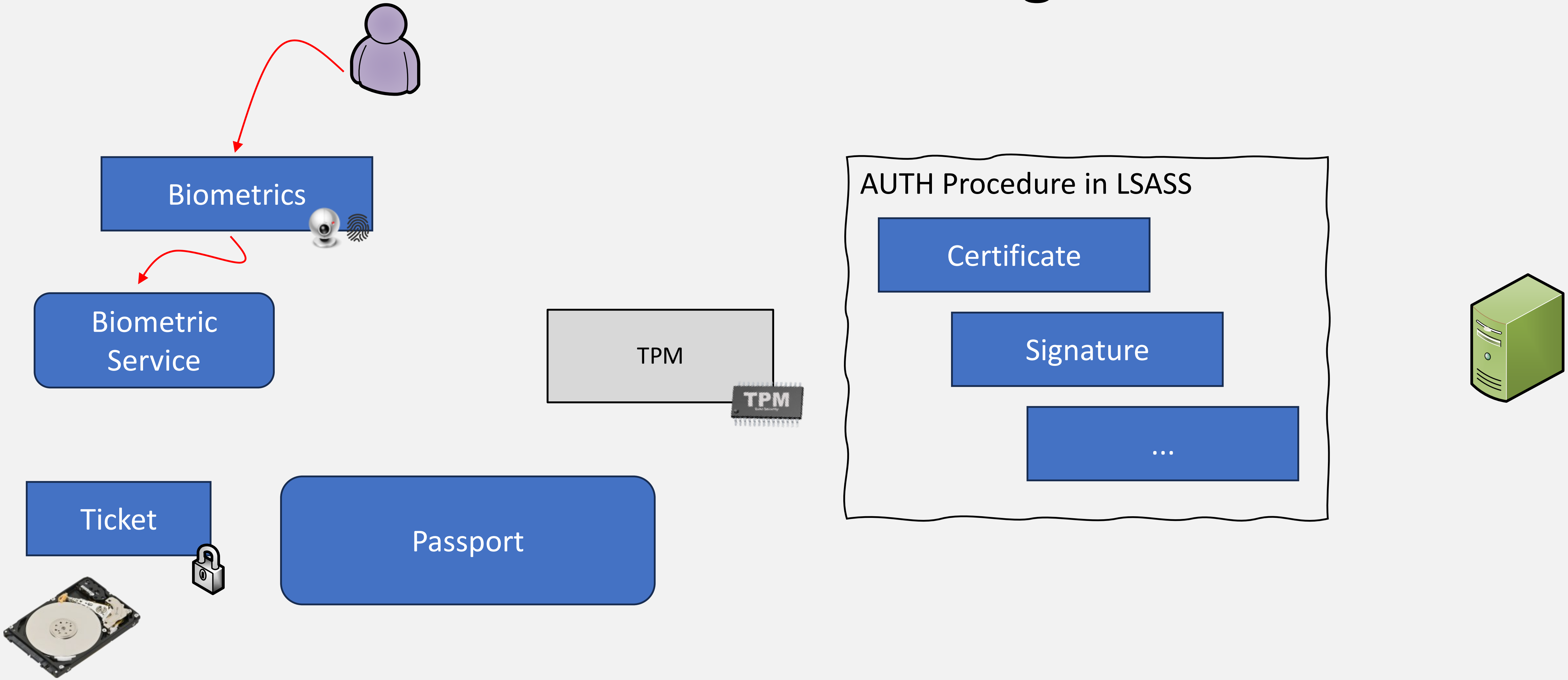
AUTH Procedure in LSASS

Certificate

Signature

...

Windows Biometric Auth management



Biometrics

Biometric Service

TPM

Ticket

Passport

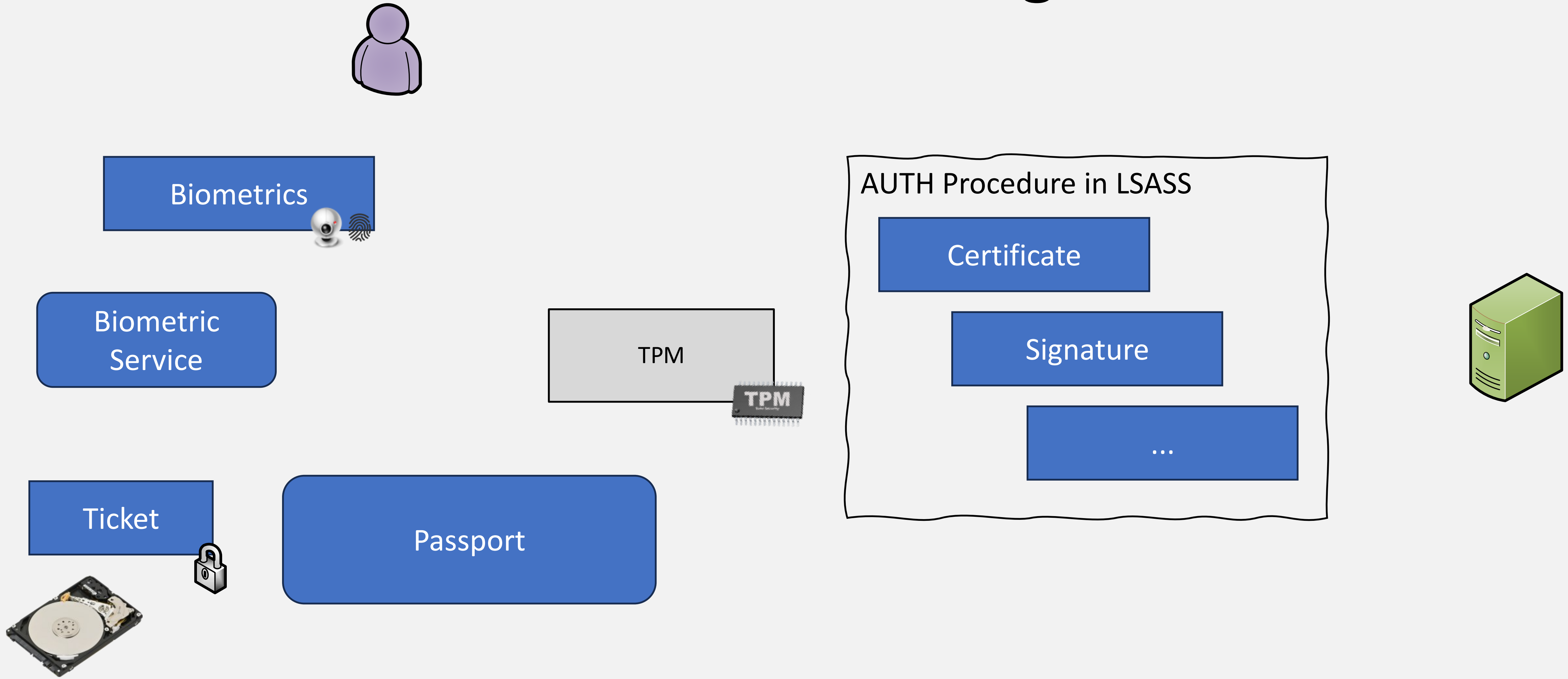
AUTH Procedure in LSASS

Certificate

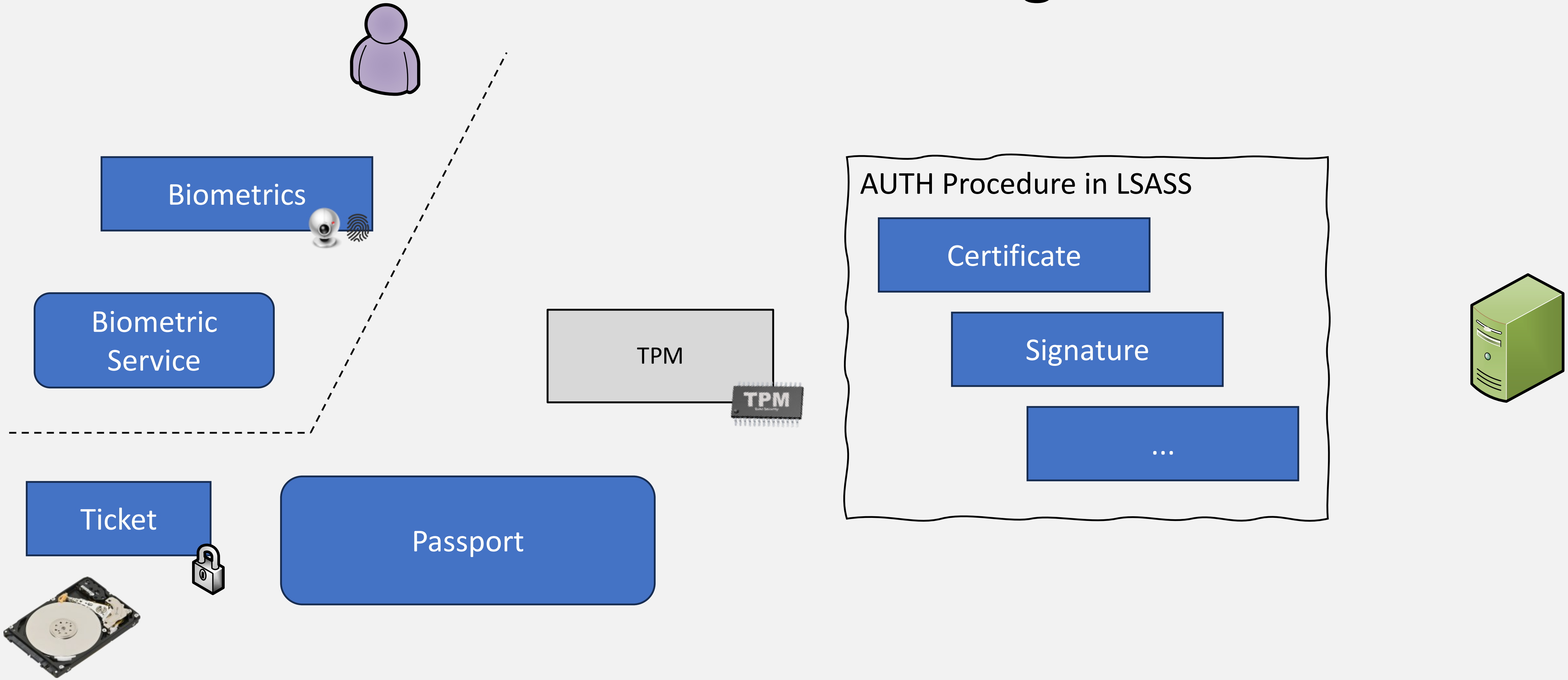
Signature

...

Windows Biometric Auth management



Windows Biometric Auth management



Biometrics

Biometric Service

Ticket

Passport

TPM

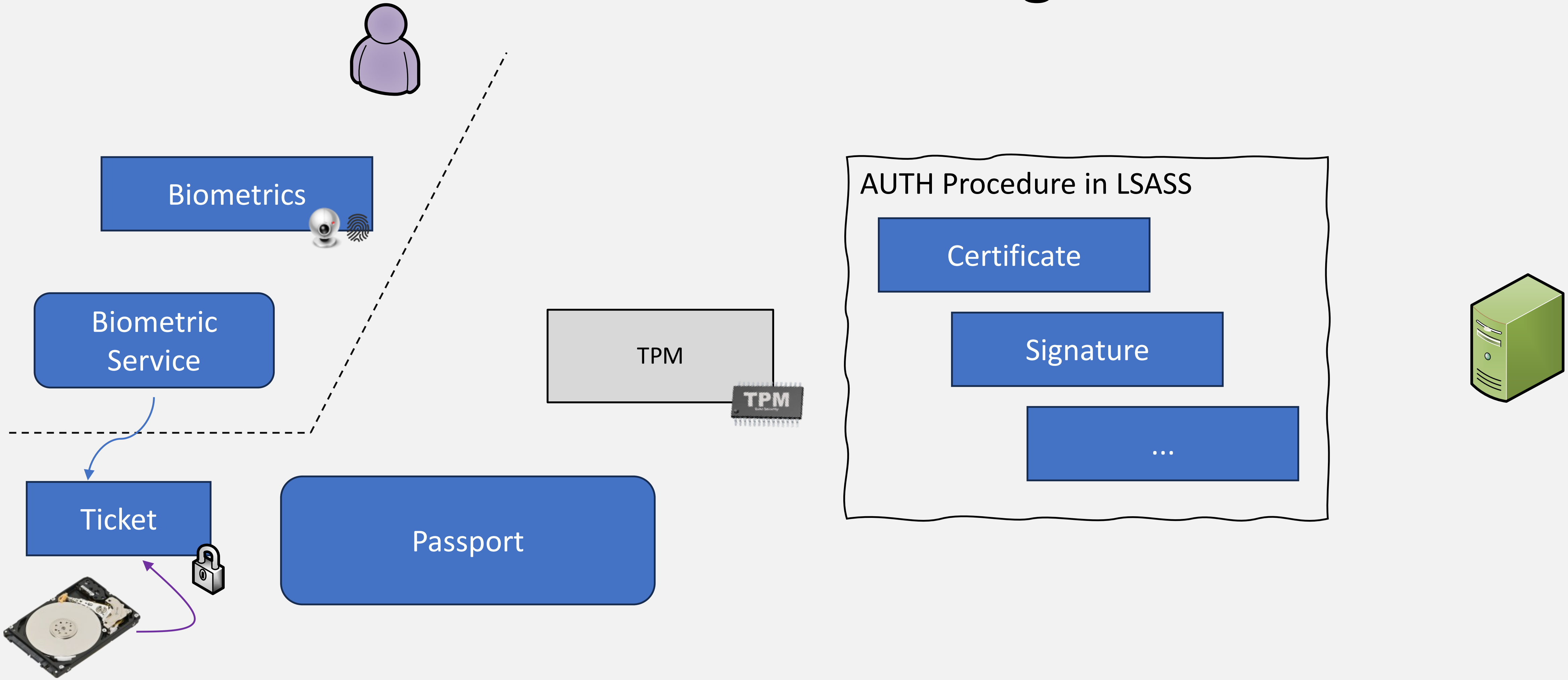
AUTH Procedure in LSASS

Certificate

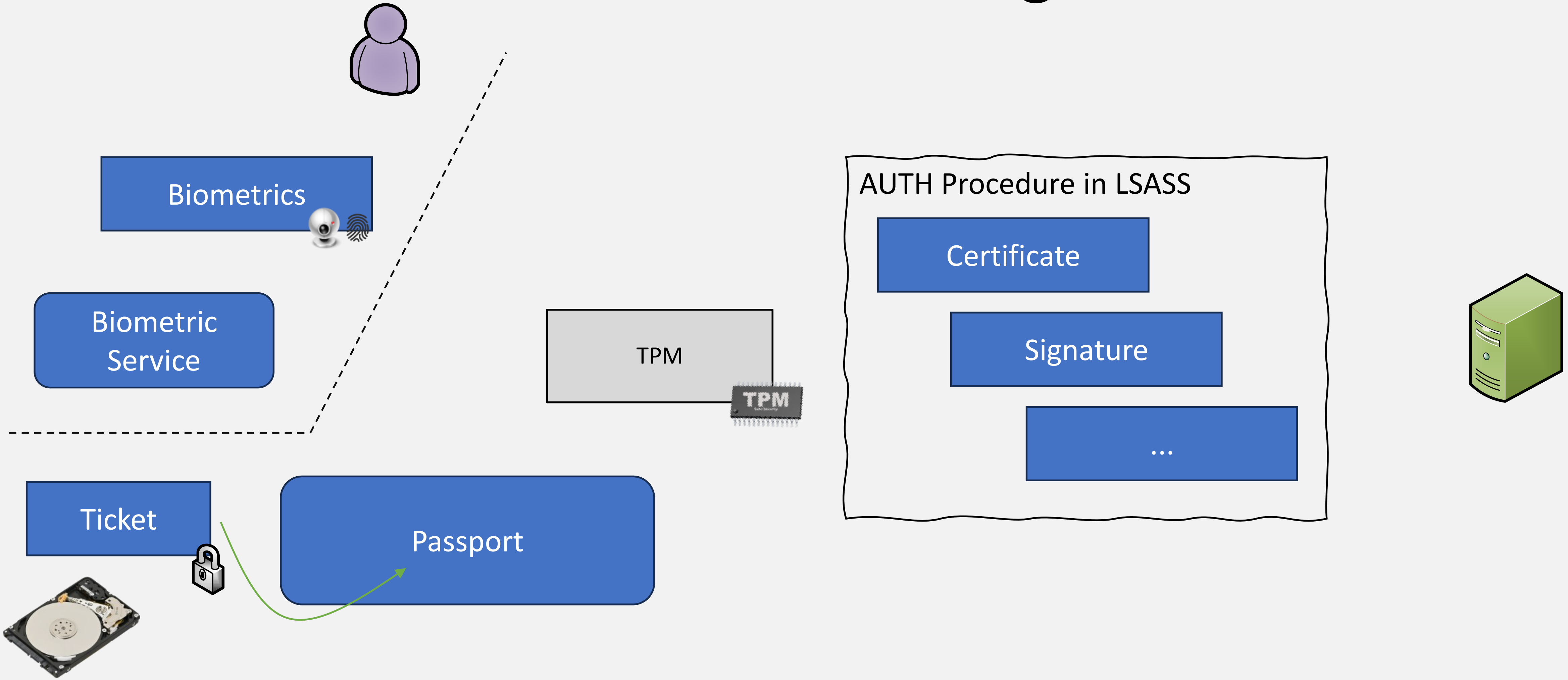
Signature

...

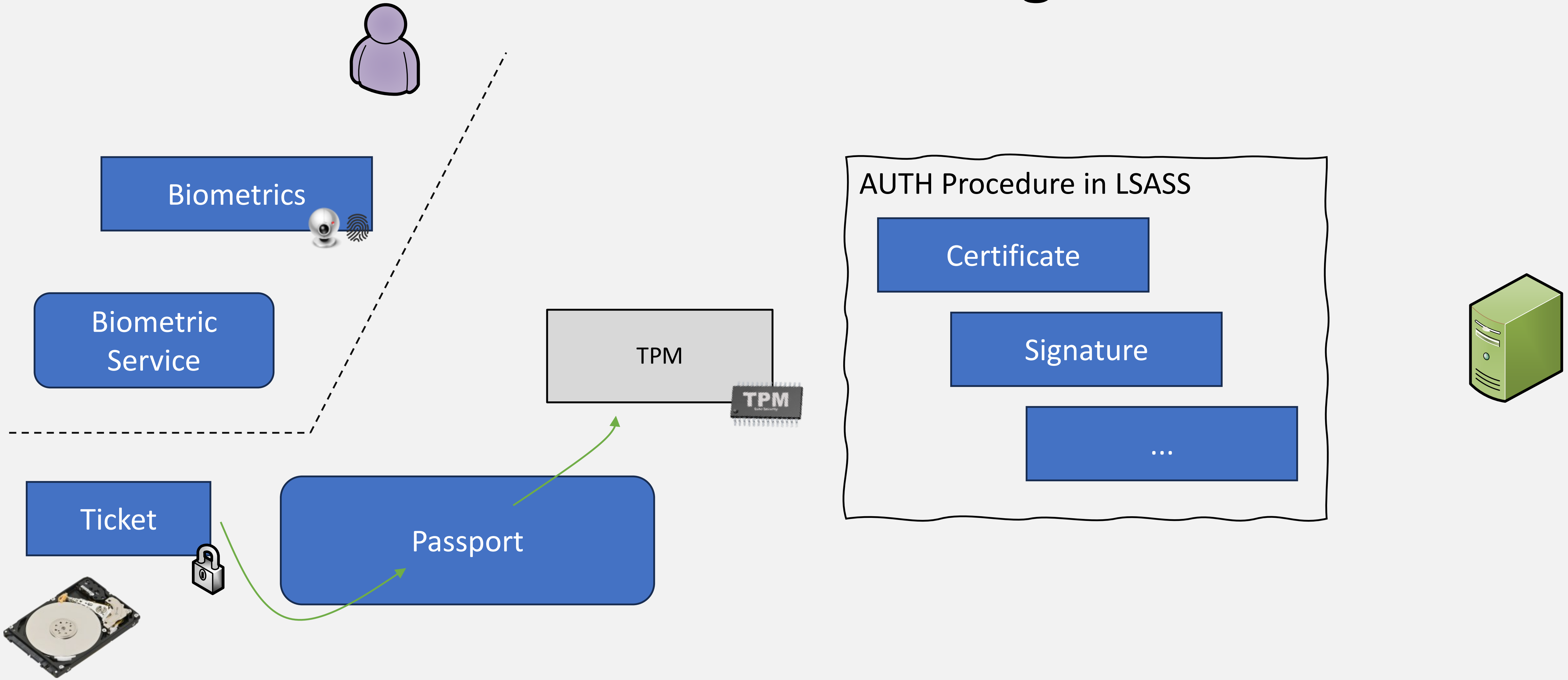
Windows Biometric Auth management



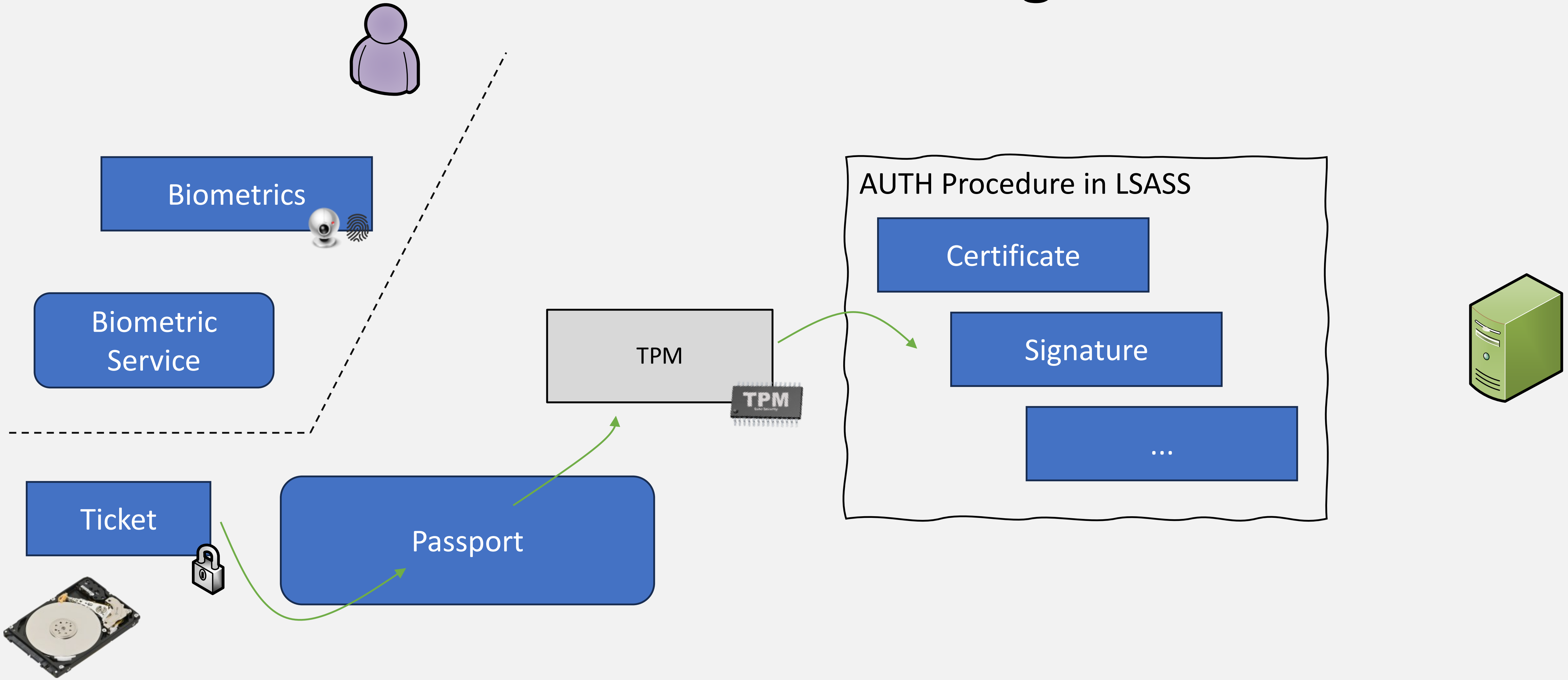
Windows Biometric Auth management



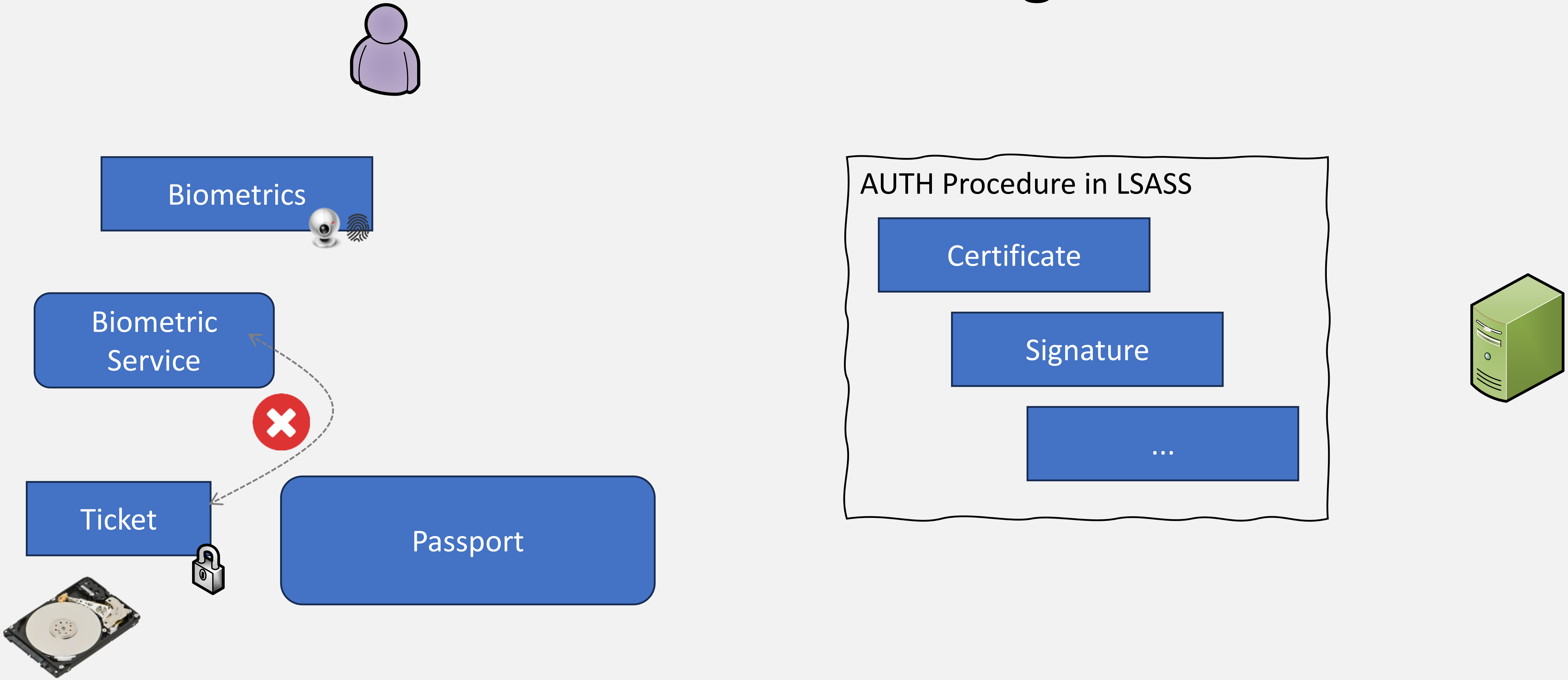
Windows Biometric Auth management



Windows Biometric Auth management



Windows Biometric Auth management



Biometrics

Biometric Service

Ticket

Passport

AUTH Procedure in LSASS

Certificate

Signature

...

Database Format

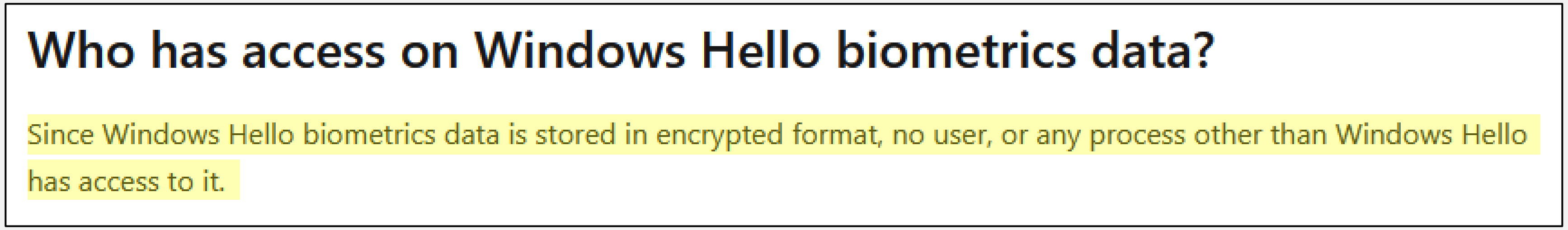
Let’s have a look inside

Database

- Let’s start with Microsoft’s FAQ.
- And some documentation … 😉

Database

- Let’s start with Microsoft’s FAQ.
- And some documentation … 😉

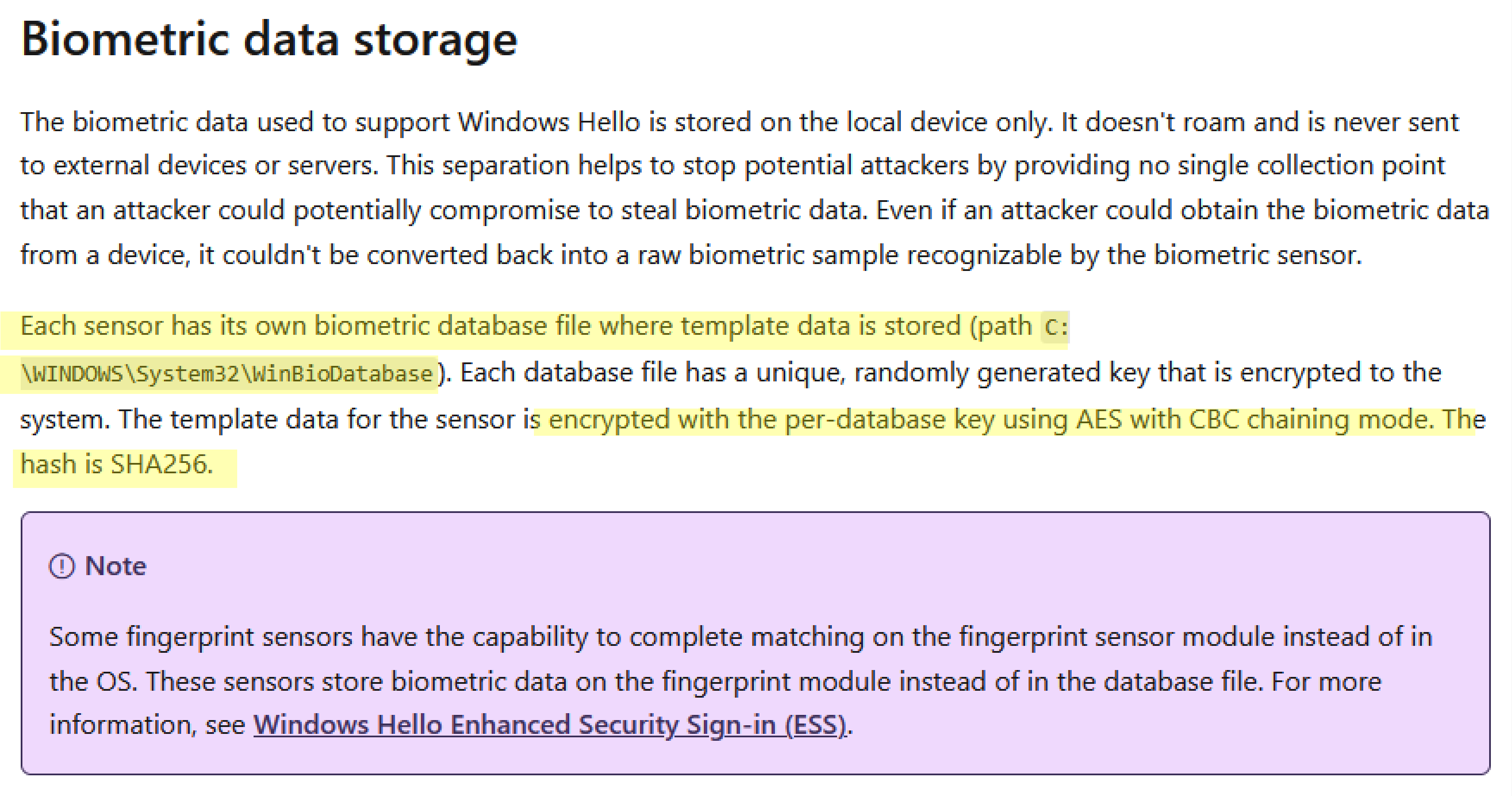


Who has access on Windows Hello biometrics data?

Since Windows Hello biometrics data is stored in encrypted format, no user, or any process other than Windows Hello has access to it.

Database

- Let’s start with
- And some doc



Biometric data storage

The biometric data used to support Windows Hello is stored on the local device only. It doesn't roam and is never sent to external devices or servers. This separation helps to stop potential attackers by providing no single collection point that an attacker could potentially compromise to steal biometric data. Even if an attacker could obtain the biometric data from a device, it couldn't be converted back into a raw biometric sample recognizable by the biometric sensor.

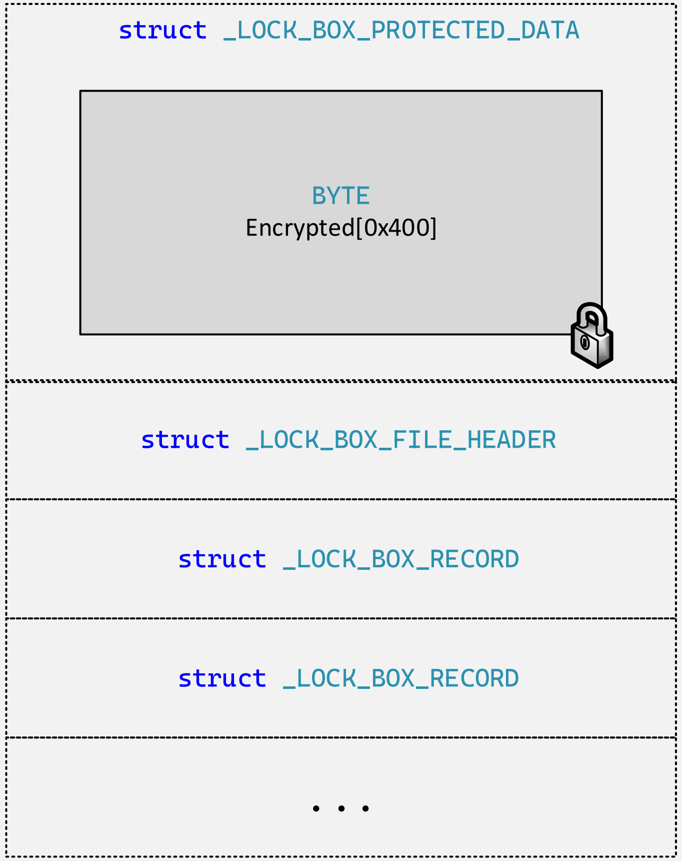
Each sensor has its own biometric database file where template data is stored (path `C:\WINDOWS\System32\WinBioDatabase`). Each database file has a unique, randomly generated key that is encrypted to the system. The template data for the sensor is encrypted with the per-database key using AES with CBC chaining mode. The hash is SHA256.

> ⓘ **Note**
>
> Some fingerprint sensors have the capability to complete matching on the fingerprint sensor module instead of in the OS. These sensors store biometric data on the fingerprint module instead of in the database file. For more information, see Windows Hello Enhanced Security Sign-in (ESS).

What do we know?

- Biometric data is the holy grail of mobile device security.
  - Therefore, we need strong encryption!
- We need something that identifies a user.
  - In Windows this is typically a security identifier (SID).
  - User authentication is the holy grail of domain security.
- The biometric unit uses the templates saved in the database.
  - We need to decrypt the template before we can compare it.
- Where is the key coming from?
  - We do not provide a password or entropy of any kind!

Database Format – Overview



struct _LOCK_BOX_PROTECTED_DATA

BYTE Encrypted[0x400]

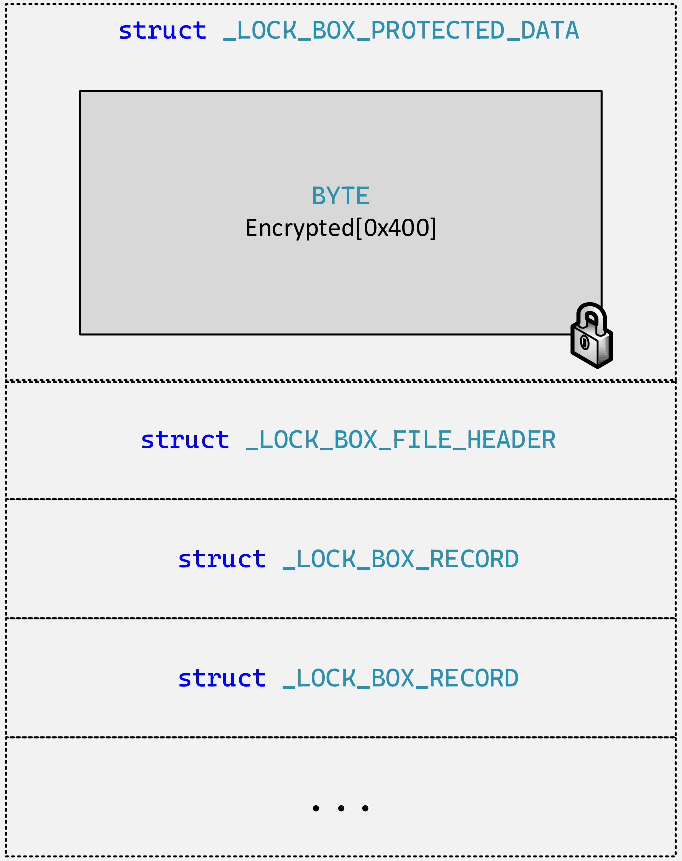
struct _LOCK_BOX_FILE_HEADER

struct _LOCK_BOX_RECORD

struct _LOCK_BOX_RECORD

. . .

Database Format – Overview



struct _LOCK_BOX_PROTECTED_DATA

BYTE
Encrypted[0x400]

struct _LOCK_BOX_FILE_HEADER

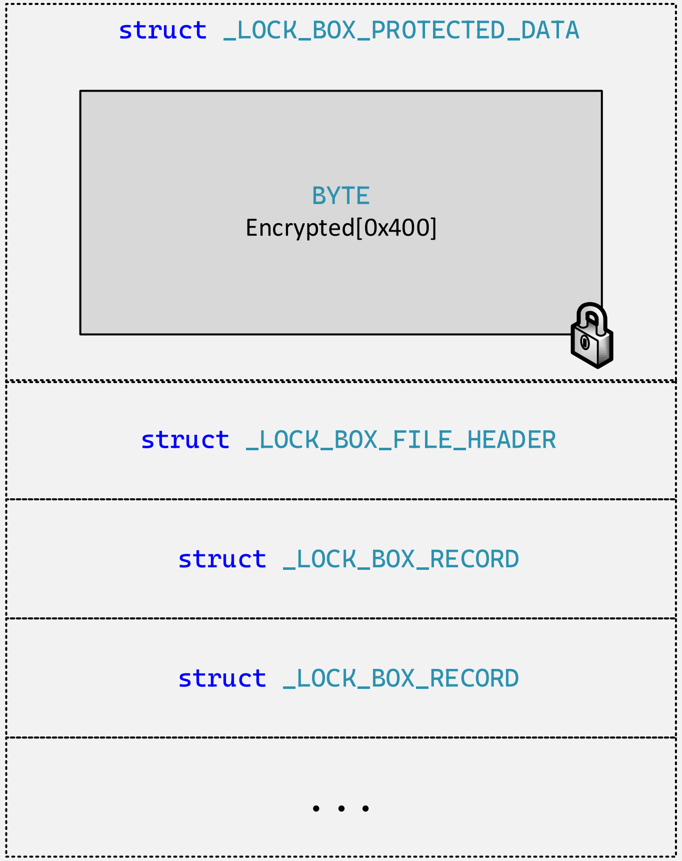
struct _LOCK_BOX_RECORD

struct _LOCK_BOX_RECORD

. . .

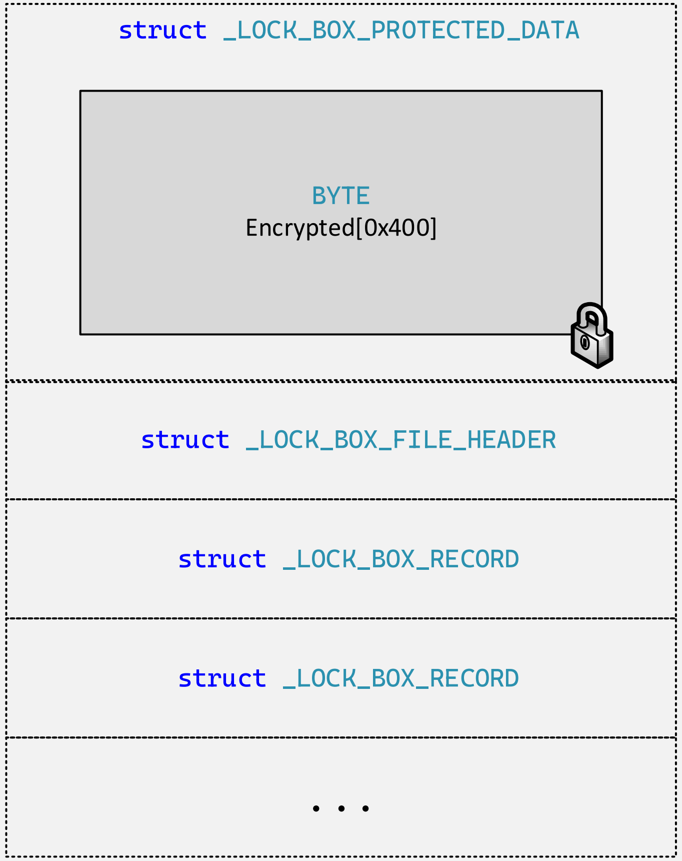
- The encrypted header
  - Ensures the integrity of the database using a SHA256 hash
  - Contains the AES key for the encrypted templates

Database Format – Overview



- The encrypted header
  - Ensures the integrity of the database using a SHA256 hash
  - Contains the AES key for the encrypted templates
- The unencrypted header holds information regarding
  - Version information
  - Number of used records and available records

Database Format – Overview



struct _LOCK_BOX_PROTECTED_DATA

BYTE
Encrypted[0x400]

struct _LOCK_BOX_FILE_HEADER

struct _LOCK_BOX_RECORD

struct _LOCK_BOX_RECORD

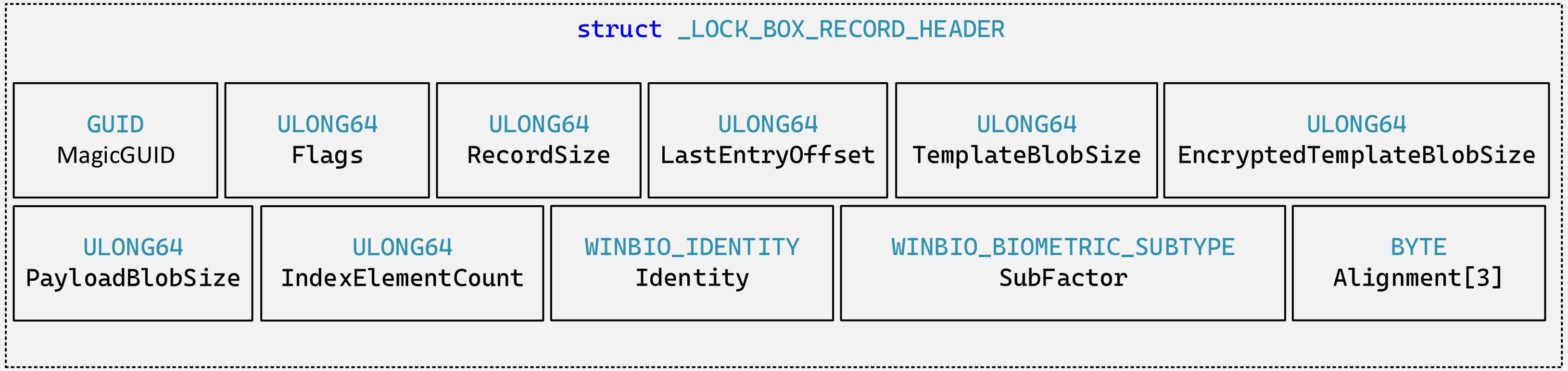
. . .

- The encrypted header
  - Ensures the integrity of the database using a SHA256 hash
  - Contains the AES key for the encrypted templates
- The unencrypted header holds information regarding
  - Version information
  - Number of used records and available records
- One record per enrolled user
  - SID
  - Encrypted template

Database Format

```
struct _LOCK_BOX_RECORD_HEADER
```

Database Format



struct _LOCK_BOX_RECORD_HEADER

GUID MagicGUID

ULONG64 Flags

ULONG64 RecordSize

ULONG64 LastEntryOffset

ULONG64 TemplateBlobSize

ULONG64 EncryptedTemplateBlobSize

ULONG64 PayloadBlobSize

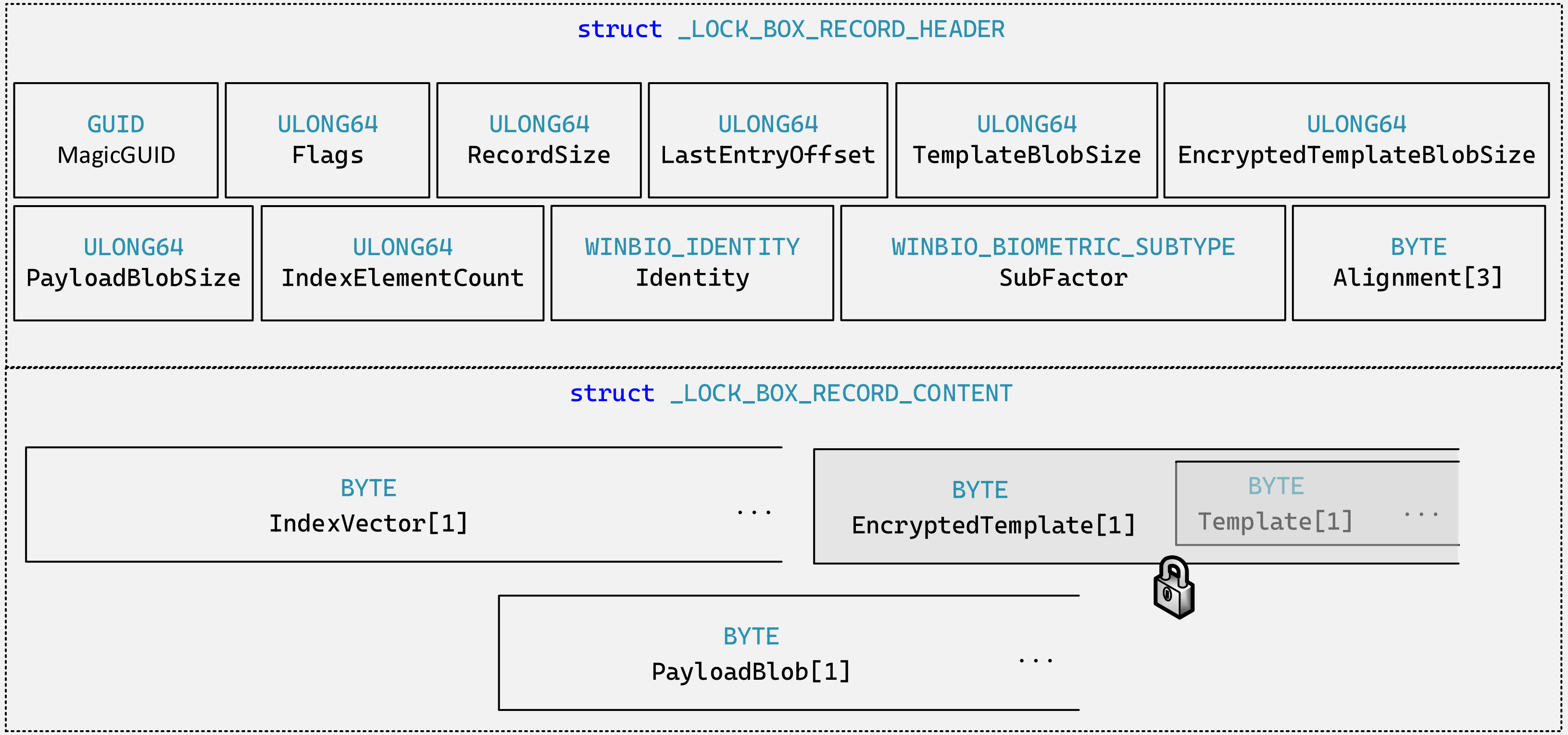
ULONG64 IndexElementCount

WINBIO_IDENTITY Identity

WINBIO_BIOMETRIC_SUBTYPE SubFactor

BYTE Alignment[3]

Database Format



struct _LOCK_BOX_RECORD_HEADER

GUID MagicGUID

ULONG64 Flags

ULONG64 RecordSize

ULONG64 LastEntryOffset

ULONG64 TemplateBlobSize

ULONG64 EncryptedTemplateBlobSize

ULONG64 PayloadBlobSize

ULONG64 IndexElementCount

WINBIO_IDENTITY Identity

WINBIO_BIOMETRIC_SUBTYPE SubFactor

BYTE Alignment[3]

struct _LOCK_BOX_RECORD_CONTENT

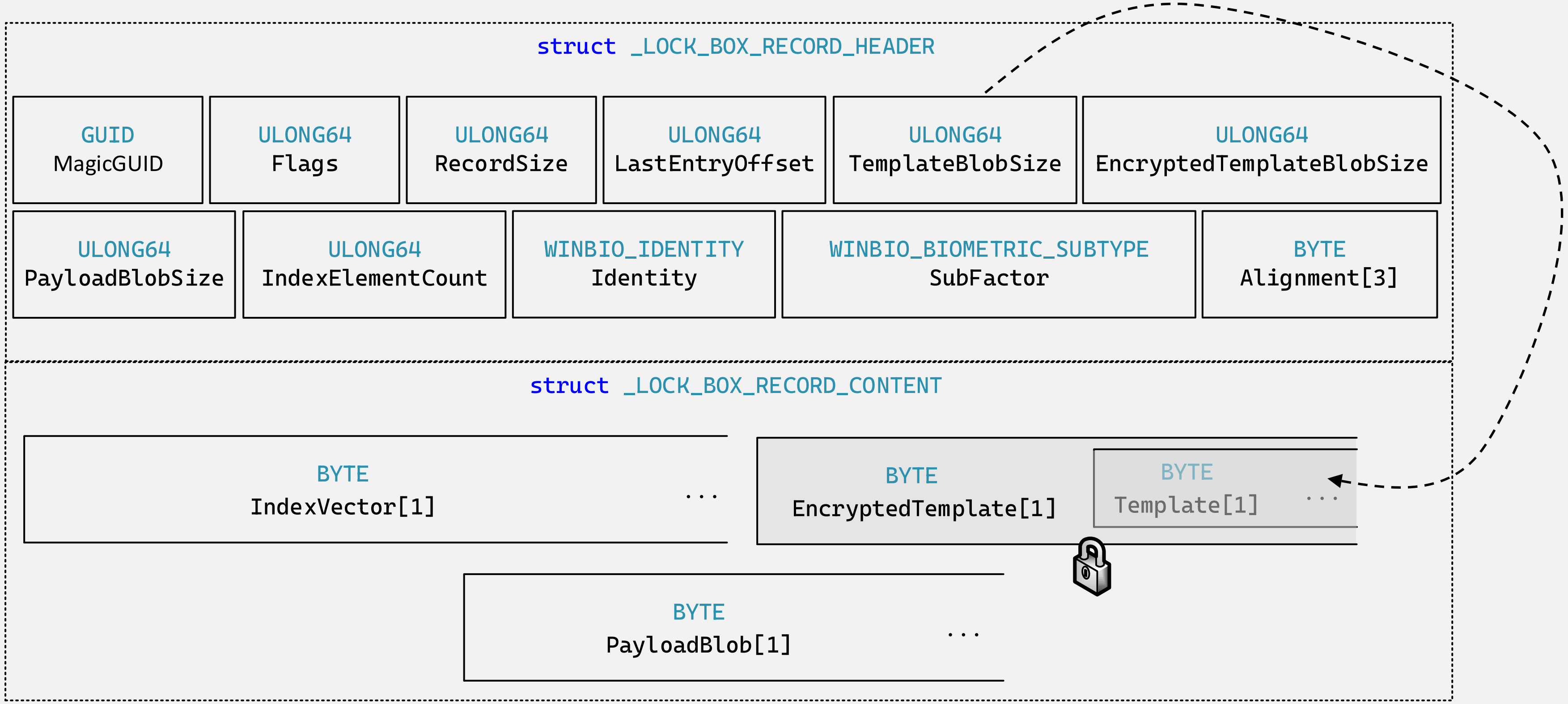
BYTE IndexVector[1] ...

BYTE EncryptedTemplate[1]

BYTE Template[1] ...

BYTE PayloadBlob[1] ...

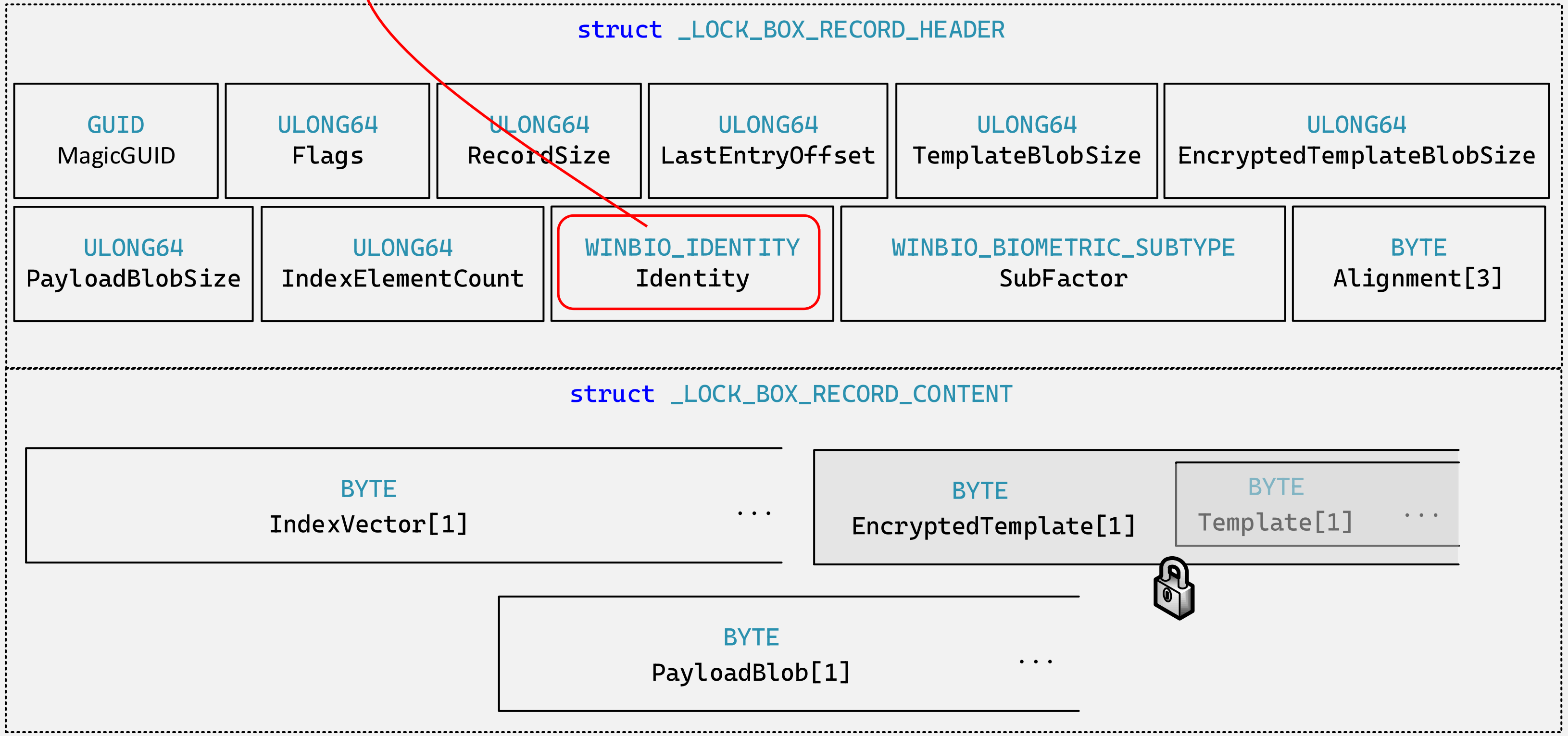
Database Format



Database Format

For instance:
“S-1-5-21-1004336348-1177238915-682003330-512”

```
typedef struct _WINBIO_IDENTITY {
  WINBIO_IDENTITY_TYPE Type;
  union {
    ULONG  Null;
    ULONG  Wildcard;
    GUID   TemplateGuid;
    struct {
      ULONG Size;
      UCHAR Data[SECURITY_MAX_SID_SIZE];
    } AccountSid;
  } Value;
} WINBIO_IDENTITY;
```



struct _LOCK_BOX_RECORD_HEADER

GUID MagicGUID	ULONG64 Flags	ULONG64 RecordSize	ULONG64 LastEntryOffset	ULONG64 TemplateBlobSize	ULONG64 EncryptedTemplateBlobSize
ULONG64 PayloadBlobSize	ULONG64 IndexElementCount	WINBIO_IDENTITY Identity	WINBIO_BIOMETRIC_SUBTYPE SubFactor	BYTE Alignment[3]	

struct _LOCK_BOX_RECORD_CONTENT

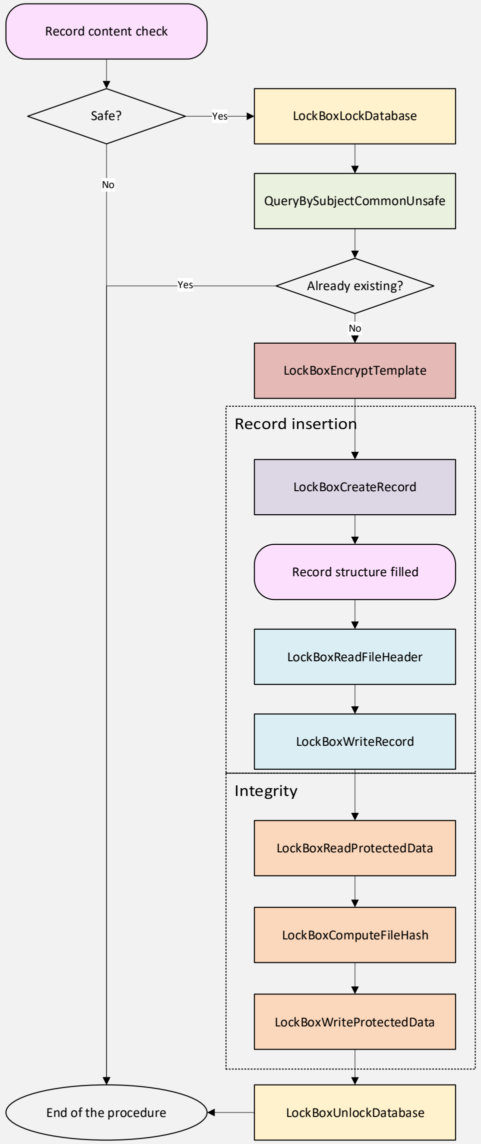
BYTE IndexVector[1] . . .

BYTE EncryptedTemplate[1] BYTE Template[1] . . .

BYTE PayloadBlob[1] . . .

Database Security

- There is an encrypted header that ensures
  - The integrity of the database and confidentiality the of biometric data
- How the header's integrity and confidentiality achieved?
  - We need functionality that does not require an additional key!
  - The header is protected with CryptProtectData/CryptUnprotectData functions.
    - Cipher keys are managed locally by NT-AUTHORITY\SYSTEM.
    - Local administrator can get access 😋.



Record content check

Safe?

Yes

No

LockBoxLockDatabase

QueryBySubjectCommonUnsafe

Already existing?

Yes

No

LockBoxEncryptTemplate

Record insertion

LockBoxCreateRecord

Record structure filled

LockBoxReadFileHeader

LockBoxWriteRecord

Integrity

LockBoxReadProtectedData

LockBoxComputeFileHash

LockBoxWriteProtectedData

LockBoxUnlockDatabase

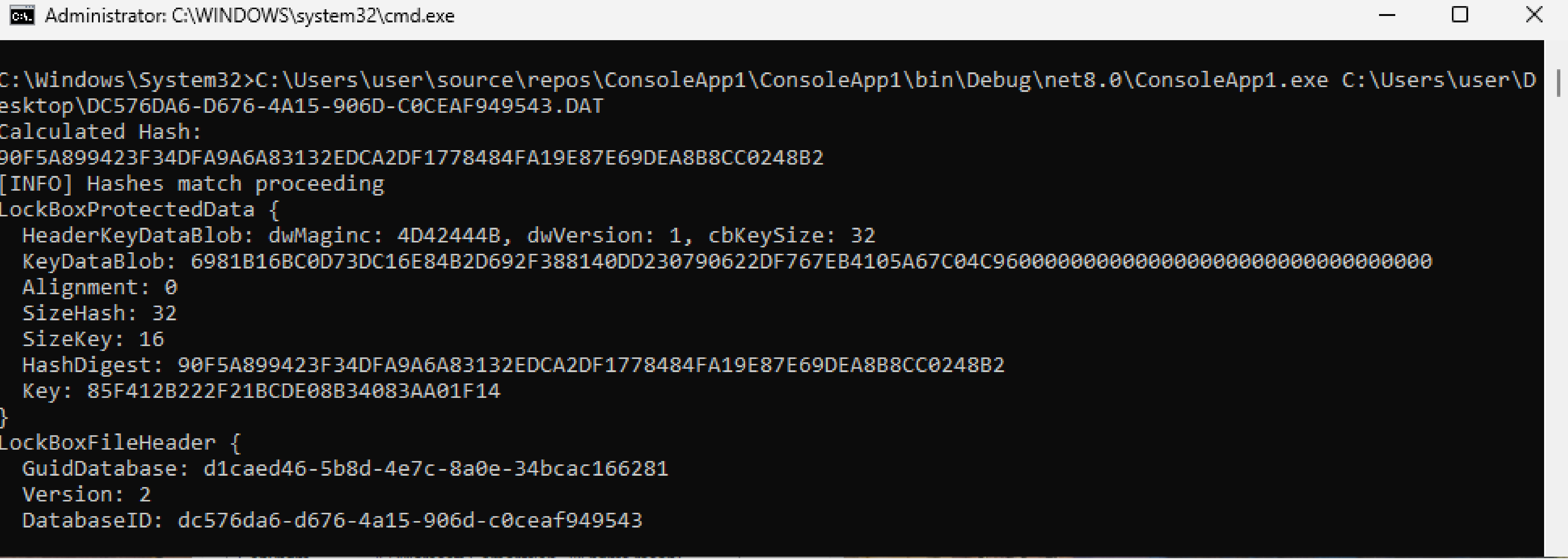
End of the procedure

Database (In)security

- Local administrators break the security of the database:
  - Decrypt and read the encrypted templates of enrolled users.
  - Change the database and circumvent the integrity controls of the database.

- This means:
  - Exchange SIDs of enrolled users.
  - Decrypt templates.
  - Bring their own biometrics to the system.
    - Authenticate as every enrolled user.

Demo – Decrypting the encrypted header



```
C:\Windows\System32>C:\Users\user\source\repos\ConsoleApp1\ConsoleApp1\bin\Debug\net8.0\ConsoleApp1.exe C:\Users\user\D
esktop\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Calculated Hash:
90F5A899423F34DFA9A6A83132EDCA2DF1778484FA19E87E69DEA8B8CC0248B2
[INFO] Hashes match proceeding
LockBoxProtectedData {
  HeaderKeyDataBlob: dwMaginc: 4D42444B, dwVersion: 1, cbKeySize: 32
  KeyDataBlob: 6981B16BC0D73DC16E84B2D692F388140DD230790622DF767EB4105A67C04C9600000000000000000000000000000000
  Alignment: 0
  SizeHash: 32
  SizeKey: 16
  HashDigest: 90F5A899423F34DFA9A6A83132EDCA2DF1778484FA19E87E69DEA8B8CC0248B2
  Key: 85F412B222F21BCDE08B34083AA01F14
}
LockBoxFileHeader {
  GuidDatabase: d1caed46-5b8d-4e7c-8a0e-34bcac166281
  Version: 2
  DatabaseID: dc576da6-d676-4a15-906d-c0ceaf949543
```

Demo Time

Conclusion

Conclusion

- Windows Hello for Business is here to stay!
    - Added as security feature to new products like Recall.
- Local administrator to domain user is still a threat.
    - Worst case local admin to domain admin.
- Securing heterogenous clients is a challenge Microsoft faces.
    - ESS mode needs hardware support – new Thinkpads with AMD do not have it.
    - ESS mode needs VBS – sadly not used enough!
    - **If you can use it!**

Make the world a safer place

- In any case:
  - Only one user per client!

- Also:
  - Consider only allowing PIN authentication.
  - Monitoring: Only WBS should open or modify the database.

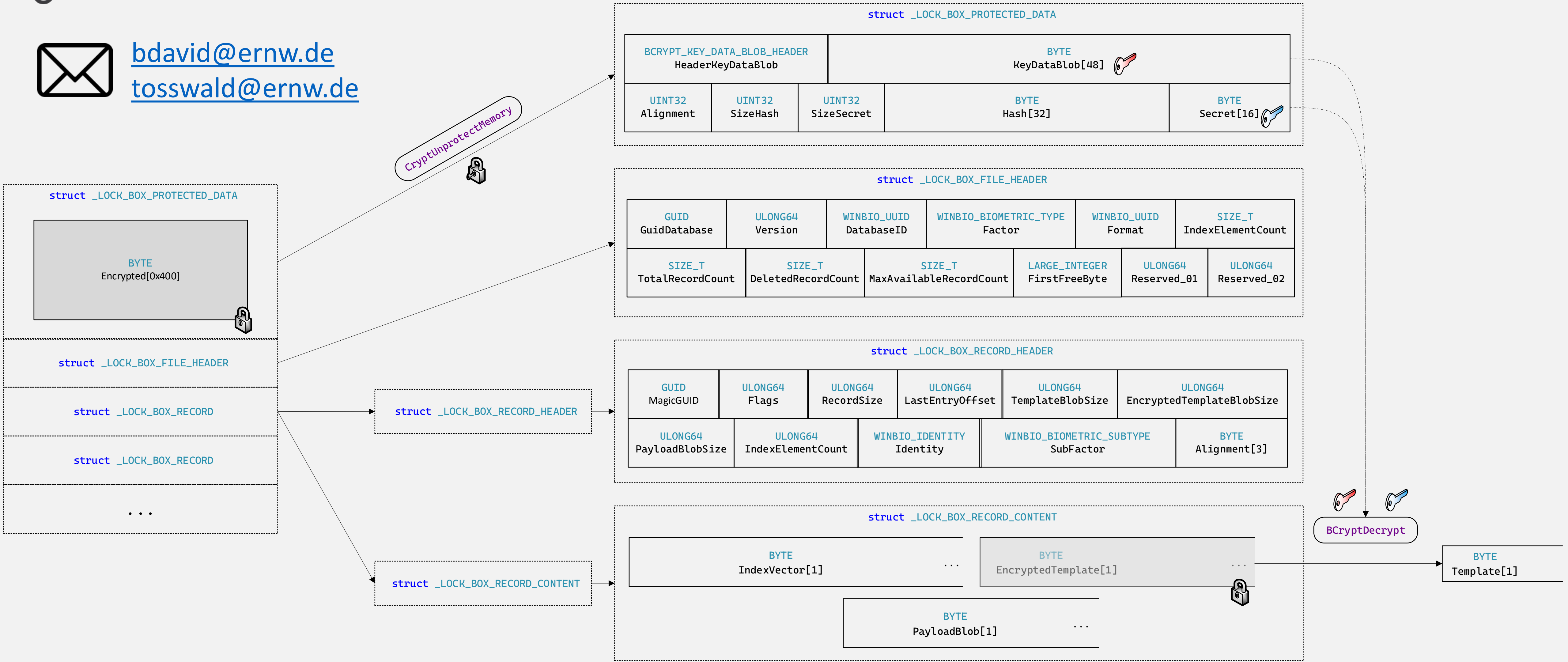
black hat BRIEFINGS

Questions?

www.ernw.de

www.insinuator.net

bdavid@ernw.de
tosswald@ernw.de



struct _LOCK_BOX_PROTECTED_DATA

BYTE
Encrypted[0x400]

struct _LOCK_BOX_FILE_HEADER

struct _LOCK_BOX_RECORD

struct _LOCK_BOX_RECORD

. . .

struct _LOCK_BOX_RECORD_HEADER

struct _LOCK_BOX_RECORD_CONTENT

struct _LOCK_BOX_PROTECTED_DATA

BCRYPT_KEY_DATA_BLOB_HEADER	BYTE
HeaderKeyDataBlob	KeyDataBlob[48]

UINT32	UINT32	UINT32	BYTE	BYTE
Alignment	SizeHash	SizeSecret	Hash[32]	Secret[16]

struct _LOCK_BOX_FILE_HEADER

GUID	ULONG64	WINBIO_UUID	WINBIO_BIOMETRIC_TYPE	WINBIO_UUID	SIZE_T
GuidDatabase	Version	DatabaseID	Factor	Format	IndexElementCount

SIZE_T	SIZE_T	SIZE_T	LARGE_INTEGER	ULONG64	ULONG64
TotalRecordCount	DeletedRecordCount	MaxAvailableRecordCount	FirstFreeByte	Reserved_01	Reserved_02

struct _LOCK_BOX_RECORD_HEADER

GUID	ULONG64	ULONG64	ULONG64	ULONG64	ULONG64
MagicGUID	Flags	RecordSize	LastEntryOffset	TemplateBlobSize	EncryptedTemplateBlobSize

ULONG64	ULONG64	WINBIO_IDENTITY	WINBIO_BIOMETRIC_SUBTYPE	BYTE
PayloadBlobSize	IndexElementCount	Identity	SubFactor	Alignment[3]

struct _LOCK_BOX_RECORD_CONTENT

BYTE	BYTE
IndexVector[1] ...	EncryptedTemplate[1] ...

BYTE
PayloadBlob[1] ...

BYTE
Template[1]

References

- Slide 6: https://thecyberconsultancy.com/hello-auth.html
- Slide 7: https://support.microsoft.com/de-de/windows/mit-recall-ihre-schritte-zur%C3%BCckverfolgen-aa03f8a0-a78b-4b3e-b0a1-2eb8ac48701c
- Slide 7: https://learn.microsoft.com/en-us/windows/security/identity-protection/passkeys/
- Slide 37: Looking after your teeth – Guernsey Dental Association
- Transition slides: https://www.socwall.com/