Windows Hello for Business

Let’s talk about WHfB ☺

Dr Baptiste David Tillmann Oßwald

bdavid@ernw.de tosswald@ernw.de

TROOPERS 25 – DEUTSCHLAND – 25/06/2025

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, C0c0n, DeepSec, …
  - And also, one called TROOPERS 😀
- I like good food and good wine 😌

Who am I?

- Oßwald Tillmann
- **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.

“Windows Dissected”

- *“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.

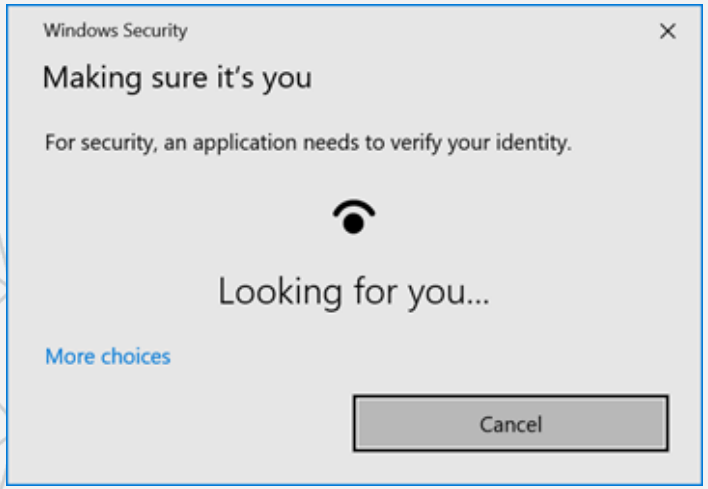
Windows Hello for Business

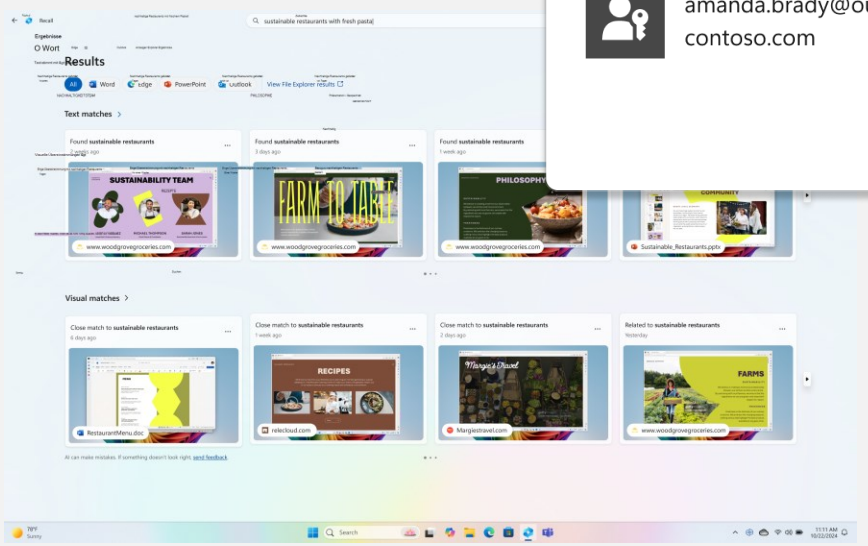
Overview

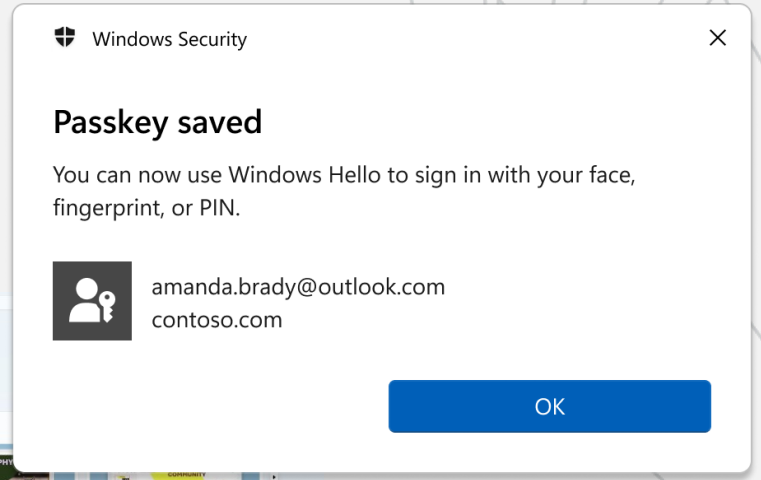
Say Hello to Windows Hello

What is Windows Hello for Business?

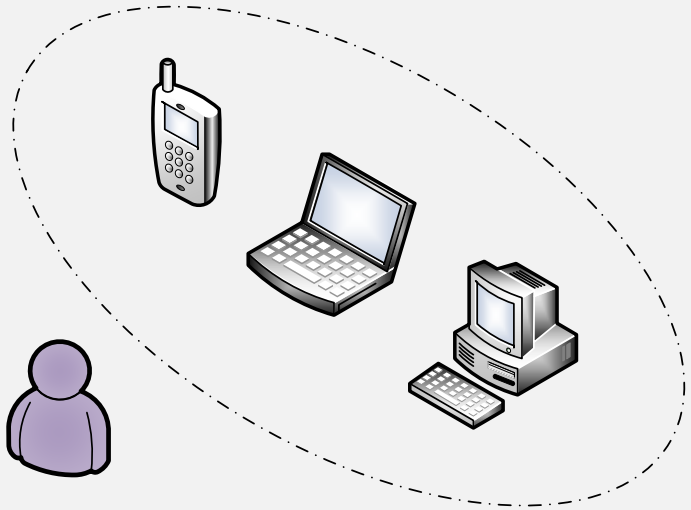
- Windows Hello for Business is Microsoft’s passwordless flagship
  - Windows Recall, Passkey, …
- Build on two key principals
  - Identification -> “Windows Hello …”
  - Authentication -> “… for Business”





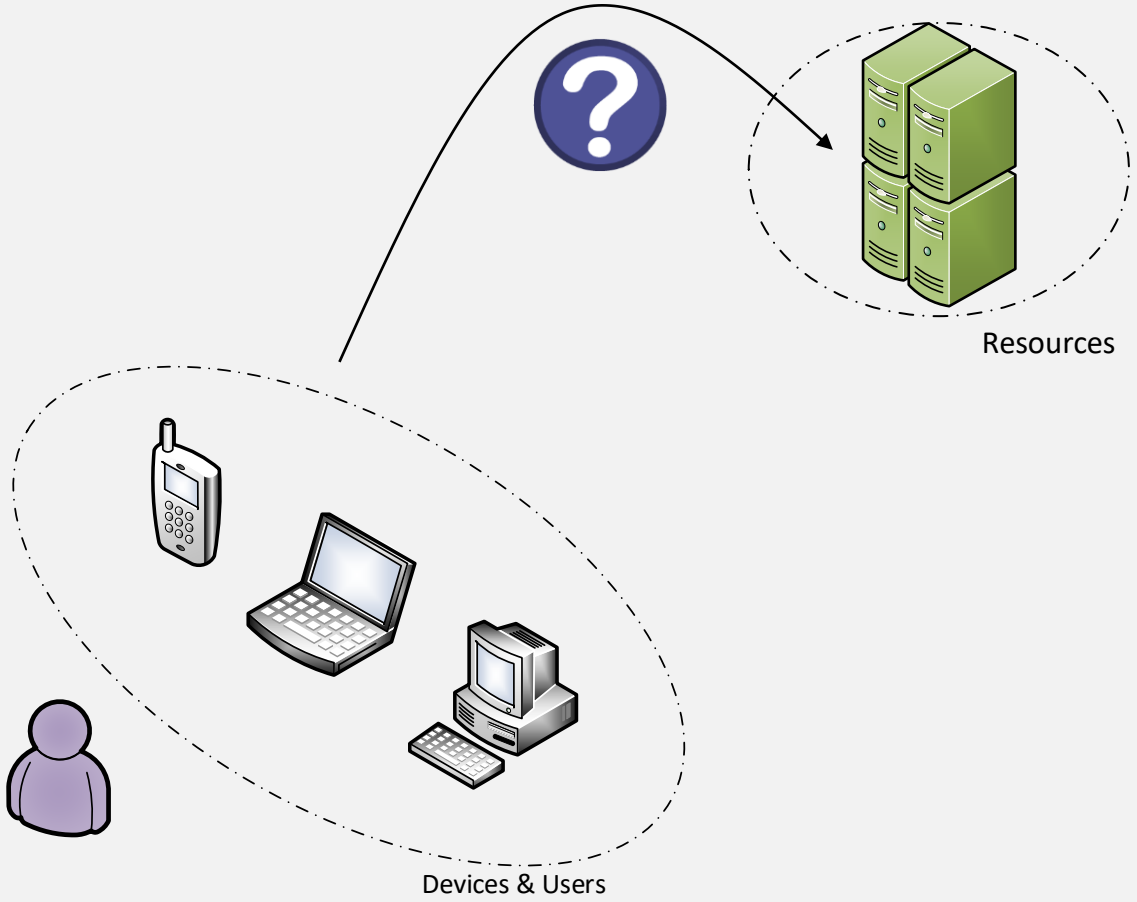


Windows Hello for Business

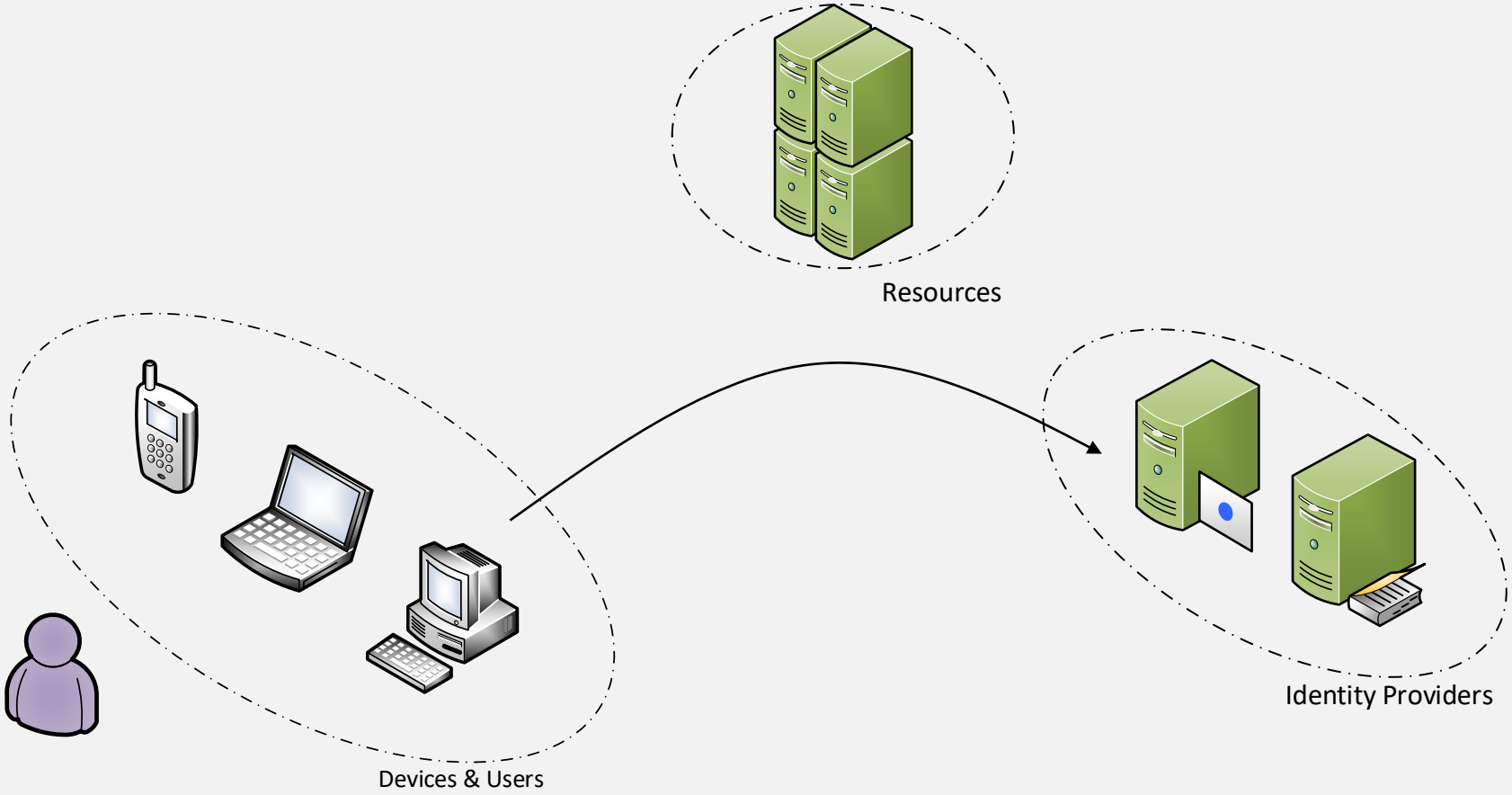


Devices & Users

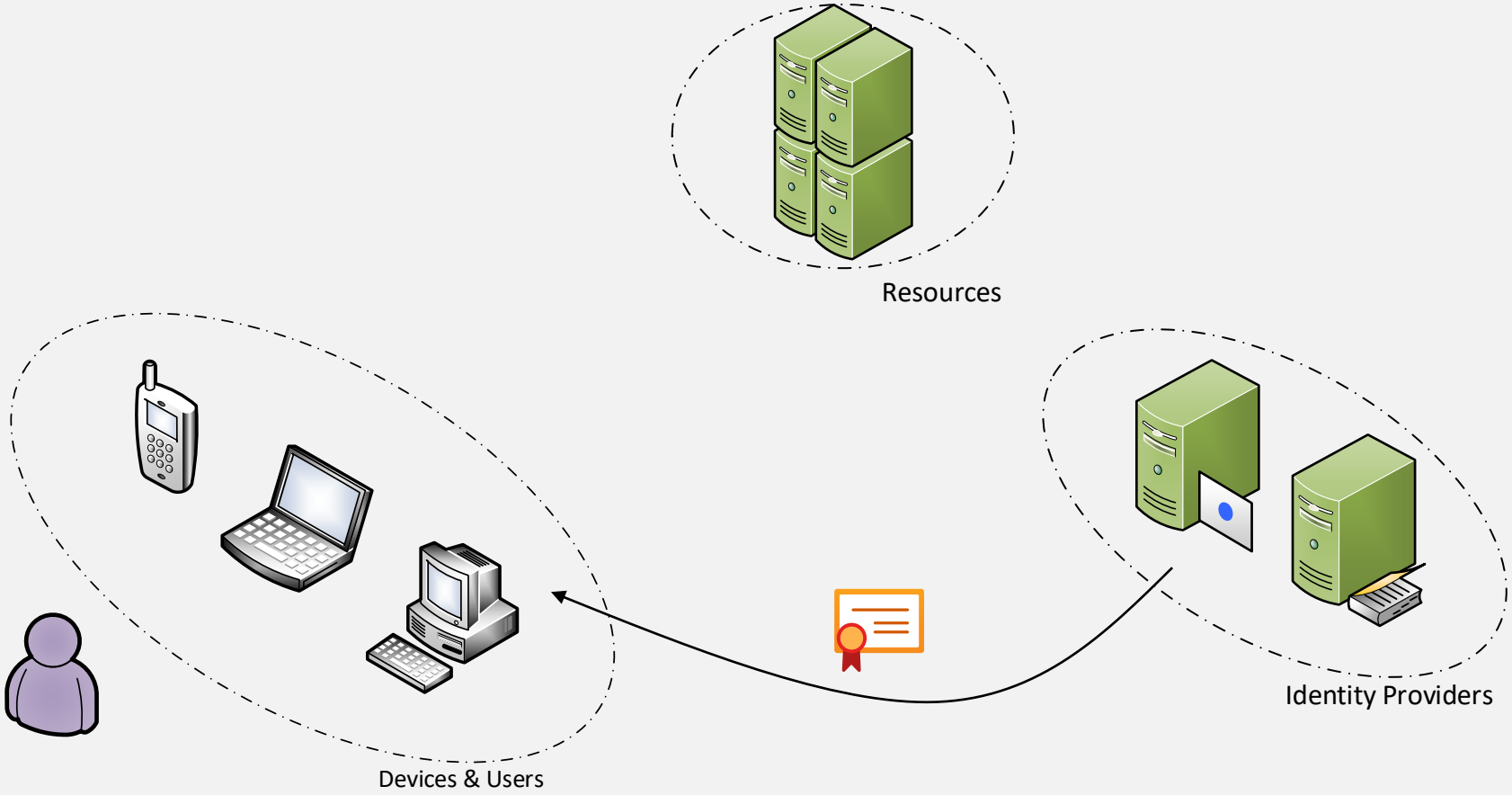
Windows Hello for Business



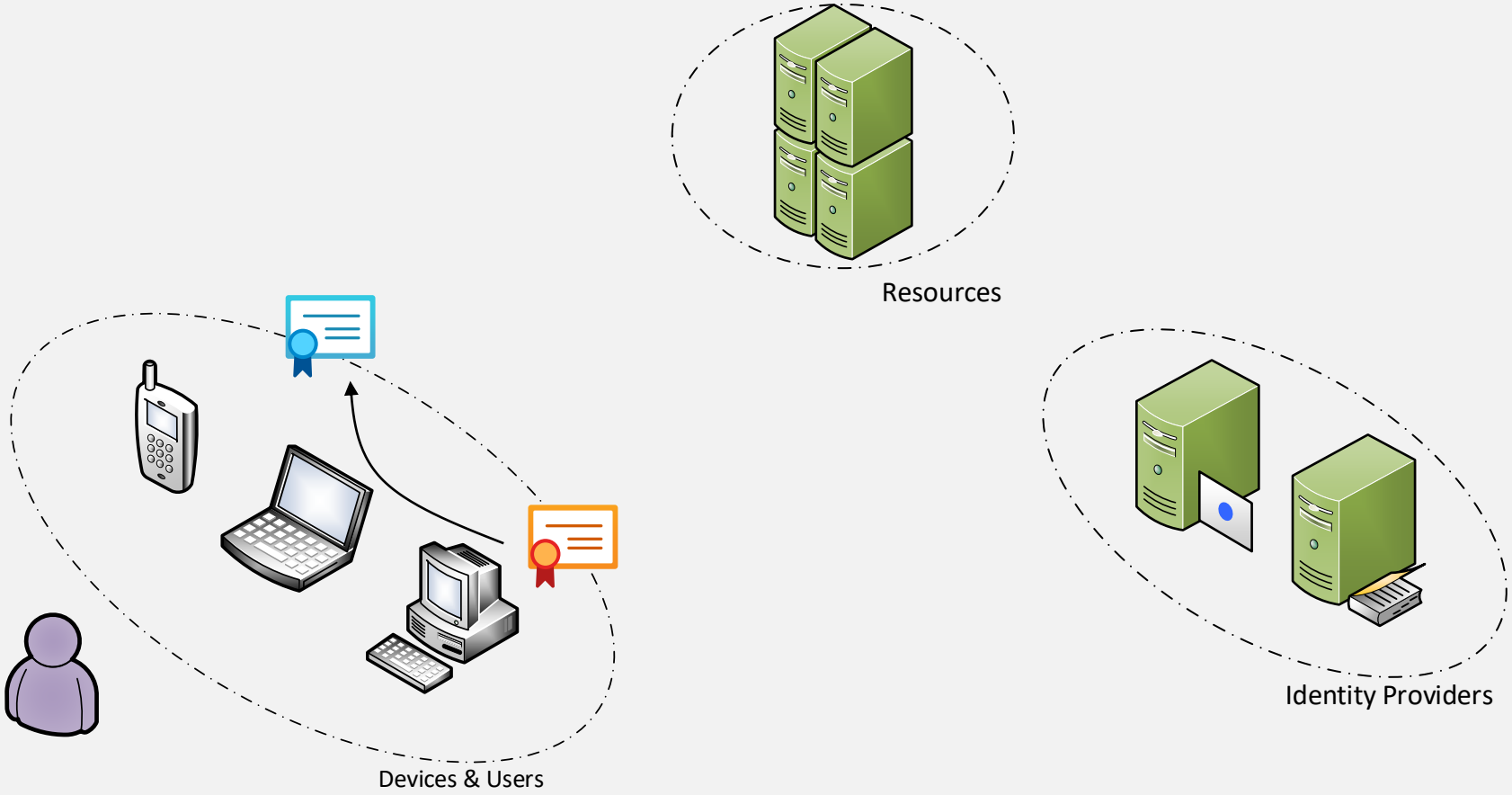
Windows Hello for Business



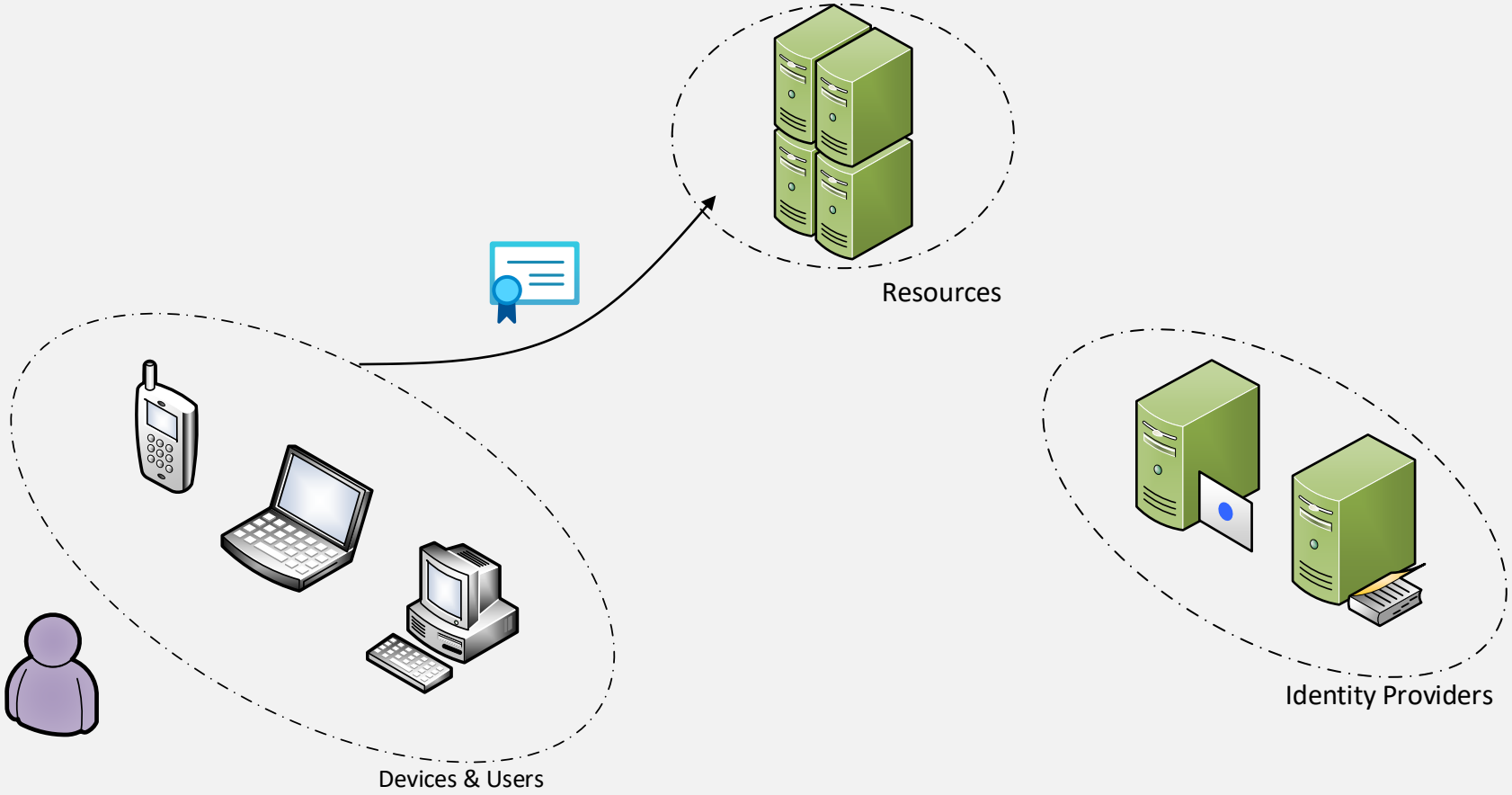
Windows Hello for Business



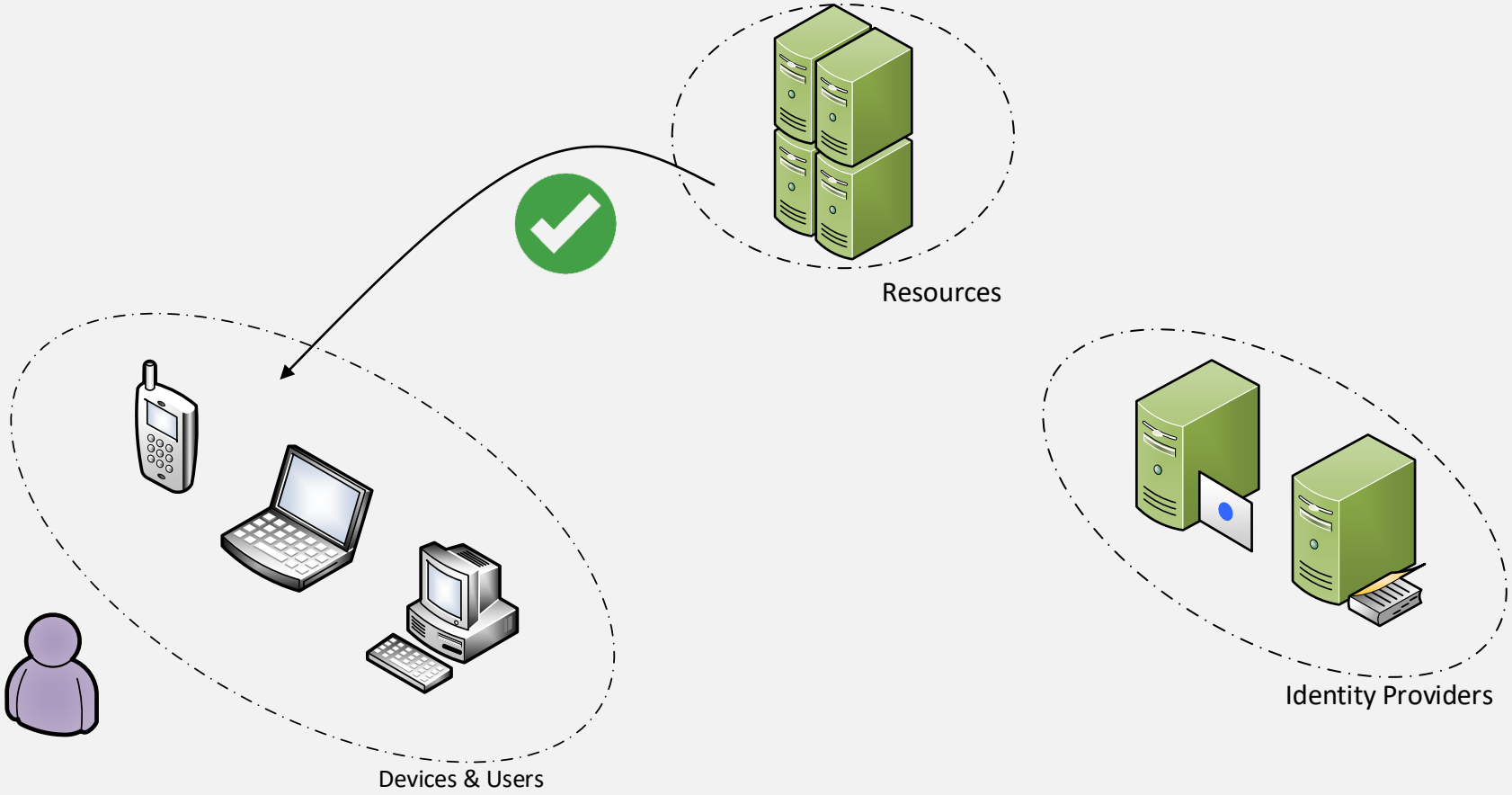
Windows Hello for Business



Windows Hello for Business



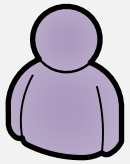
Windows Hello for Business



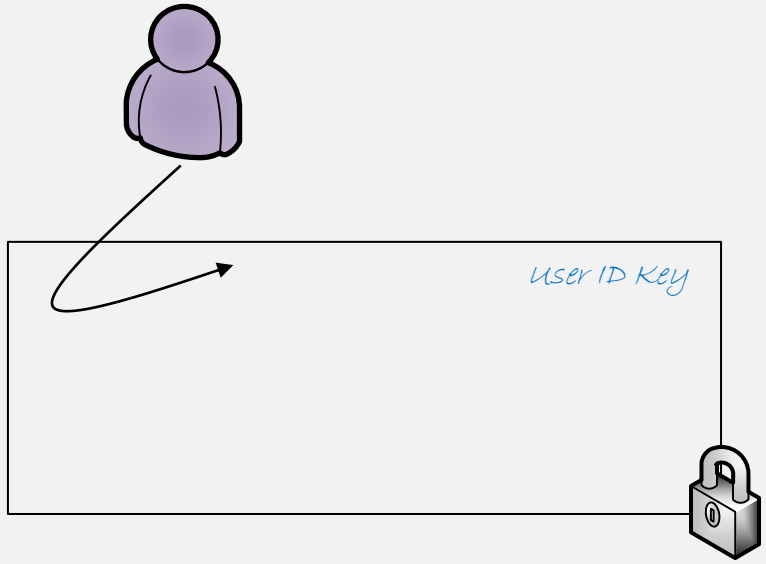
Windows Hello for Business

- Relationship between biometry and authentication at enrollment step.
  - The identification of the user in front of that device is performed through their biometrics and PIN.
  - In Microsoft documentation a gesture is a way for the user to interface with Windows Hello.
    - Usually biometrics: Fingerprint, Face, Iris, Voice ...
    - But also: PIN code.
  - During the enrollment procedure, a Windows Hello Container is created.
    - Logical grouping of cryptographic material.
      - For example: key, certificates, credentials, and possibly data.
      - The container holds the cryptographic material of users that are registered in the identity provider.
    - Protecting authentication material is the holy grail of domain security 😉.

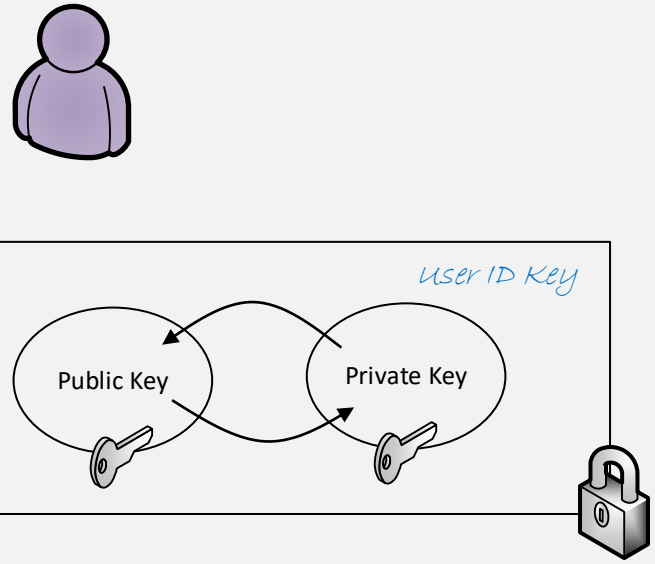
Windows Hello for Business – Enrollment



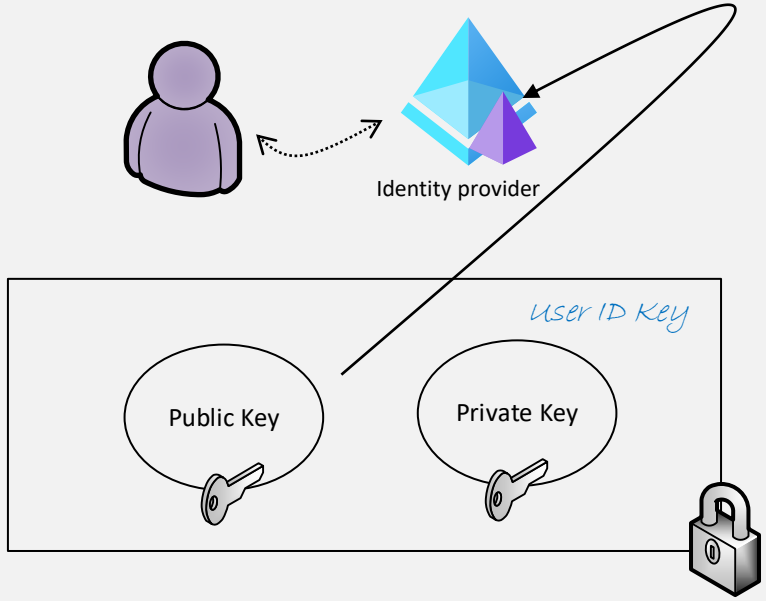
Windows Hello for Business – Enrollment



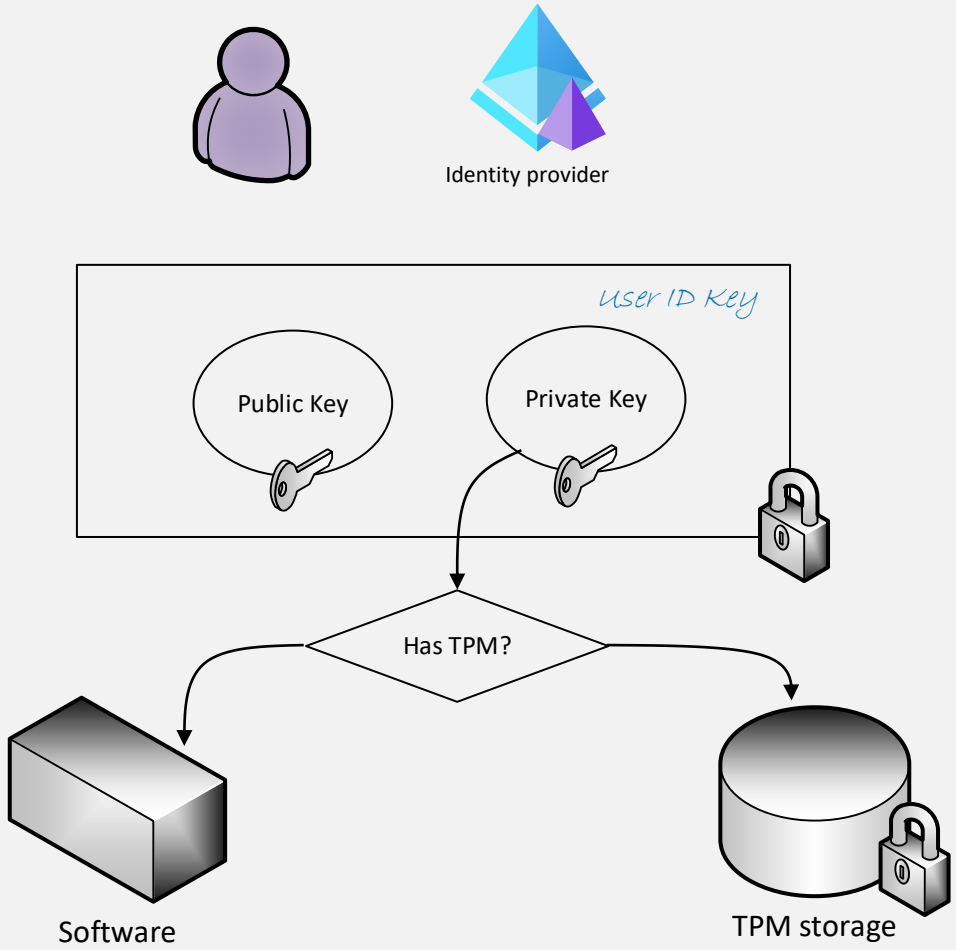
Windows Hello for Business – Enrollment



Windows Hello for Business – Enrollment



Windows Hello for Business – Enrollment

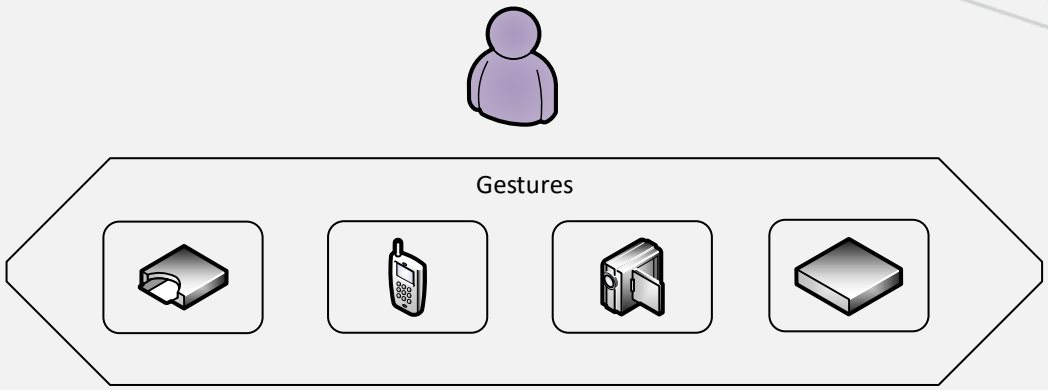


Windows Hello for Business

- User’s key access

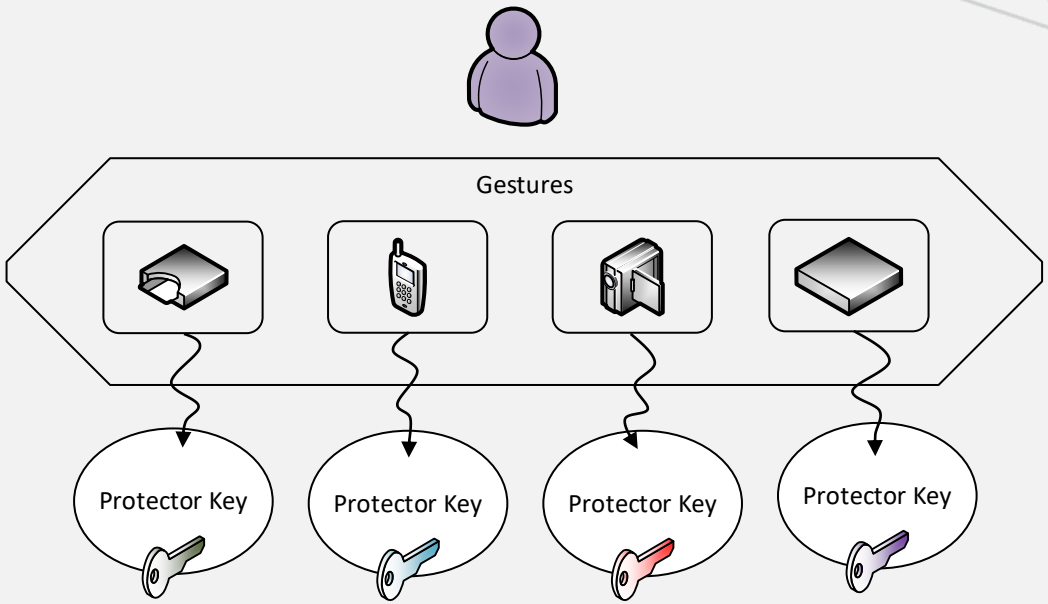
Windows Hello for Business

- User’s key access



Windows Hello for Business

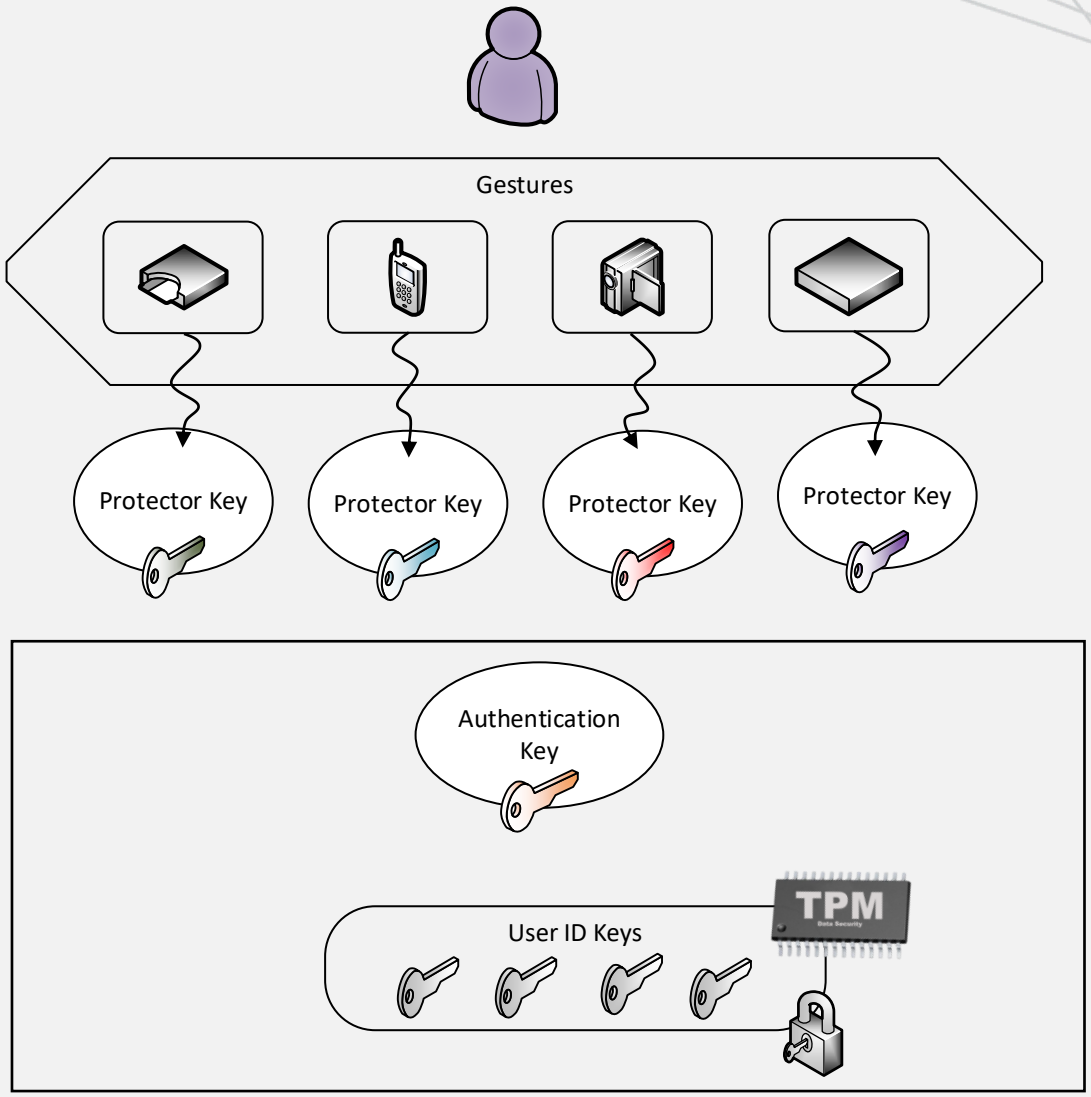
- User's key access



Each protector encrypts its own copy of the authentication key.

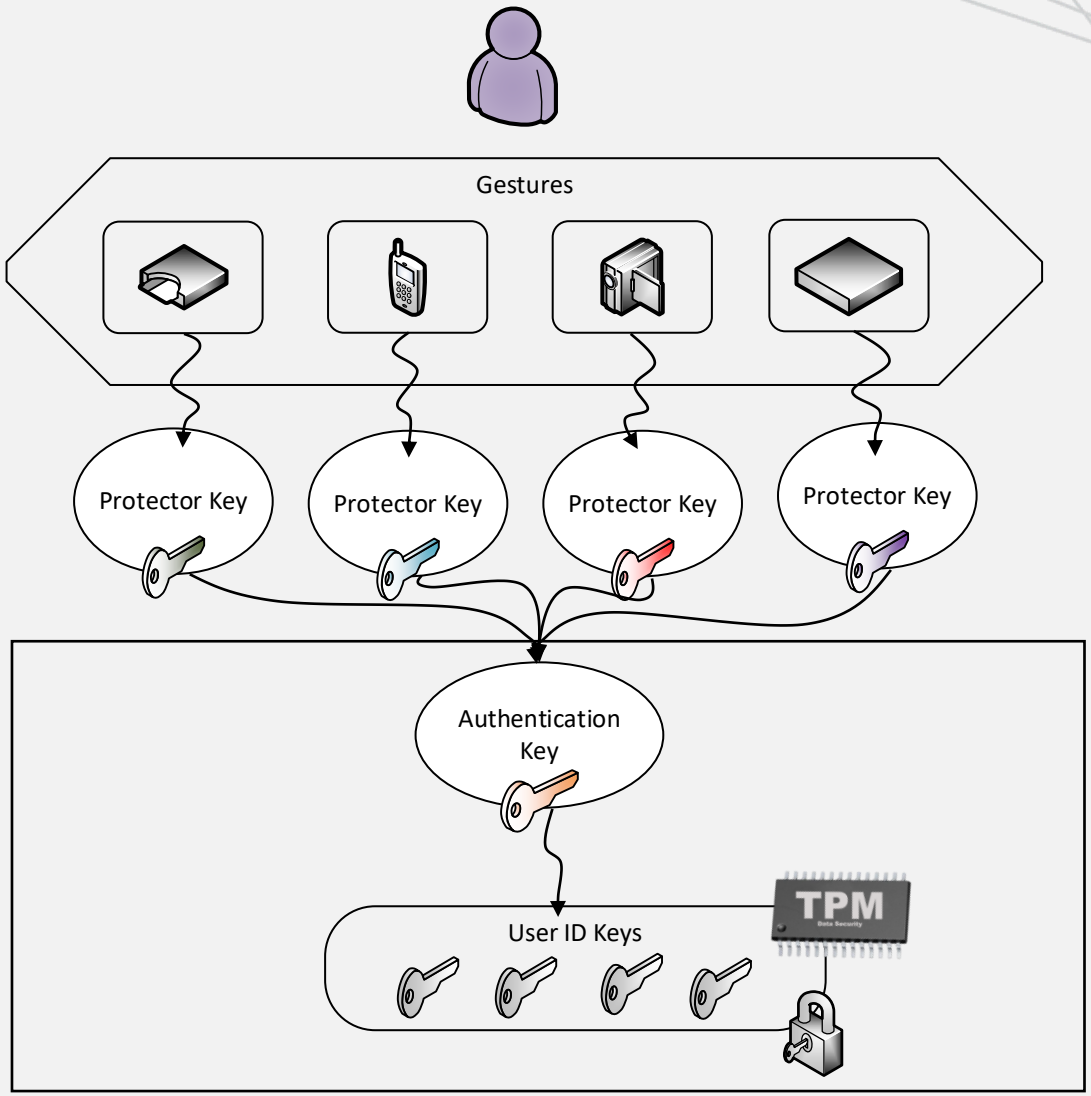
Windows Hello for Business

- User’s key access



Windows Hello for Business

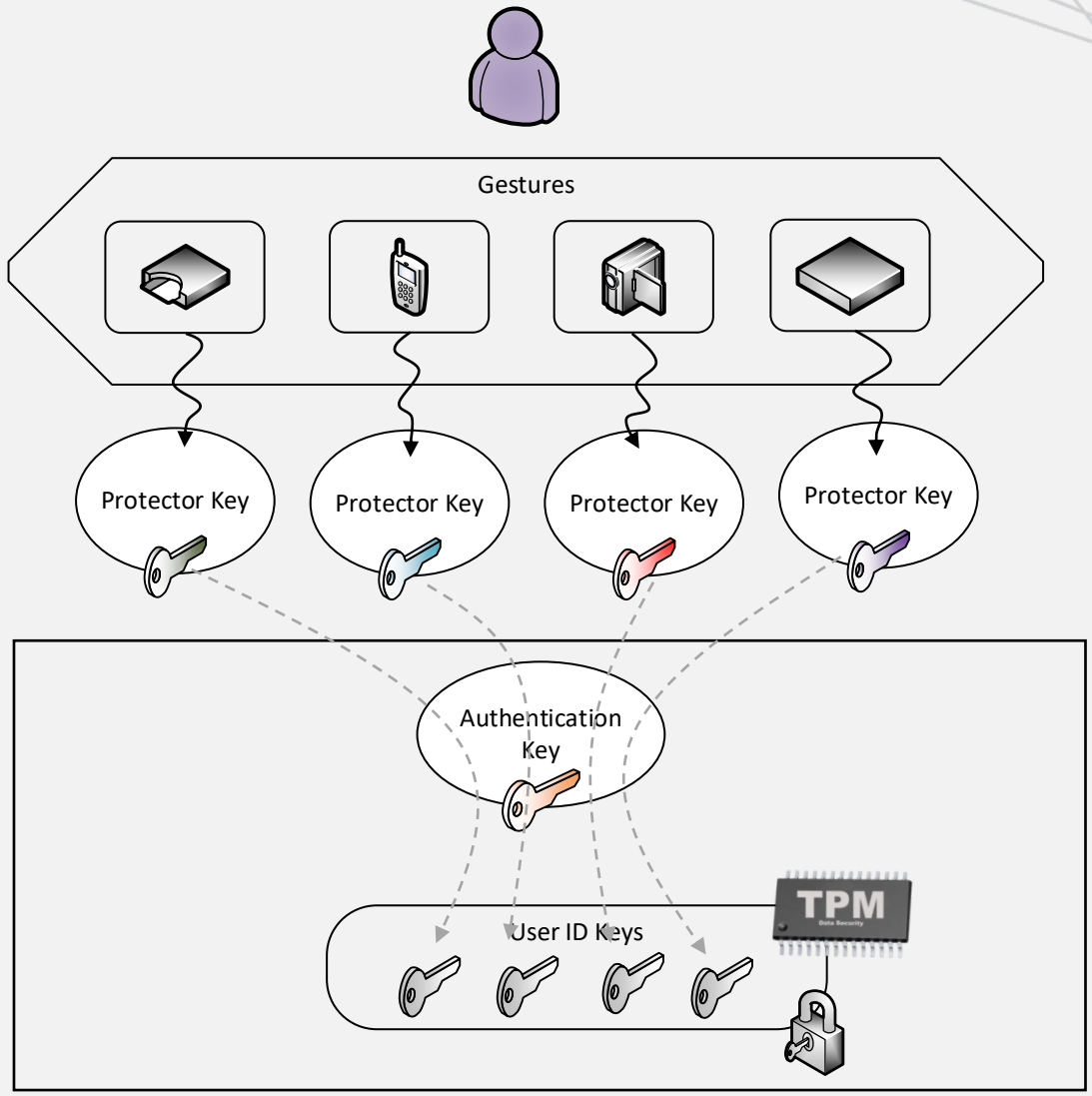
- User's key access



The container has only one authentication key, but there can be multiple copies of that key wrapped with different unique protector keys.

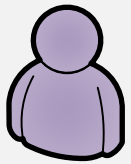
Windows Hello for Business

- User's key access

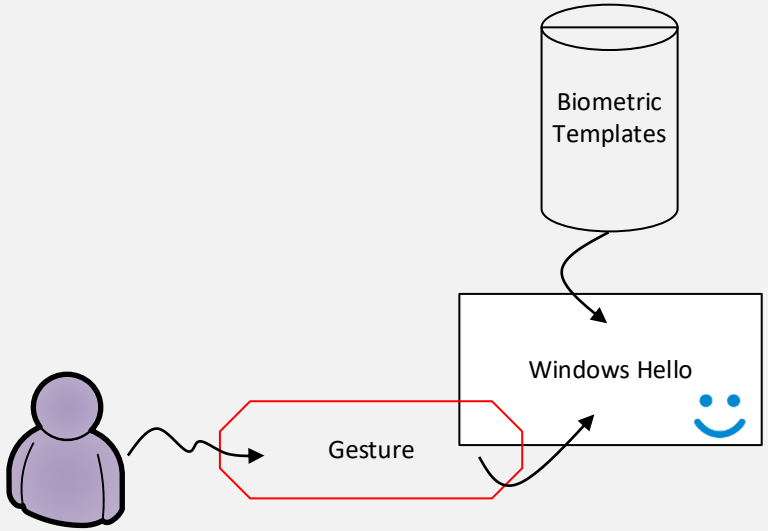


The container has only one authentication key, but there can be multiple copies of that key wrapped with different unique protector keys.

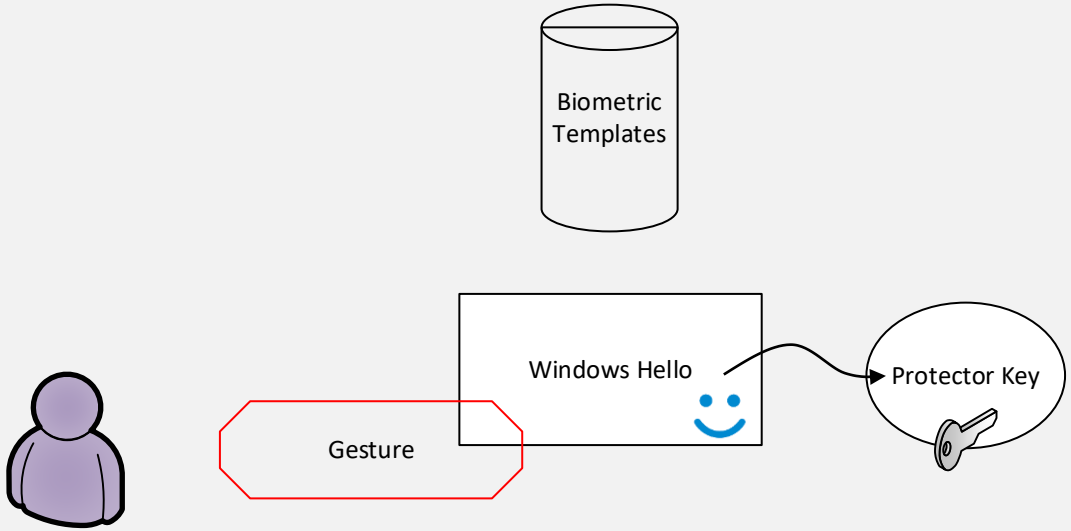
Windows Hello for Business



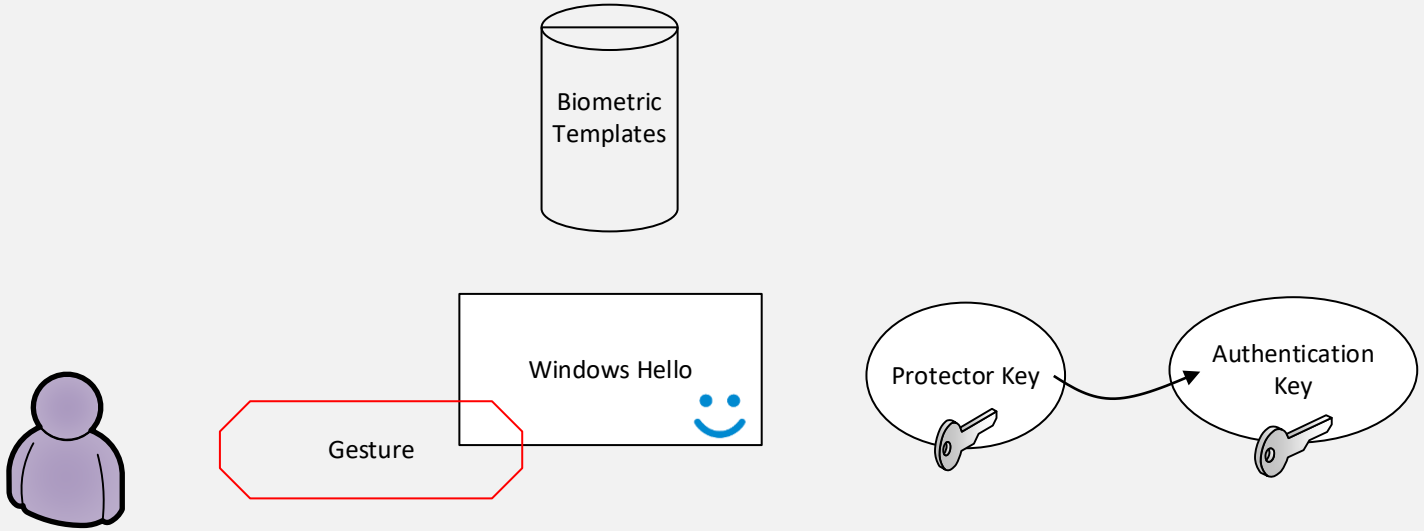
Windows Hello for Business



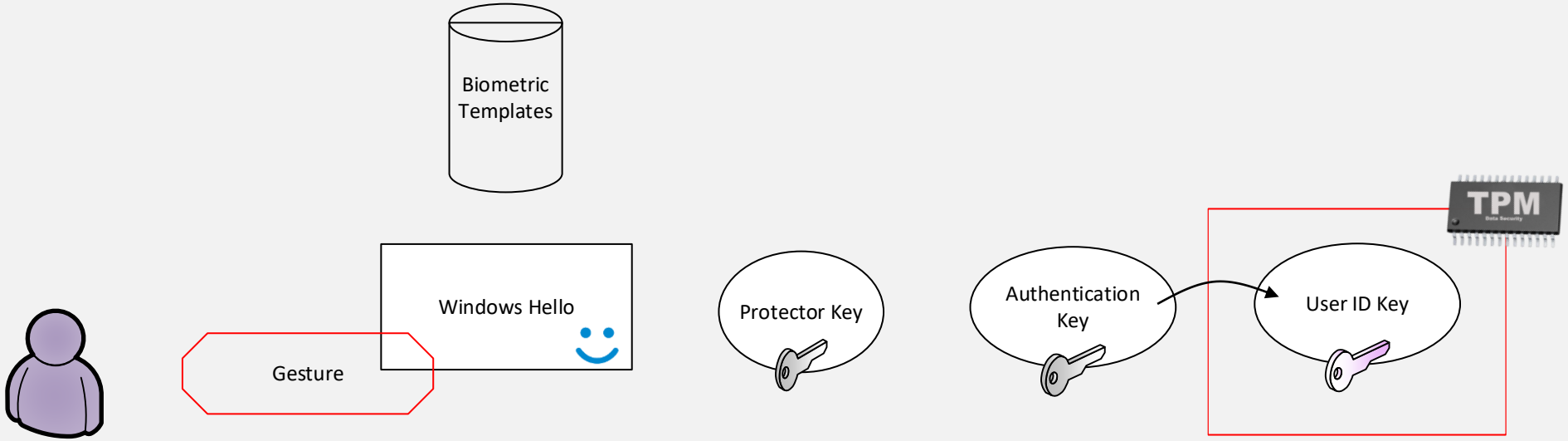
Windows Hello for Business



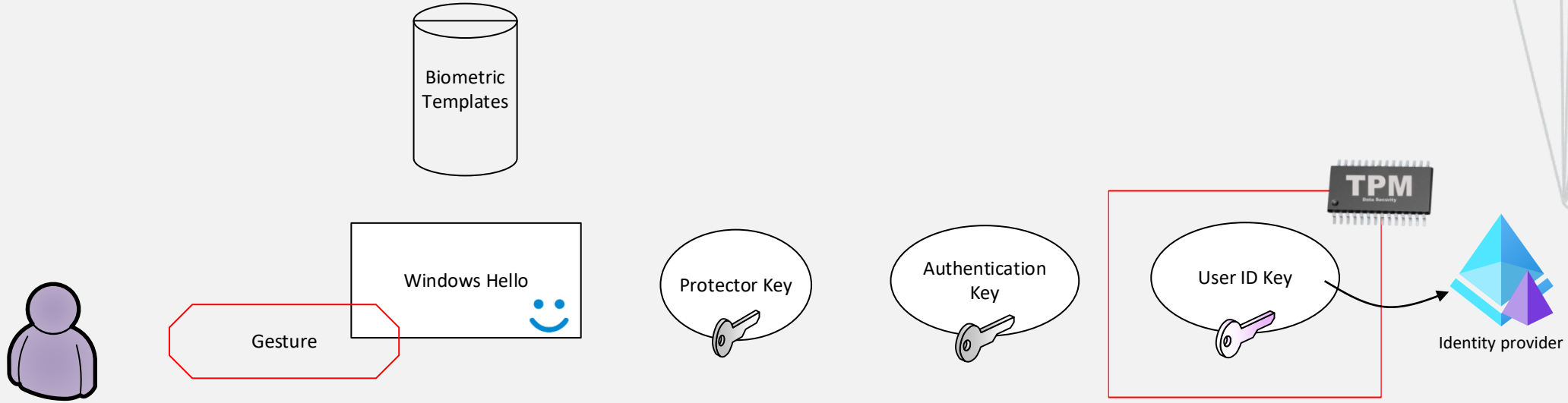
Windows Hello for Business



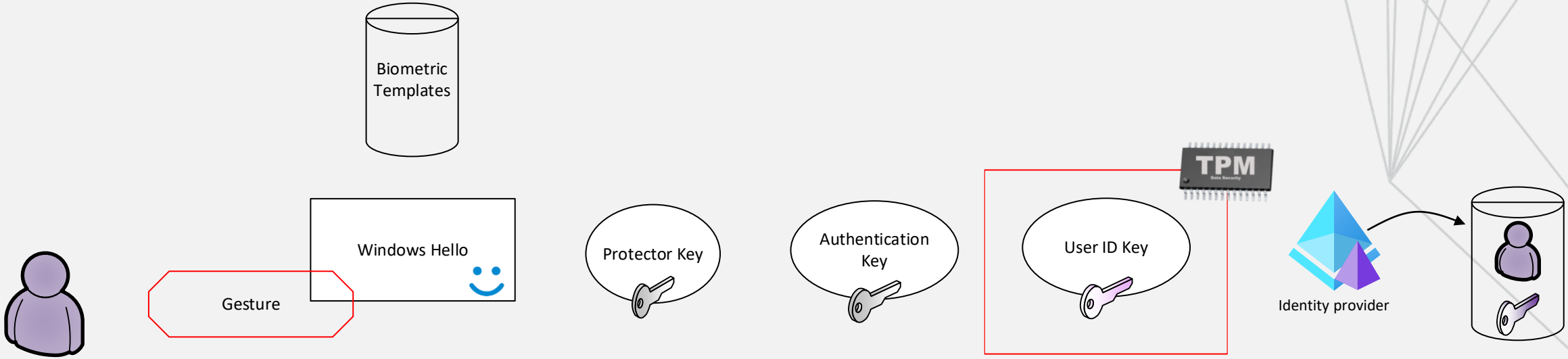
Windows Hello for Business



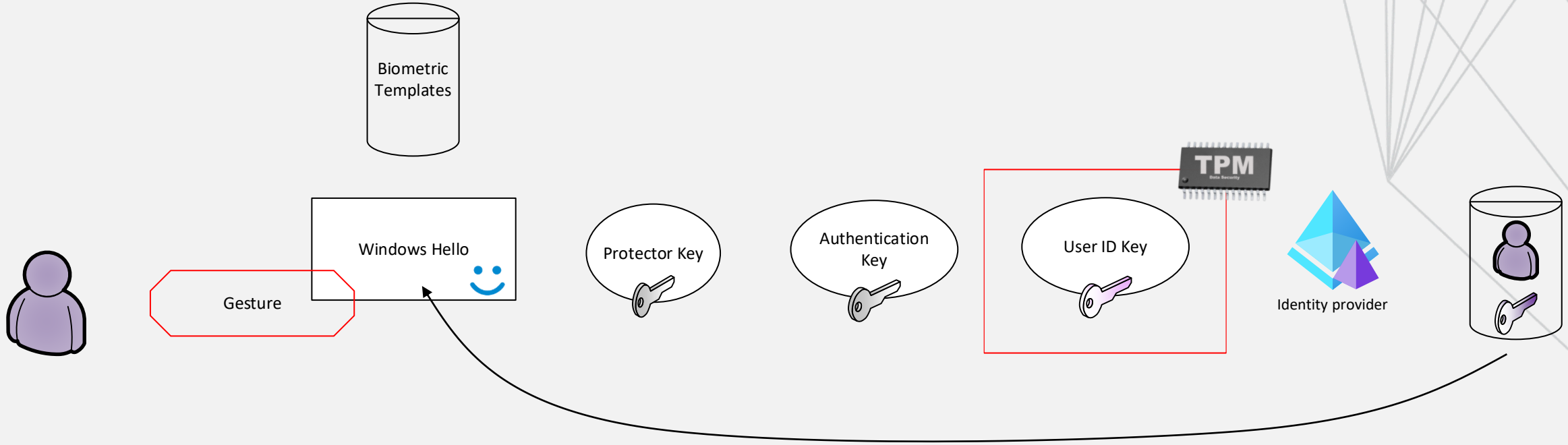
Windows Hello for Business



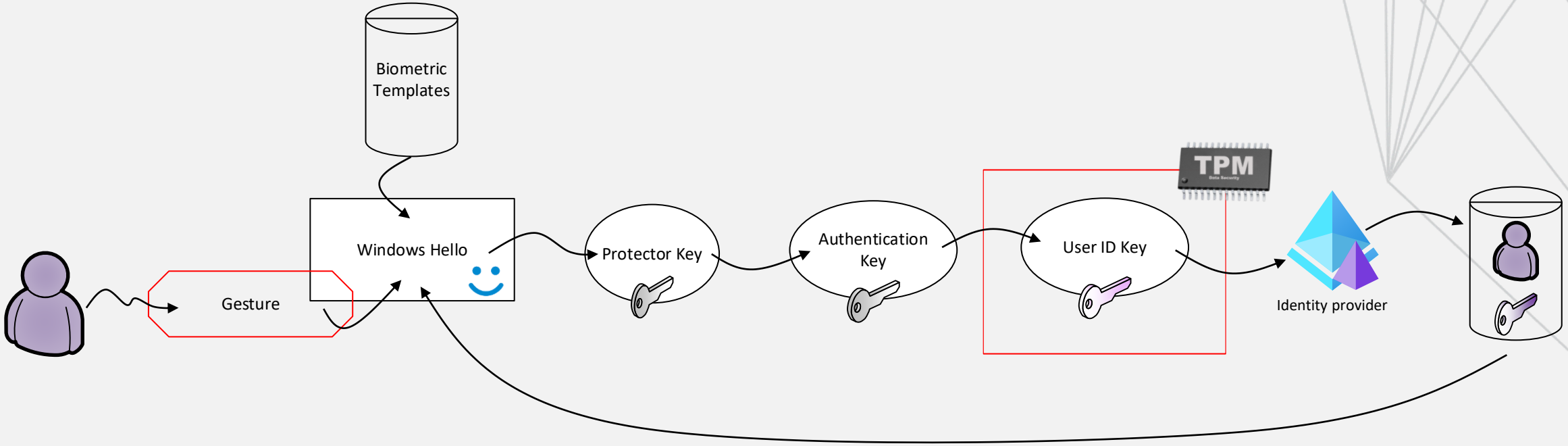
Windows Hello for Business



Windows Hello for Business



Windows Hello for Business

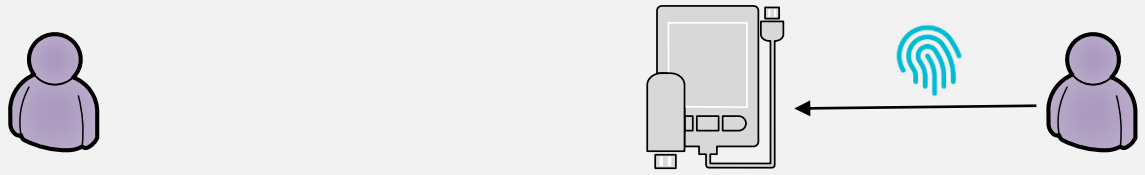


Windows Hello

- Simplified view

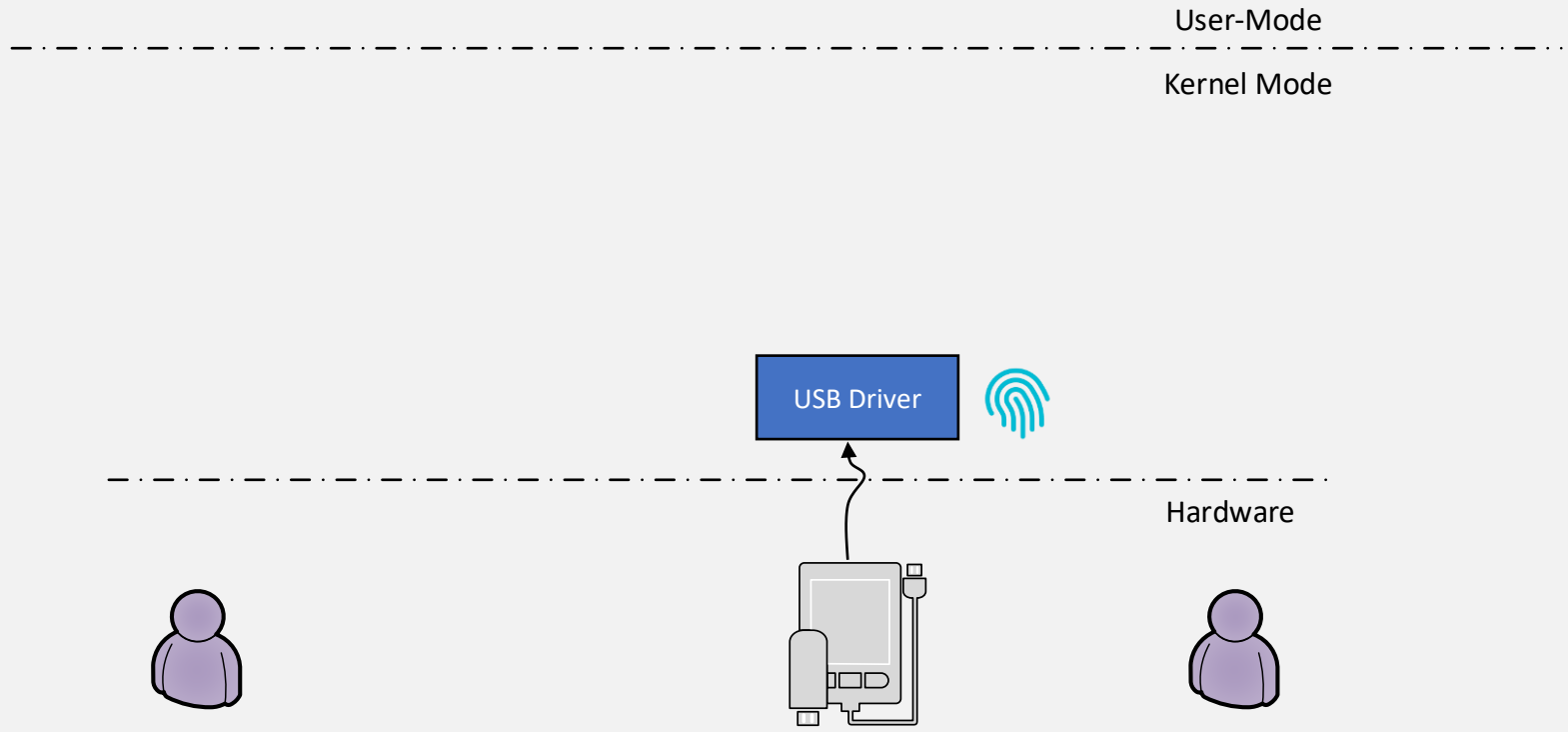
Windows Hello

- Simplified view



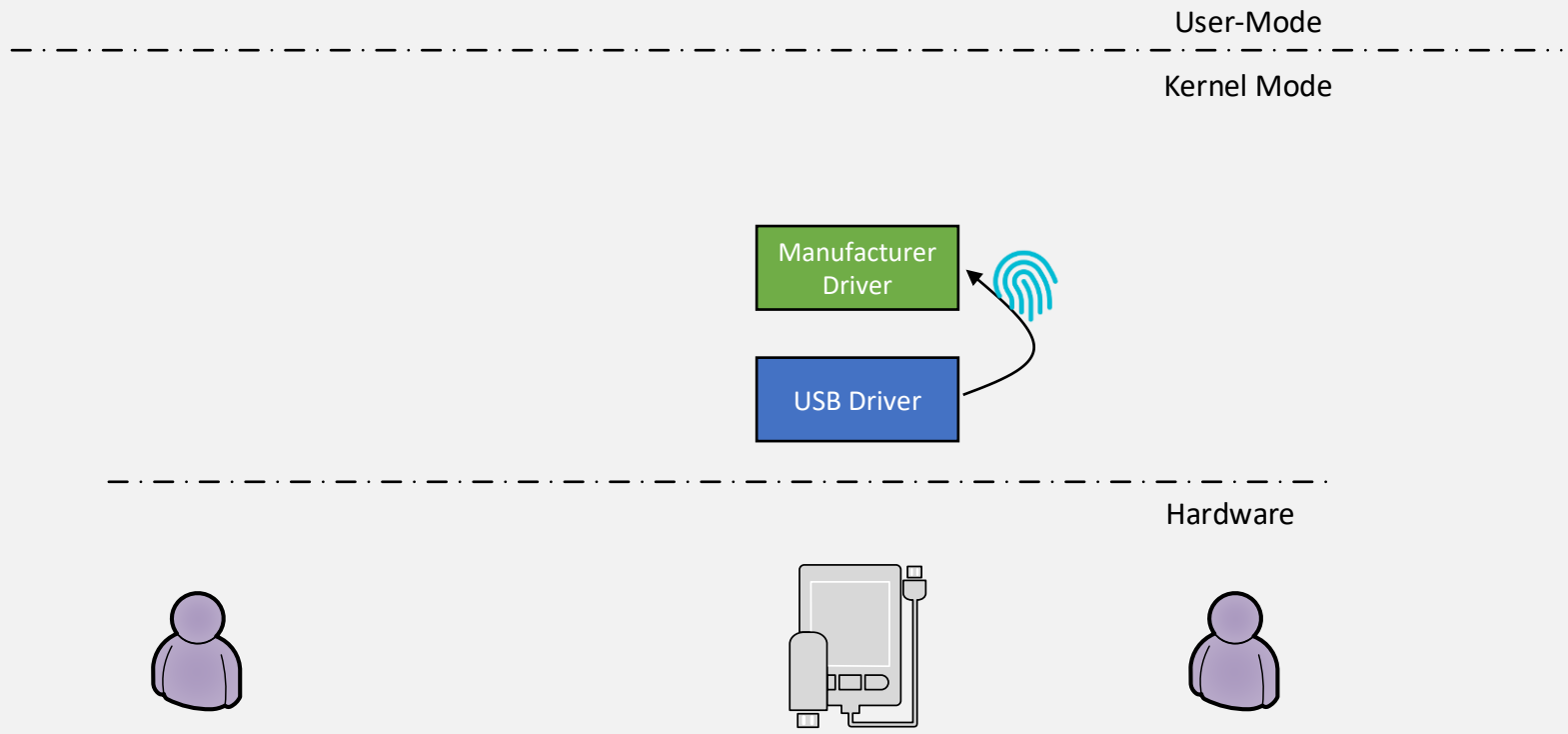
Windows Hello

- Simplified view



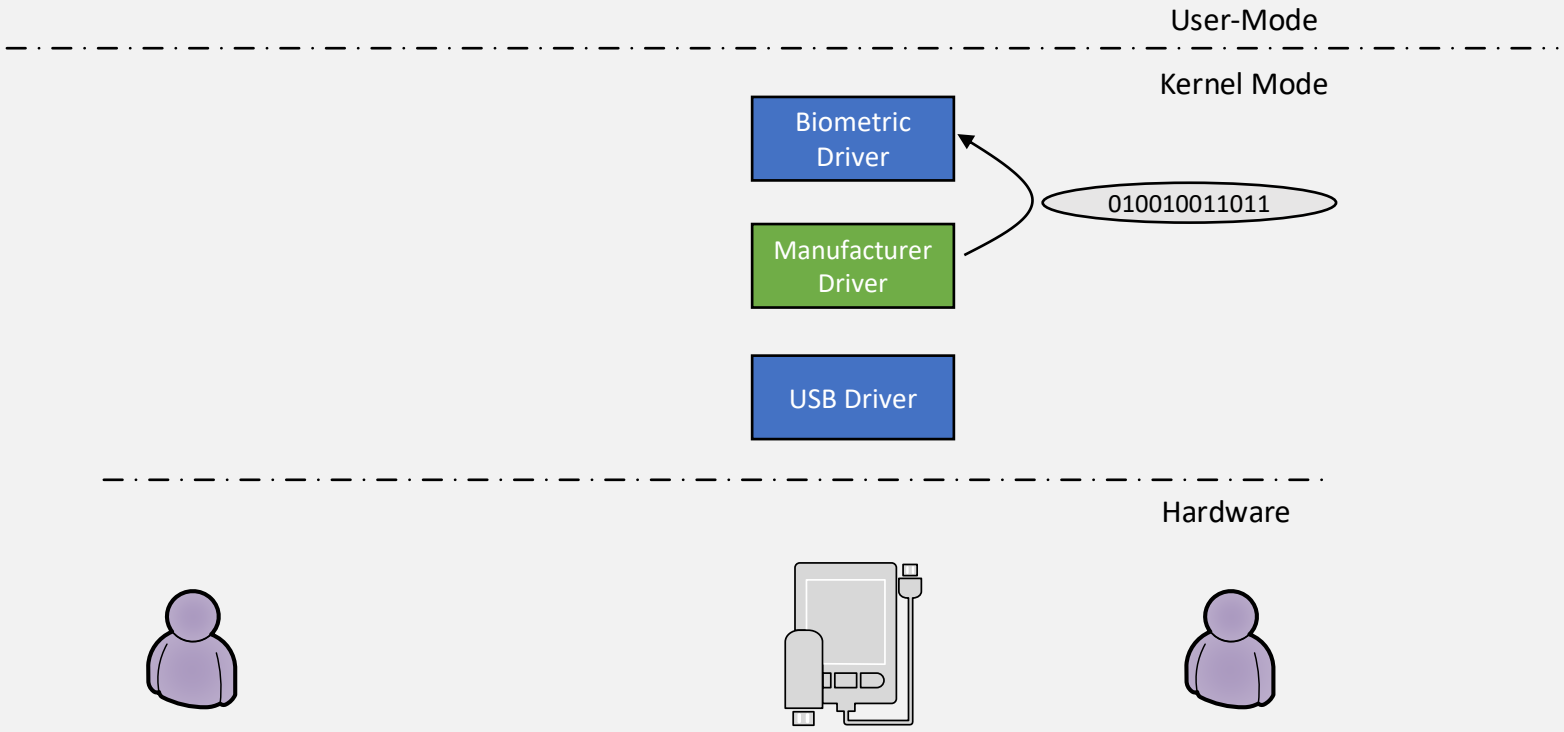
Windows Hello

- Simplified view



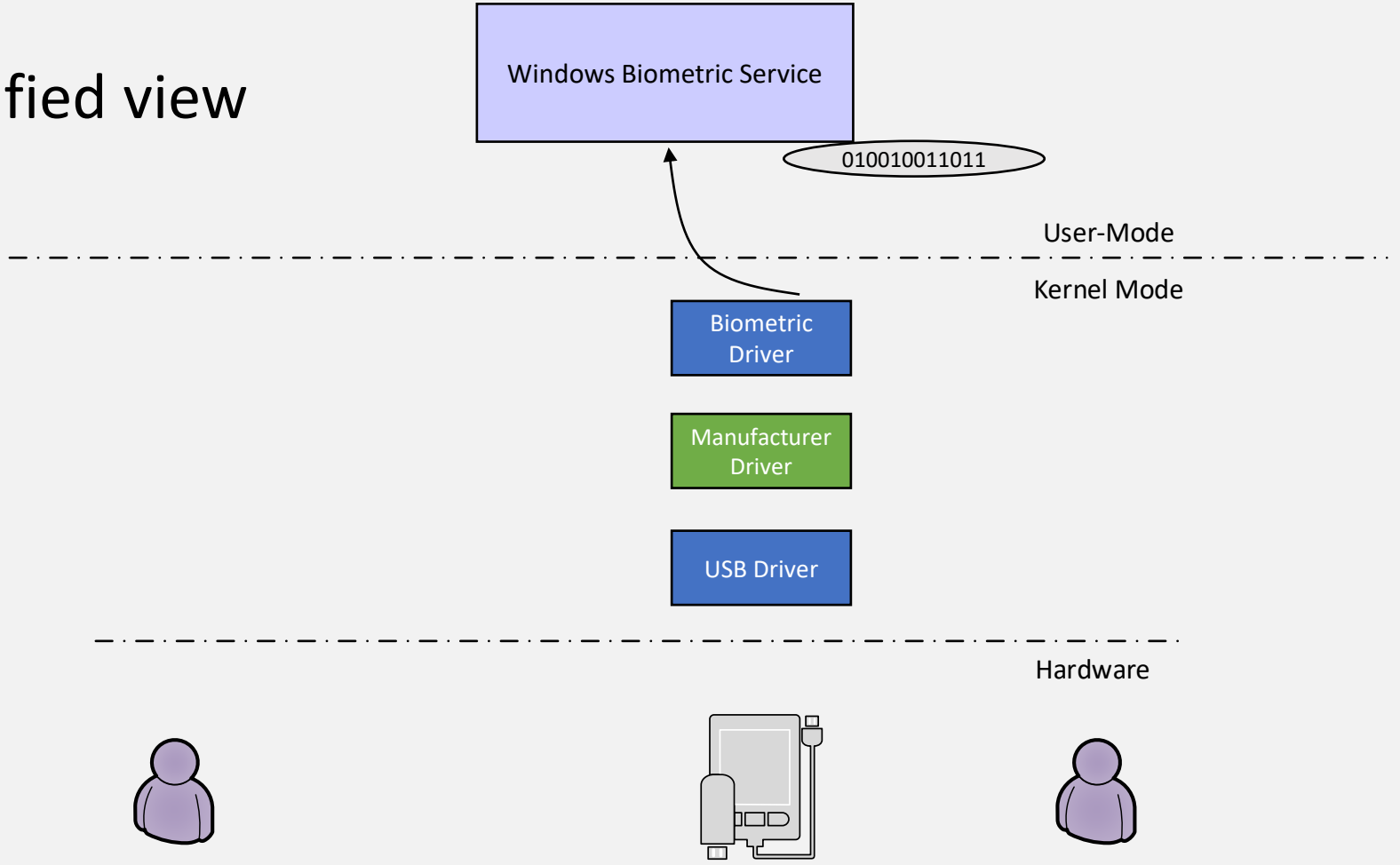
Windows Hello

- Simplified view



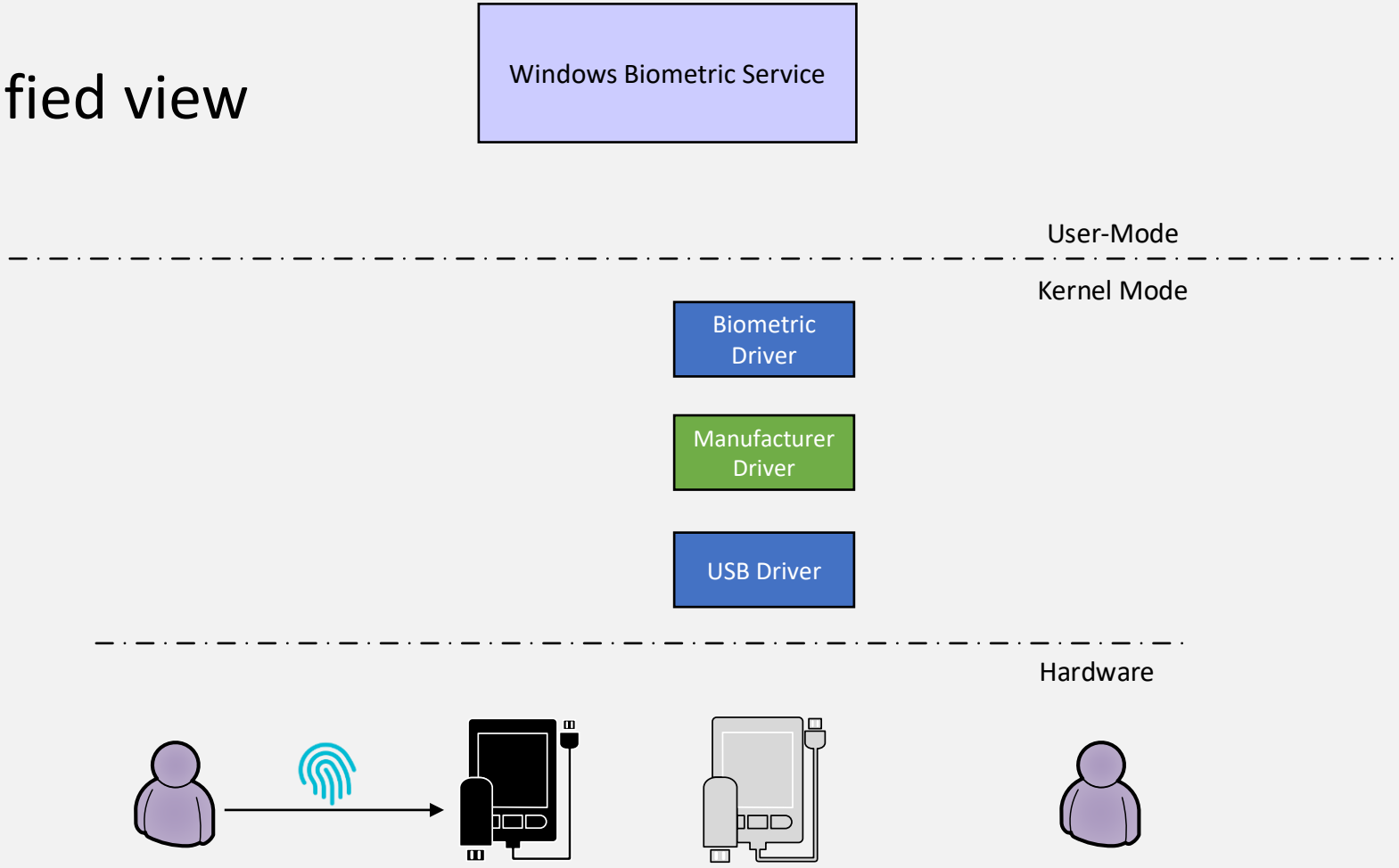
Windows Hello

- Simplified view



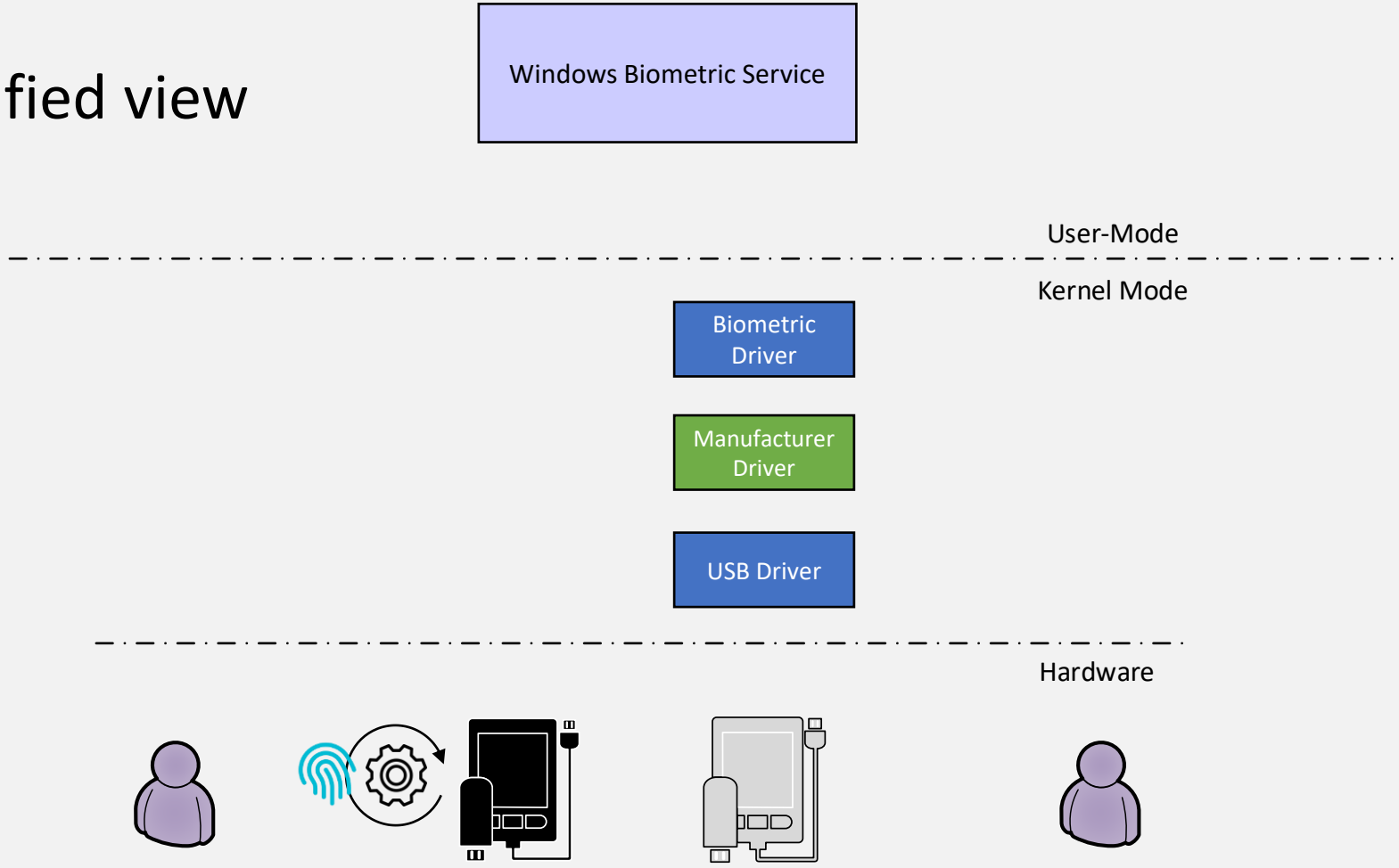
Windows Hello

- Simplified view



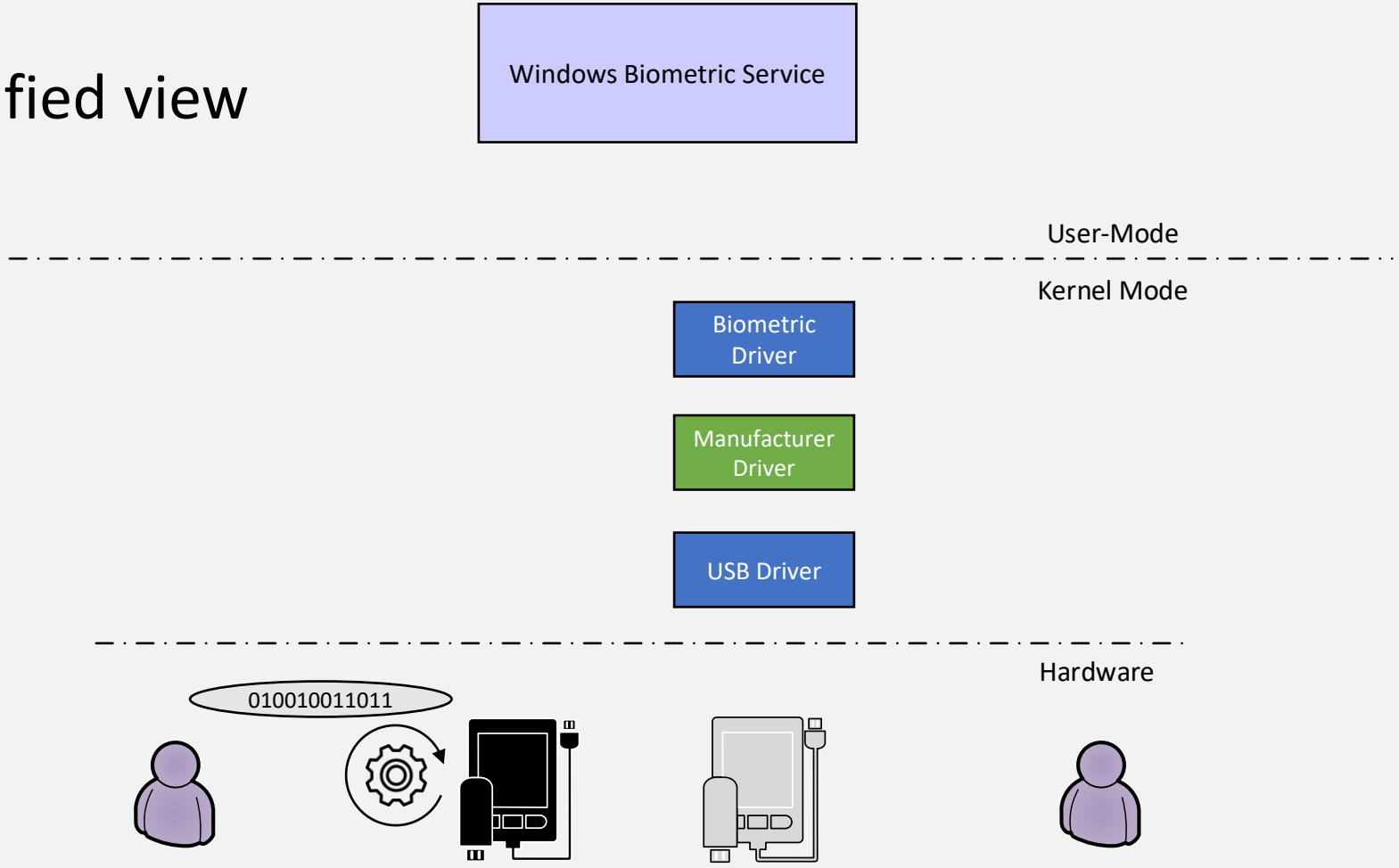
Windows Hello

- Simplified view



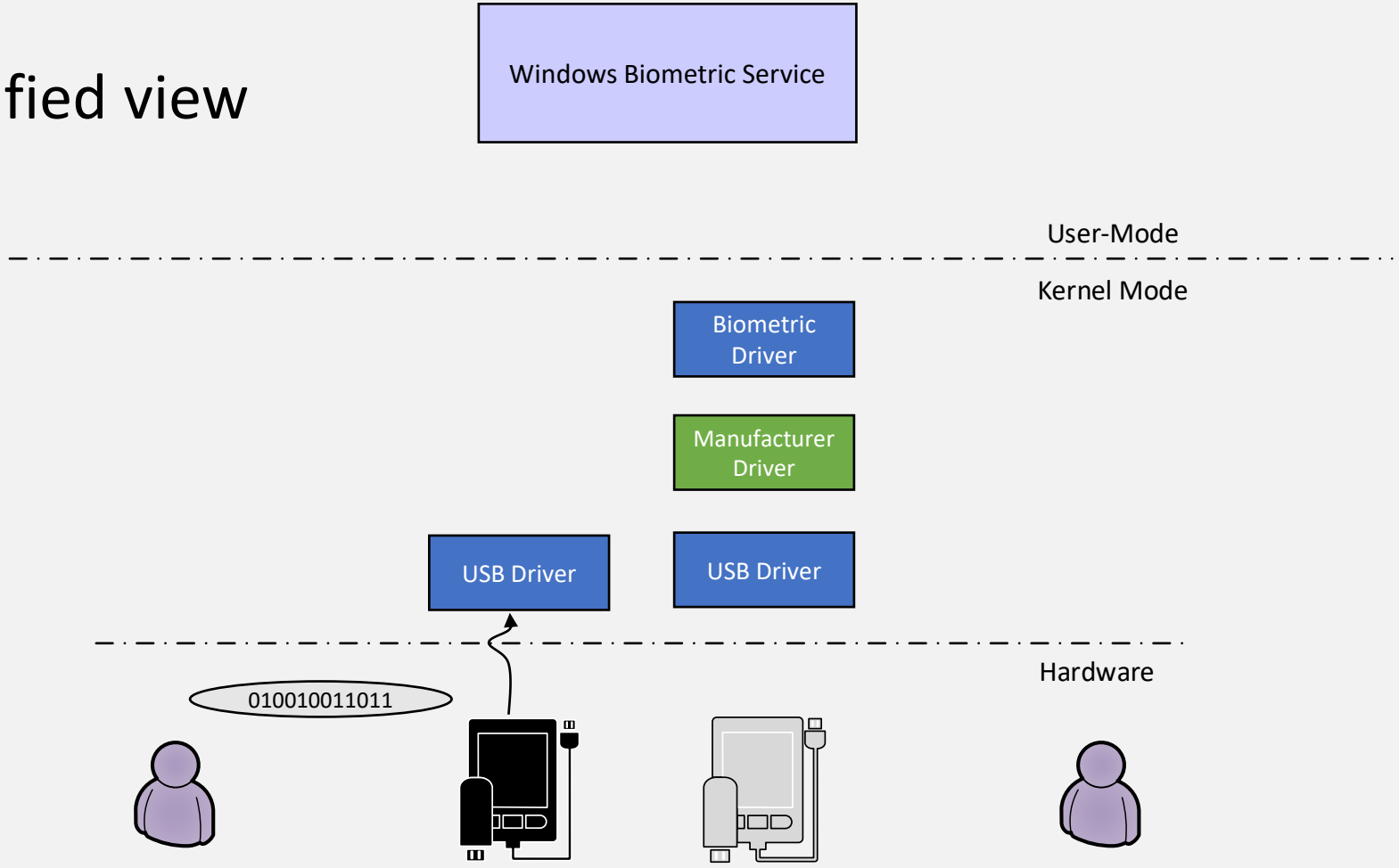
Windows Hello

- Simplified view



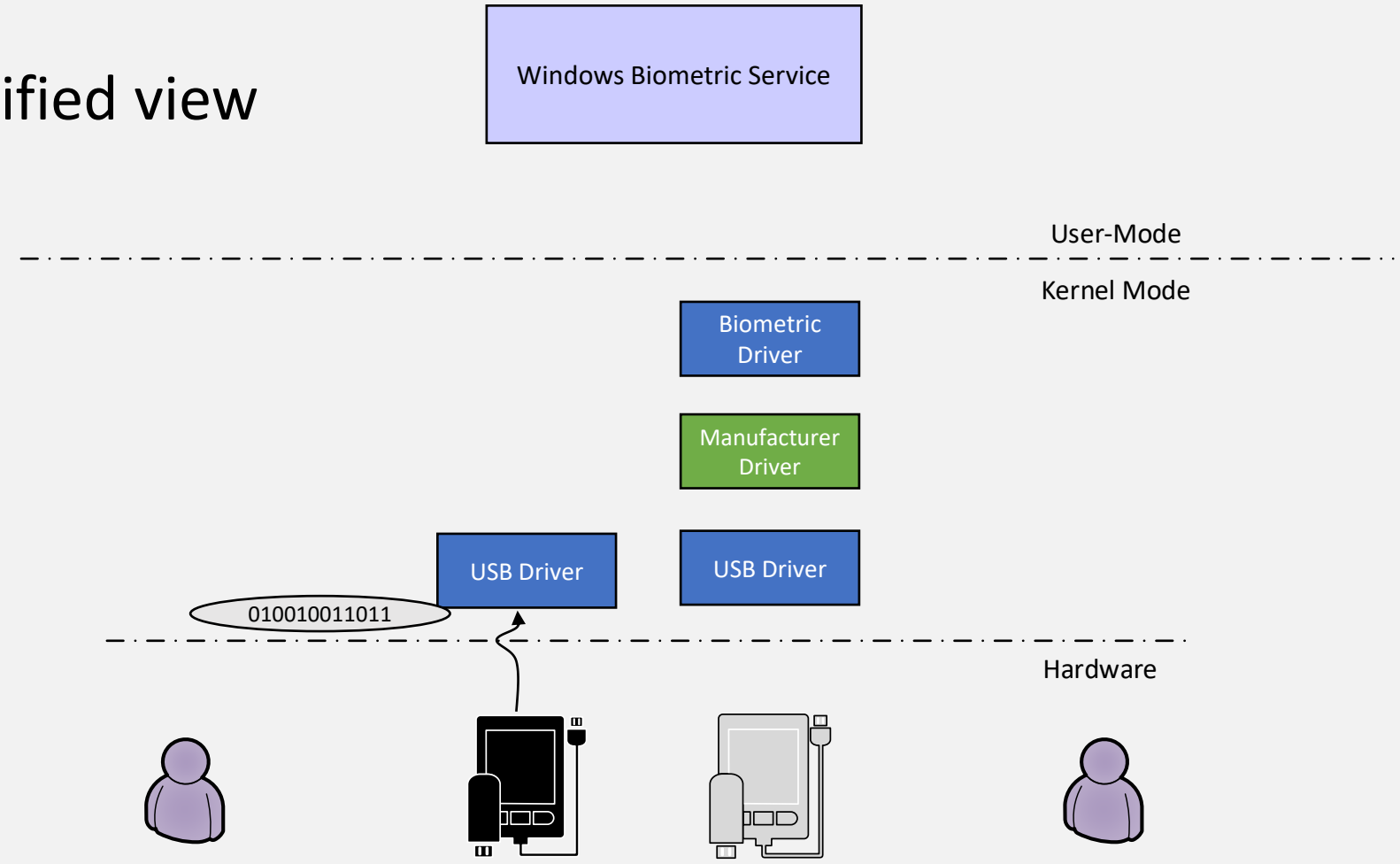
Windows Hello

- Simplified view



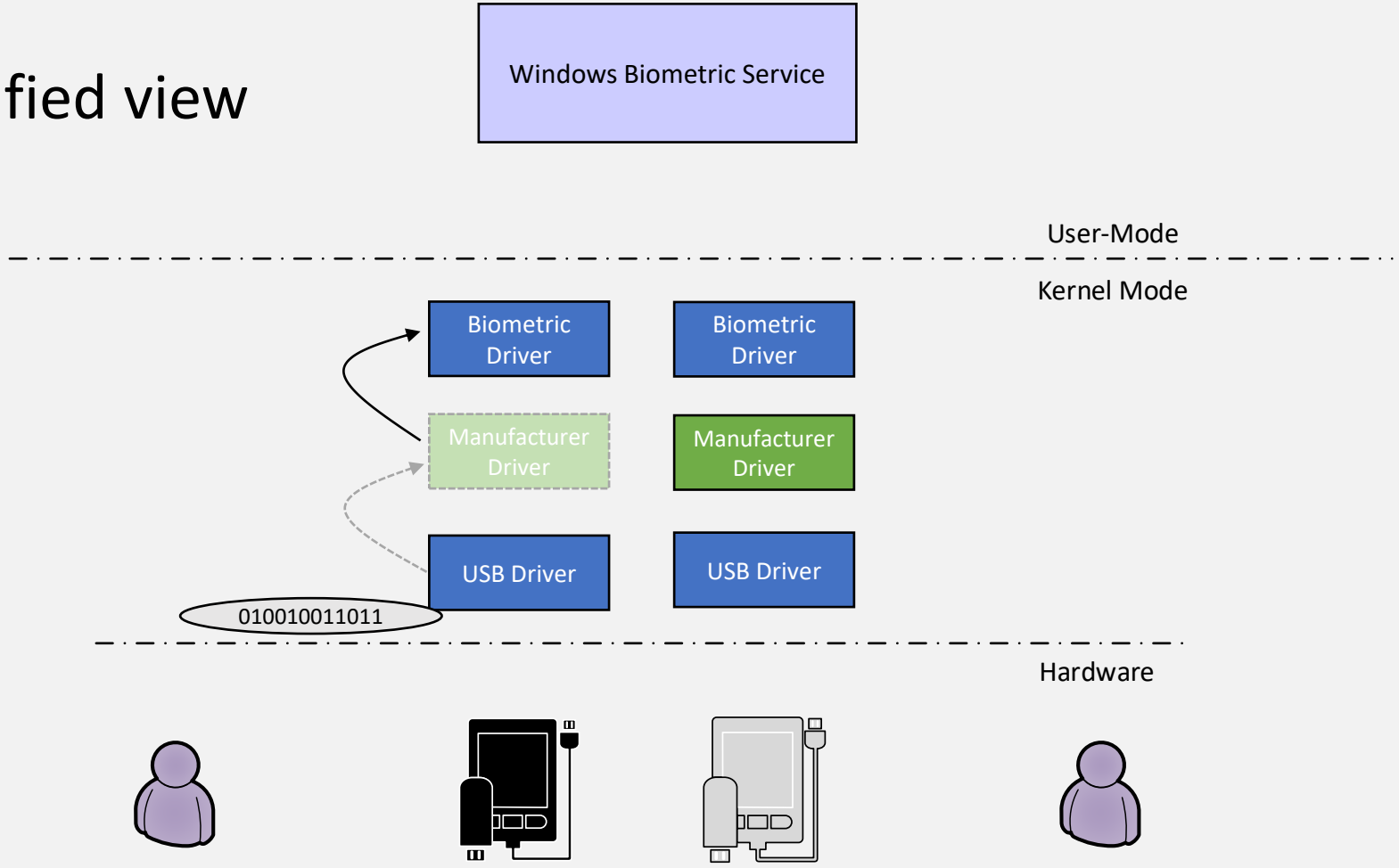
Windows Hello

- Simplified view



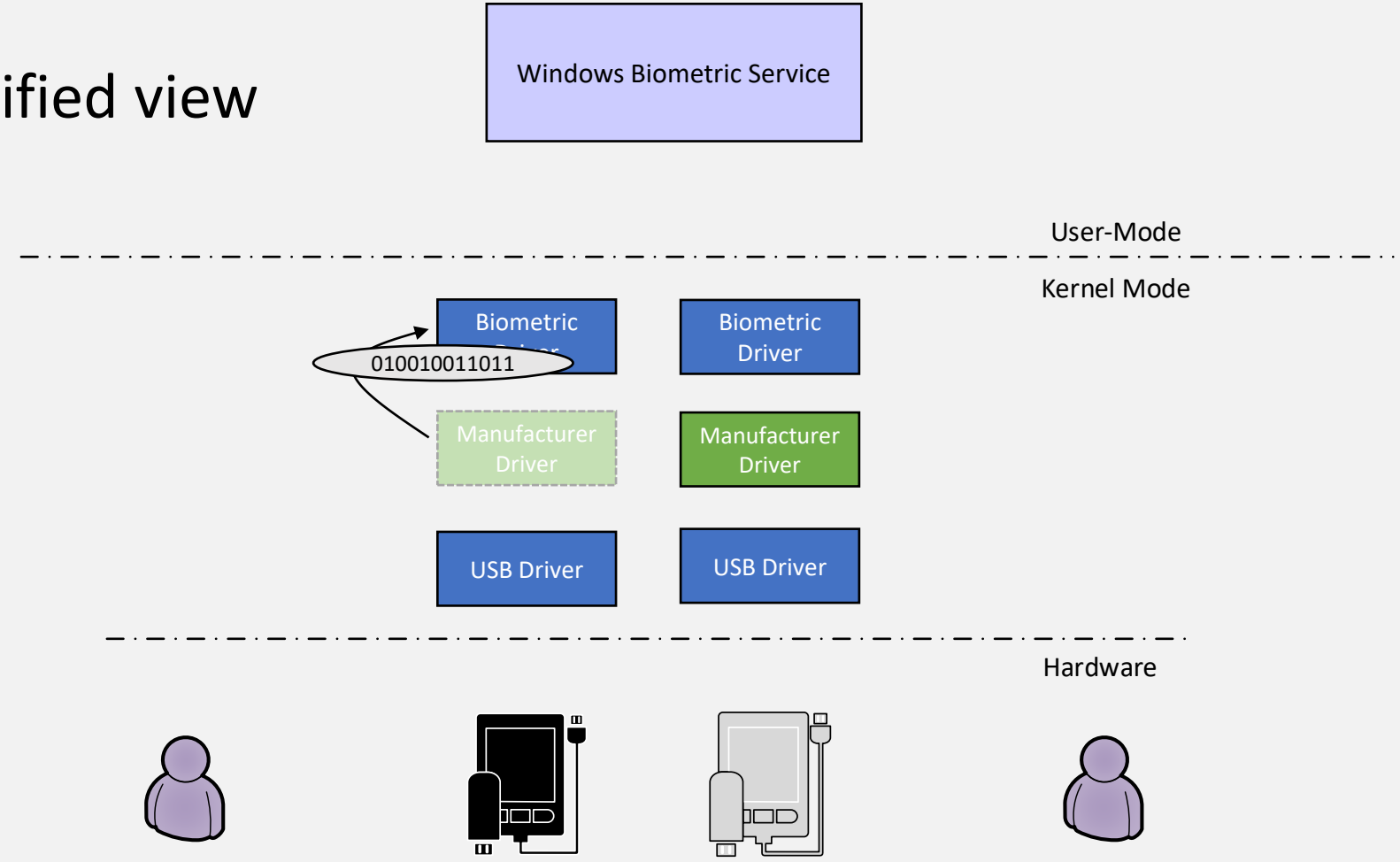
Windows Hello

- Simplified view



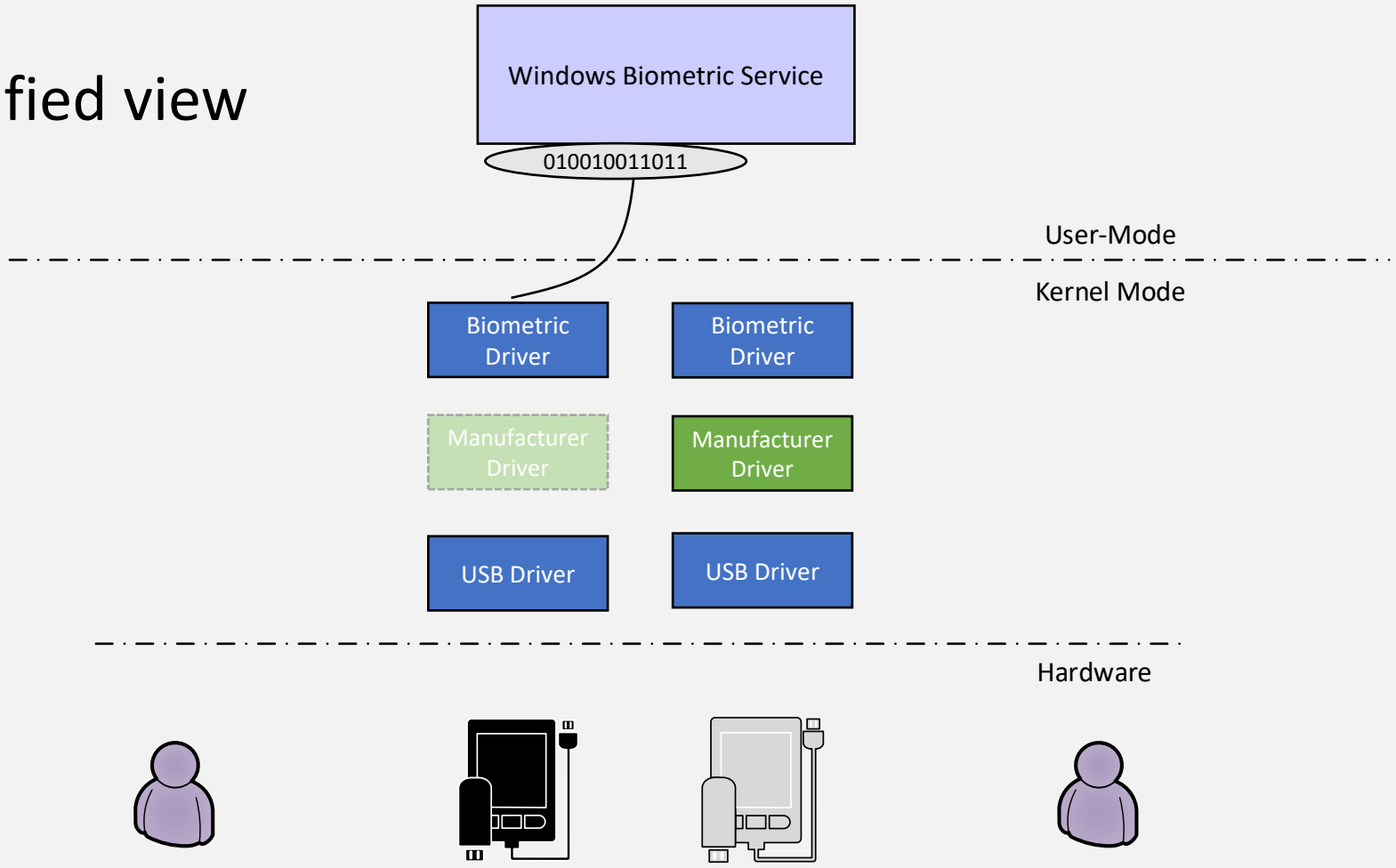
Windows Hello

- Simplified view



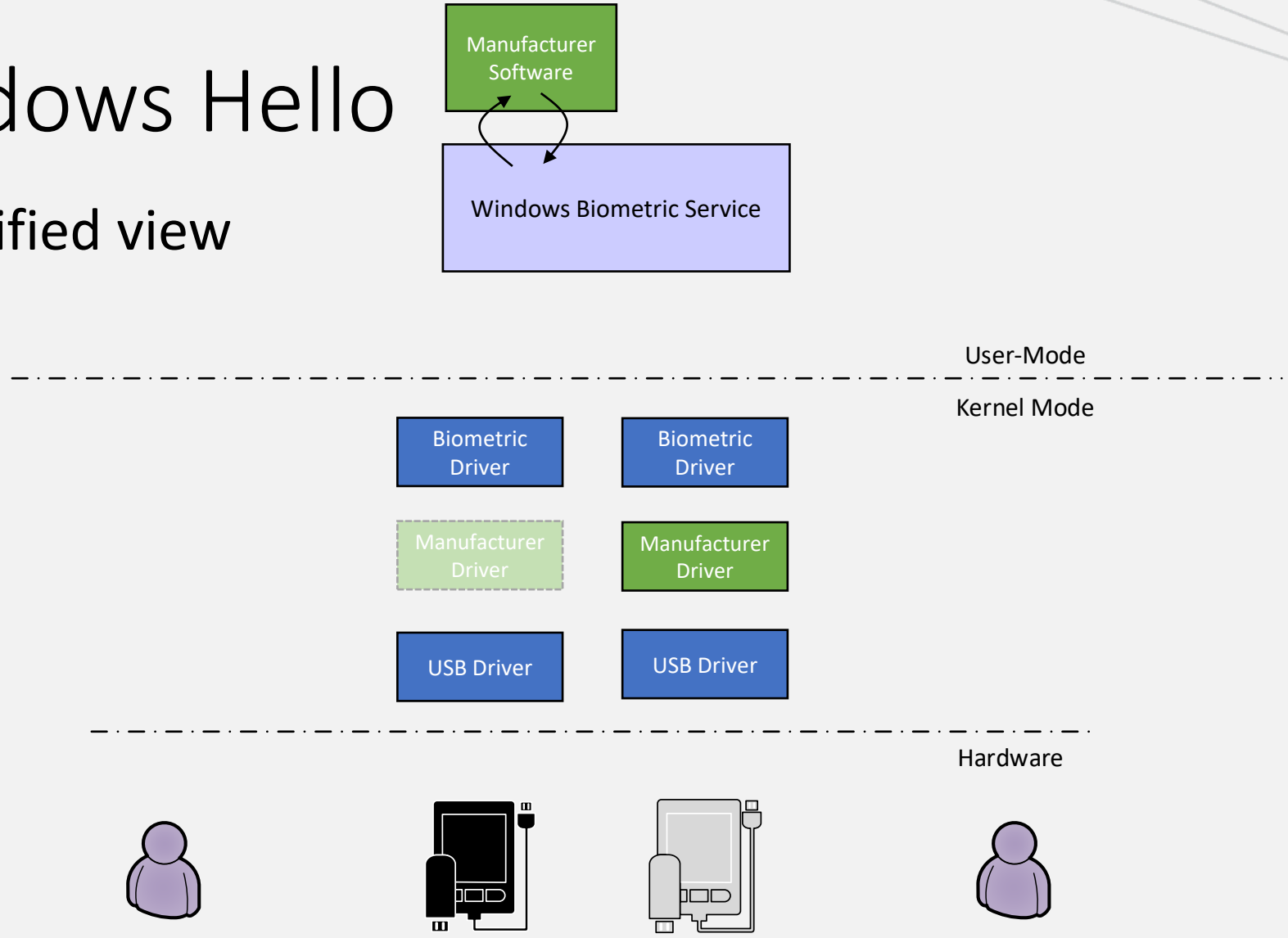
Windows Hello

- Simplified view



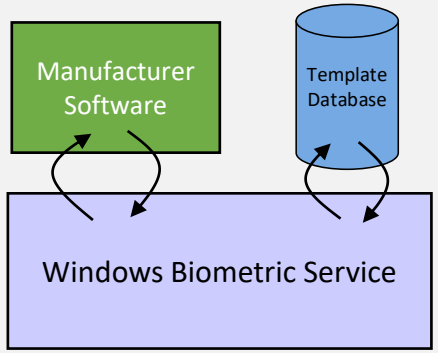
Windows Hello

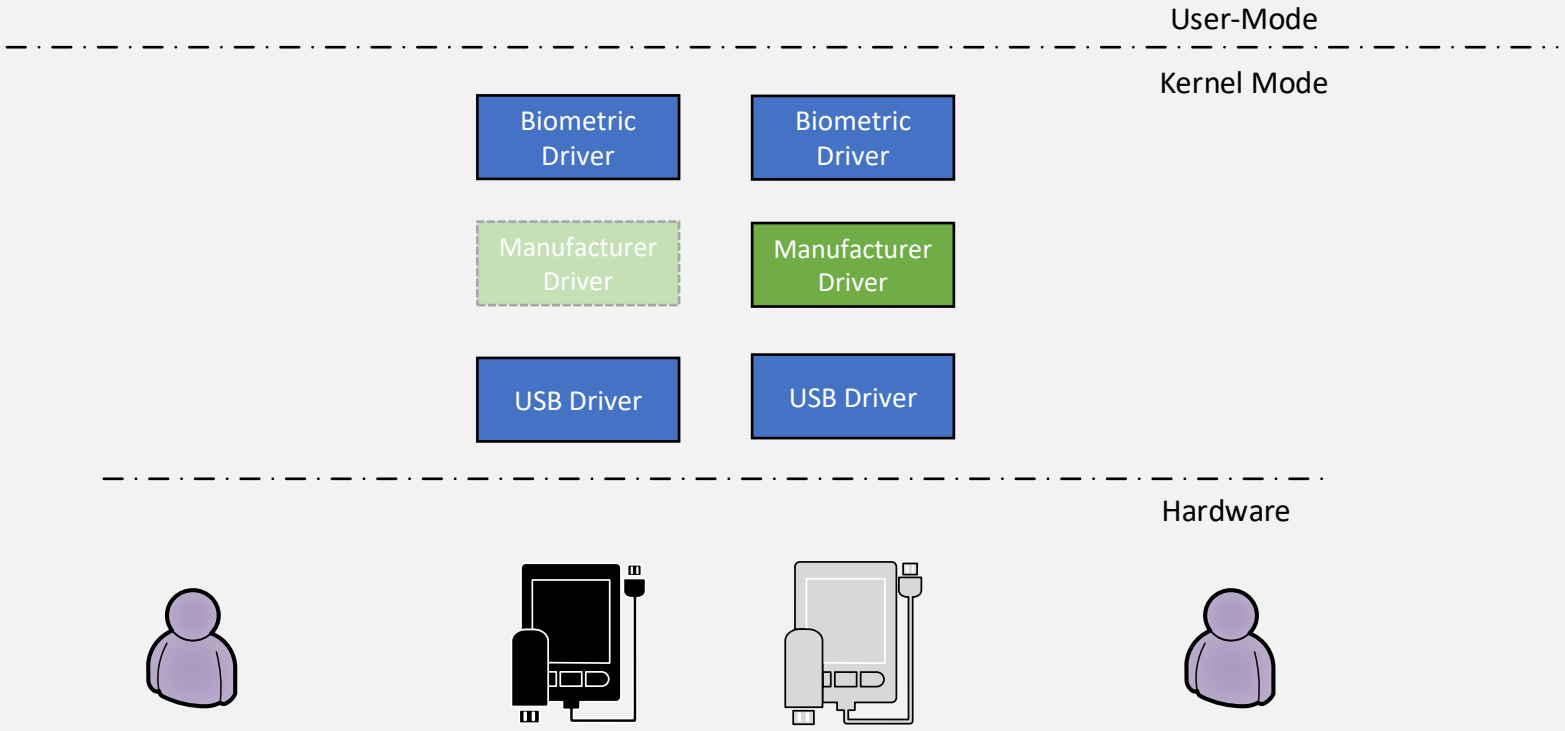
- Simplified view



Windows Hello

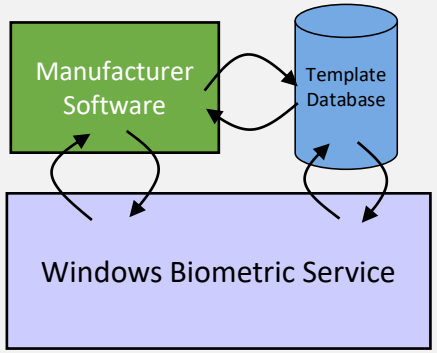
- Simplified view

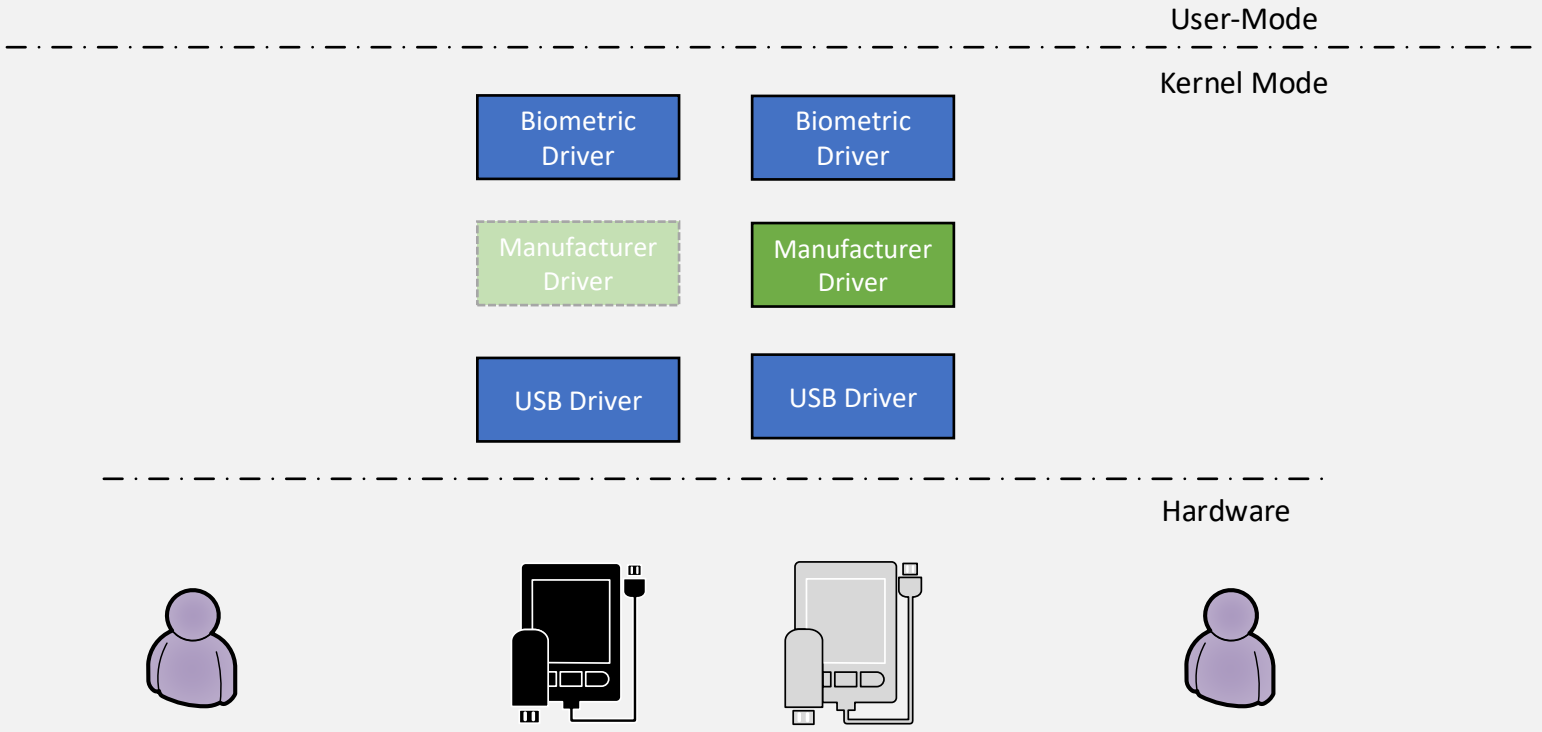




Windows Hello

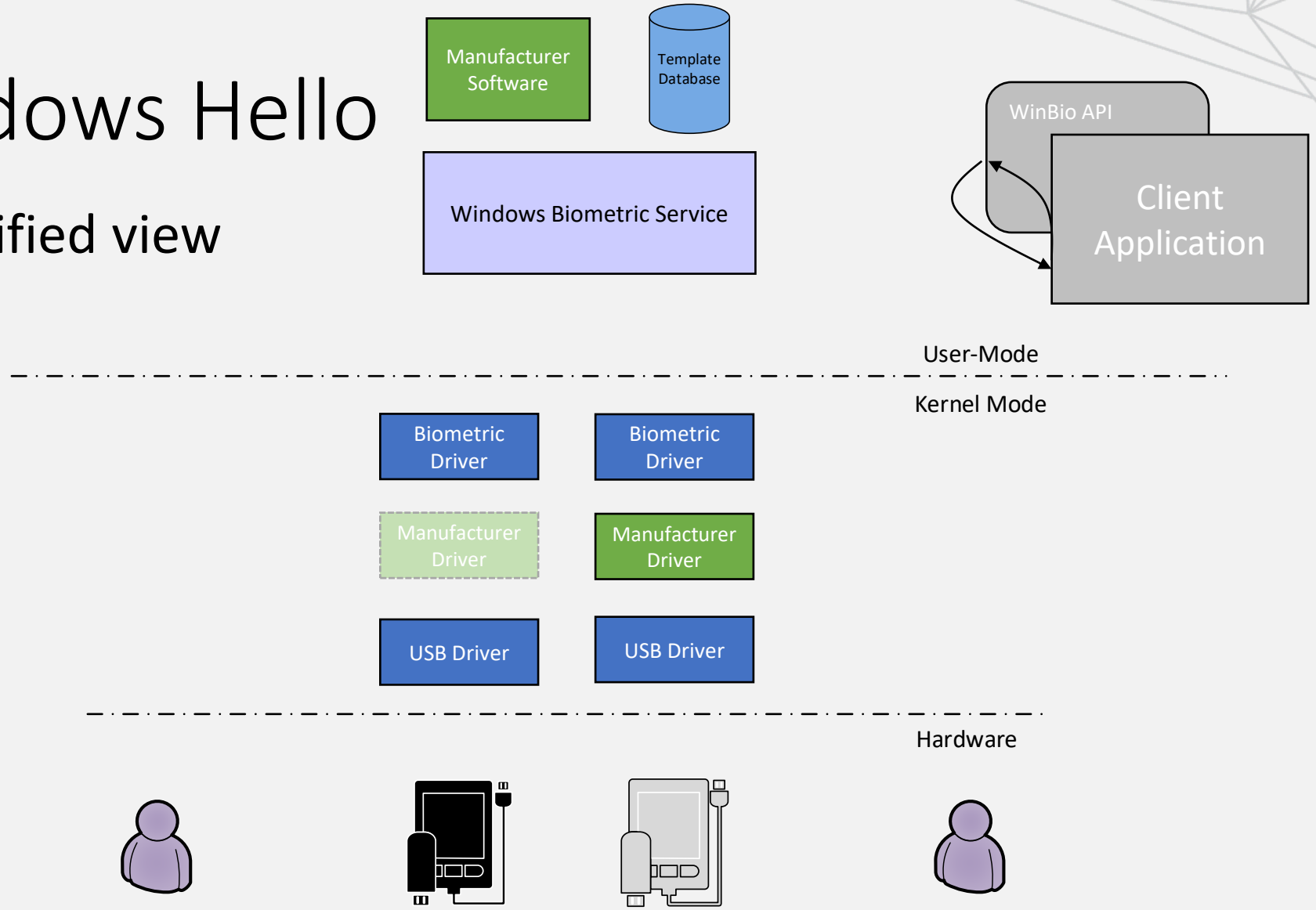
- Simplified view





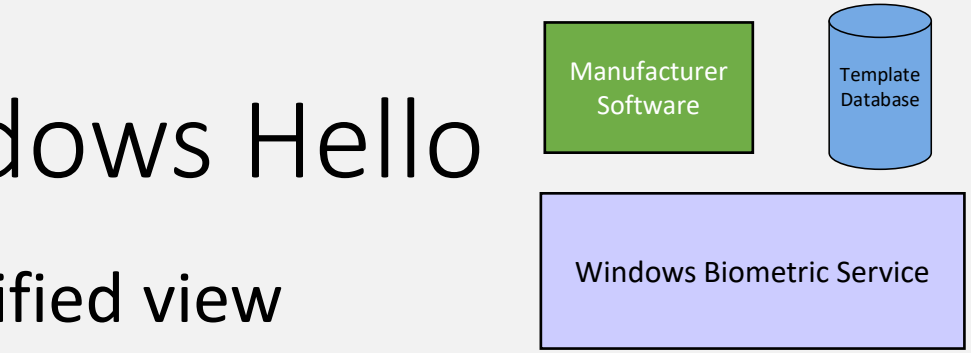
Windows Hello

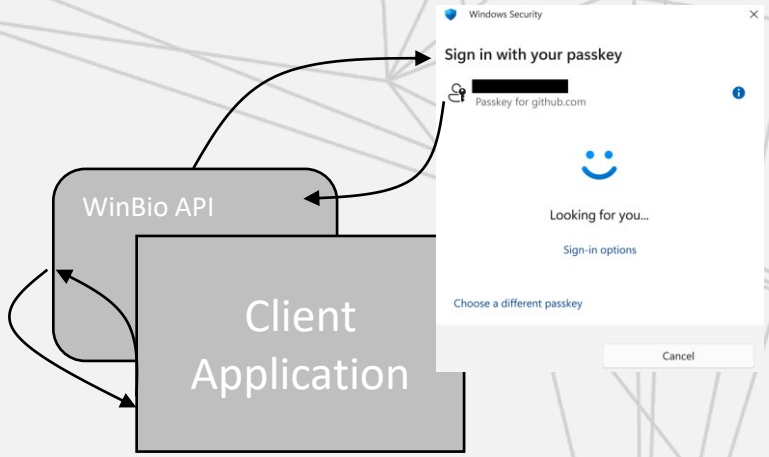
- Simplified view

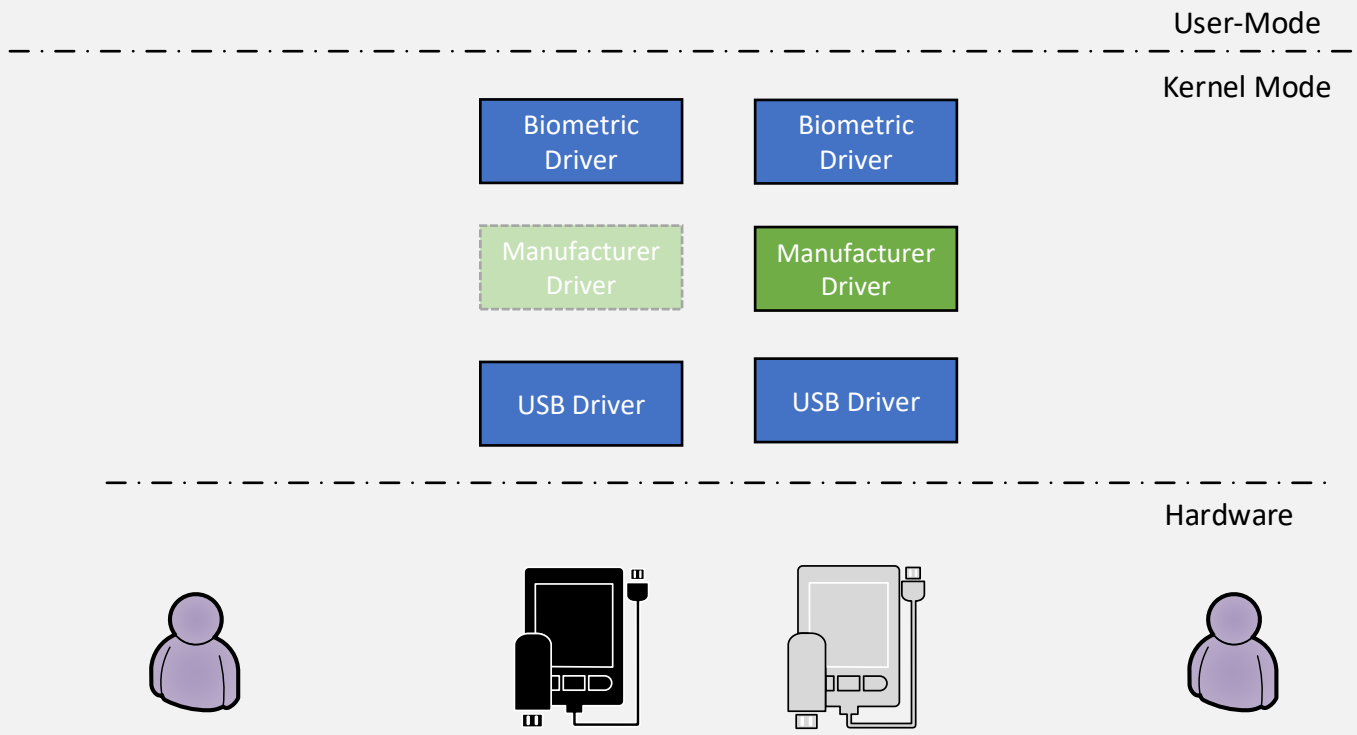


Windows Hello

- Simplified view

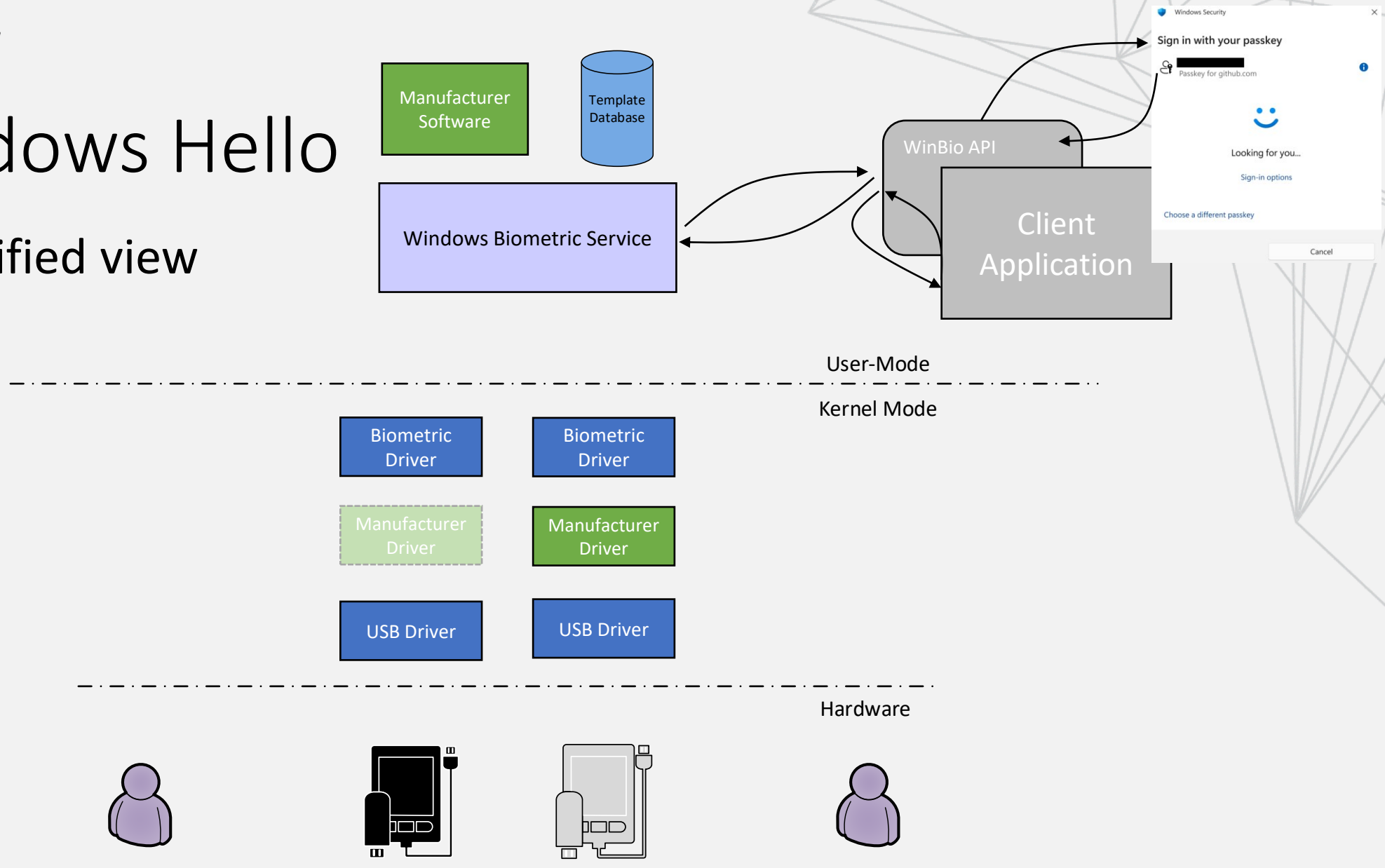






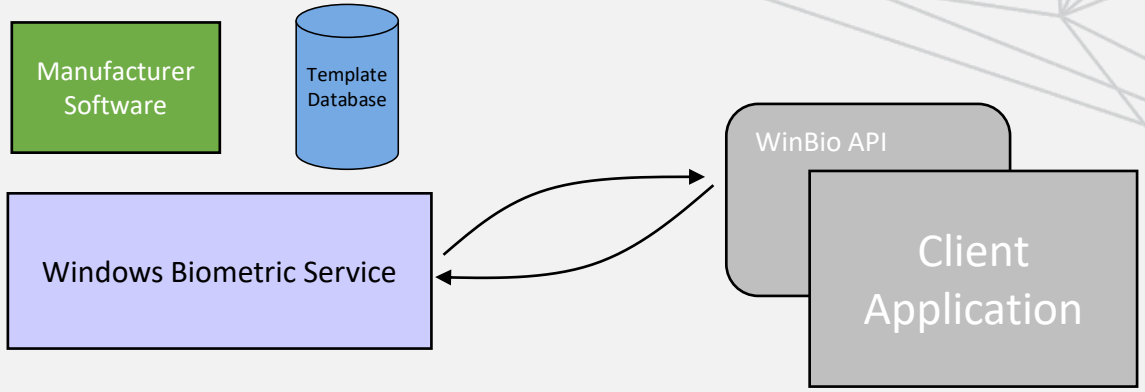
Windows Hello

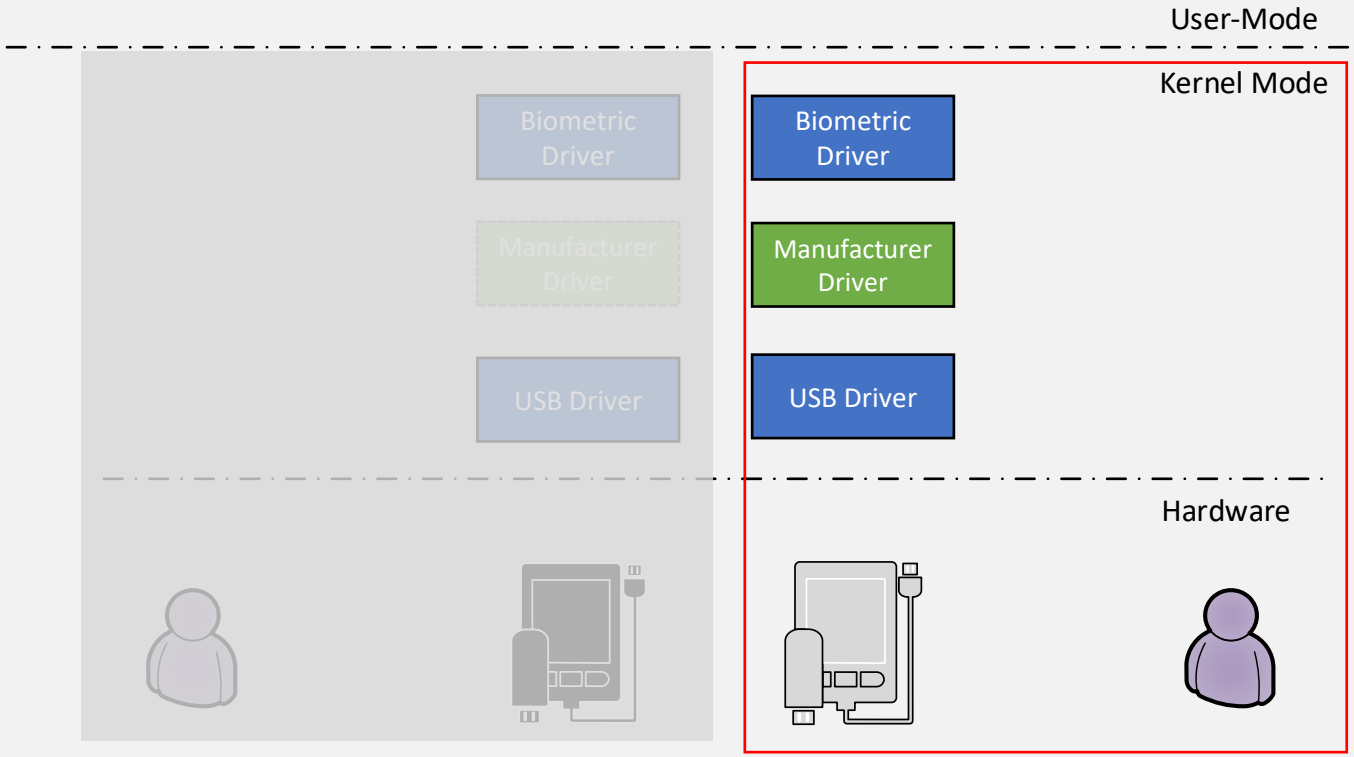
- Simplified view



Windows Hello

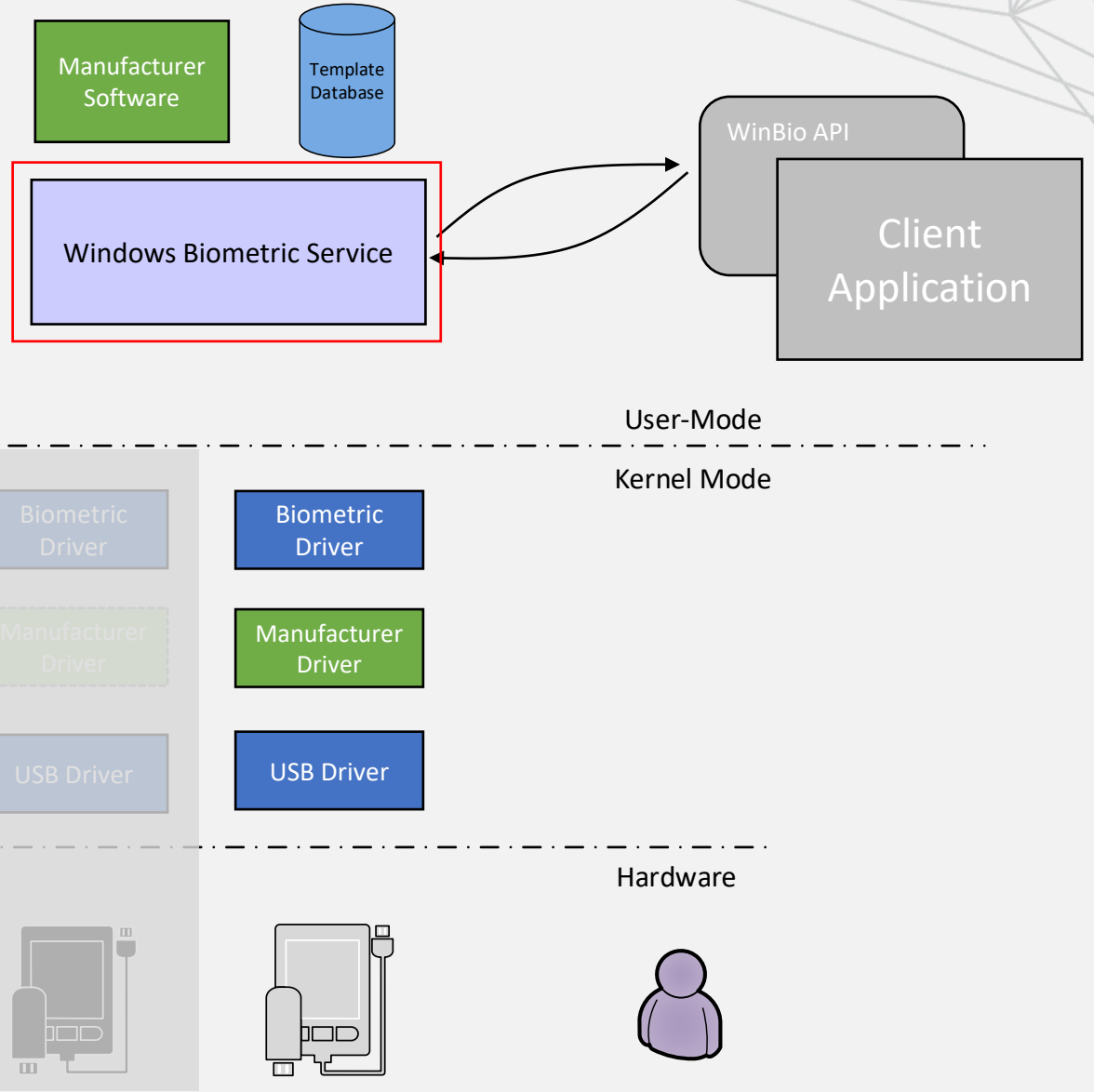
- Simplified view





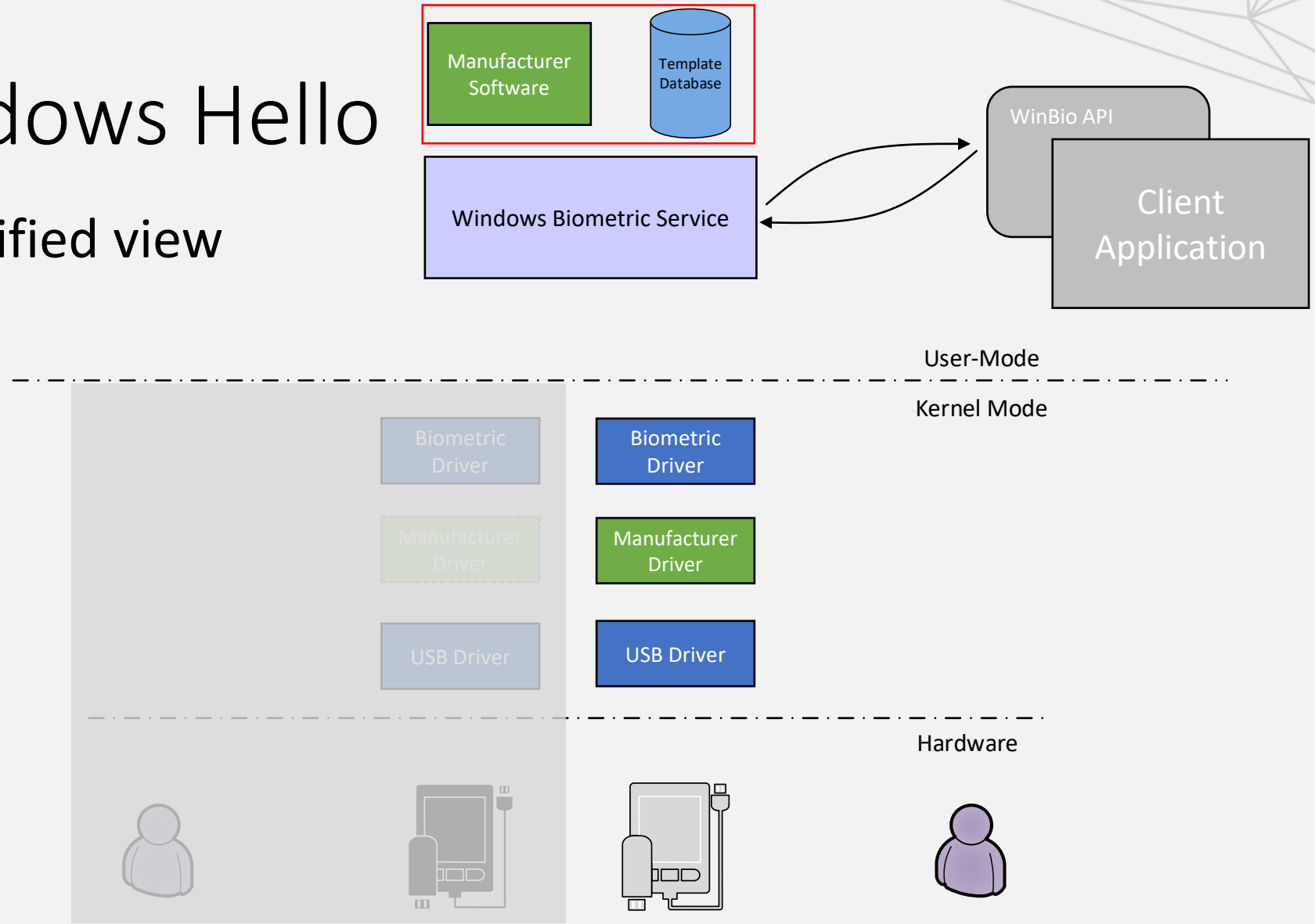
Windows Hello

- Simplified view

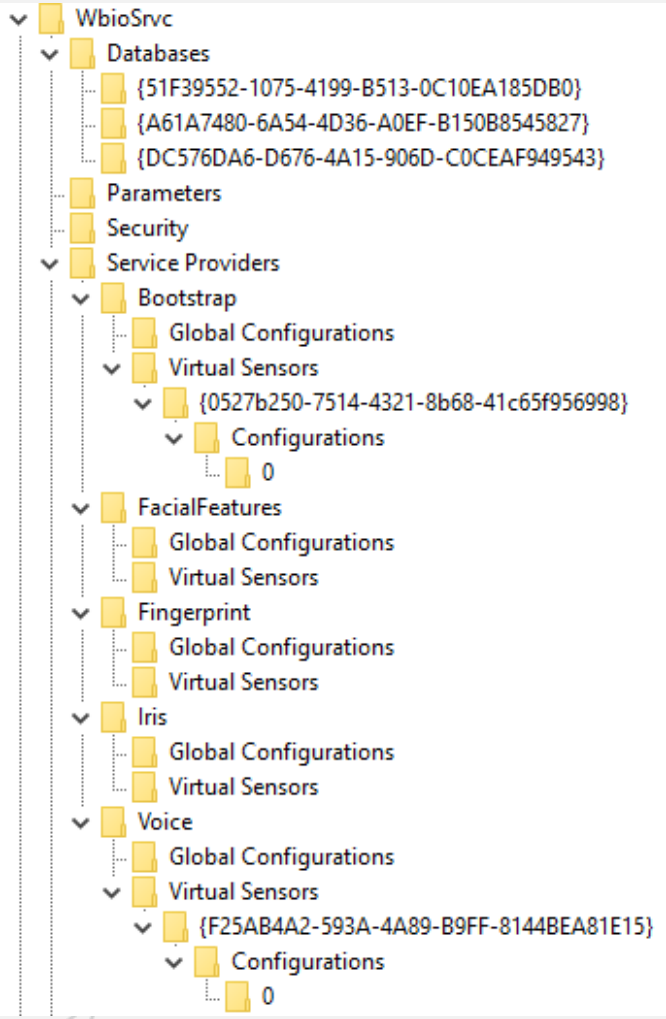


Windows Hello

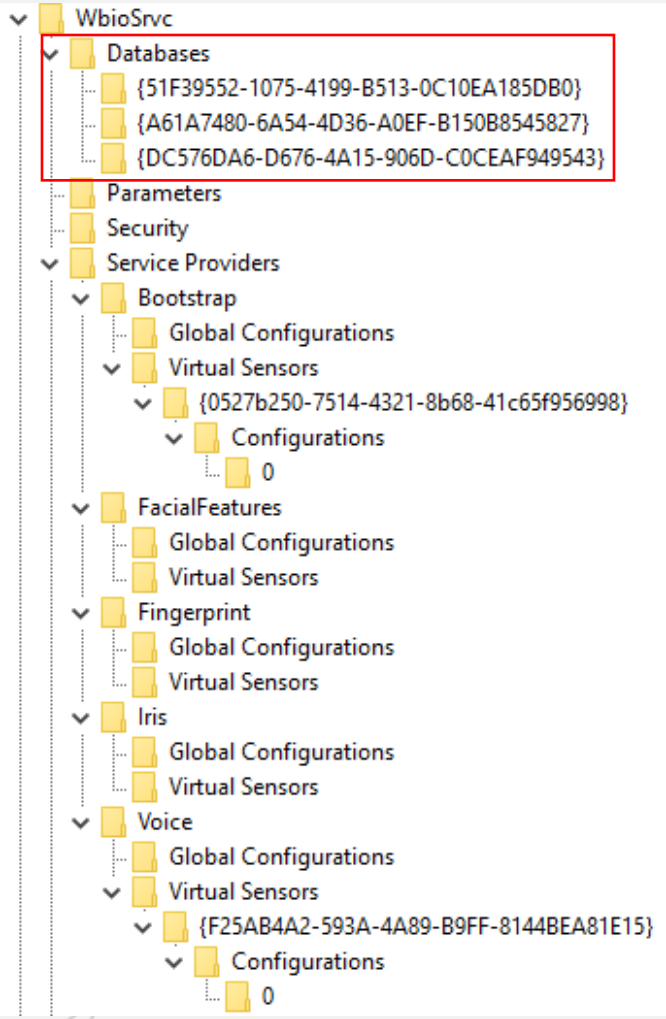
- Simplified view

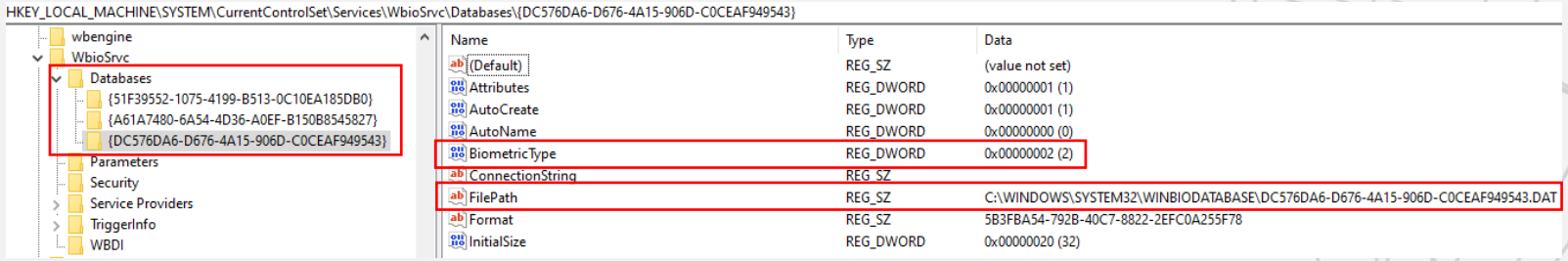


Windows Biometric Service – Configuration

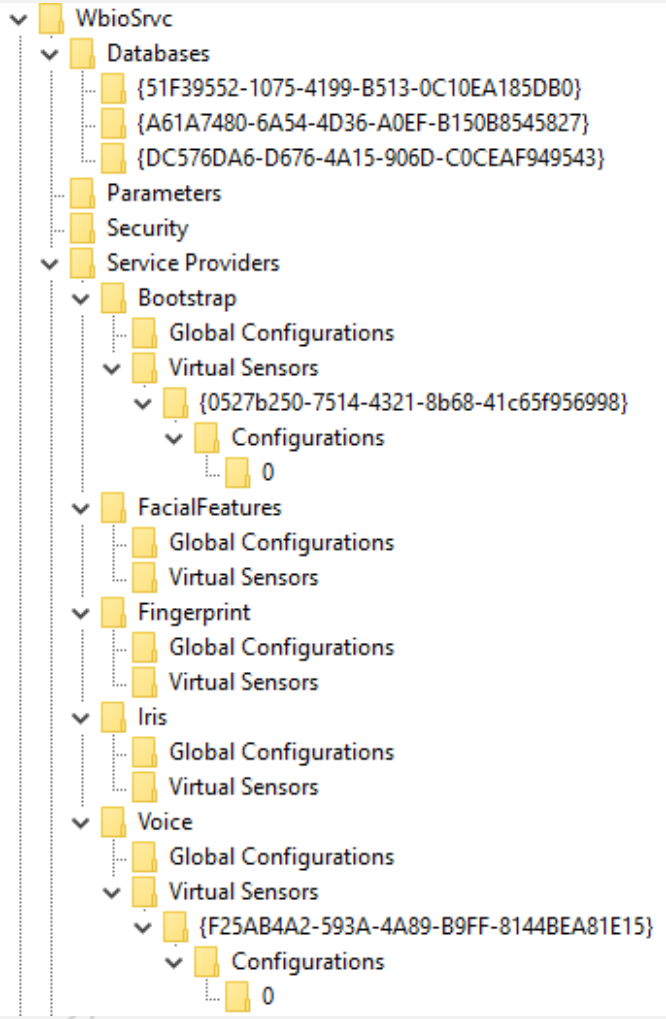


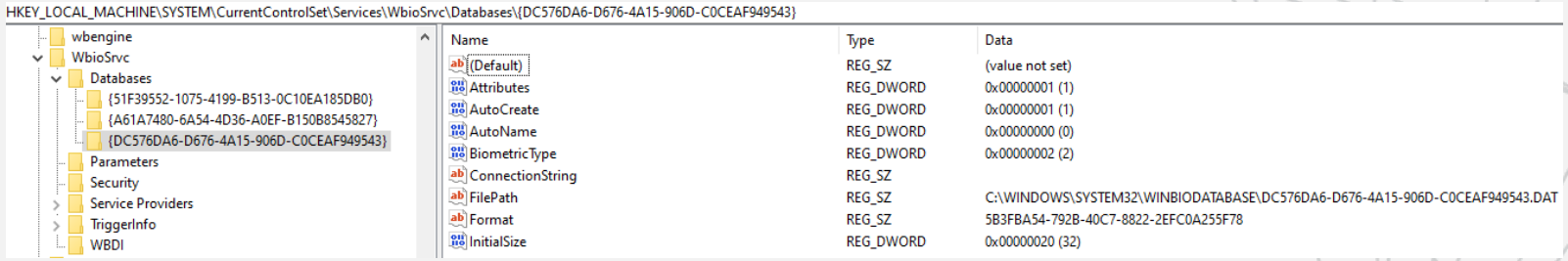
Windows Biometric Service – Configuration



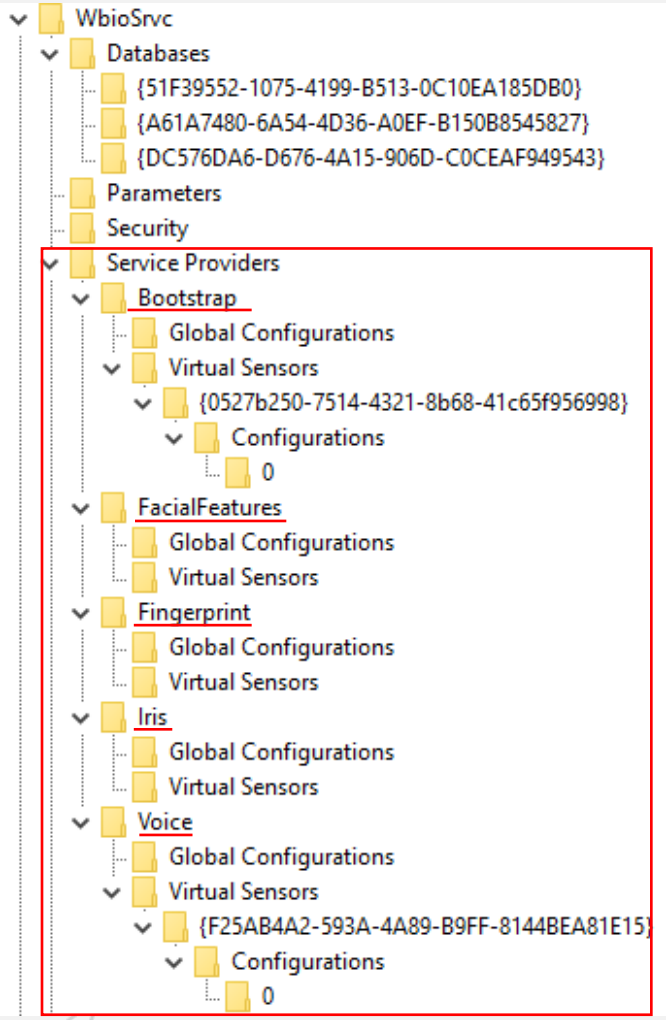


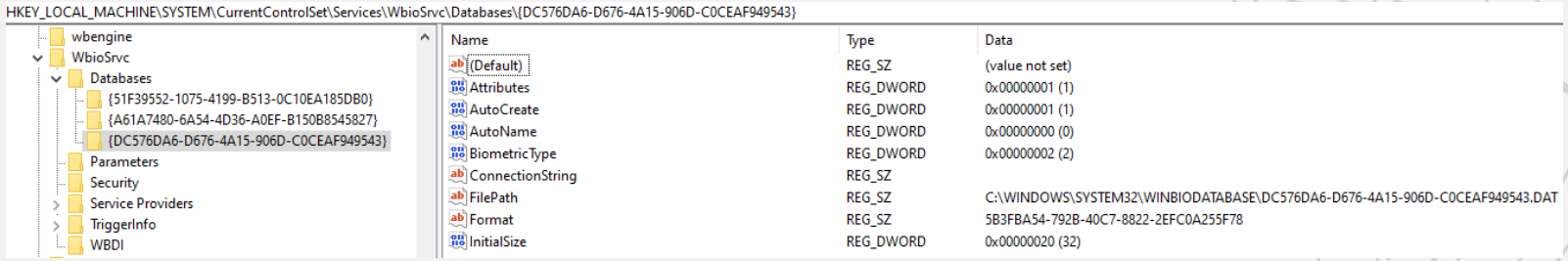
Windows Biometric Service – Configuration



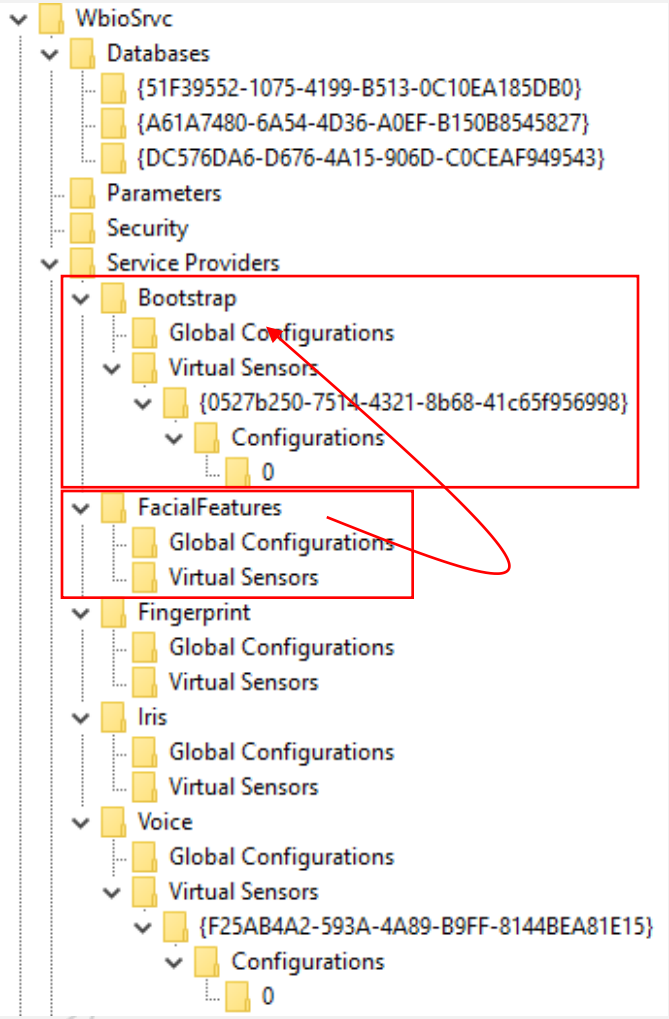


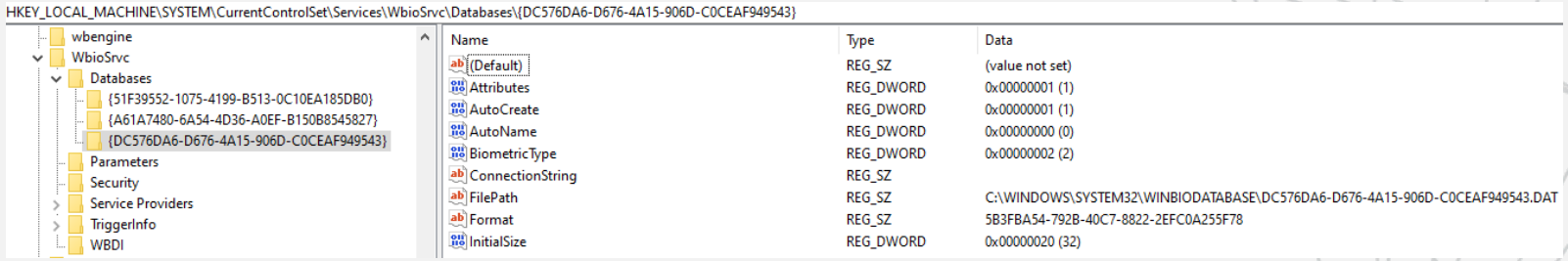
Windows Biometric Service – Configuration



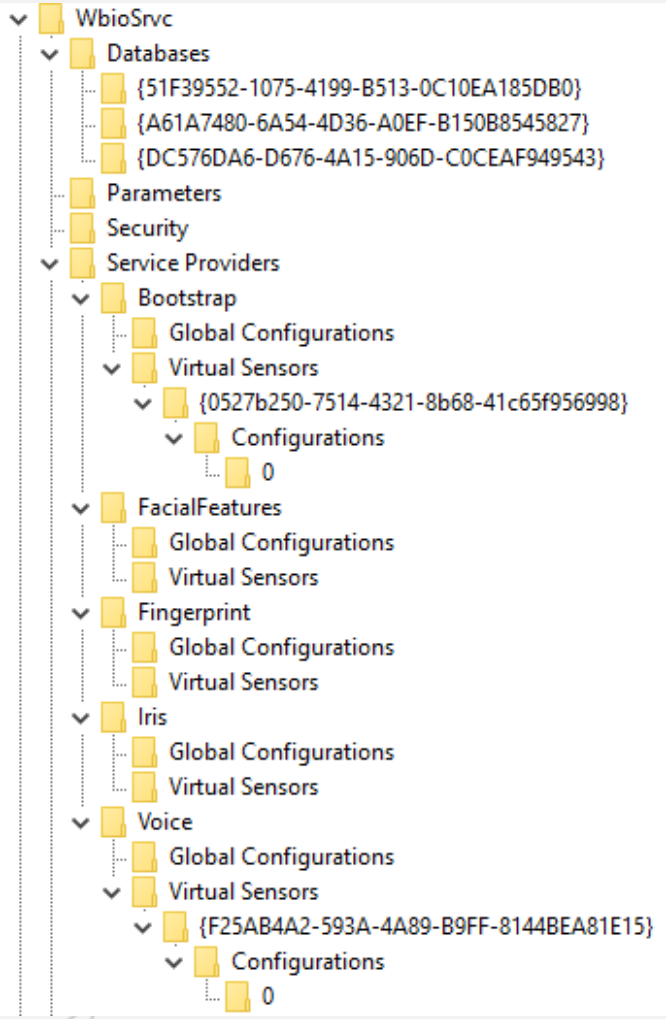


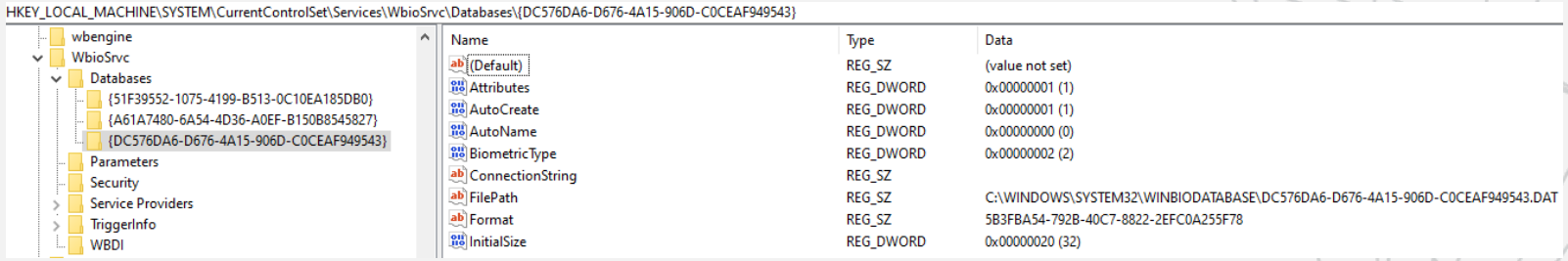
Windows Biometric Service – Configuration



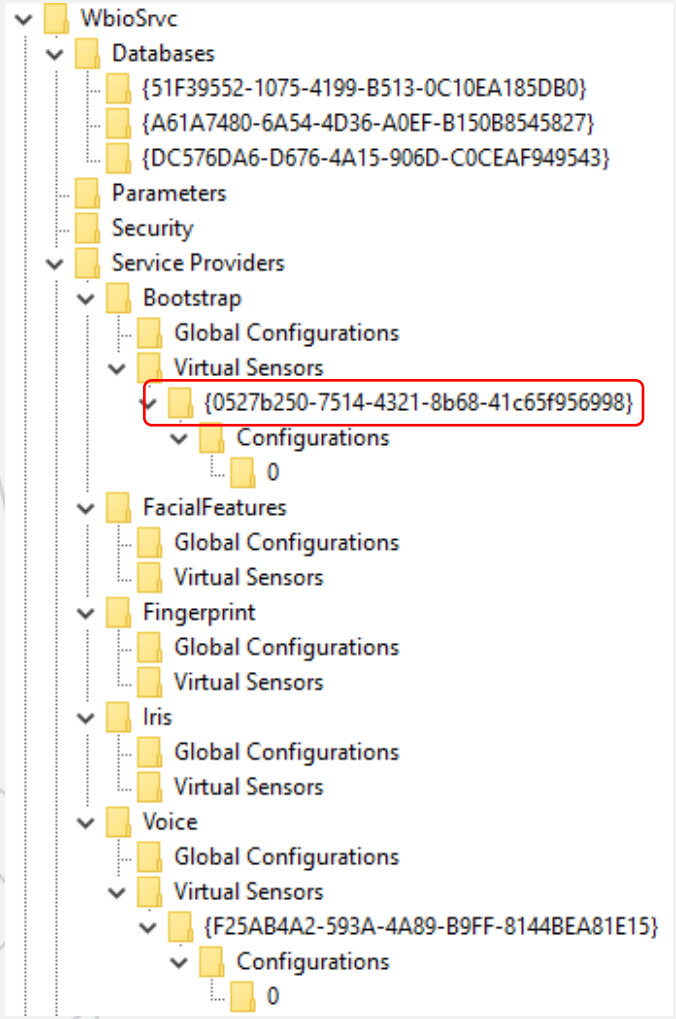


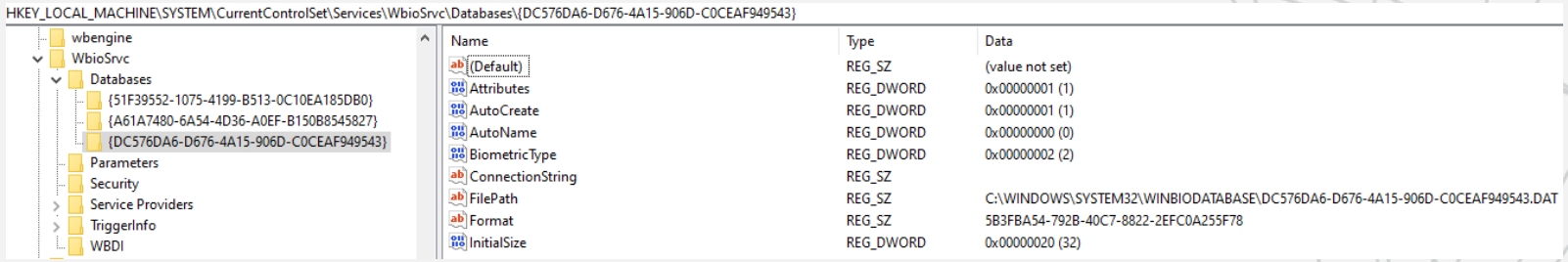
Windows Biometric Service – Configuration

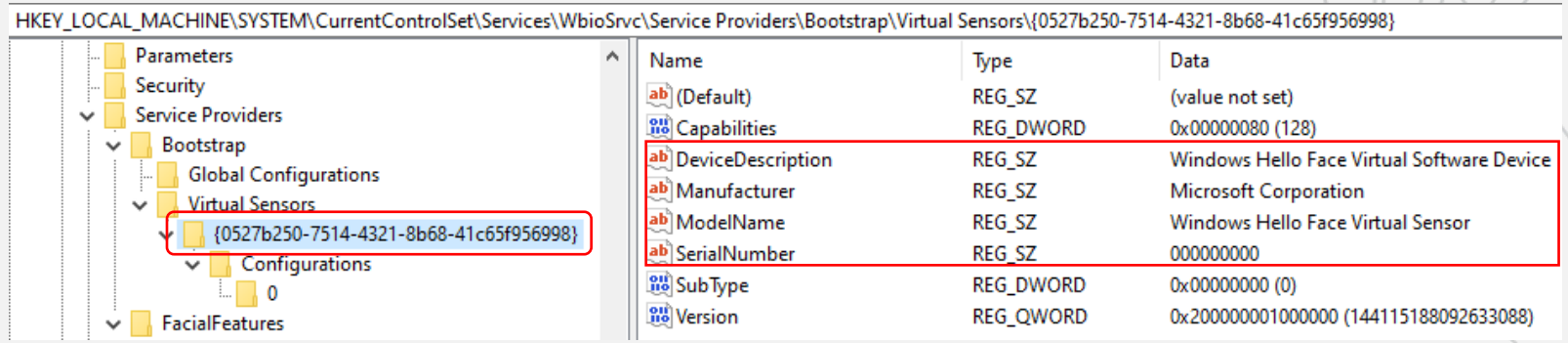




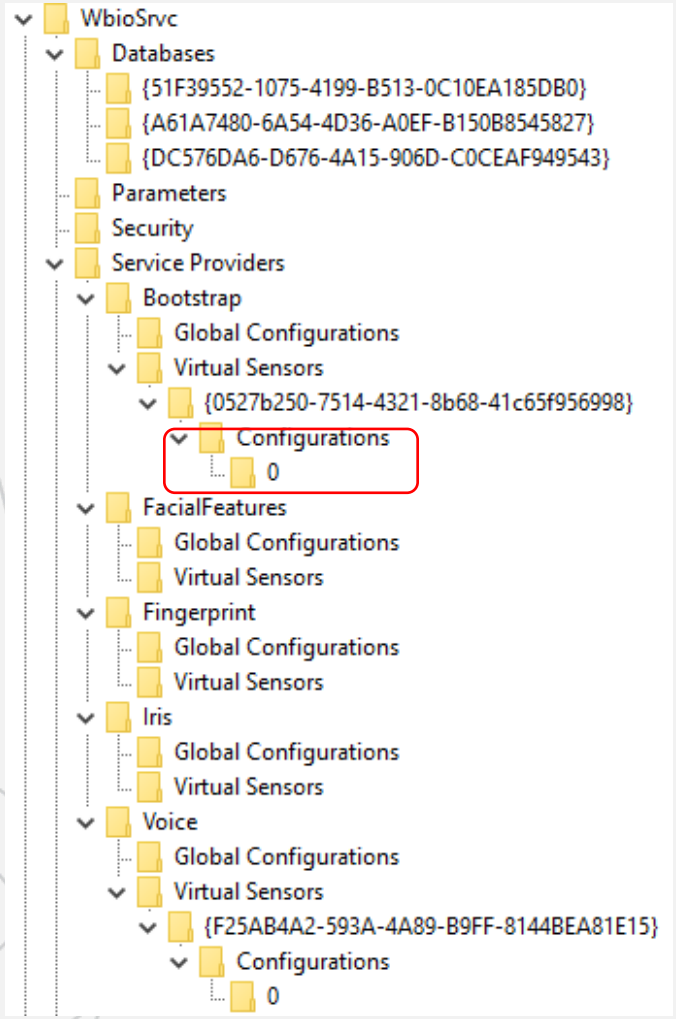
Windows Biometric Service – Configuration

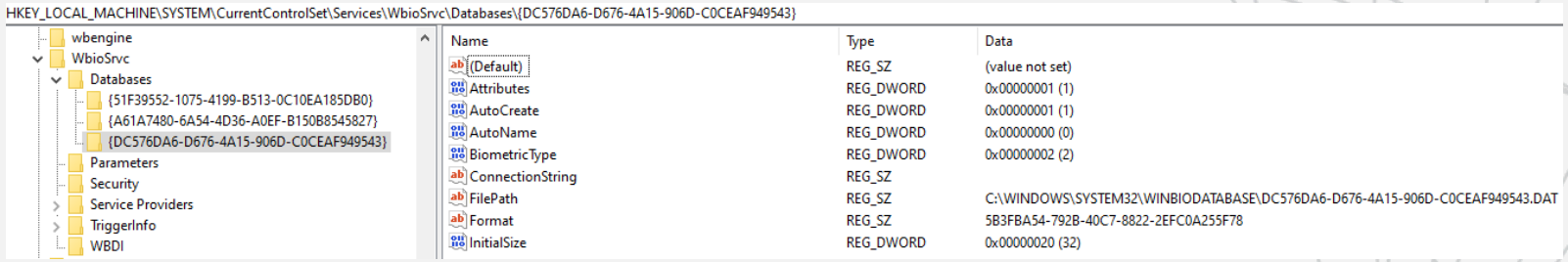


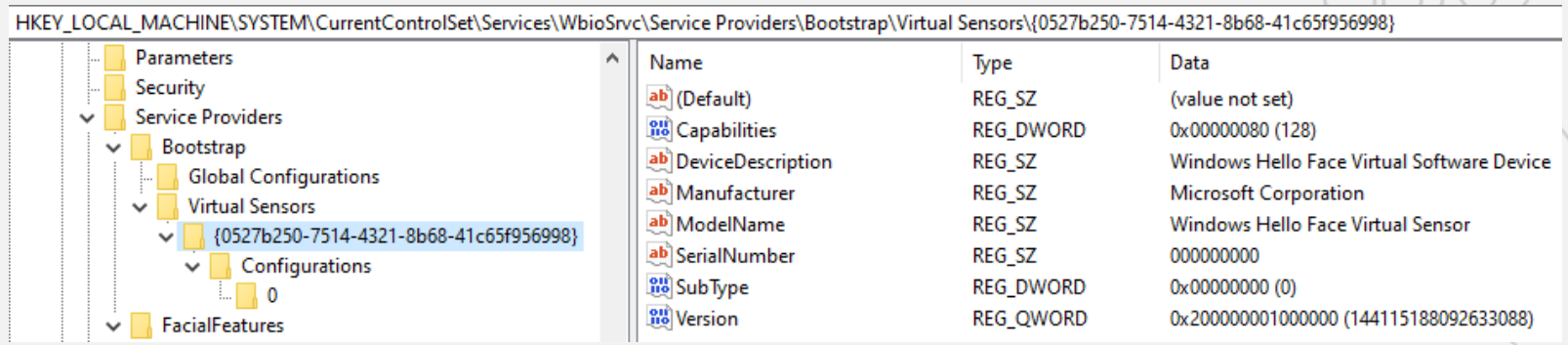


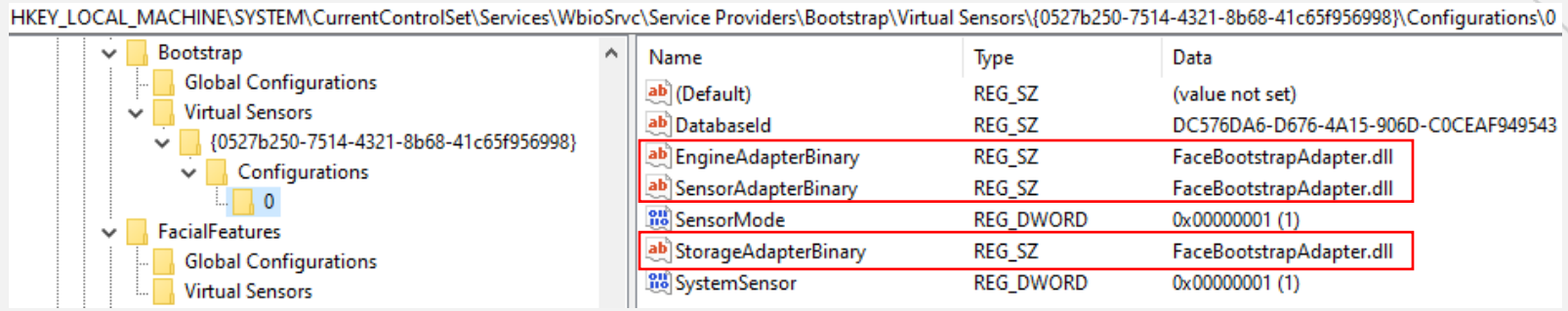


Windows Biometric Service – Configuration

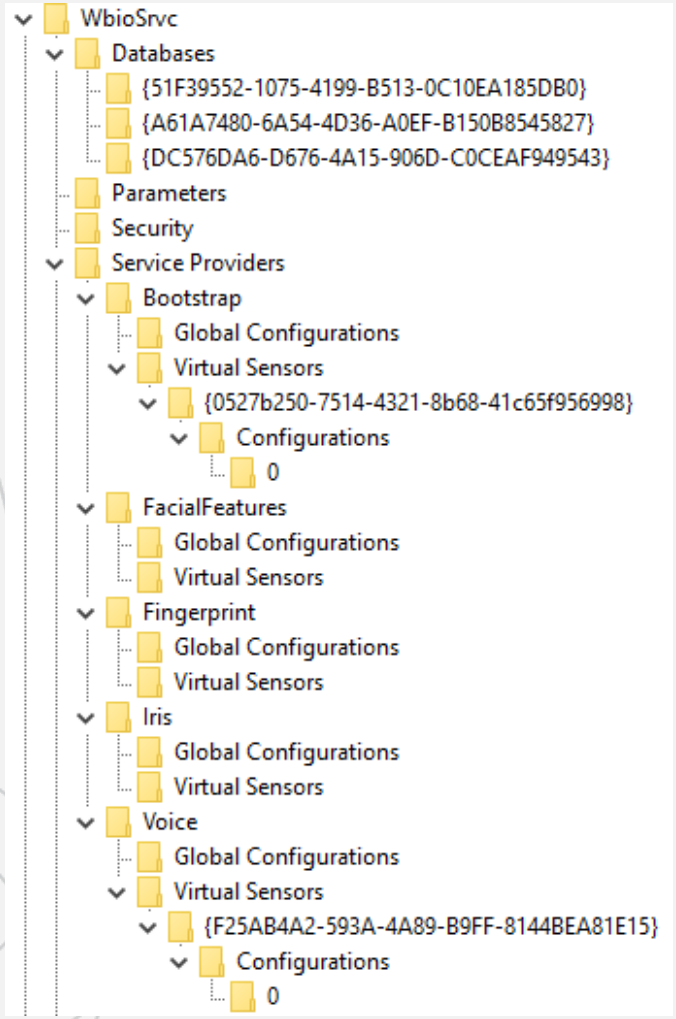


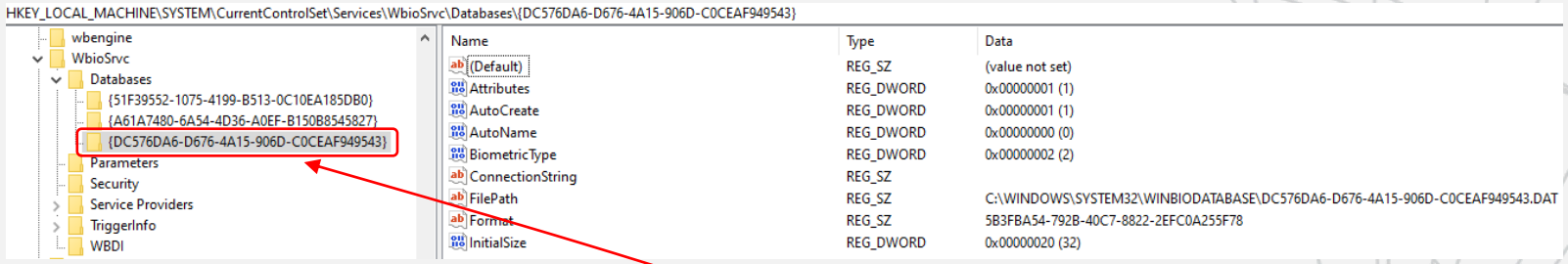


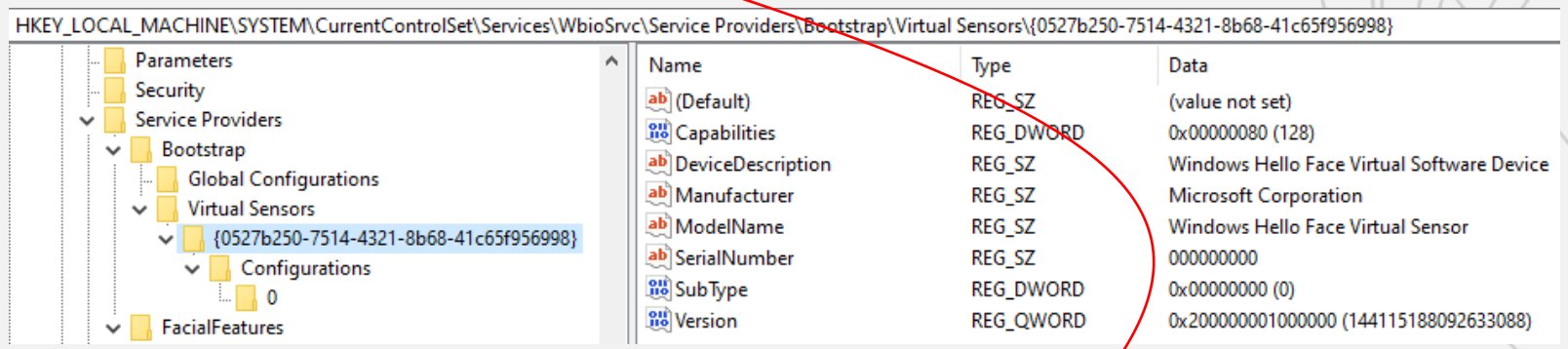


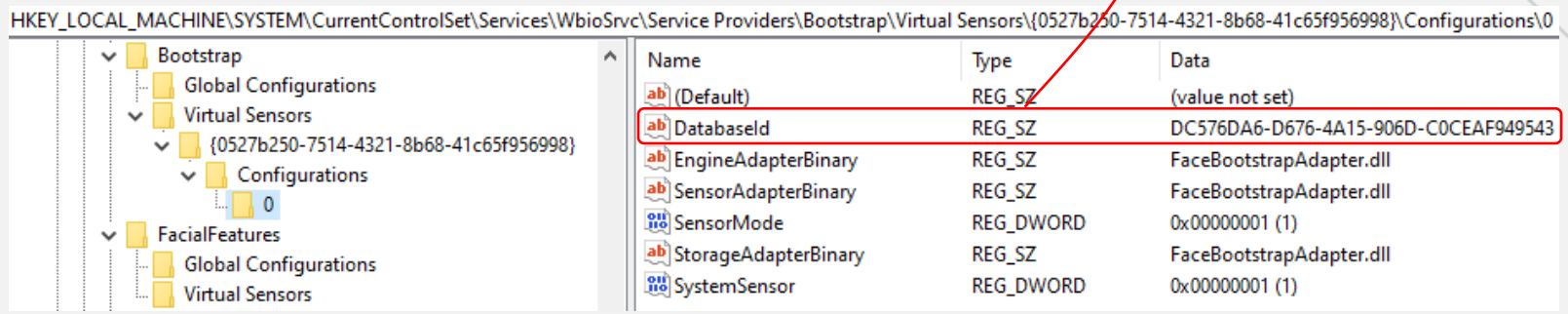


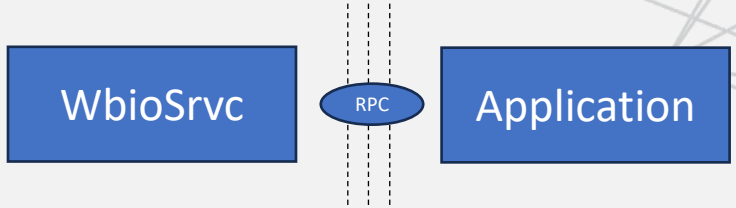
Windows Biometric Service – Configuration











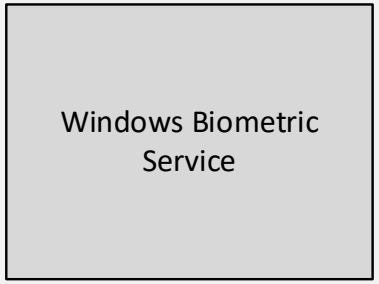
WbioSrvc RPC Interface

- RPC Interface:
- Windows Biometric service provides is running as "NT Authority\SYSTEM".
- The two RPC interfaces are defined with the following UUIDs:
  - `C0E9671E-33C6-4438-9464-56B2E1B1C7B4`: WinBioService interface
  - `4BE96A0F-9F52-4729-A51D-C70610F118B0`: WinBioCredentialManager interface
- These RPC interfaces are open to any user in the system.
  - SDDL: "`D:(A;;GA;;;WD)(A;;GA;;;AC)`“
- This dual architecture …
  - Service running in NT Authority\SYSTEM
  - Application interfacing with RPC
- … allows an isolation of the biometrics in memory

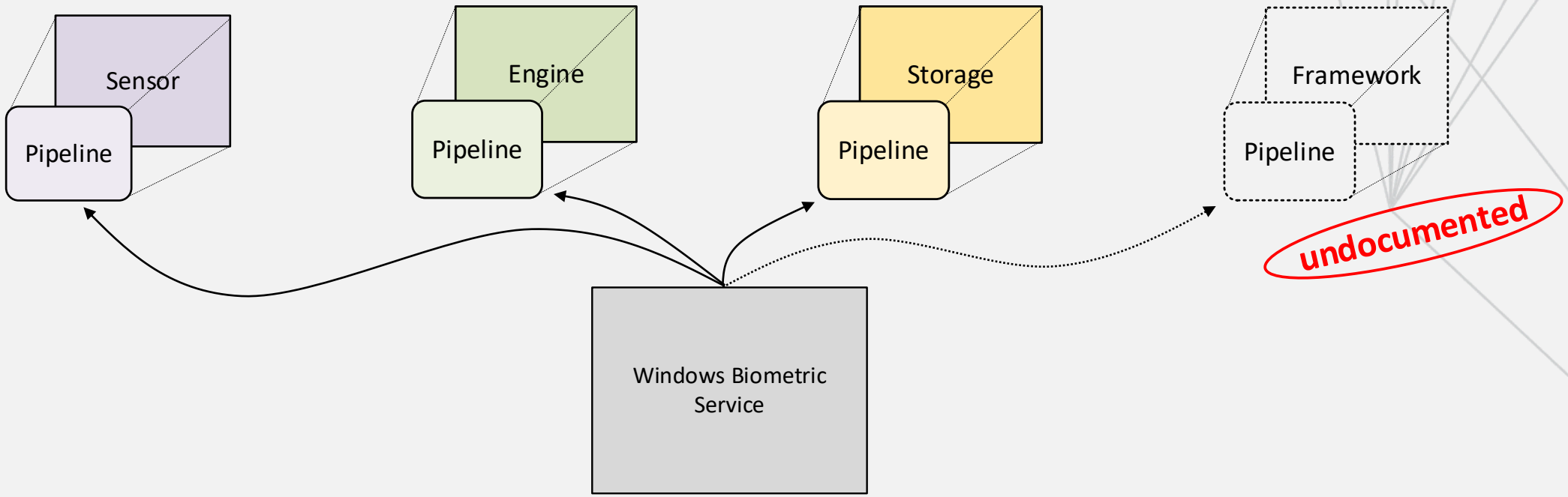
```
1  WinBioSrvOpenFrameworkSession
2  WinBioSrvCloseFrameworkSession
3  WinBioSrvEnumBiometricUnits
4  WinBioSrvEnumServiceProviders
5  WinBioSrvMonitorFrameworkChanges
6  WinBioSrvOpenBiometricSession
7  WinBioSrvCloseBiometricSession
8  WinBioSrvCancel
9  WinBioSrvVerify
10 WinBioSrvIdentify
11 WinBioSrvVerifyAndReleaseTicket
12 WinBioSrvIdentifyAndReleaseTicket
13 WinBioSrvLocateSensor
14 WinBioSrvEnrollAuthorize
15 WinBioSrvEnrollRevoke
16 WinBioSrvEnrollBegin
17 WinBioSrvEnrollSelect
18 WinBioSrvEnrollCapture
19 WinBioSrvEnrollCommit
20 WinBioSrvEnrollDiscard
21 WinBioSrvEnumEnrollments
22 WinBioSrvGetEvent
23 WinBioSrvGetPresenceData
24 WinBioSrvCaptureSample
25 WinBioSrvDeleteTemplate
26 WinBioSrvLockUnit
27 WinBioSrvUnlockUnit
28 WinBioSrvControlUnit
29 WinBioSrvControlUnitPrivileged
30 WinBioSrvGetProperty
31 WinBioSrvSetProperty
32 WinBioSrvAcquireFocus
33 WinBioSrvReleaseFocus
34 WinBioSrvLogonIdentifiedUser
35 _BioSrvGetLogonUserIdentity
36 WinBioSrvProtectData
37 WinBioSrvUnprotectData
38 WinBioSrvDiscardTicket
39 WinBioSrvGetGestureMetadata
40 WinBioSrvNgcOpenAuthorizationSession
41 WinBioSrvNgcAuthorizeEnrollment
42 WinBioSrvNgcCloseAuthorizationSession
43 WinBioSrvNgcGetAuthorizationWithTicket
```

```
1 WinBioCredMgrSrvSetCredential
2 WinBioCredMgrSrvRemoveCredential
3 WinBioCredMgrSrvRemoveAllCredentials
4 WinBioCredMgrSrvRemoveAllDomainCredentials
5 WinBioCredMgrSrvGetCredentialState
6 WinBioCredMgrSrvGetCredentialWithTicket
7 WinBioSrvGetServiceMonitorEvent
```

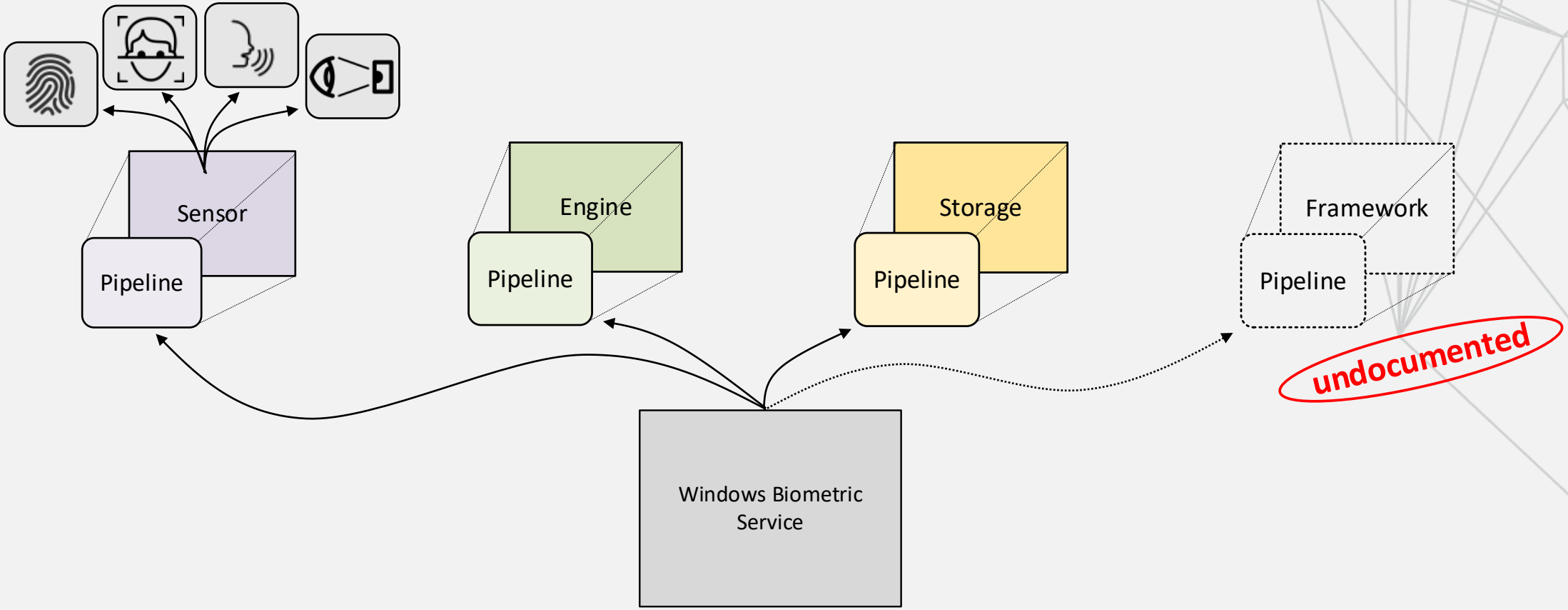
Biometric Unit



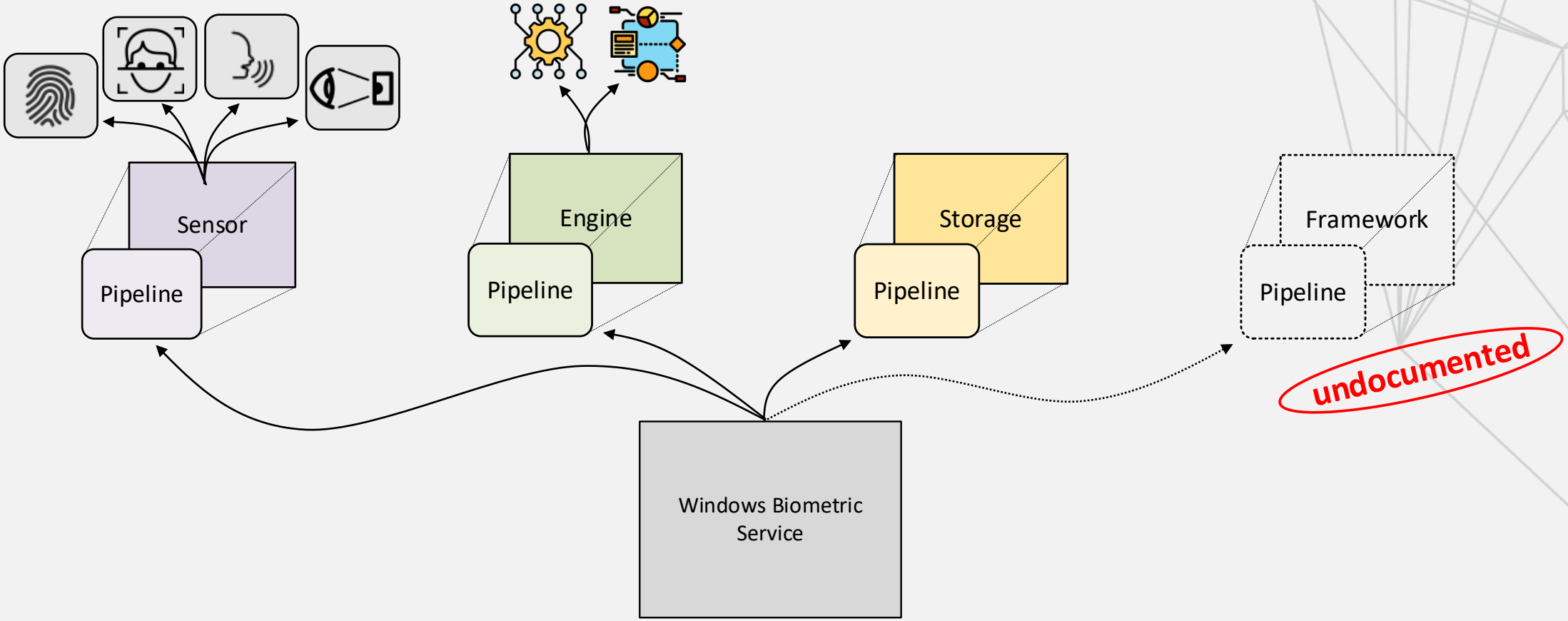
Biometric Unit



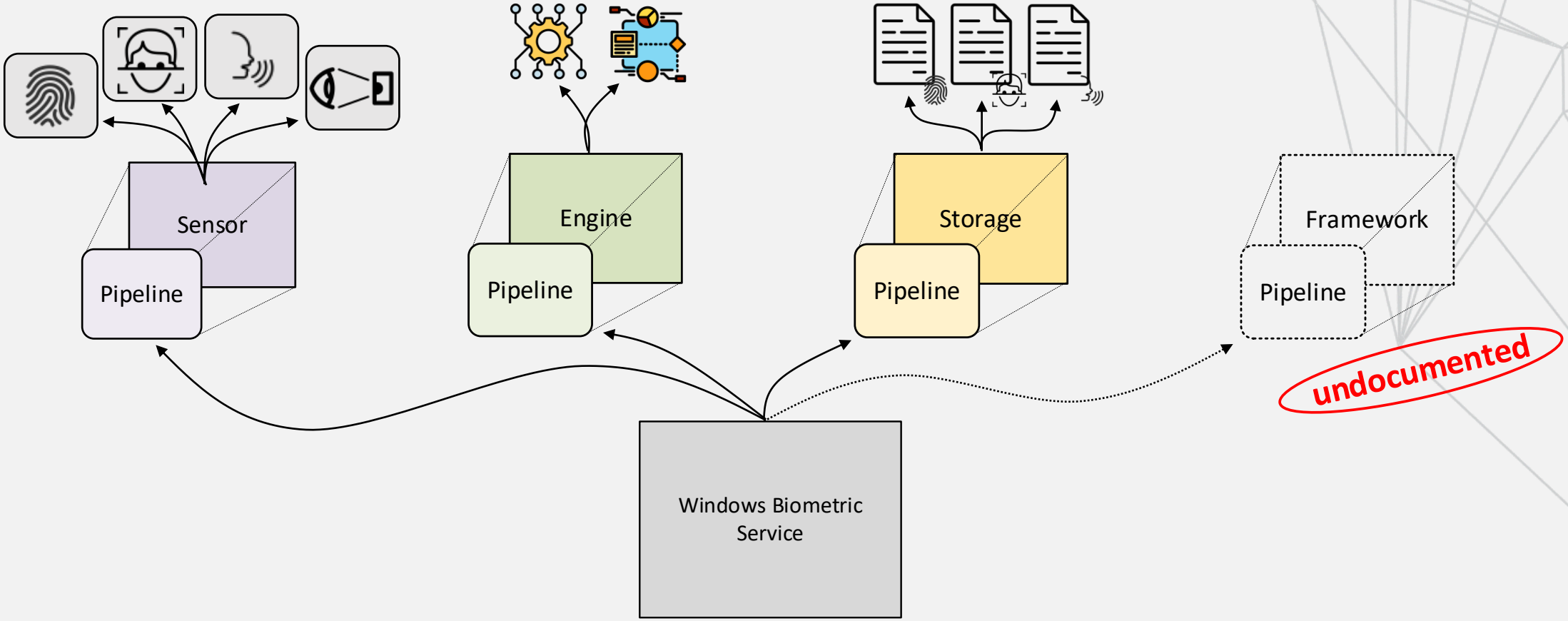
Biometric Unit



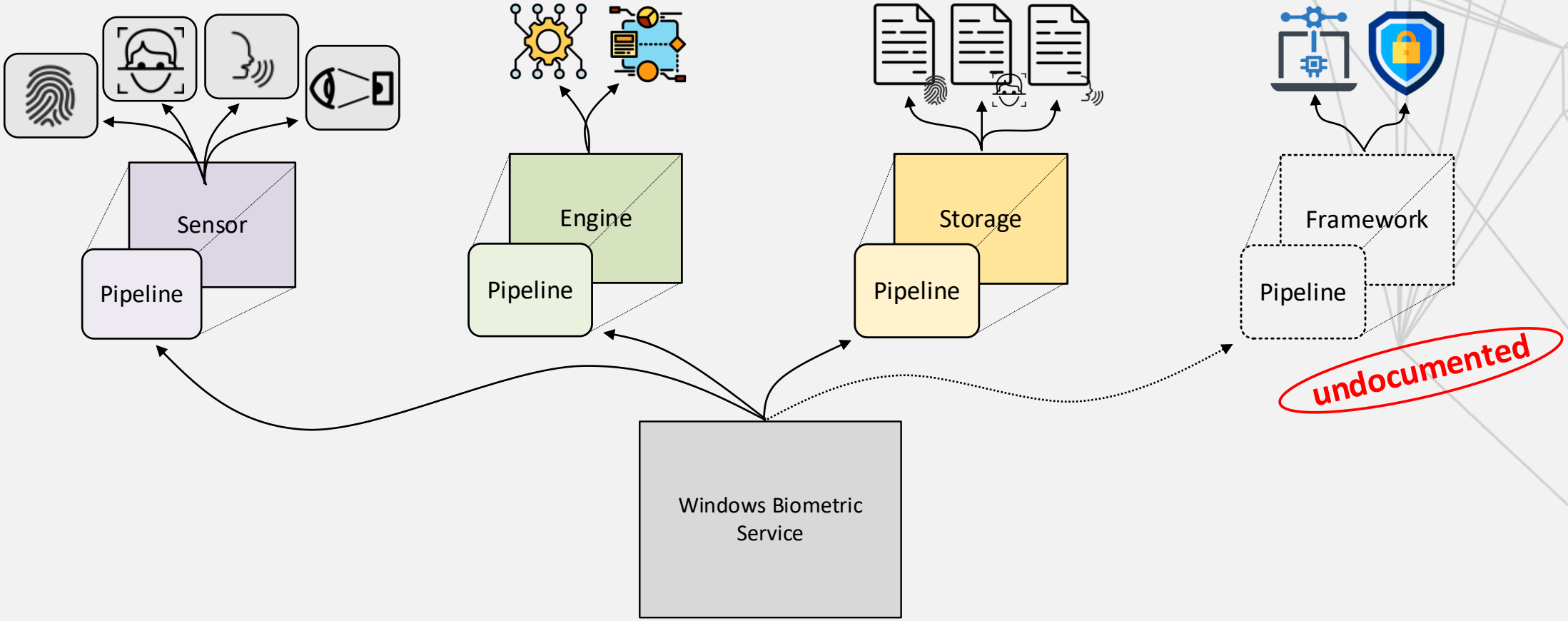
Biometric Unit



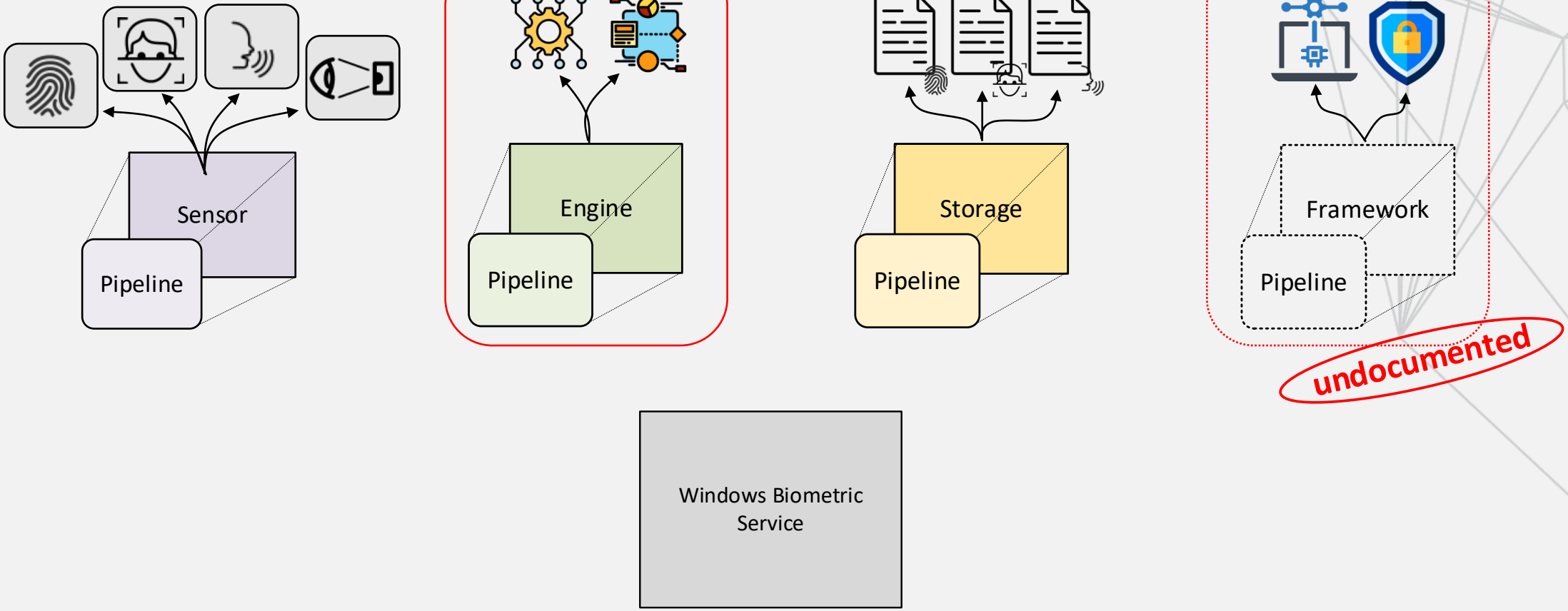
Biometric Unit



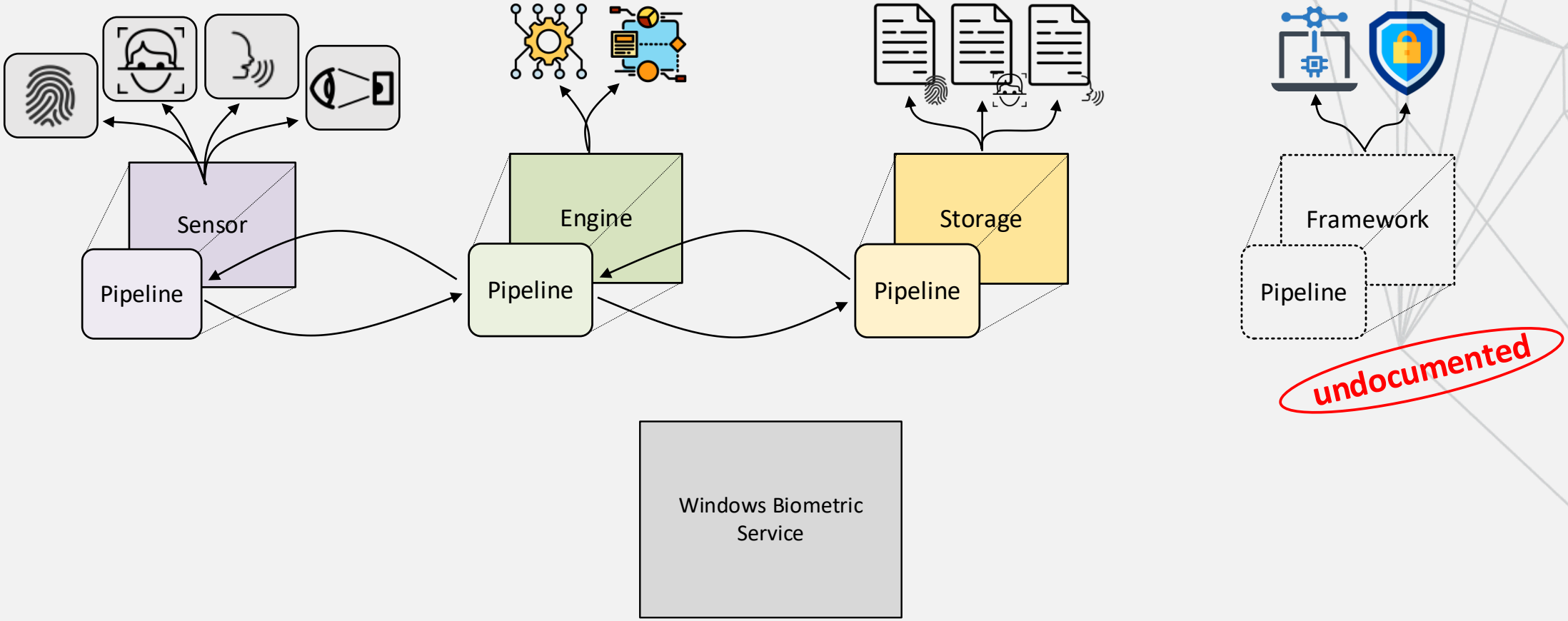
Biometric Unit



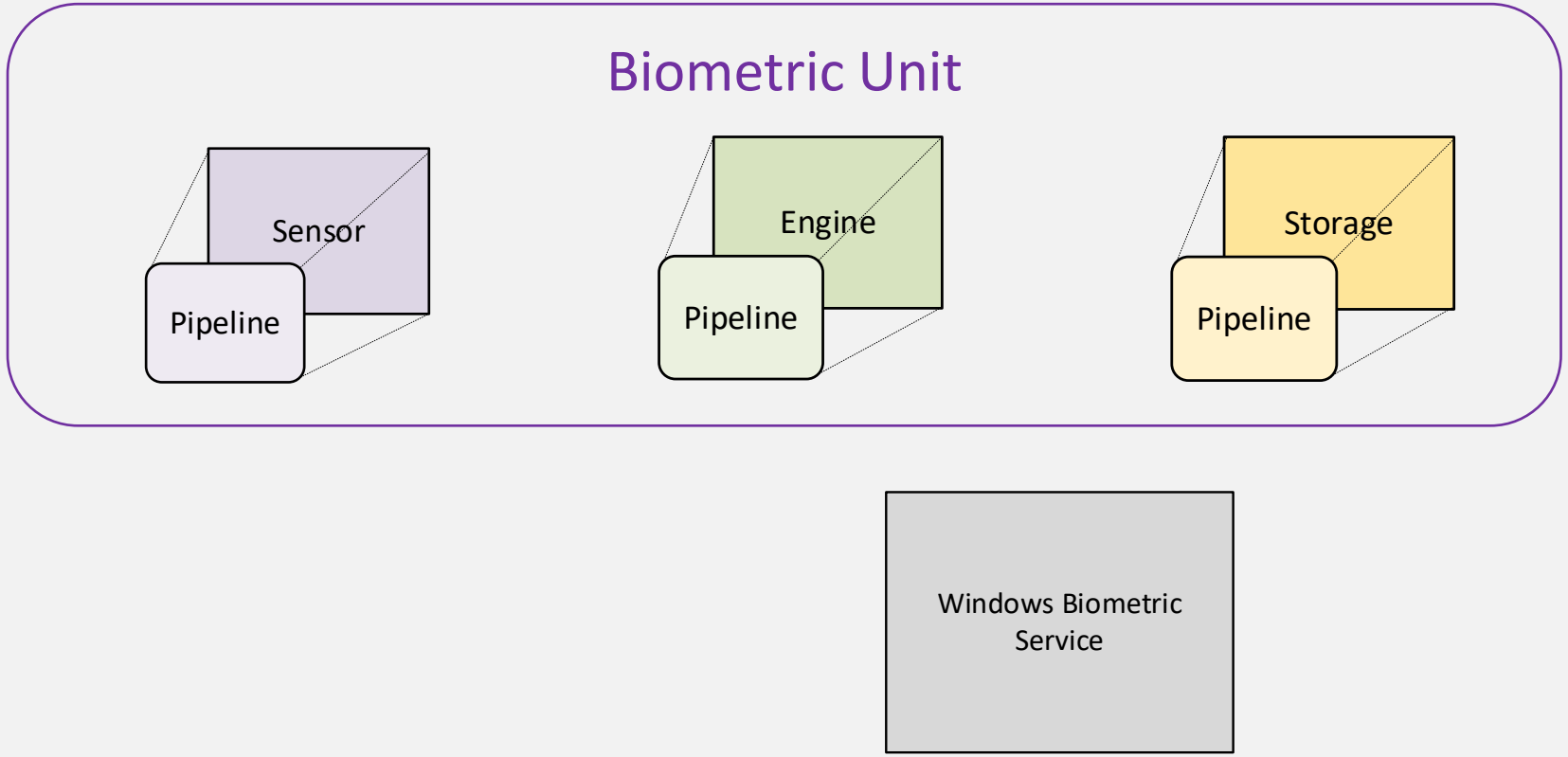
Biometric Unit



Biometric Unit



Biometric Unit



Biometric Unit – DLLs

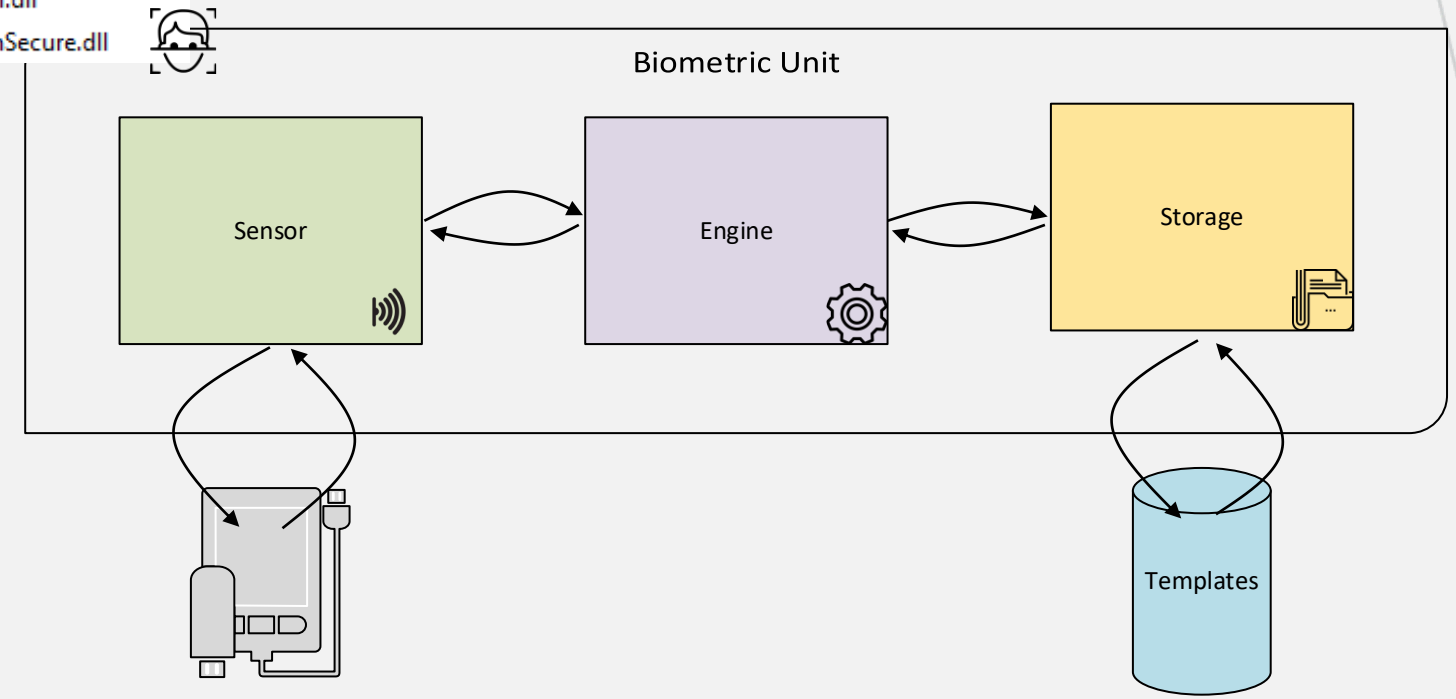
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

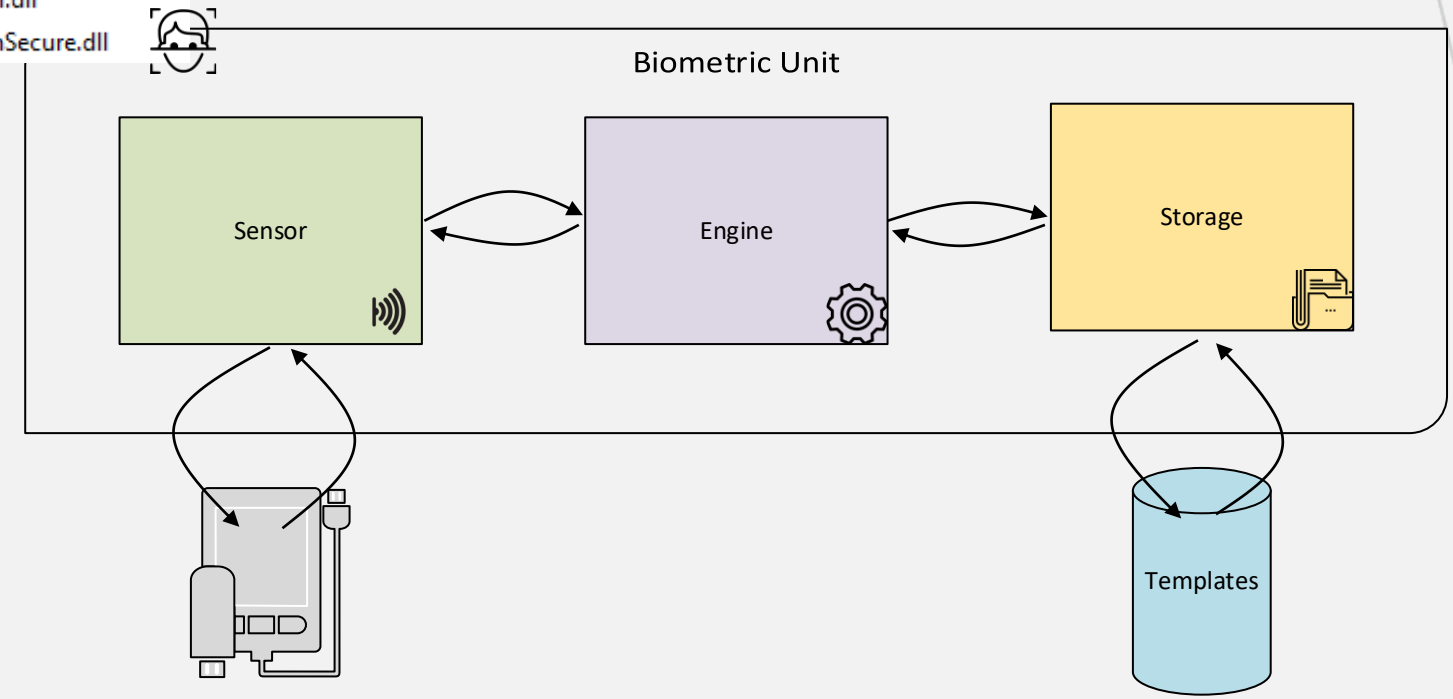
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

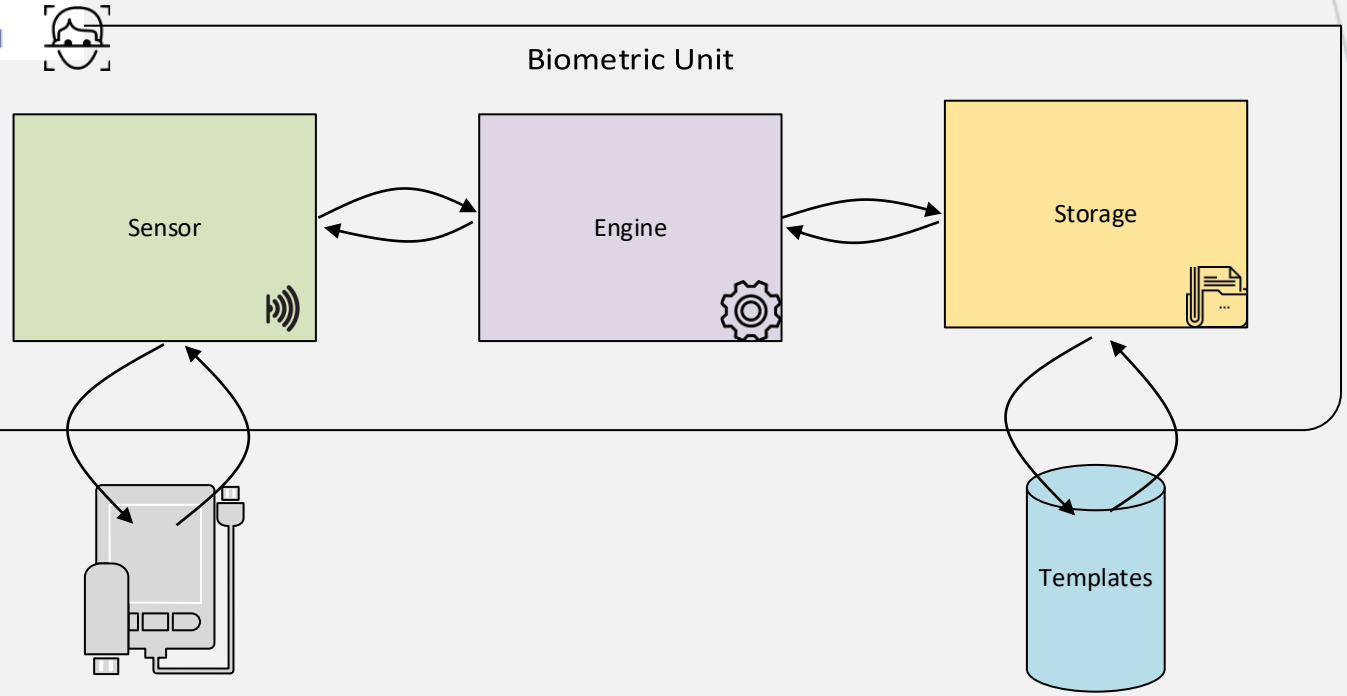
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

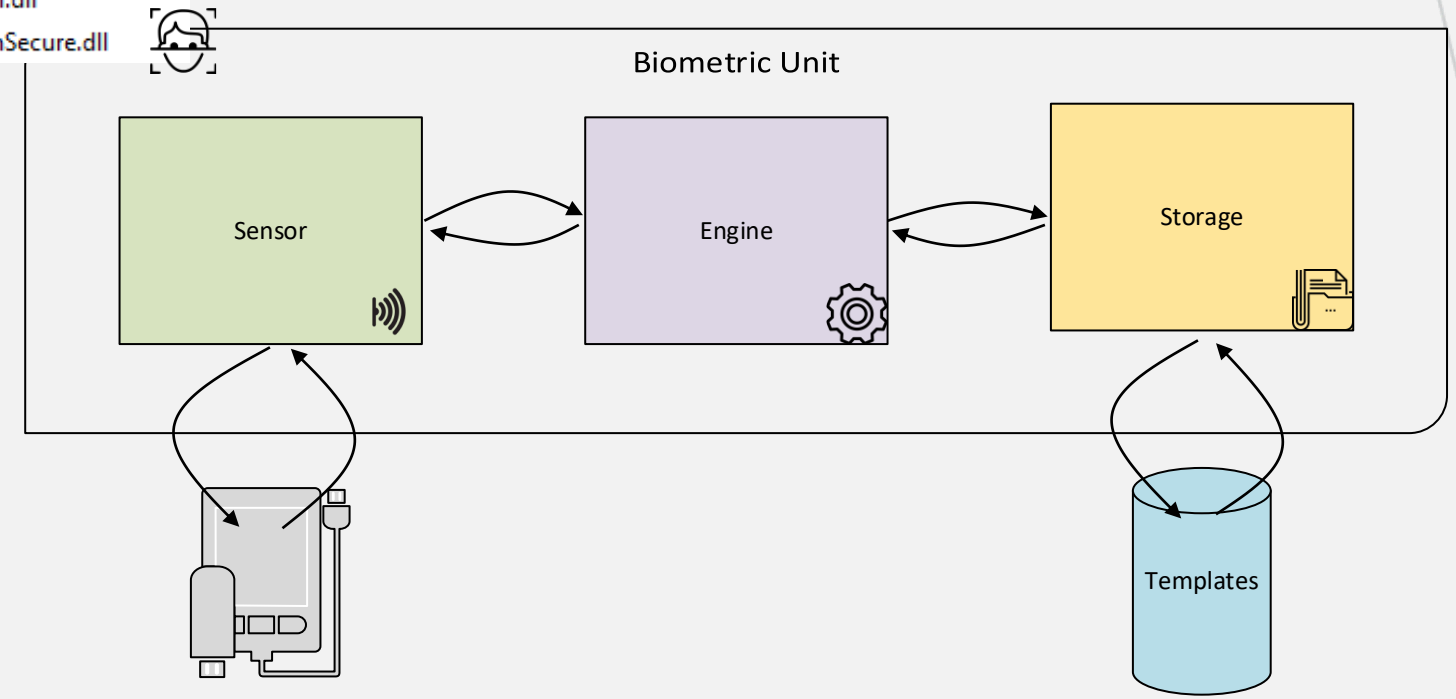
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

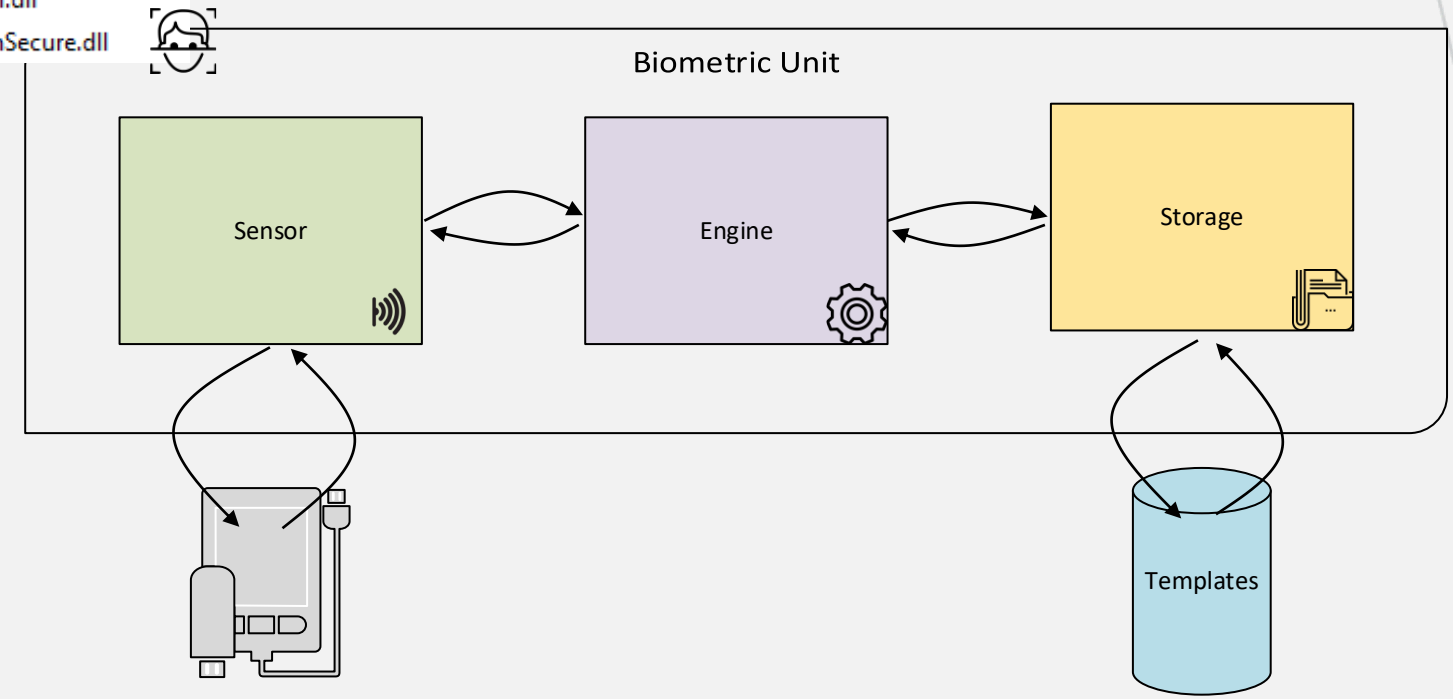
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

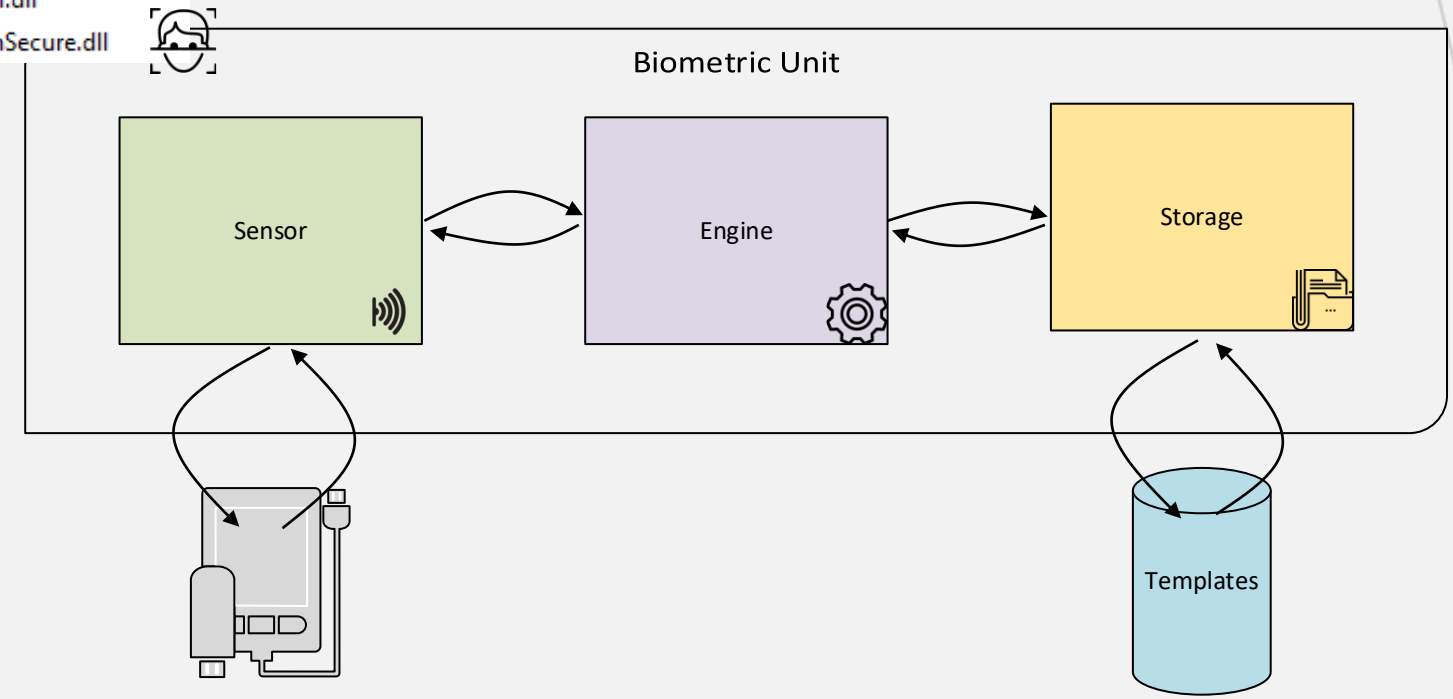
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

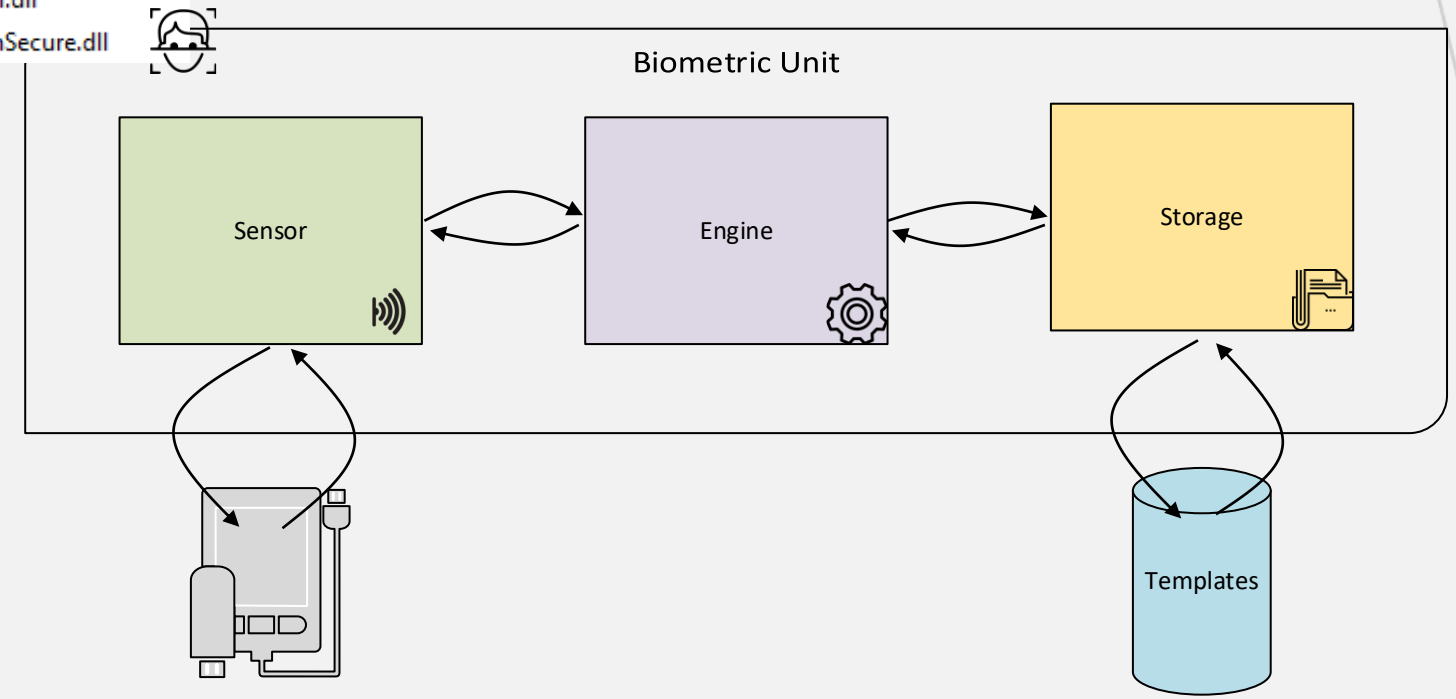
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

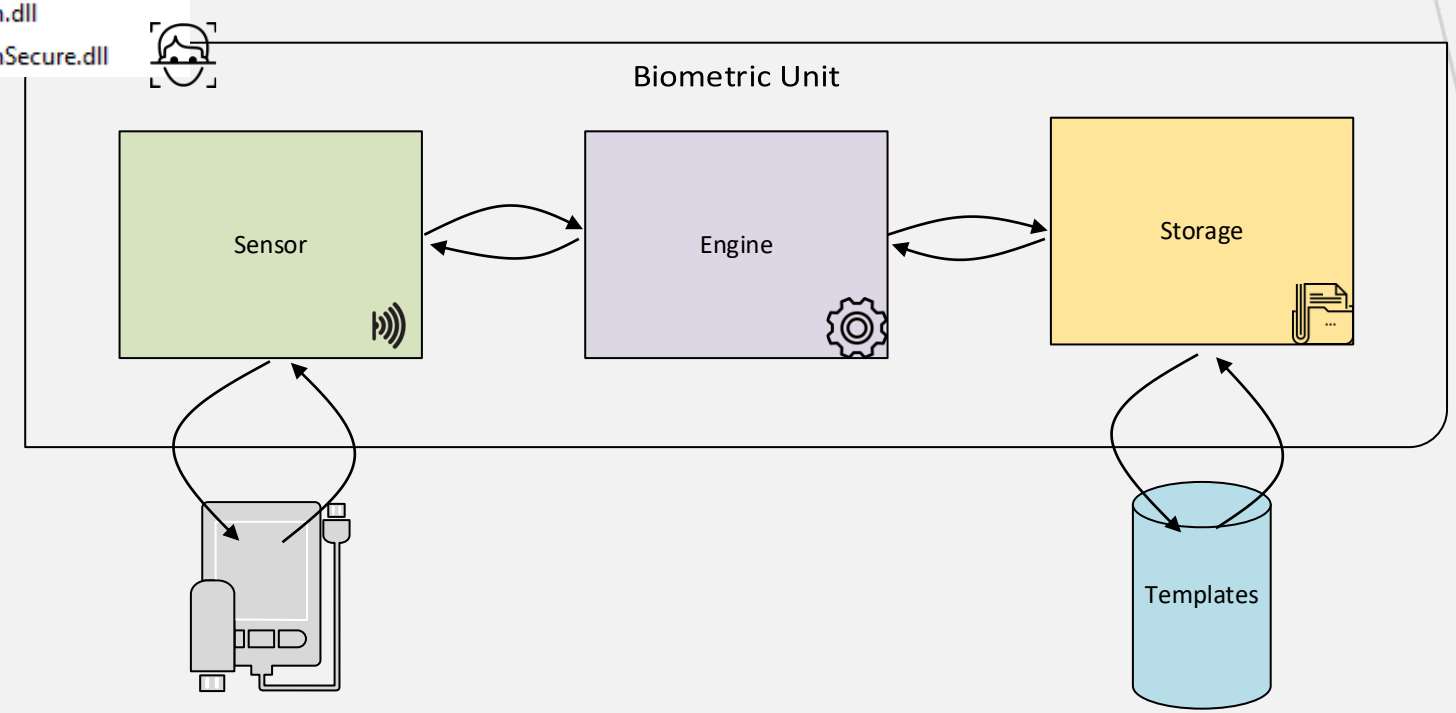
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

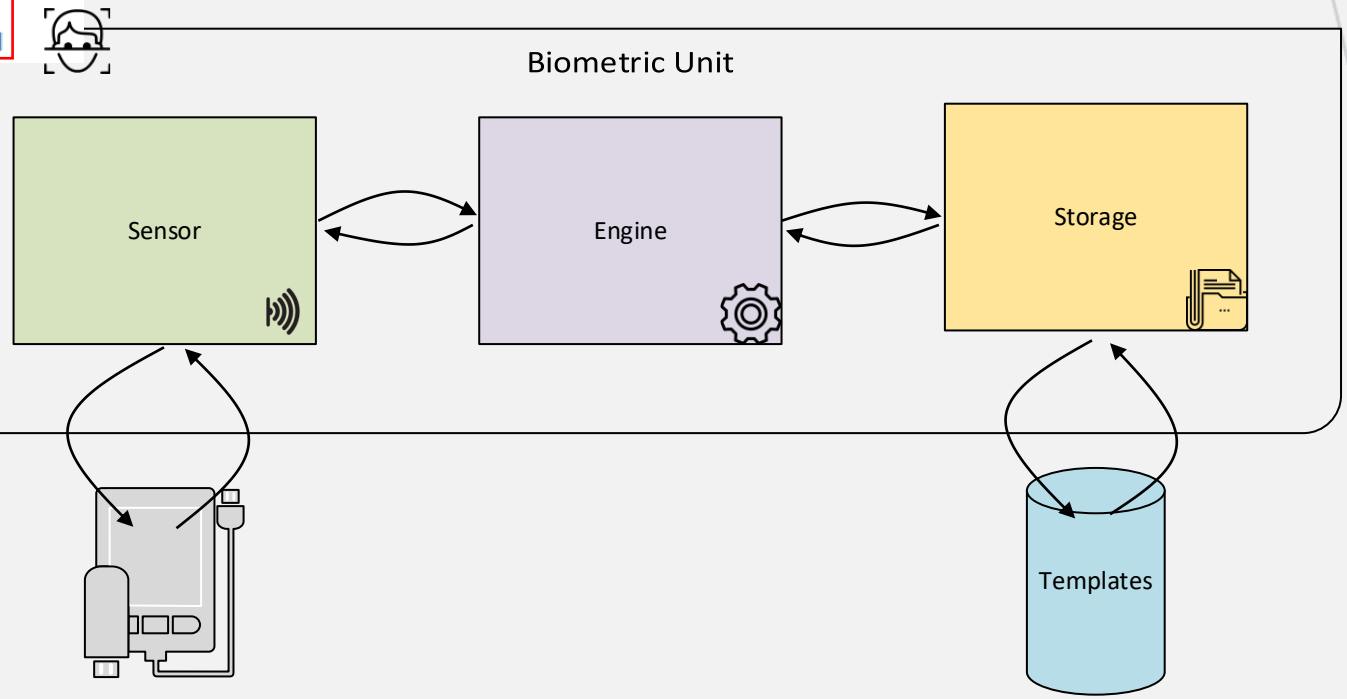
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

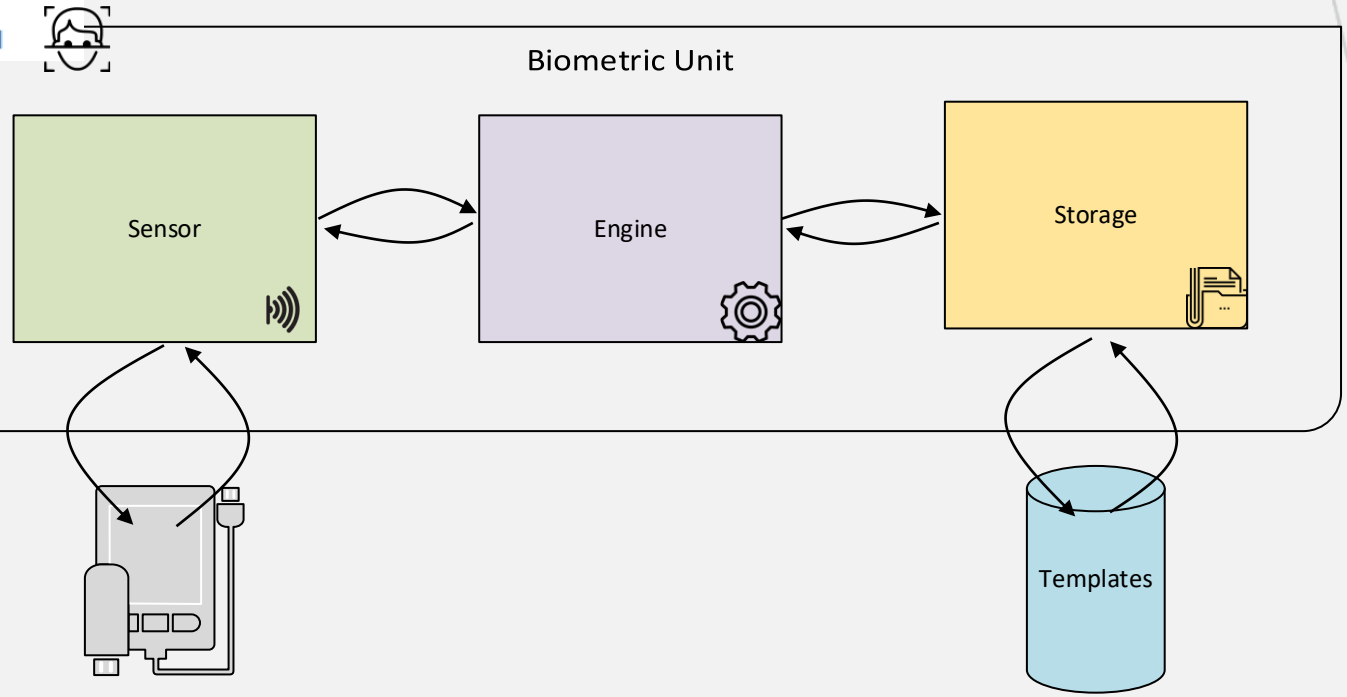
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



Biometric Unit – DLLs

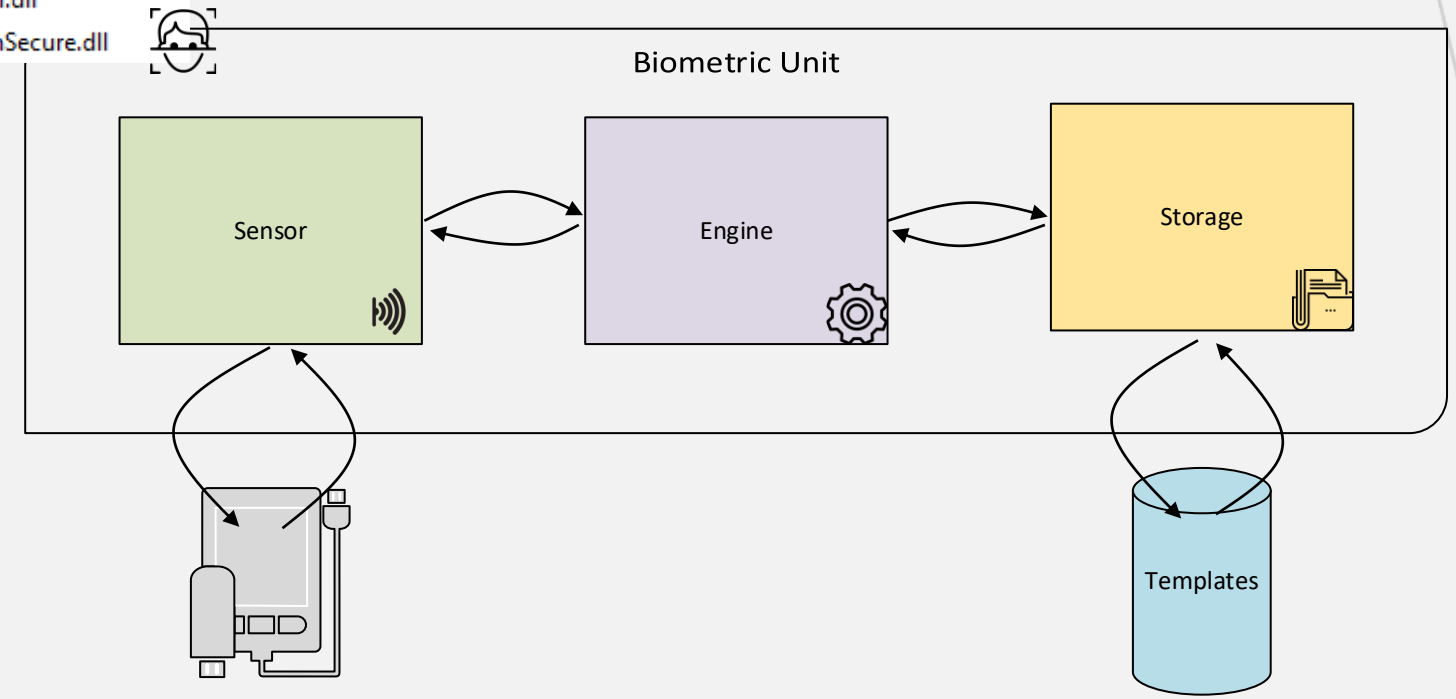
FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll

Microsoft

NUIVoiceWBSAdapters.dll



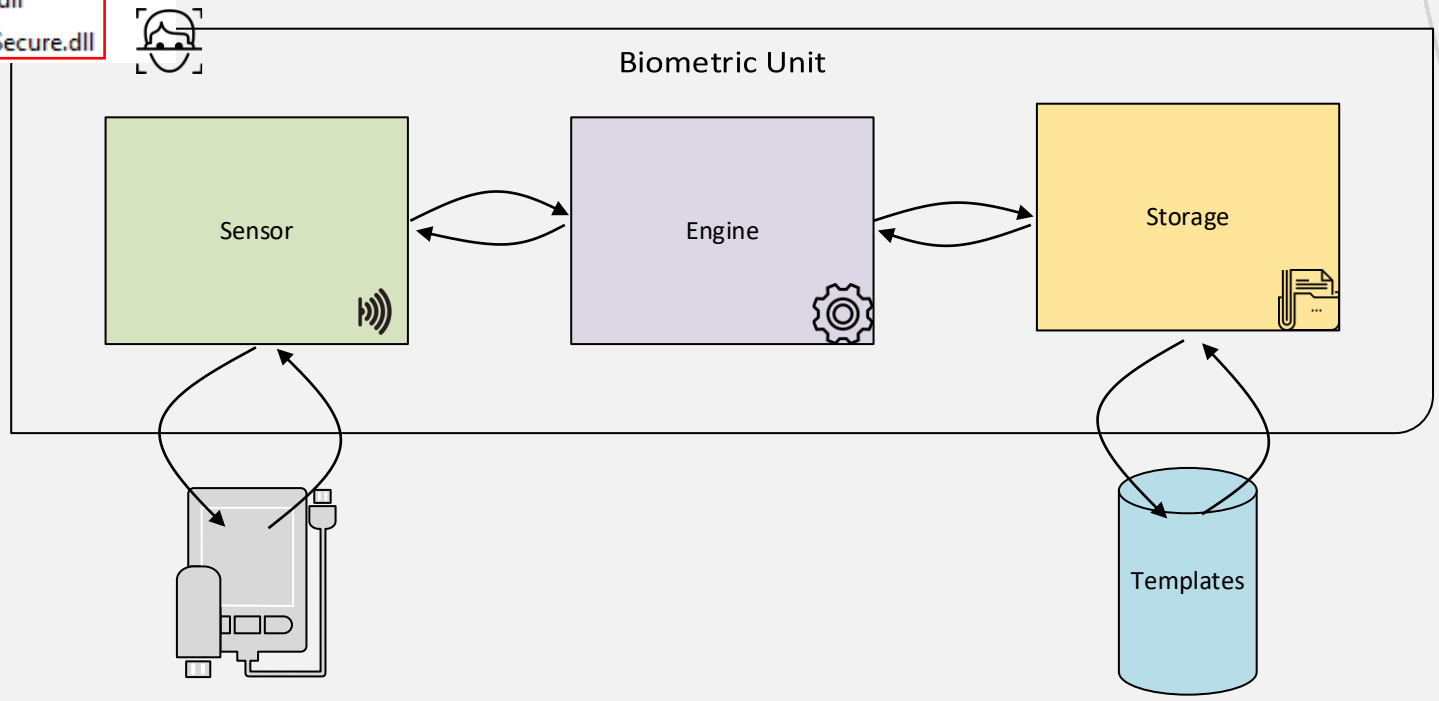
Biometric Unit – DLLs

FaceBootstrapAdapter.dll
FaceDetectorResources.dll
FaceRecognitionEngineAdapter.dll
FaceRecognitionEngineAdapterResources_v4.dll
facerecognitionengineadapterresourcescore.dll
facerecognitionengineadapterresourcessecure.dll
FaceRecognitionSensorAdapter.dll
facerecognitionsensoradapterresources.dll
FaceRecognitionSensorAdapterVsm.dll
FaceRecognitionSensorAdapterVsmSecure.dll

GoodixMocEngineAdapter.dll
GoodixMocEngineAdapterNw.dll
GoodixMocSensorAdapter.dll
GoodixMocSensorAdapterNw.dll
GoodixMocStorageAdapter.dll
GoodixMocStorageAdapterNw.dll

winbiosensoradapter.dll
winbiostorageadapter.dll
winbiovsmstorageadapter.dll
Microsoft

NUIVoiceWBSAdapters.dll

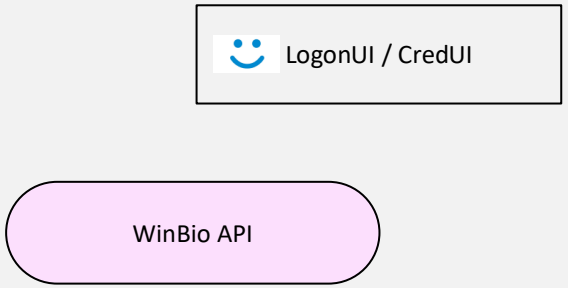


Observed loading order:

"FaceBootstrapAdapter.dll"
"FaceBootstrapAdapter.dll"
"NUIVoiceWBSAdapters.dll"
"NUIVoiceWBSAdapters.dll"
"WinBioStorageAdapter.dll"
"FaceRecognitionSensorAdapter.DLL"
"FaceRecognitionEngineAdapter.DLL"
"WinBioStorageAdapter.DLL"
"GoodixMocSensorAdapterNw.dll"
"GoodixMocEngineAdapterNw.dll"
"GoodixMocStorageAdapterNw.dll"

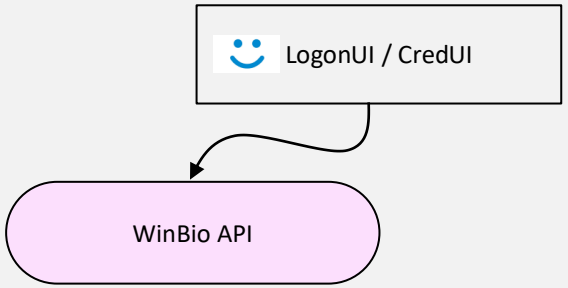
Enhanced Sign-in Security (ESS)

Face Recognition



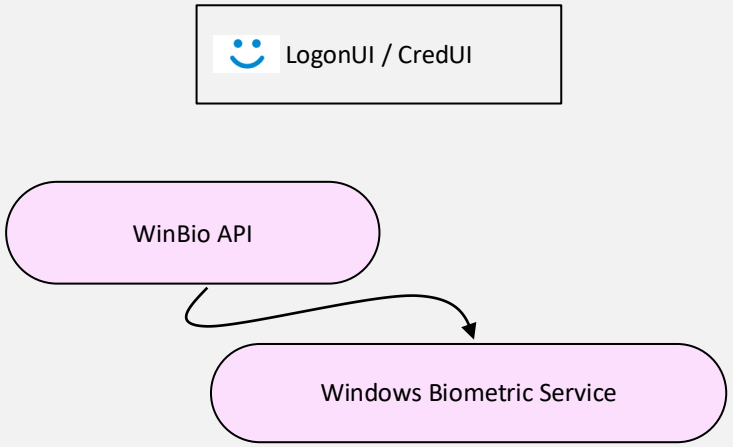
Enhanced Sign-in Security (ESS)

Face Recognition



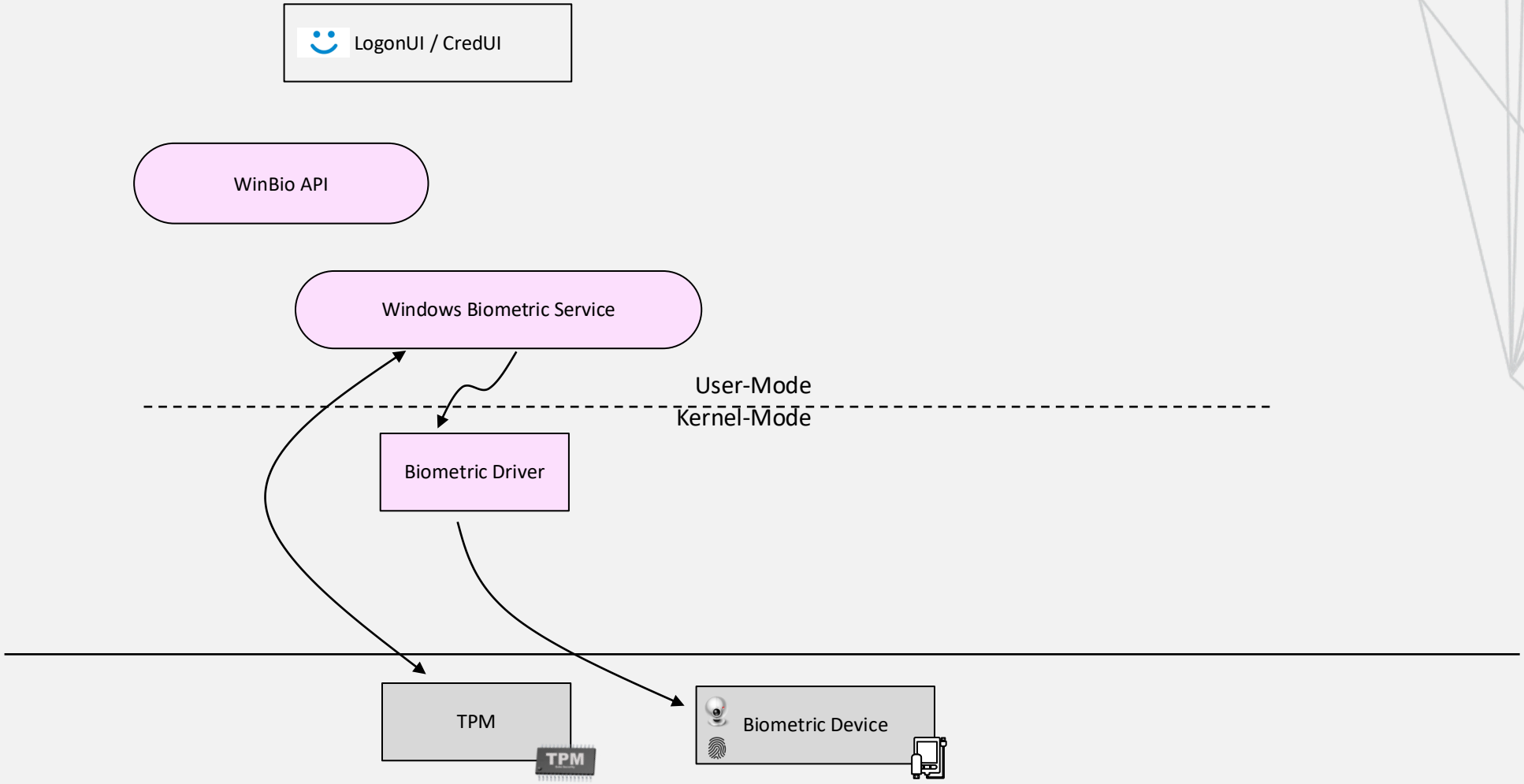
Enhanced Sign-in Security (ESS)

Face Recognition



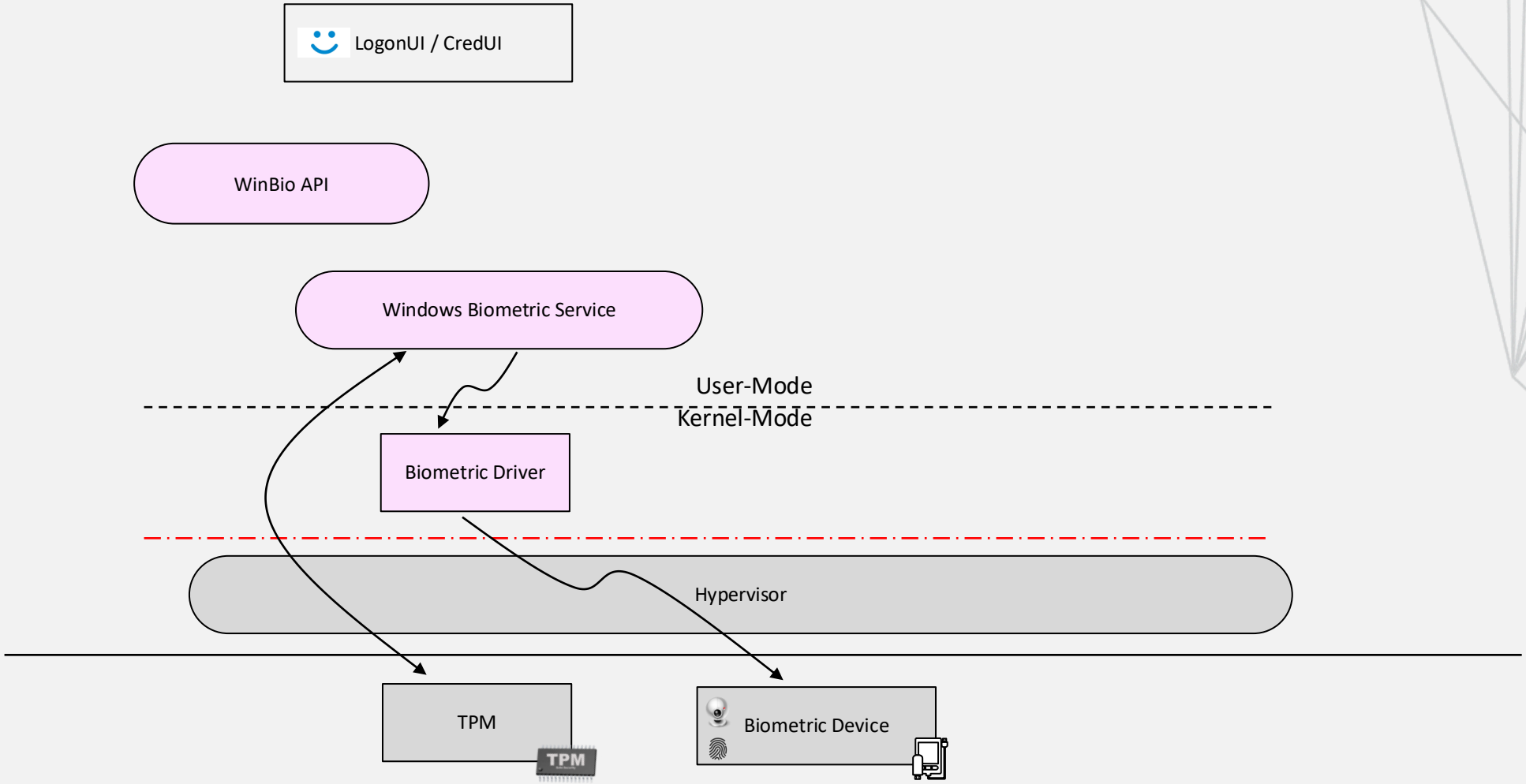
Enhanced Sign-in Security (ESS)

Face Recognition



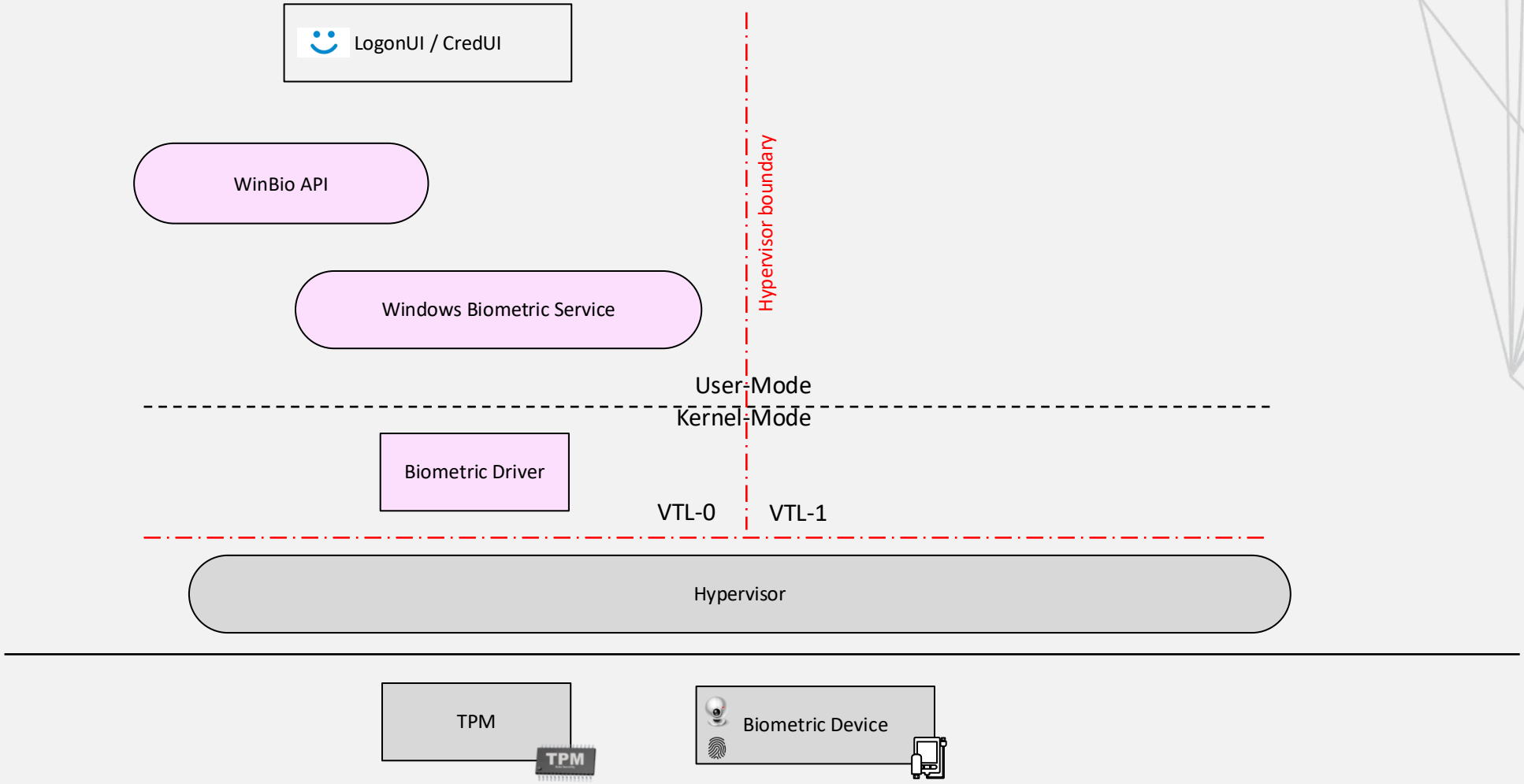
Enhanced Sign-in Security (ESS)

Face Recognition



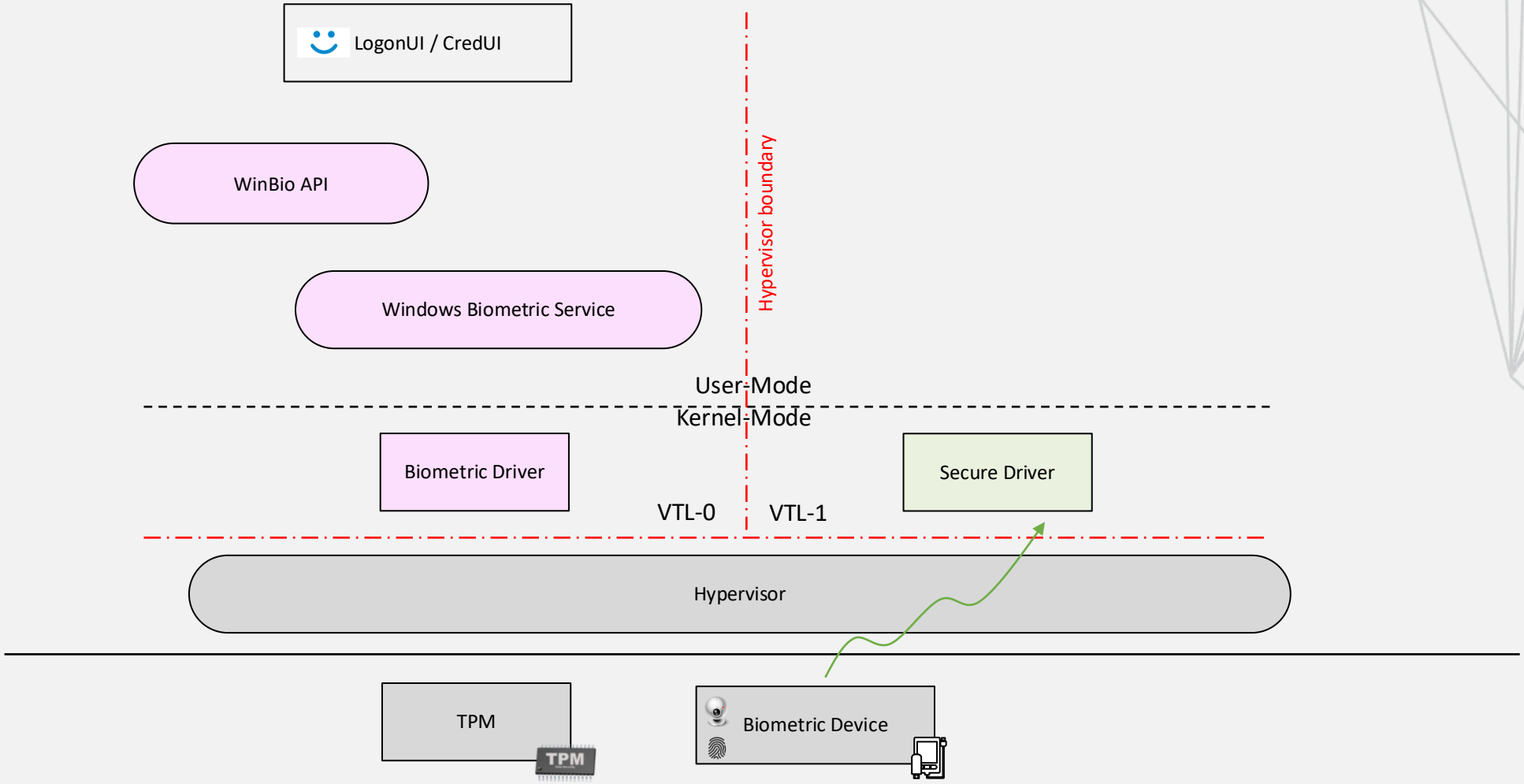
Enhanced Sign-in Security (ESS)

Face Recognition



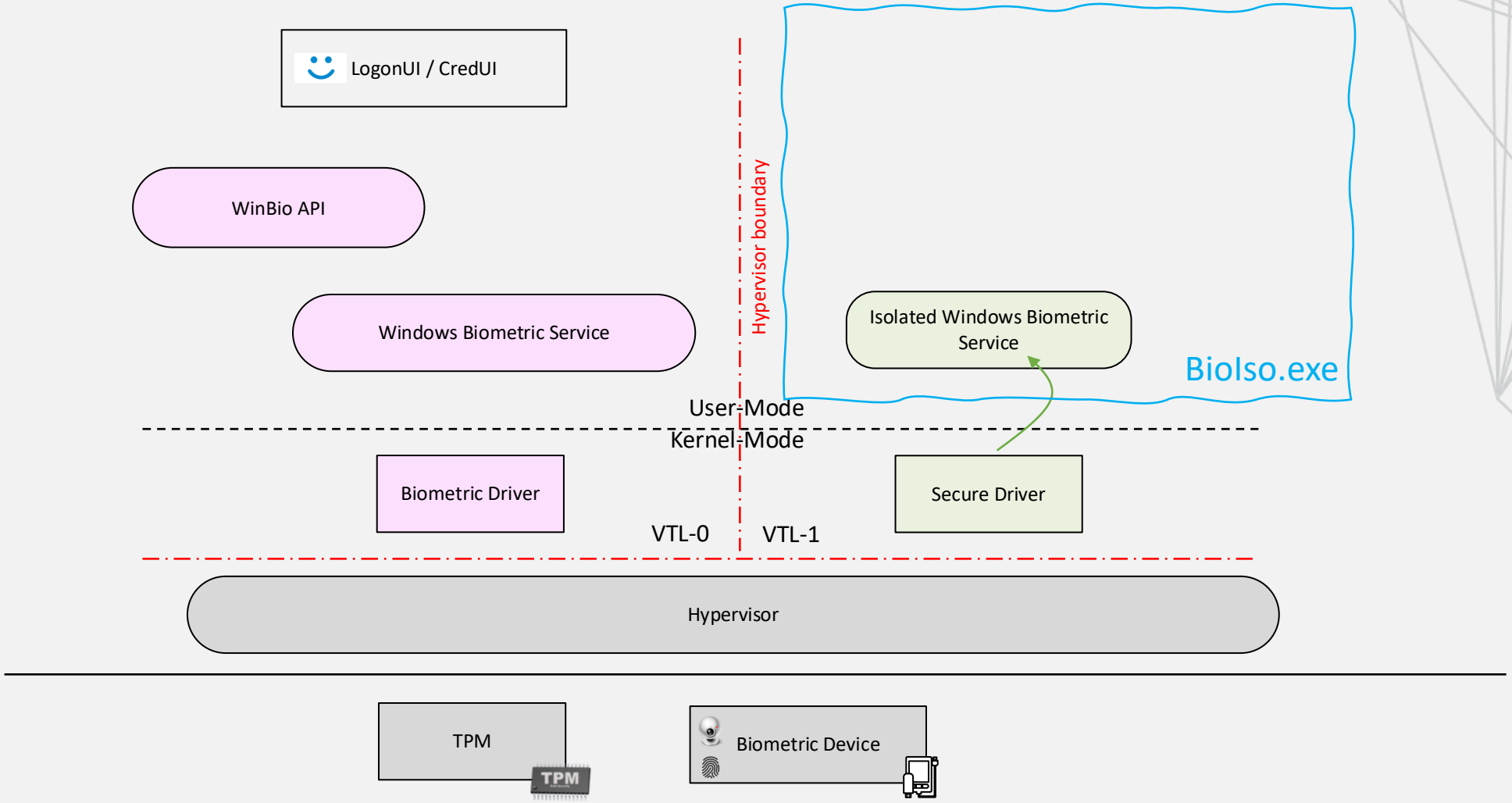
Enhanced Sign-in Security (ESS)

Face Recognition



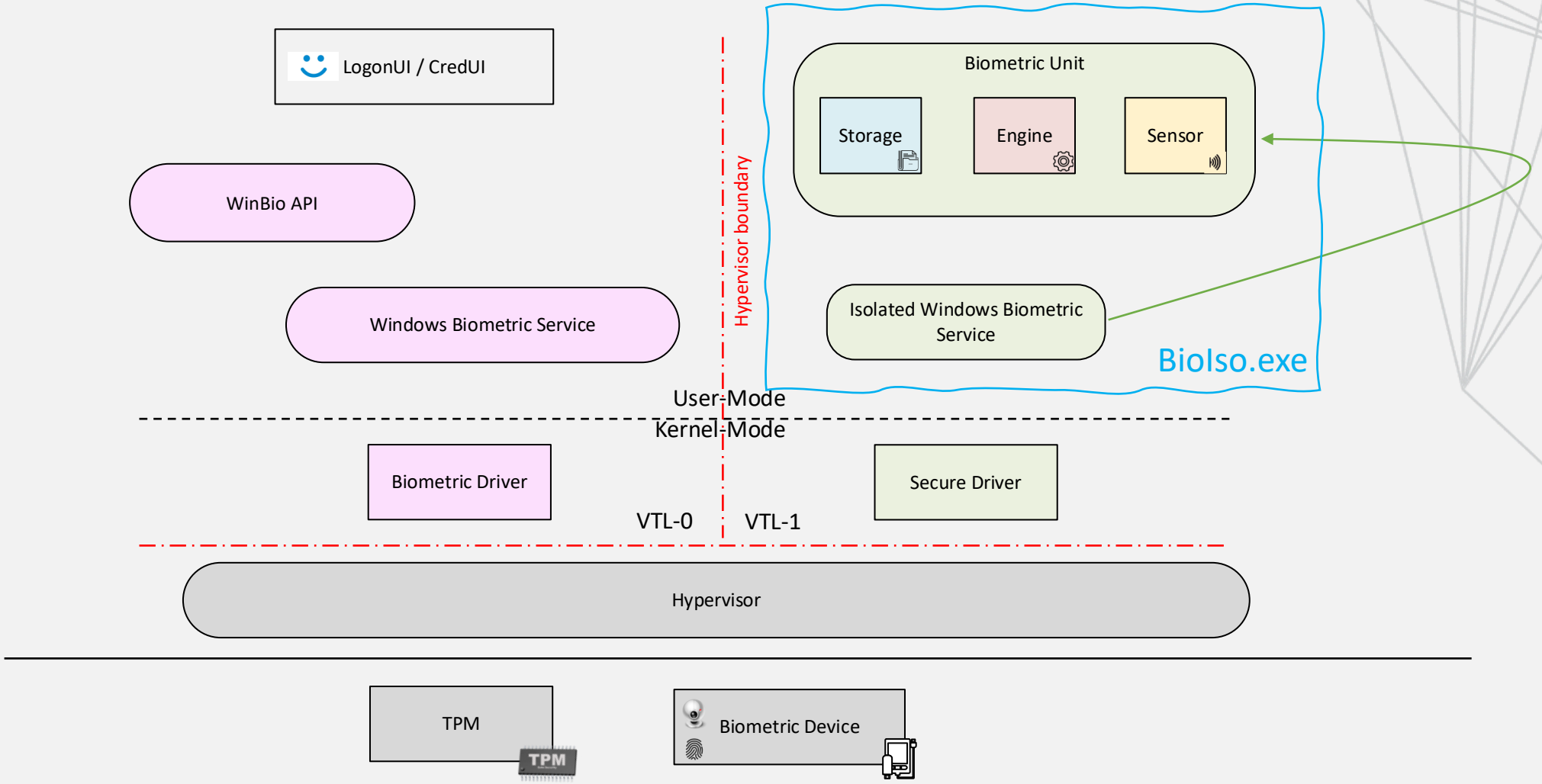
Enhanced Sign-in Security (ESS)

Face Recognition



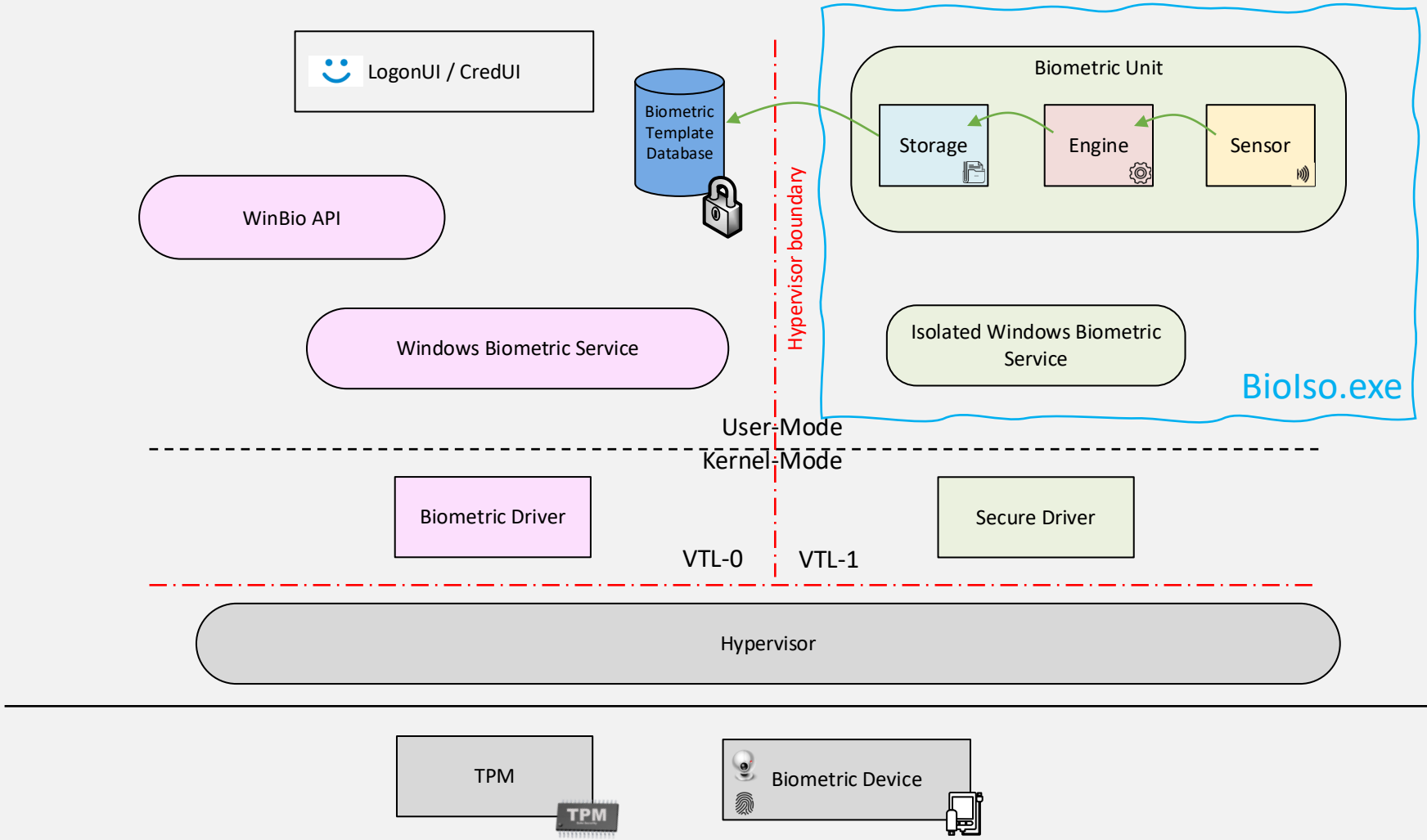
Enhanced Sign-in Security (ESS)

Face Recognition



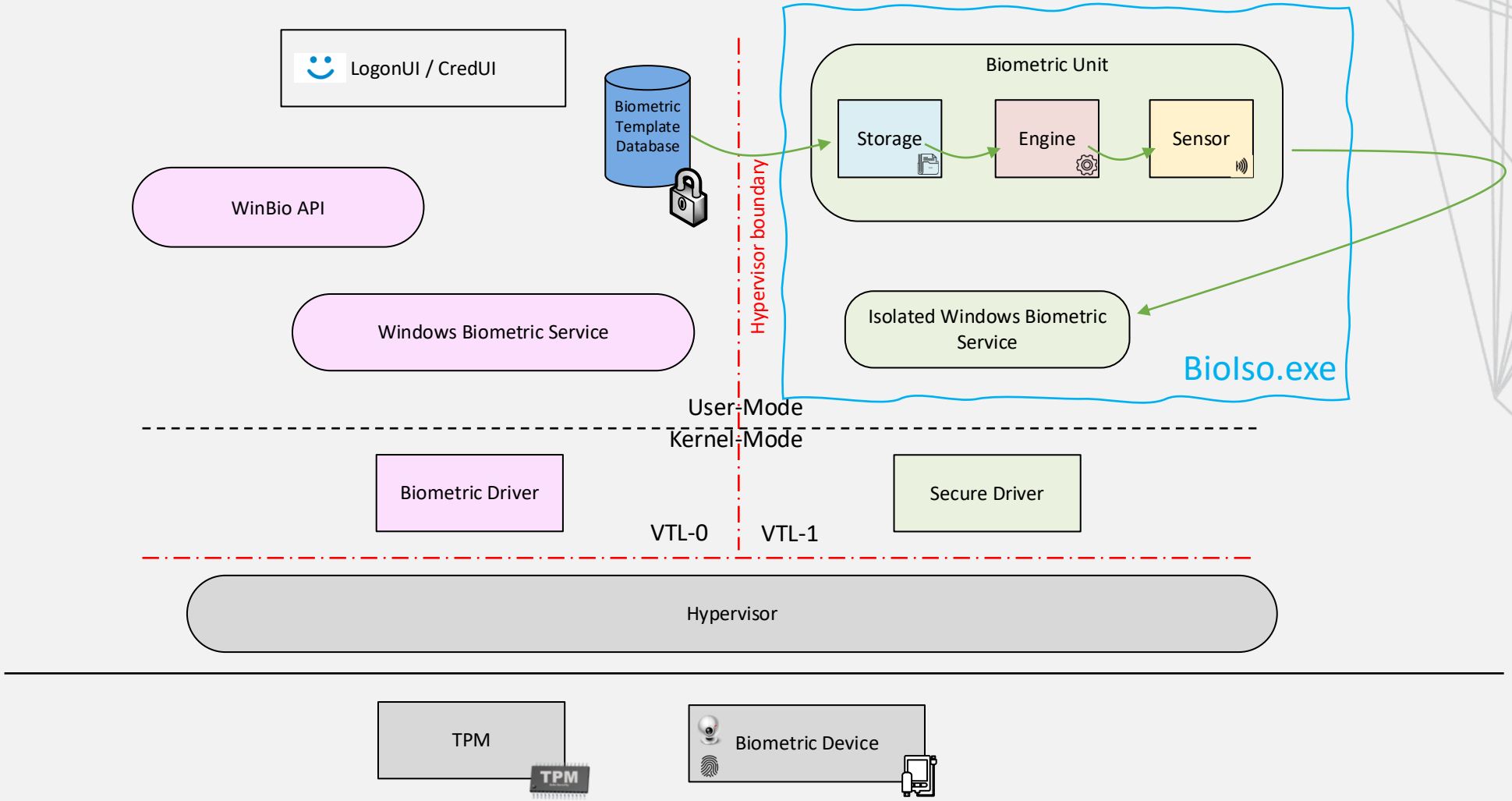
Enhanced Sign-in Security (ESS)

Face Recognition



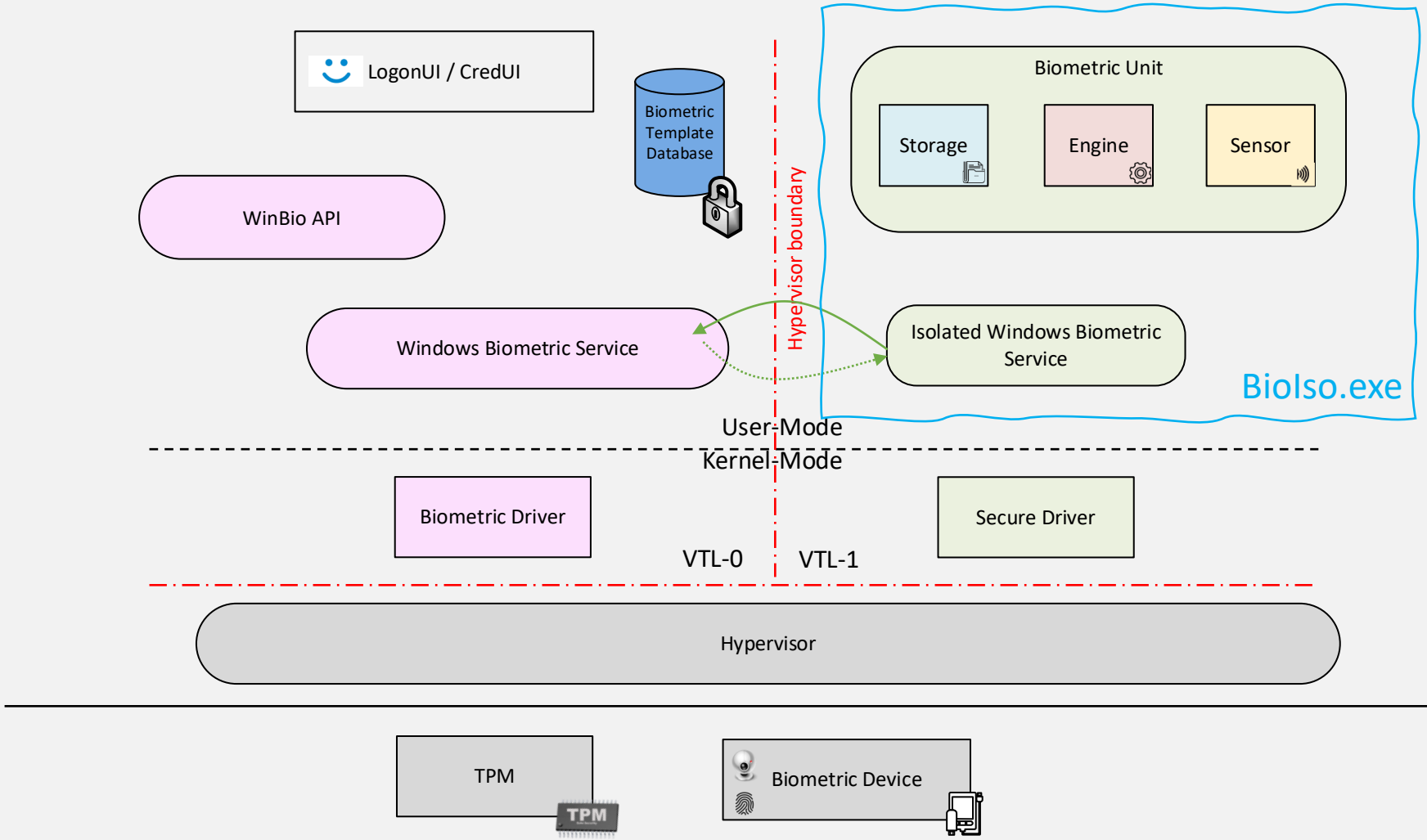
Enhanced Sign-in Security (ESS)

Face Recognition



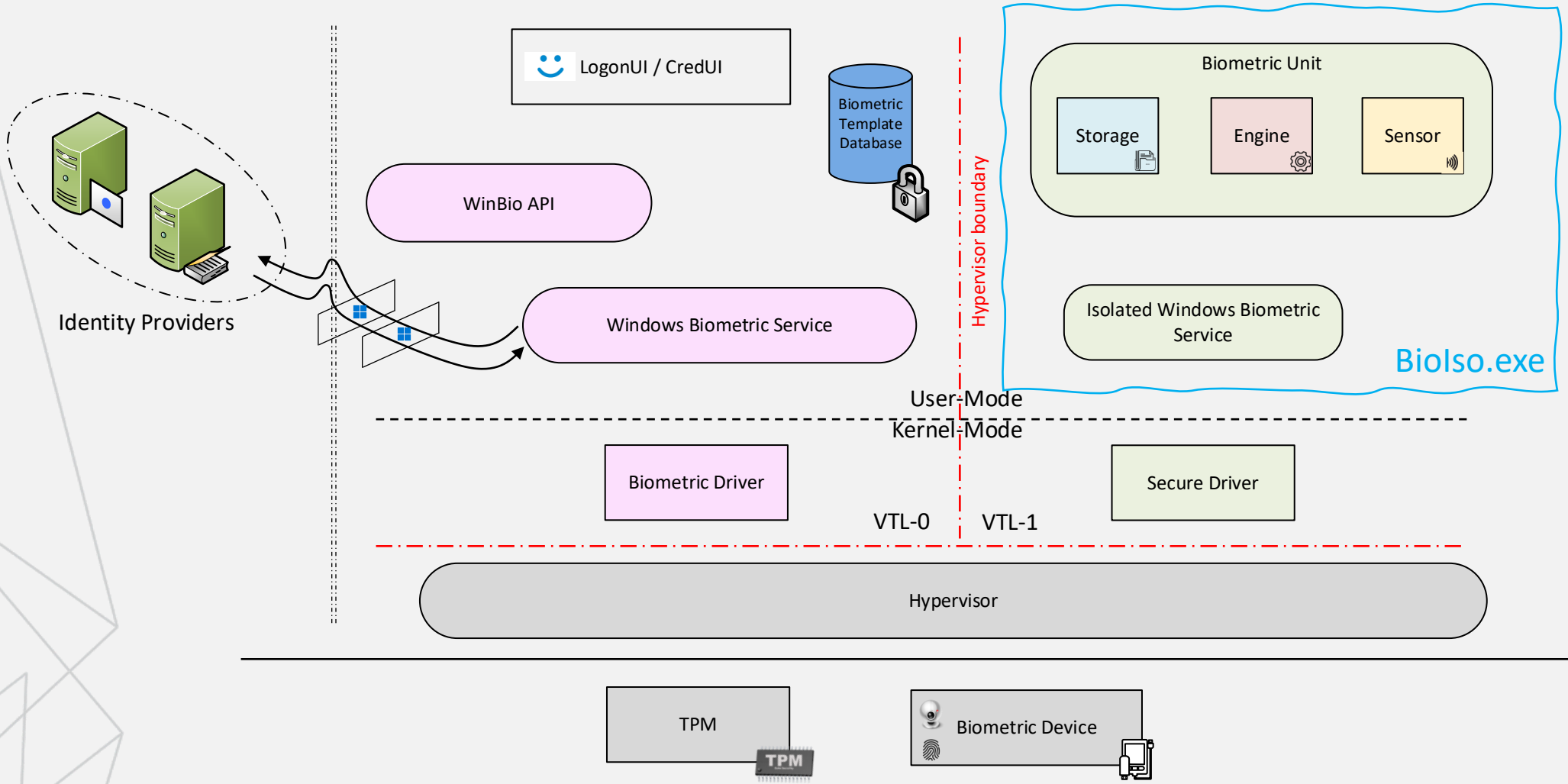
Enhanced Sign-in Security (ESS)

Face Recognition



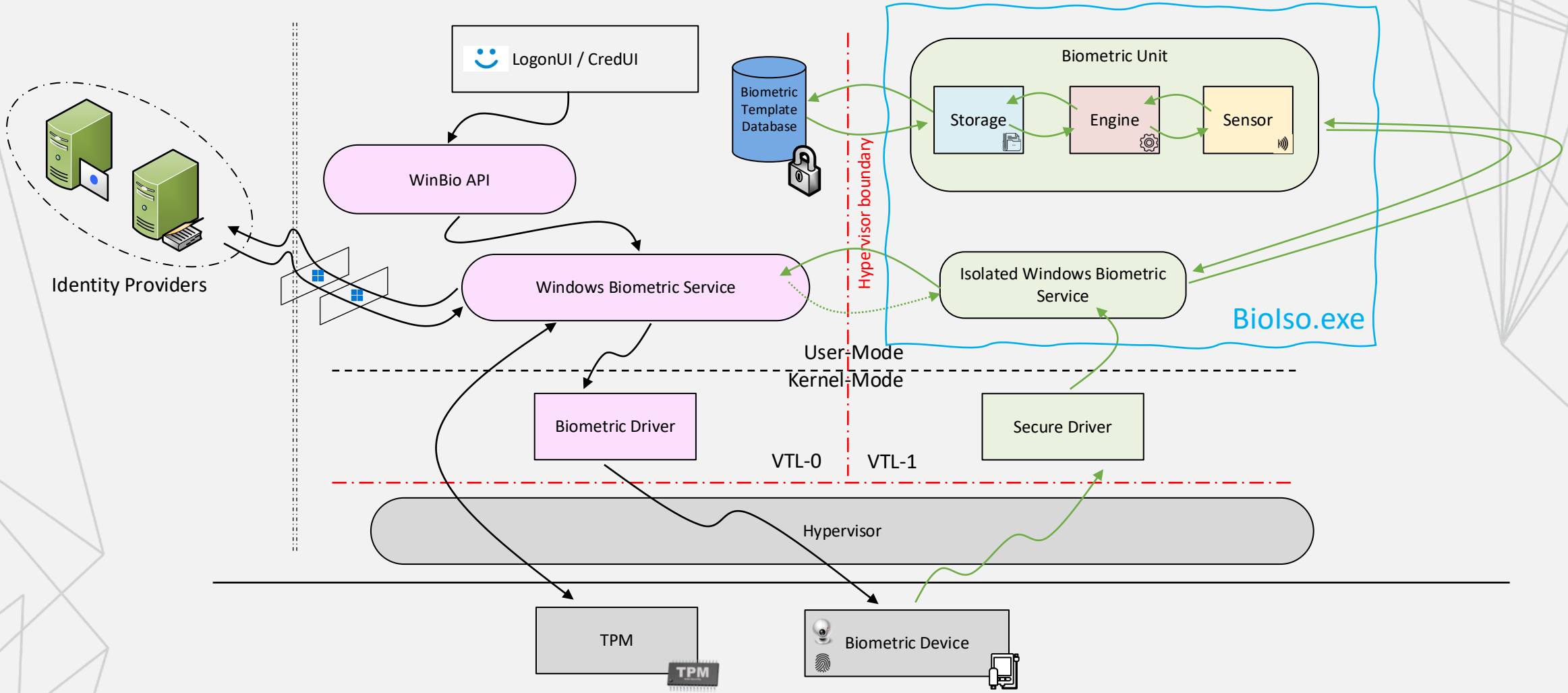
Enhanced Sign-in Security (ESS)

Face Recognition

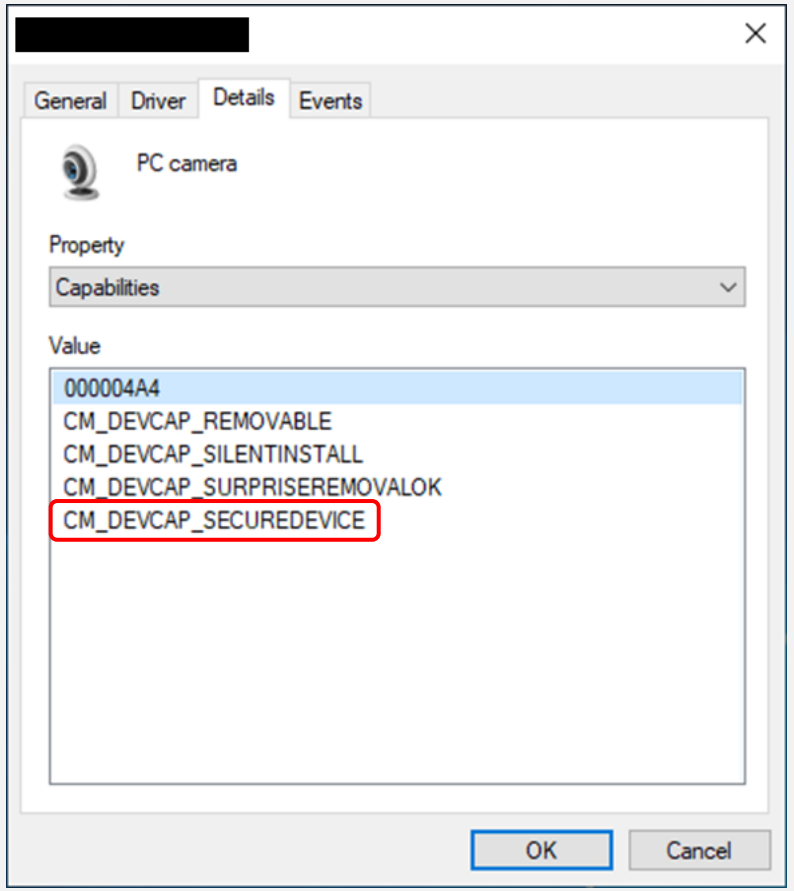


Enhanced Sign-in Security (ESS)

Face Recognition



Enhanced Sign-in Security (ESS)



Authentication Procedure

Once the identification happened

Windows Biometric Auth management

Biometrics

Biometric Service

Cryptographic procedure

Key

TPM

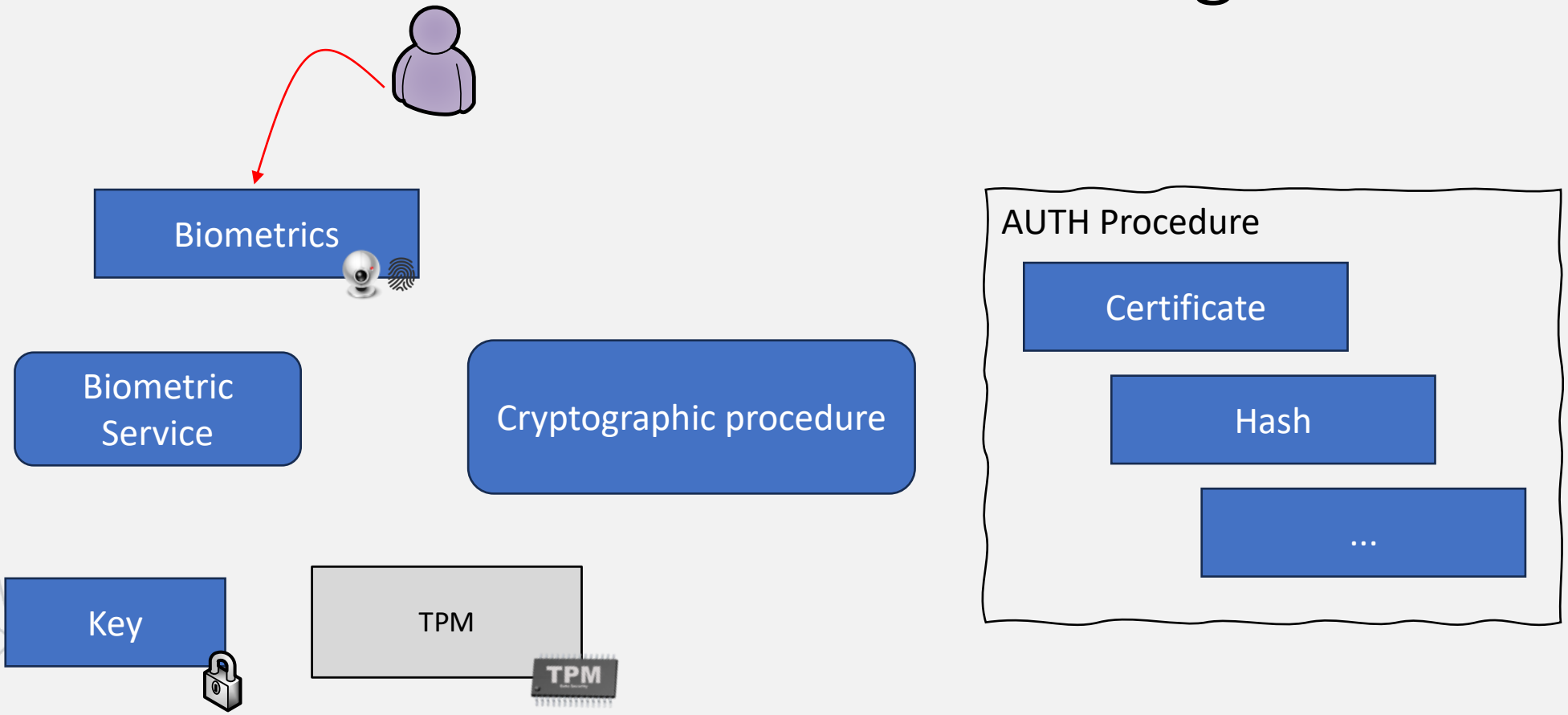
AUTH Procedure

Certificate

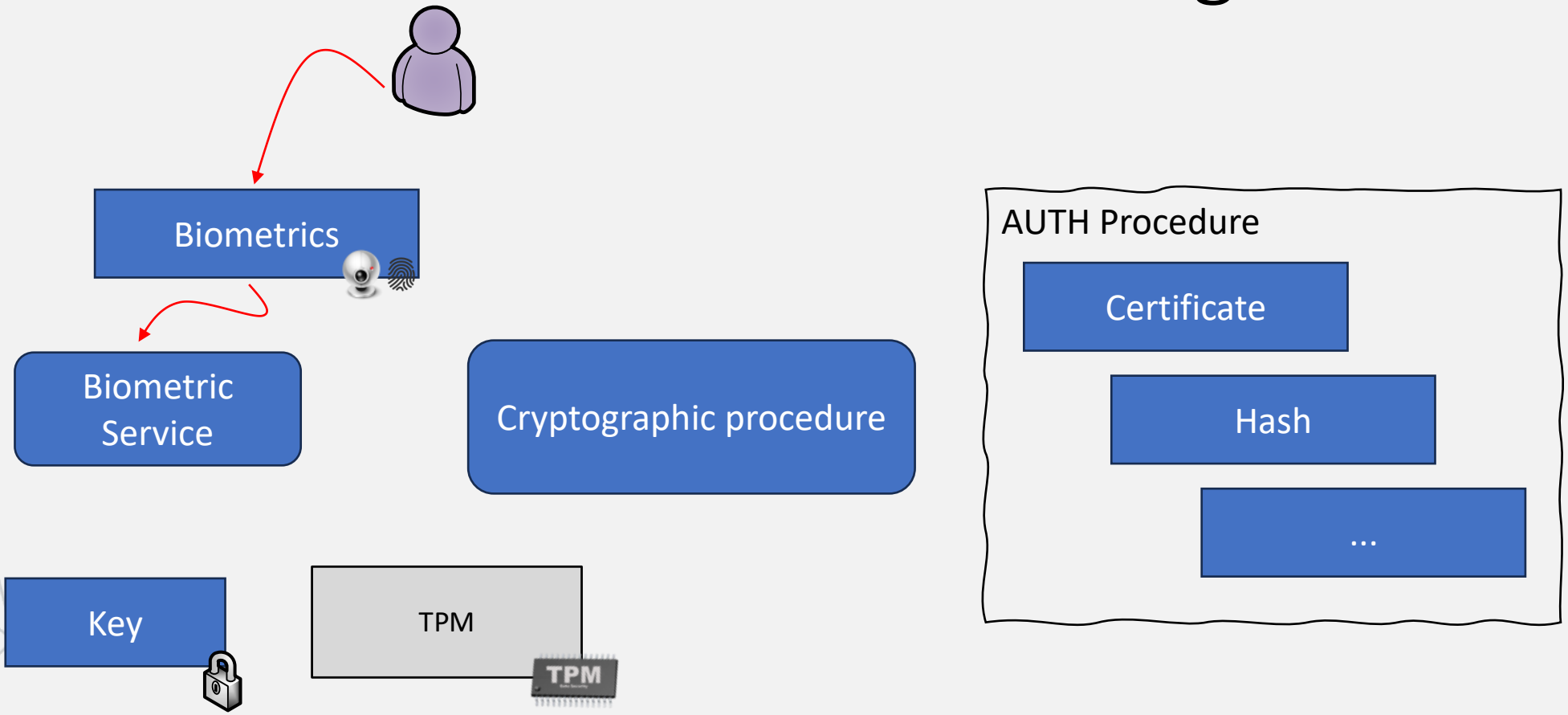
Hash

...

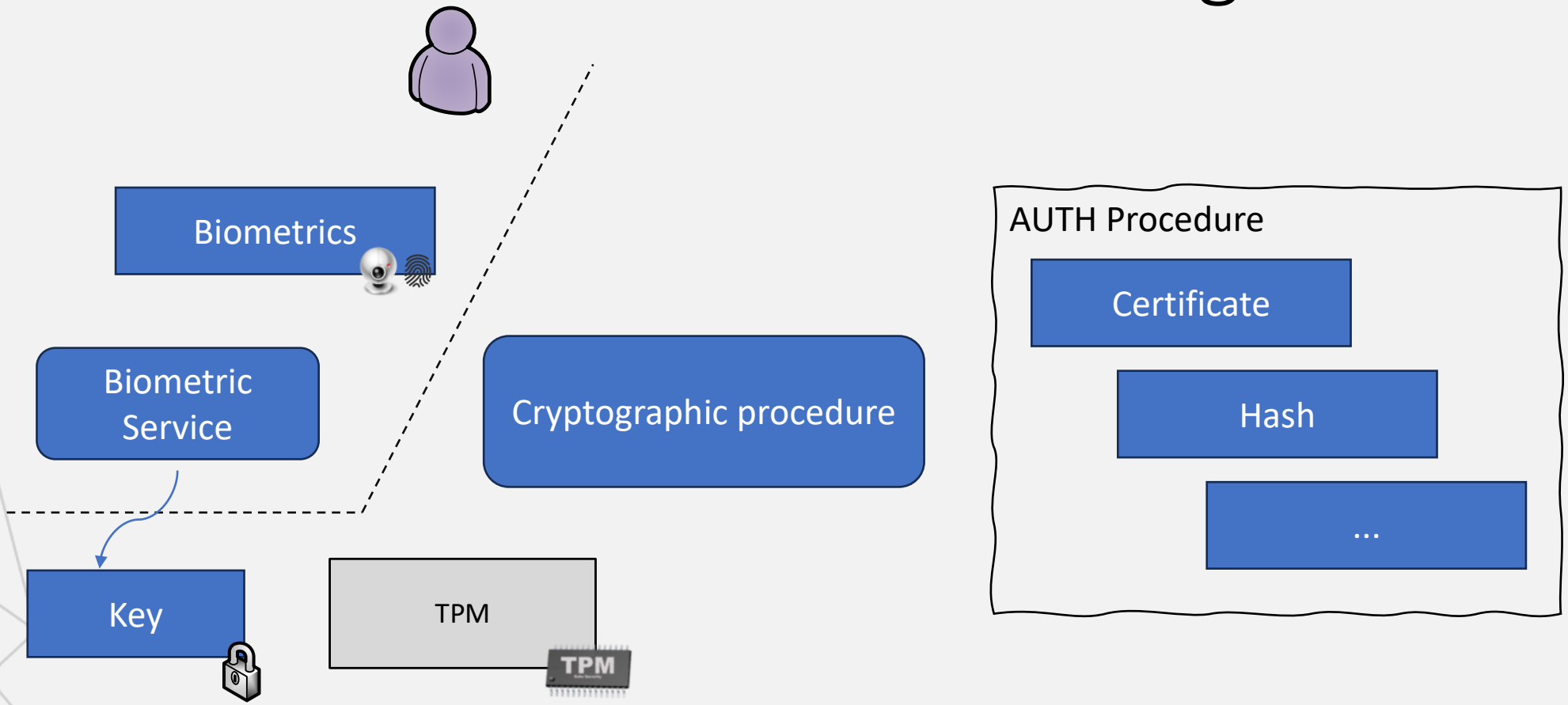
Windows Biometric Auth management



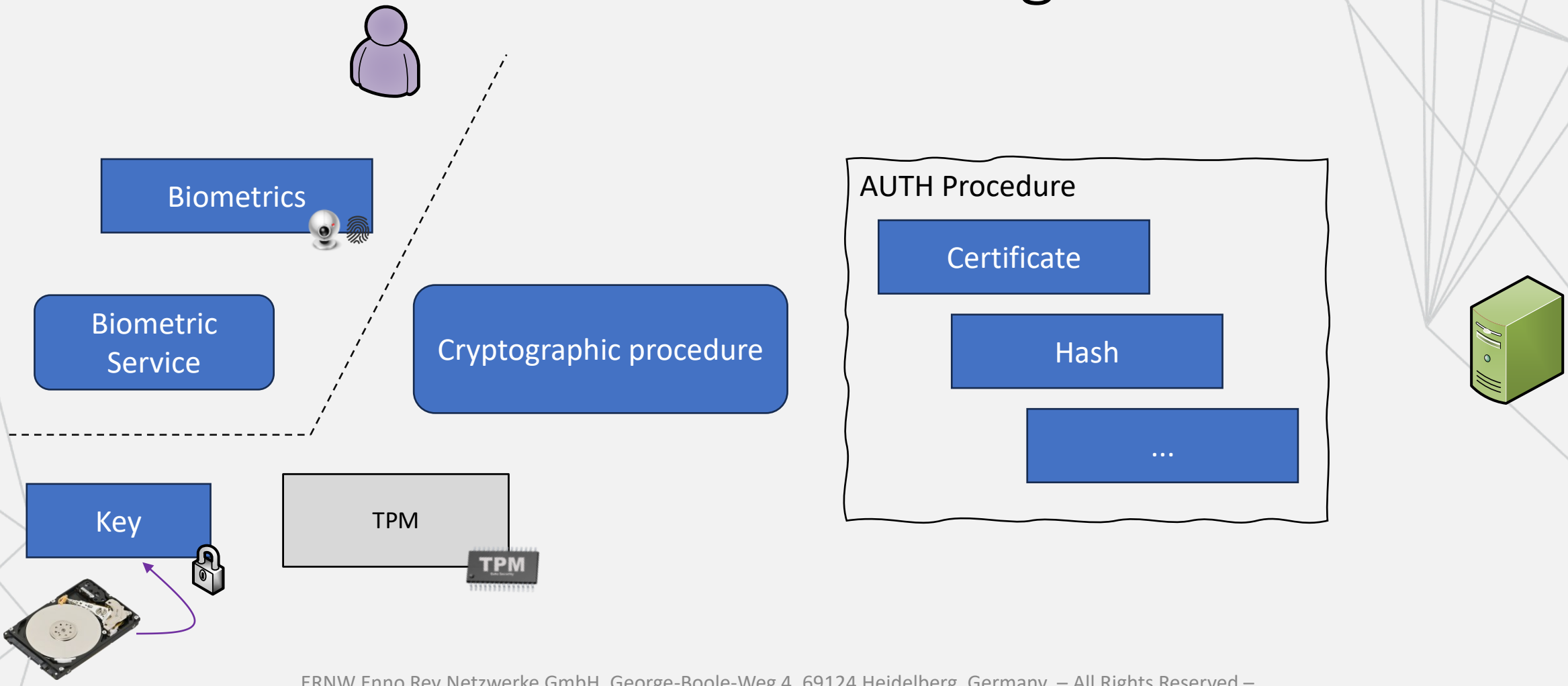
Windows Biometric Auth management



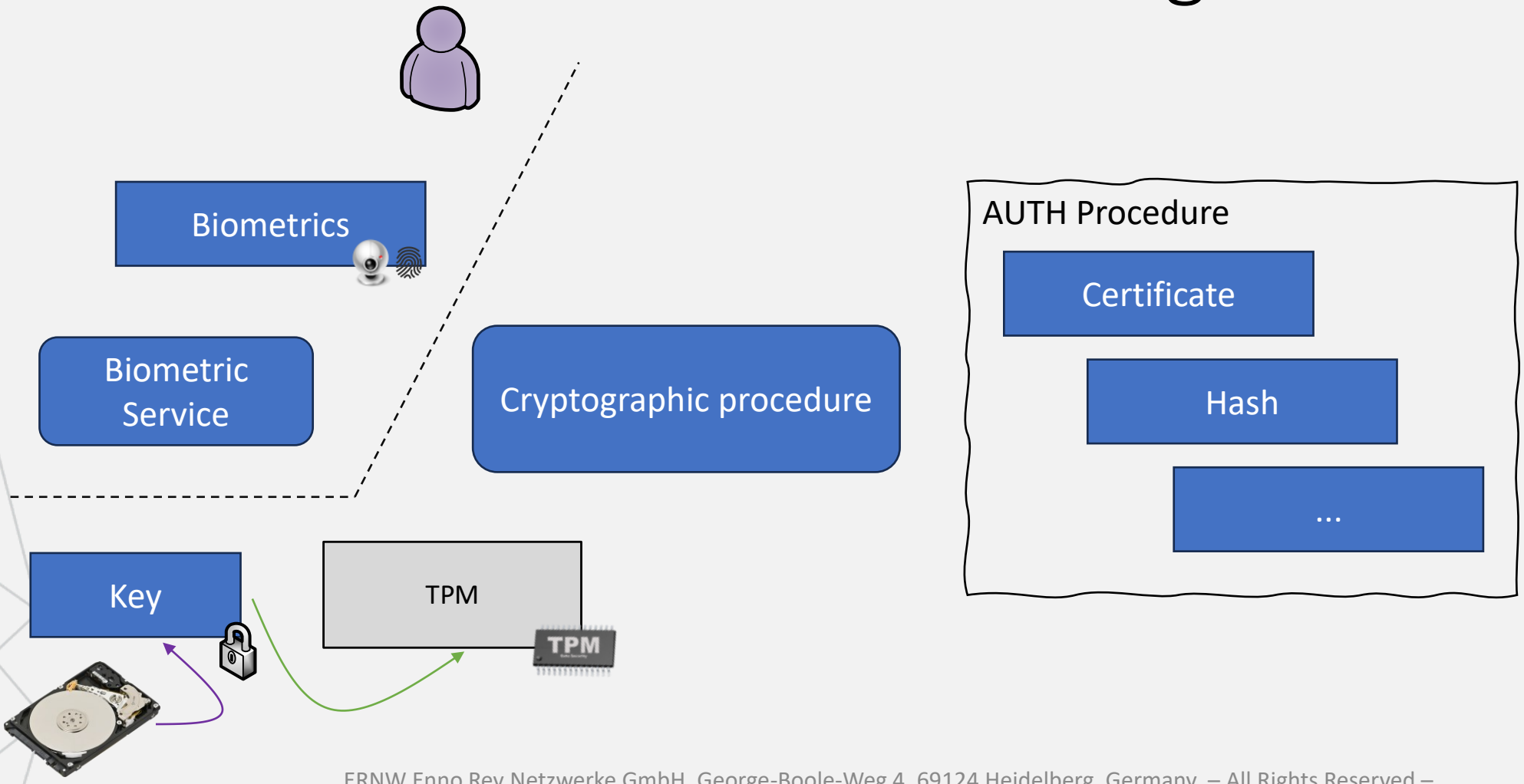
Windows Biometric Auth management



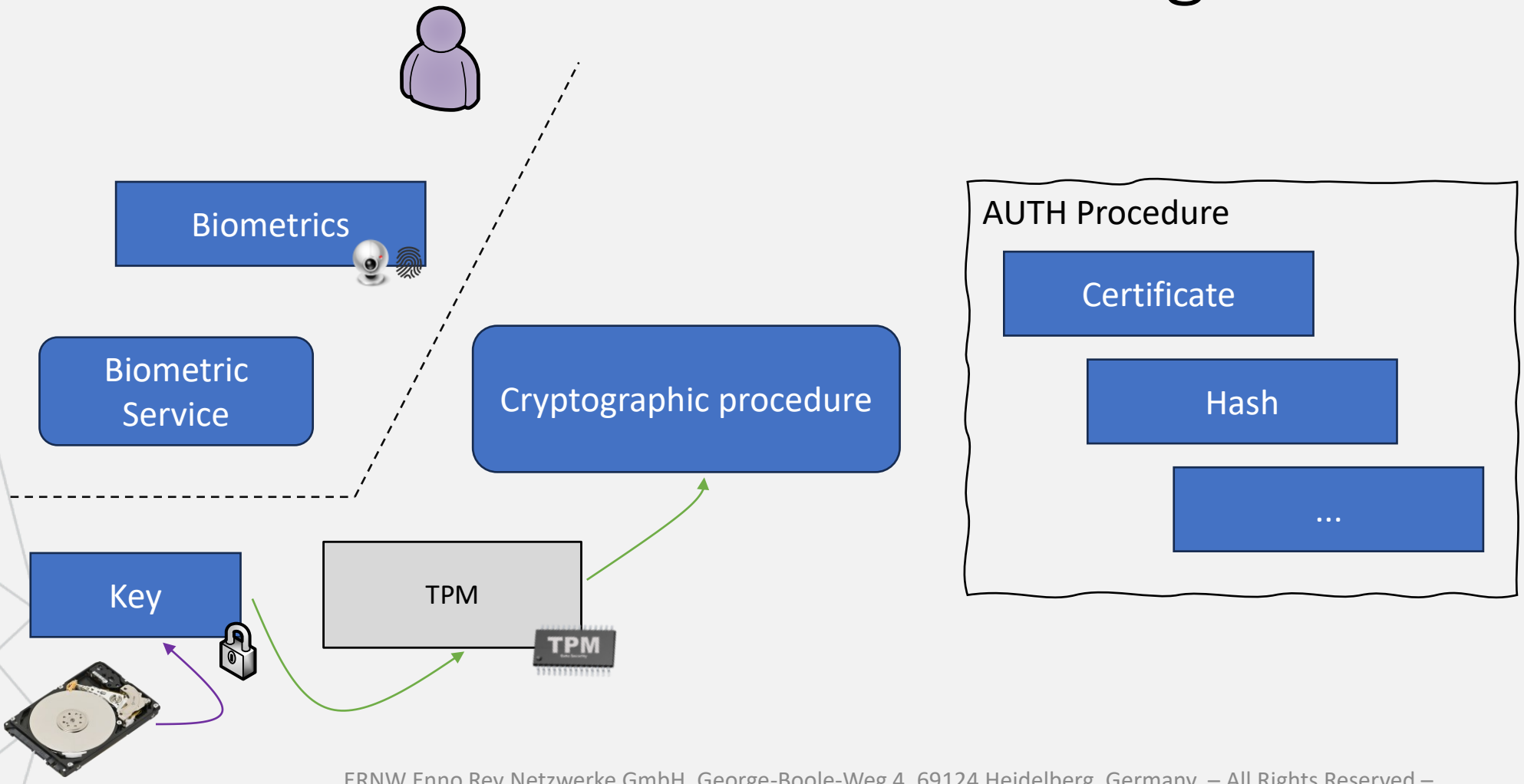
Windows Biometric Auth management



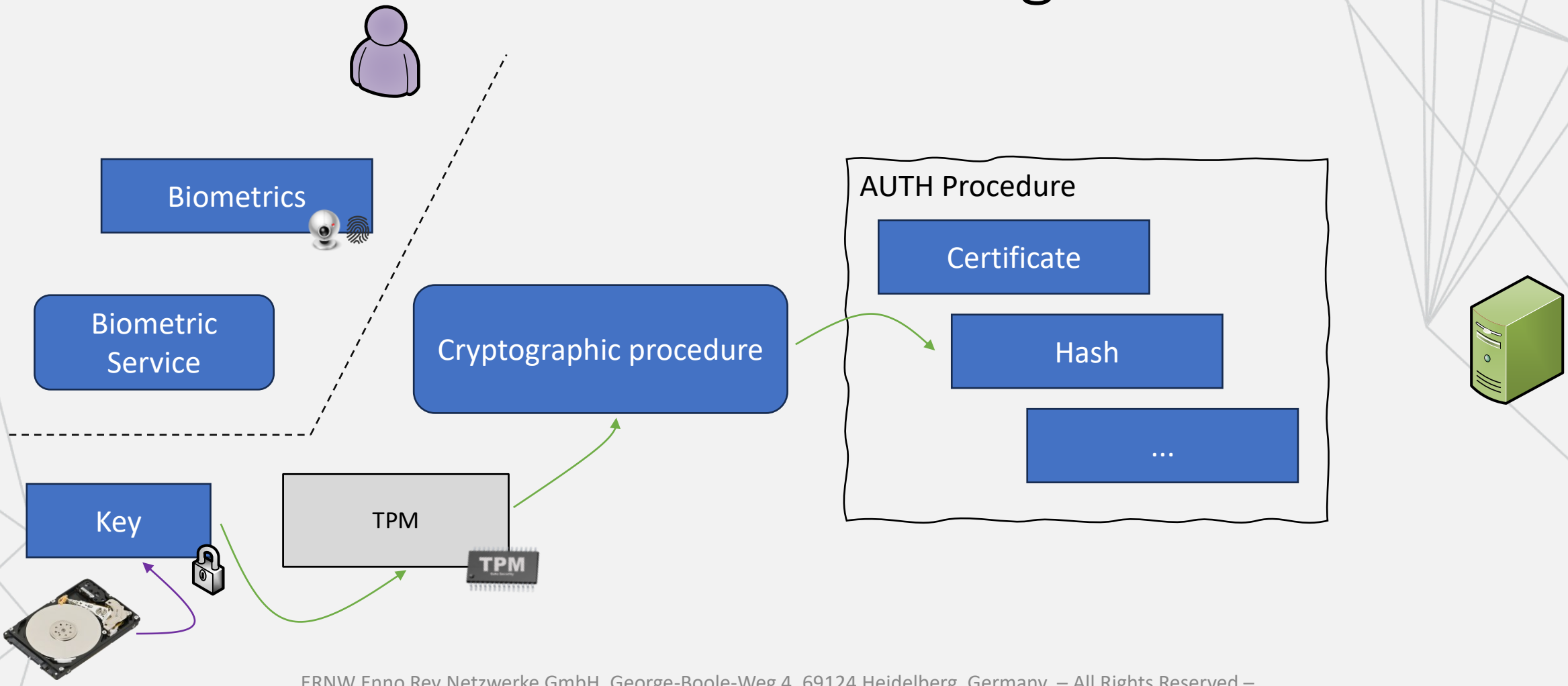
Windows Biometric Auth management



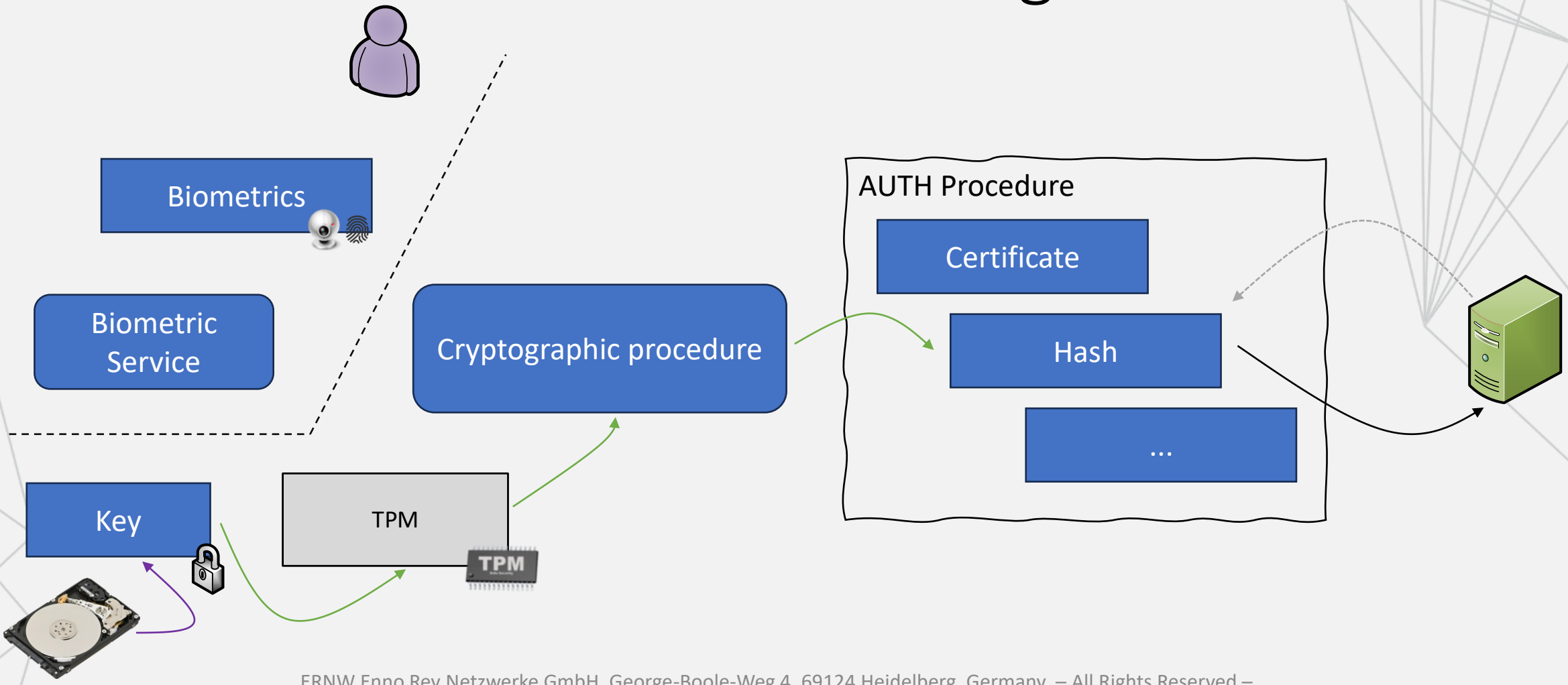
Windows Biometric Auth management



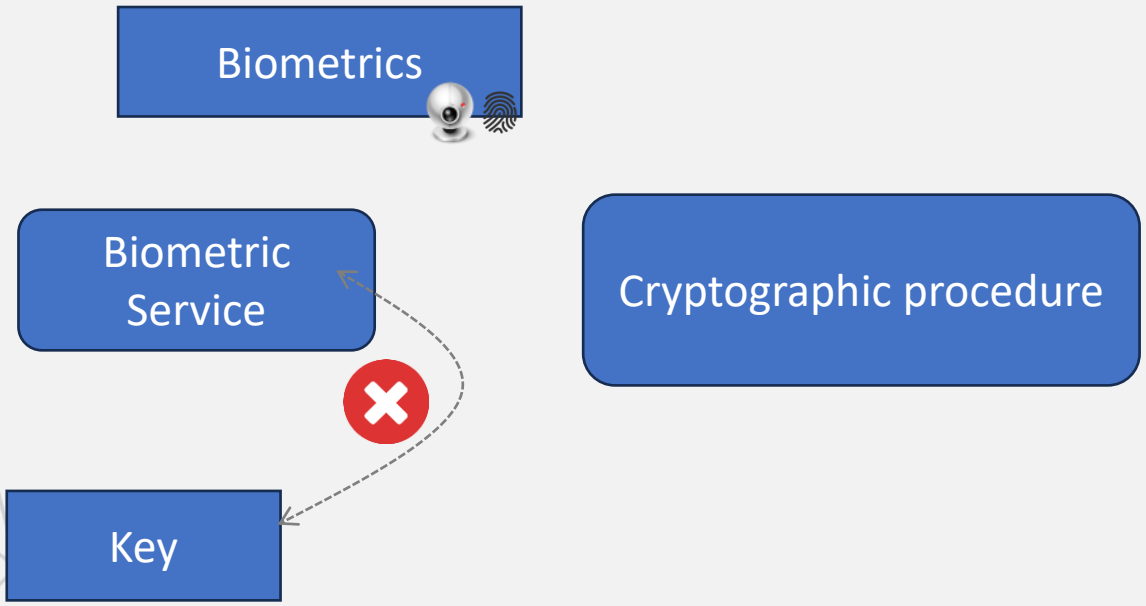
Windows Biometric Auth management



Windows Biometric Auth management



Windows Biometric Auth management



Traditional Auth management

Password

Cryptographic procedure

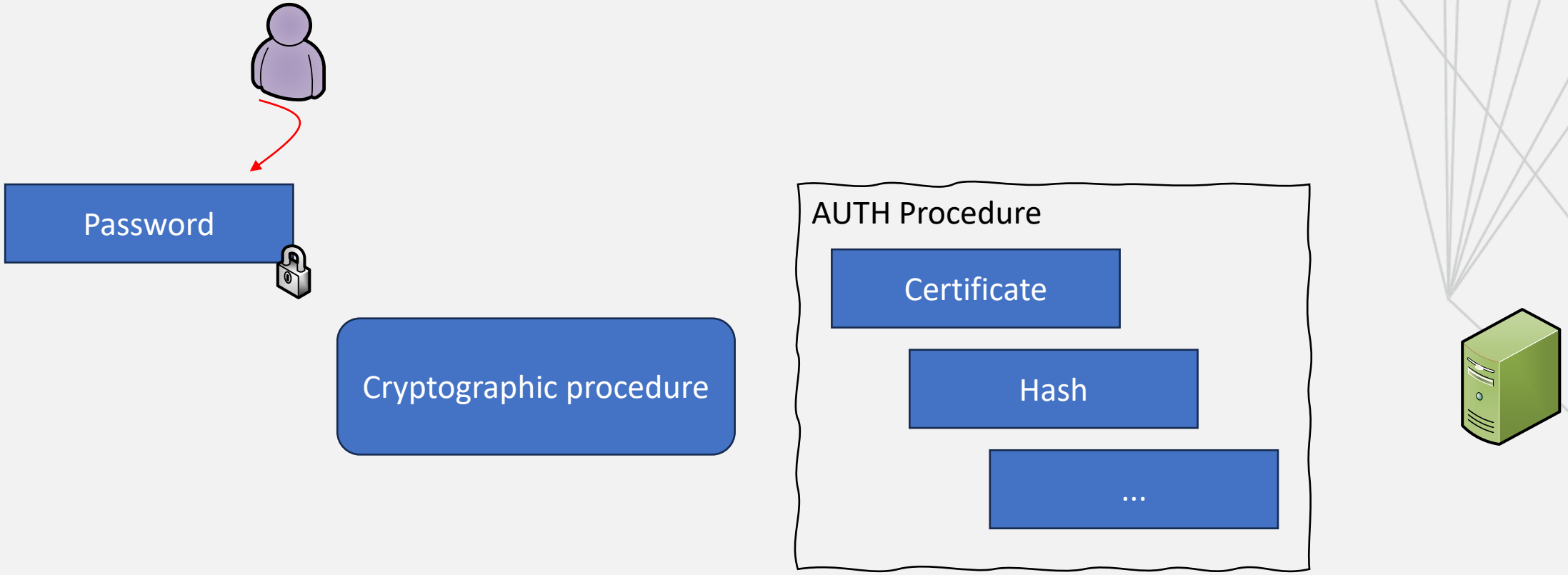
AUTH Procedure

Certificate

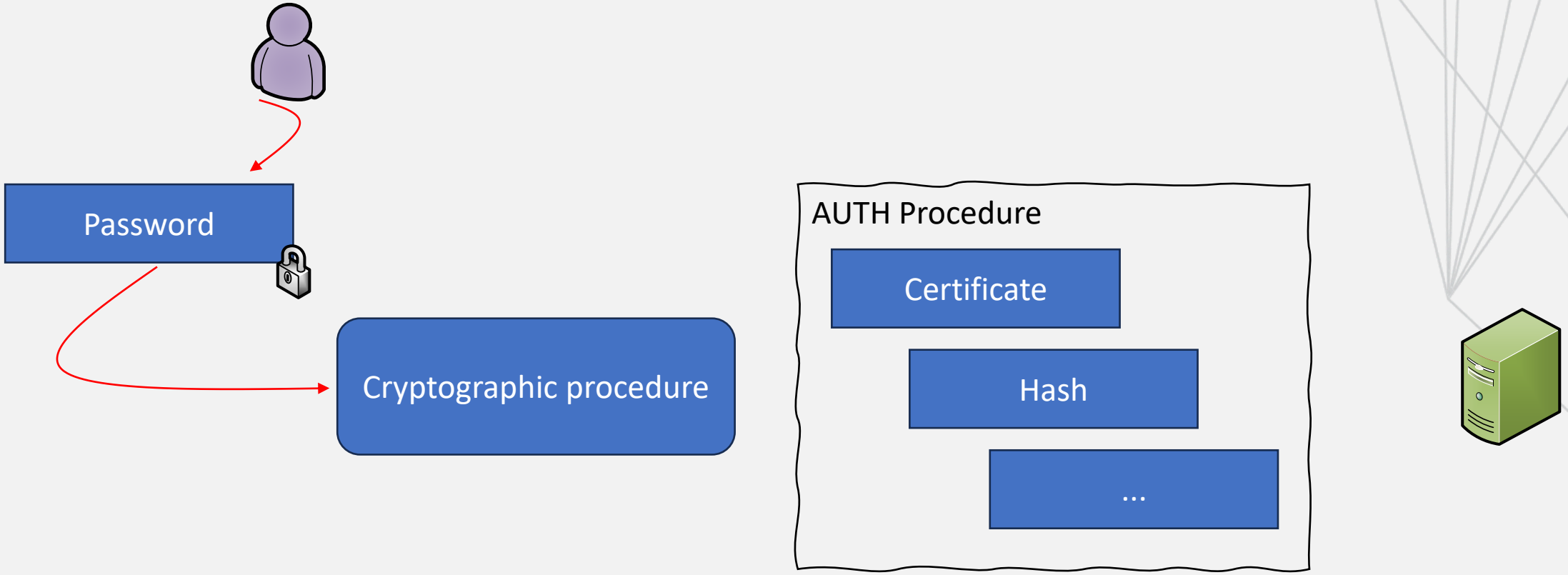
Hash

...

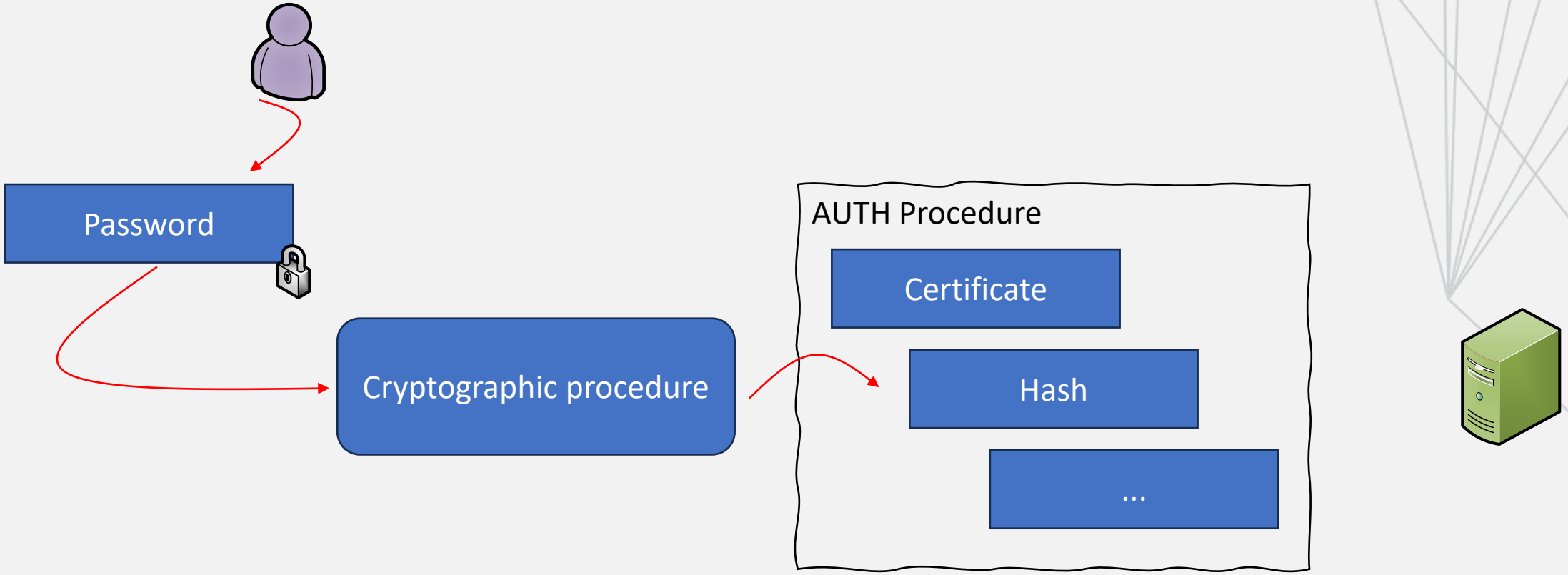
Traditional Auth management



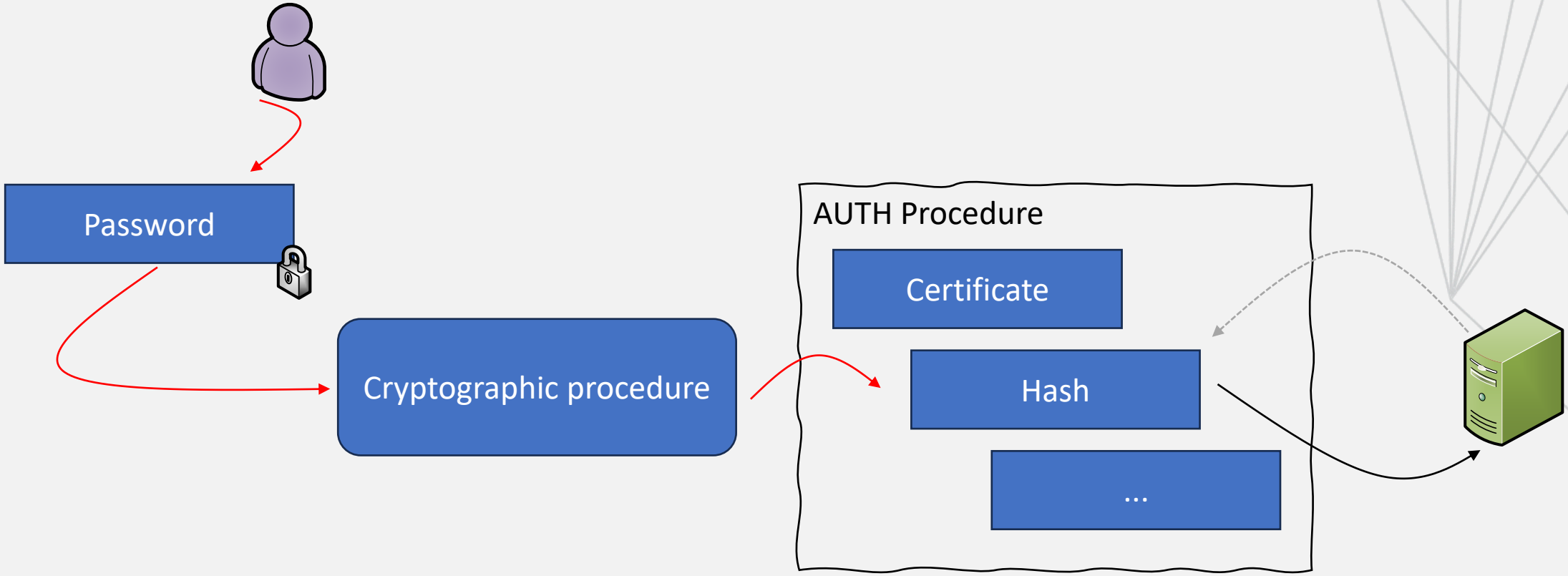
Traditional Auth management



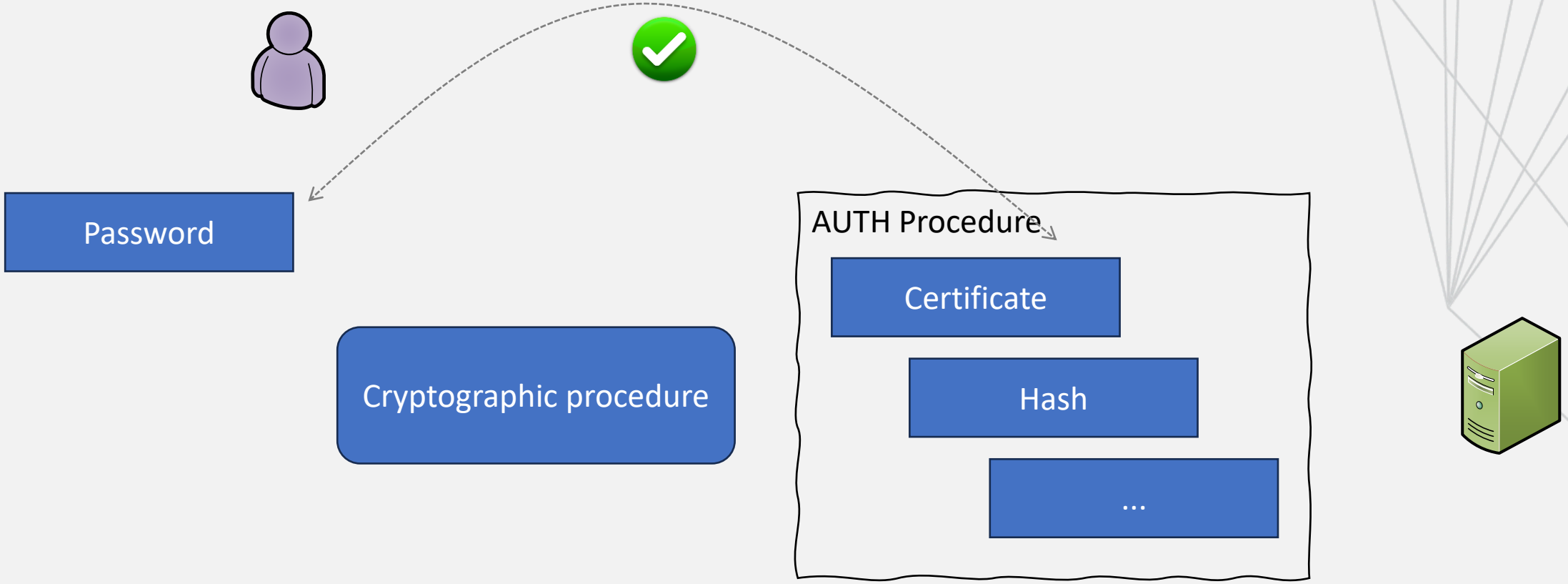
Traditional Auth management

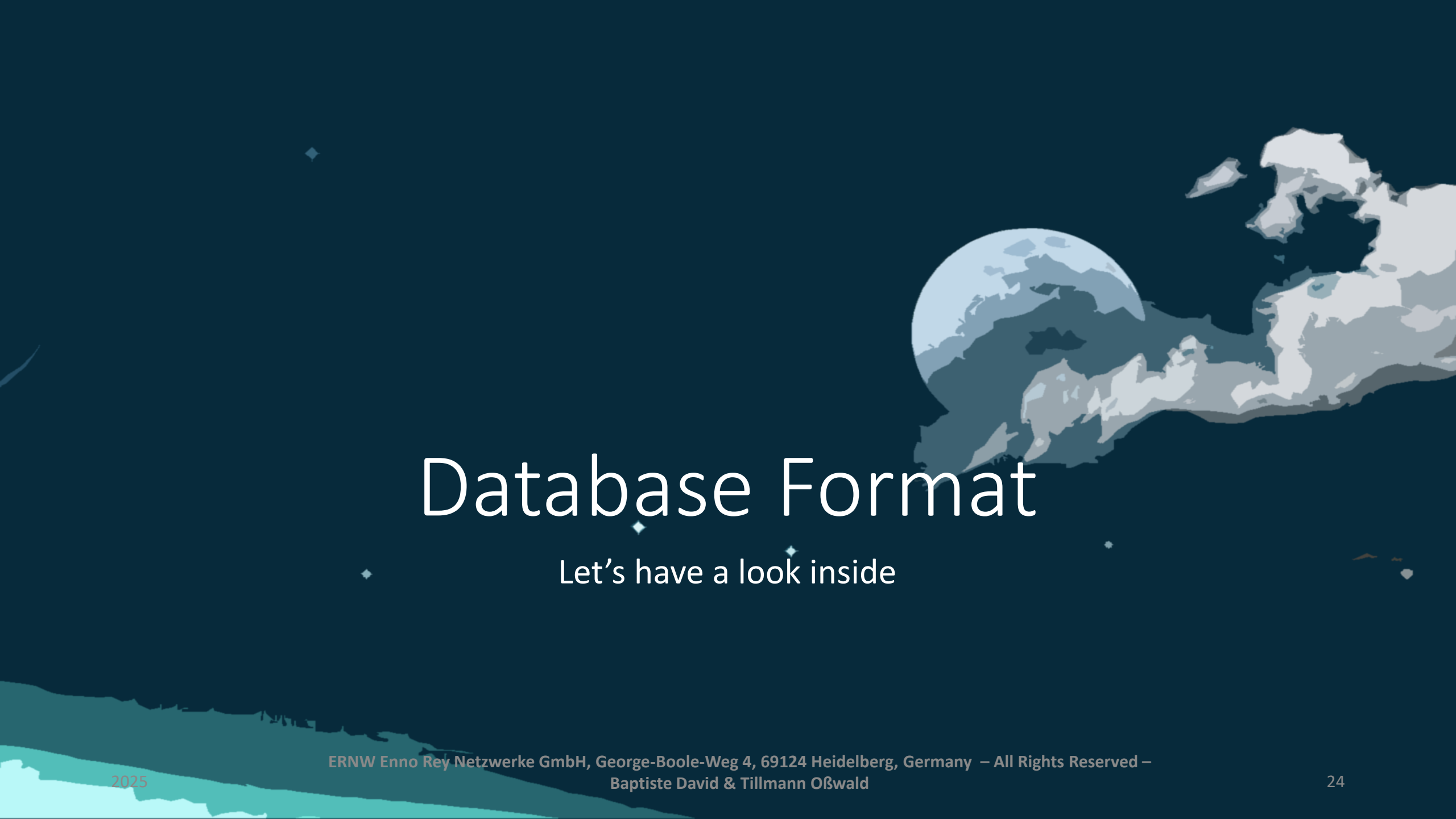


Traditional Auth management



Traditional Auth management





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.

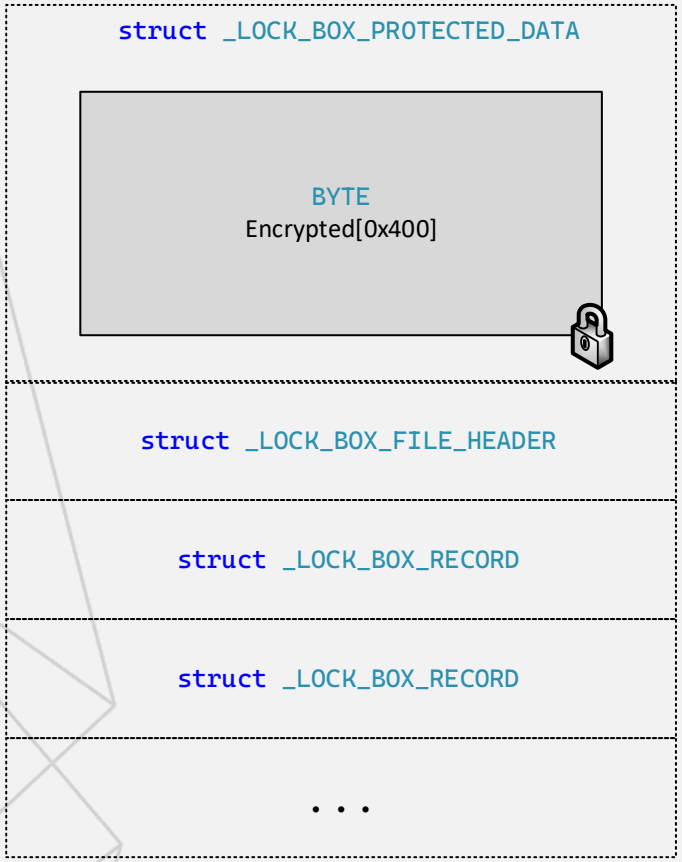
Each sensor has its own biometric database file where template data is stored (path `C:\WINDOWS\System32\WinBioDatabase`). Each database file has a unique, randomly generated key that is encrypted to the system. The template data for the sensor is encrypted with the per-database key using AES with CBC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

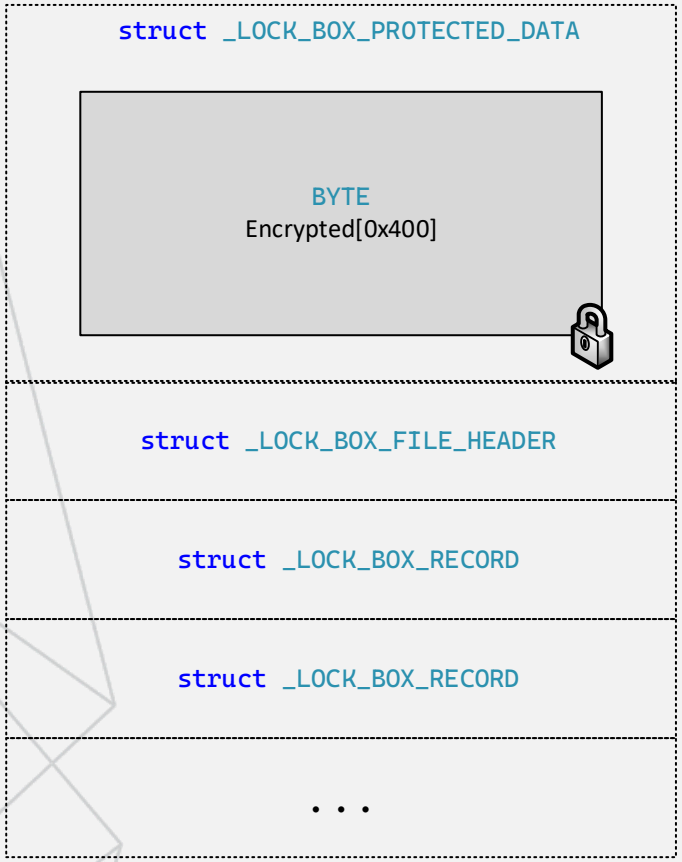
What do we know?

- 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

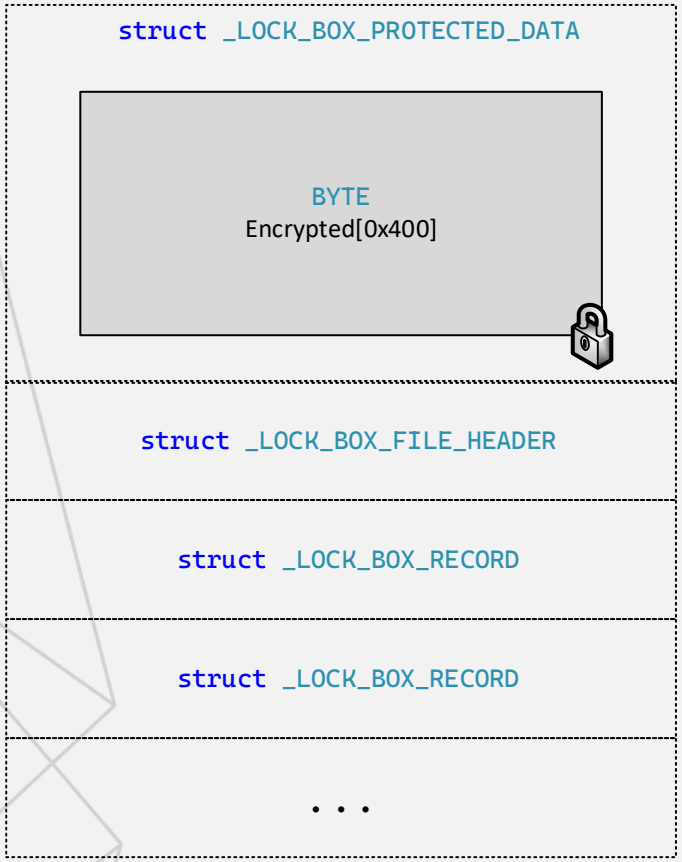


Database Format – Overview



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

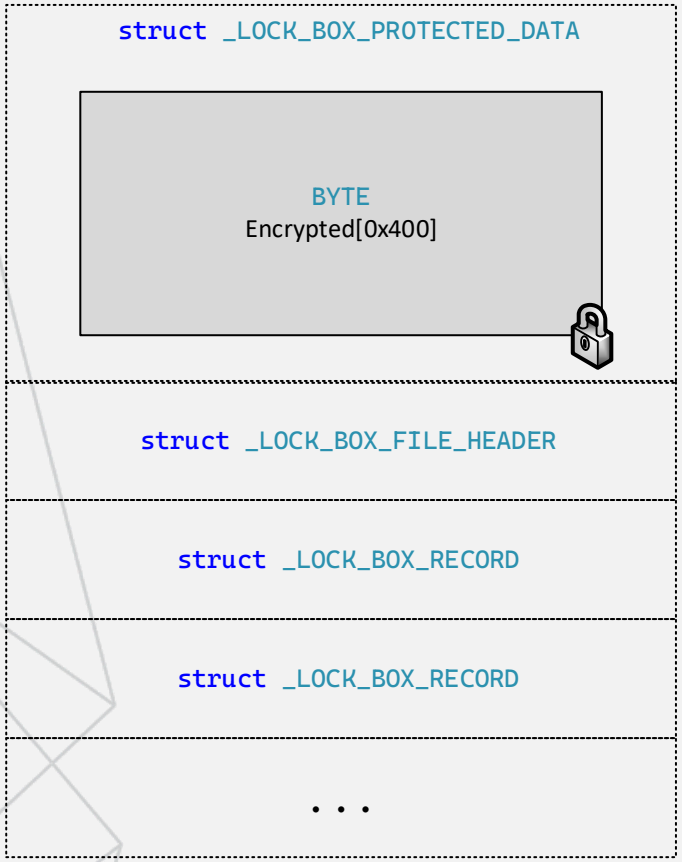
Database Format – Overview



- 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

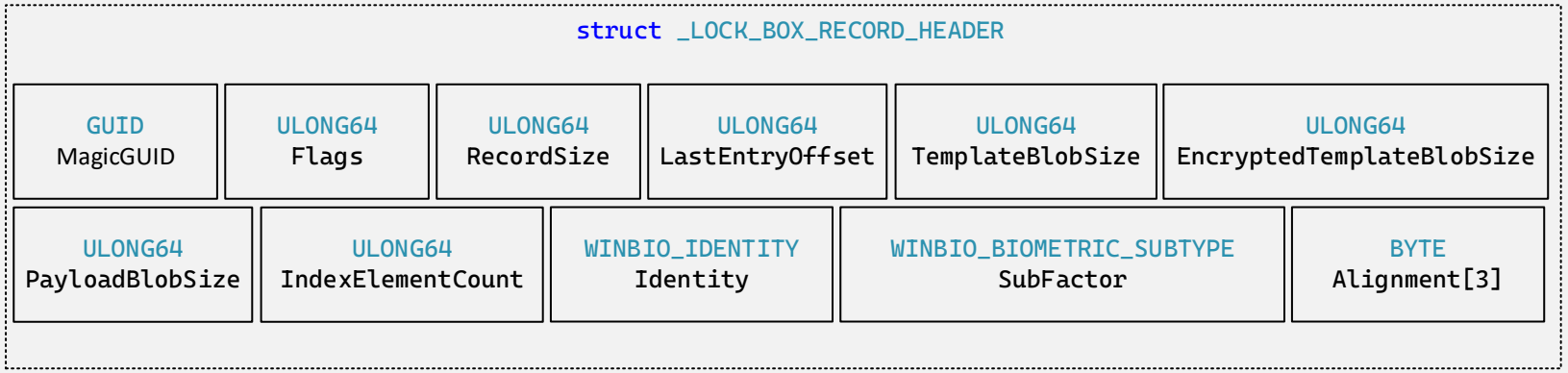


- The encrypted header:
  - Ensures the integrity of the database using a SHA256 hash.
  - Contains the AES key for the encrypted templates.
- The unencrypted header holds information regarding:
  - Version information.
  - Number of used records and available records.
- One record per enrolled user: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

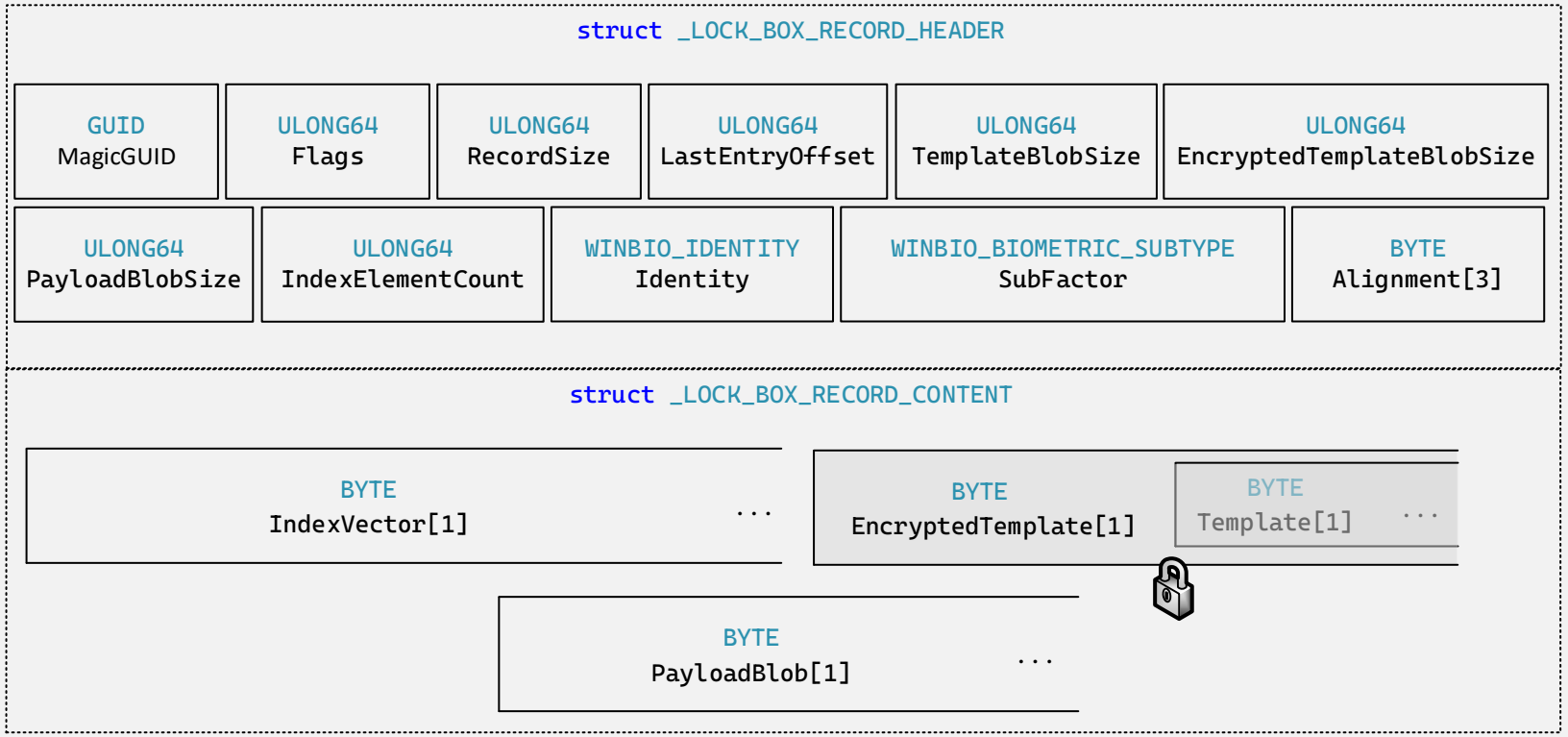
Database Format

```
struct _LOCK_BOX_RECORD_HEADER
```

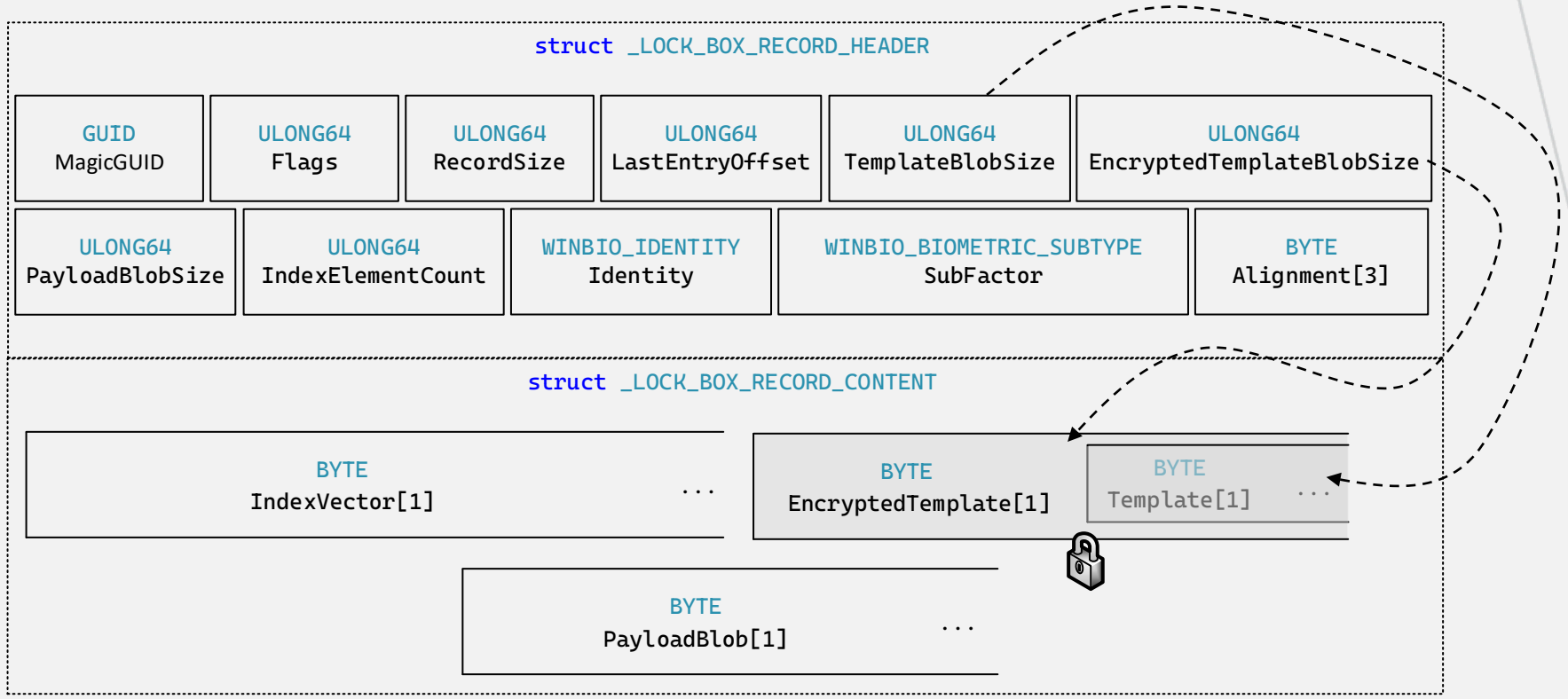
Database Format



Database Format



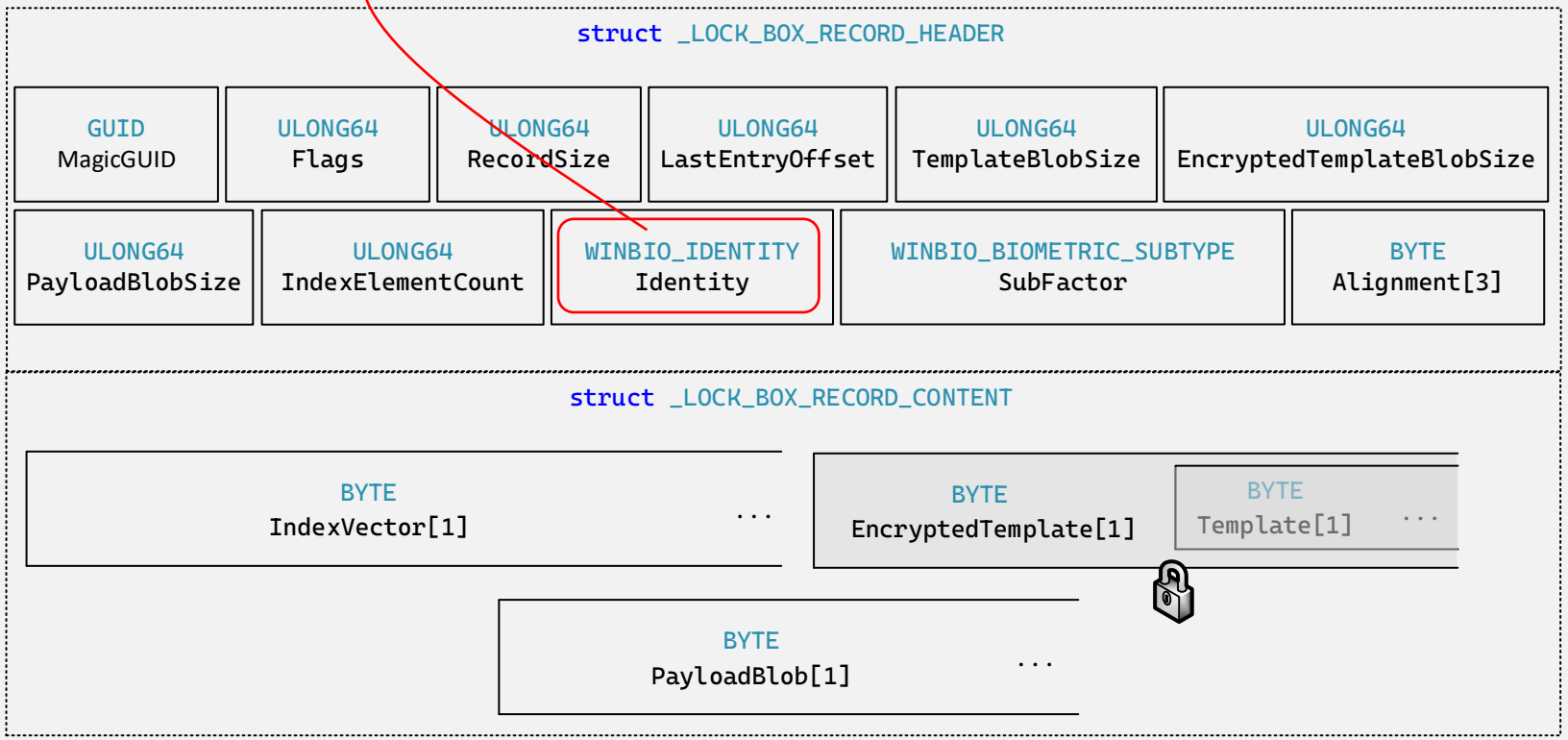
Database Format



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

Database Format

```
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;
```



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 😋.

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

Administrator: C:\WINDOWS\system32\cmd.exe

```
C:\WINDOWS\system32>C:\Users\user\Desktop\WHfB\WbioSrvcDecrypter.exe C:\Windows\System32\WinBi
oDatabase\DC576DA6-D676-4A15-906D-C0CEAF949543.DAT
Calculated Hash:
15FC65FD22756A4A7ABC9BD87F39A26C6A671EA98993AD5E8DAD795836191BF0
[INFO] Hashes match proceeding
LockBoxProtectedData {
  HeaderKeyDataBlob: dwMagic: 4D42444B, dwVersion: 1, cbKeySize: 32
  KeyDataBlob: AD09B4A7375310037BD969EC[illegible]0AC2636AB18C52ABD224D0A2C91B0A32D39F84B90000000000000
B0500000000000000
  Alignment: 0
  SizeHash: 32
  SizeKey: 0
  HashDigest: 15FC65FD22756A4A7ABC9BD87F39A26C6A671EA98993AD5E8DAD7[illegible]
  Key: 729C175C14E91F2667778B0952AE6DEE
}
LockBoxFileHeader {
  GuidDatabase: d1caed46-5b8d-4e7c-8a0e-34bcac166281
  Version: 2
  DatabaseID: dc576da6-d676-4a15-906d-c0ceaf949543
  Factor: 2
  Format: 5b3fba54-792b-40c7-8822-2efc0a255f78
  Alignment: 0
  IndexElementCount: 0
  TotalRecordCount: 2
  DeletedRecordCount: 0
```

Members

dwMag[illegible]

The magic value for the key.

This member must be the following val[illegible]

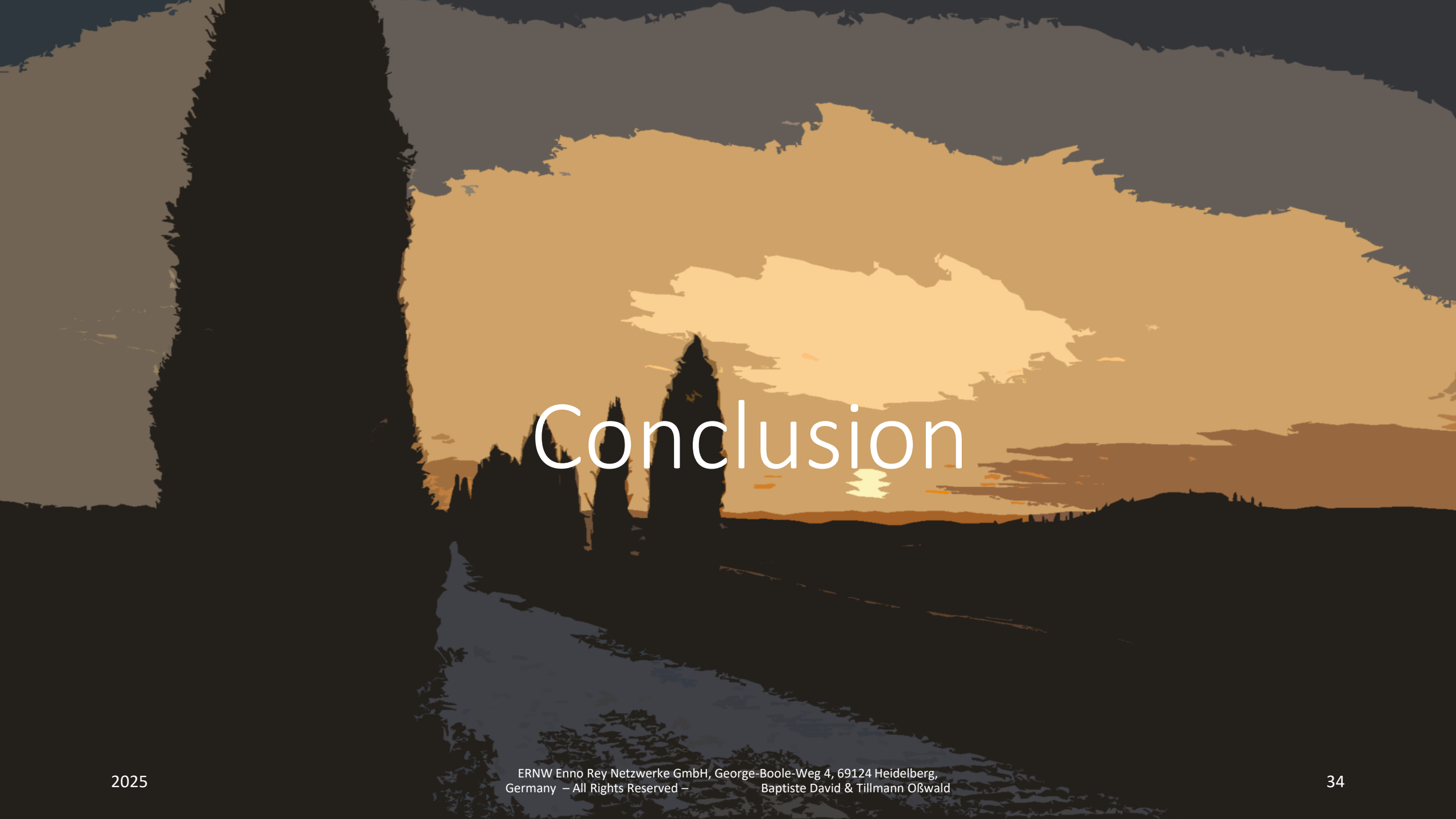
BCRYPT_KEY_DATA_BLOB_MAGIC (0x4d42444b)

Demo

It’s time to say hello 😁.

No Entropy – Big Problem

- This architecture allows us to:
  - Get access to **biometric data** – the holy grail of **mobile device security**.
    - We can change and extract this data!
  - Break the holy grail of **domain security** – **secure authentication**
    - In the worst case leading to Domain Administrator!



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!

Make the world a safer place

- If possible:
  - Use ESS mode and VBS!
- In any case:
  - Only one user per client!
- Also:
  - Consider only allowing PIN authentication.
  - Monitoring: Only WBS should open or modify the database.

Thank you for your attention

bdavid@ernw.de

tosswald@ernw.de

www.ernw.de

www.insinuator.net

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/
- Transition slides: https://www.socwall.com/