PLAI Biometrics Adapter Developer Guide

(Physical Logical Access Interoperability)

Security Classification:	Protected
Version:	1.5
Revision:	Rev1
Control:	Uncontrolled when printed
Date	06/27/2019

Disclaimer

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, PSIA disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and PSIA disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

No license, express or implied, by estoppel or otherwise, to any PSIA or PSIA member intellectual property rights is granted herein.

Except when a license is hereby granted by PSIA to copy and reproduce, this specification is for internal use only.

Contact the Physical Security Interoperability Alliance at info@psialliance.org for information on specification licensing through membership agreements.

Any logos and brands contained herein are the property of their respective owners.

Table of Contents

Purpose of this Document

This document covers the architecture and information flow of a PLAI system integration. The purpose and role of each component in the system is provided below.

1.0 References

1	PLAI Adapter Developer Guide
2	ISO Biometric Standard 19785-1-2015.pdf
3	PSIA Area Control Specification (Later than V3.1)

1. Introduction to PLAI Biometrics interoperability

1 .1 Purpose

Physical-Logical Access Interoperability (PLAI) was established to provide interoperability between disparate Physical Access Control Systems (PACS) by way of a common authoritative source. The biometrics specification extends the PLAI specification by facilitating the movement of biometric data as part of the PLAI framework. The PLAI specification is designed to allow interoperability between disparate and similar biometric systems by facilitating the movement of both proprietary and open standard biometric information, whether that be in raw or processed formats.

For a full explanation and implementation guide refer to the PLAI Adapter Developer Guide. This guide is provided only to highlight the additions to the main guide.

1 .2 Biometric Integration use cases

- Movement of biometric data between systems of biometric vendors that support the same modality of biometrics, for purposes of single enrolment.
- Movement of data between systems of the same biometric vendor to synchronize data across multiple sites.
- Movement of data between systems of the same biometric vendor for the purpose of consistency of biometric data, backup, scalability and high availability.
- Migration of biometric data from one system to another, ensuring both can continue to operate concurrently.
- Creation of a universal biometric enrolment station to share data across systems that can consume data across biometric systems.
- OSDP implementation for template on panel where the templates are sent back from the biometric system and the biometric template can be provided at the point of transaction.

1 .3 Basic Biometric Integration Process

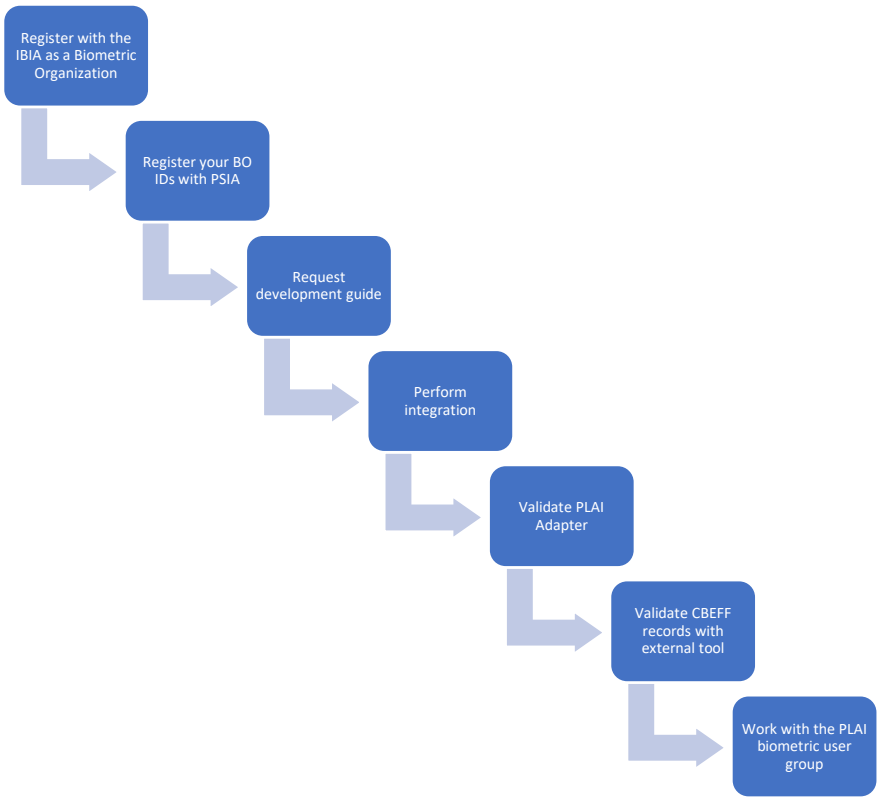

Figure 1 – Workflow to properly register a biometric vendor for formal compliance with PLAI

1.3 Profile

The PLAIBiometrics profile is an extension of the PLAIBase profile. (More information about PLAIBase can be found in the PLAI Adapter Developer Guide; Section 3.1) The implementation of the PLAIBiometrics profile is dependent on having the PLAIBase profile implemented.

The PLAI Agent will request the supported profiles from the PLAI Adapter and only if the PLAIBiometrics profile is supported will it send the relevant biometric extension information as part of the PLAIBase profile. This ensures smaller packets and lower network usage for adapters where biometric information is not relevant. Additionally, the separation of profiles provides backward compatibility with all systems that have already created a PLAI adapter.

1.4 Basic Data Structure

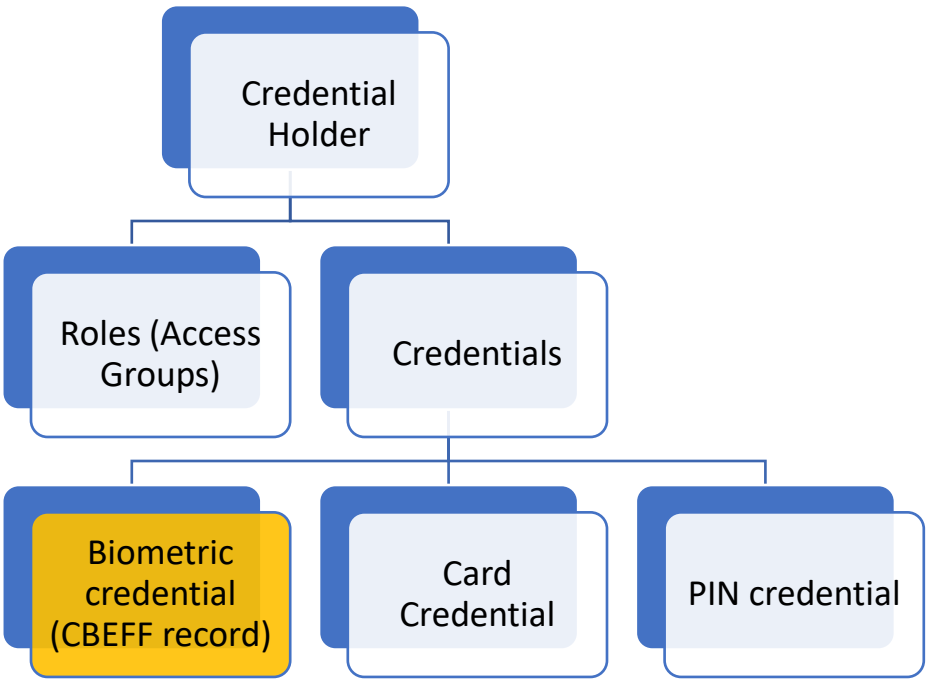

Figure 2 – PLAIBase with PLAIBiometric credential extension (highlighted in gold)

The basic structure of the PLAIBase specification can be seen in Figure 2. The biometric data specification extends an existing credential. Each biometric record will have its own credential represented separately from other types of credentials like Card, PIN, Tag etc. The CredentialInfo structure makes use of a type property that specifies the nature of credential being used.

The biometric data is encoded in a CBEFF (Common Biometric Exchange Format Framework) record. This is an open international standard used by government as well as private organizations to facilitate the transfer of biometrics between biometric systems. The full details of the CBEFF structure are not described in this document and can be found in the ISO Biometric Standard 19785-1-2015.

1.5.1 CredentialInfo

The basic CredentialInfo class structure follows the following XML structure for a biometric record.

```
<CredentialInfo version="1.0">
	<ID>0</ID>
	<UID>{01dc2123-9999-4444-0034-111110222111}</UID>
	<Name>Idemia Record</Name>
	<Description>Idemia Record for interoperability</Description>
	<AssignedToID>
		<GUID>{21c3c623-3181-42e7-9426-cd40a65f65ac}</GUID>
	</AssignedToID>
	<State>Active</State>
	<IdentifierInfoList>
		<IdentifierInfo>
			<Type>Biometric</Type>
			<Value>CBEFF RECORD HERE</Value>
			<ValueEncoding>Base64</ValueEncoding>
```

```
            </IdentifierInfo>
        </IdentifierInfoList>
        <PermissionIDList />
</CredentialInfo>
```

CredentialInfo	ID	
	UID	
	Name	
	Description	
	AssignedToID	ID; or
		UID
	Version	
	Disability	
	Valid From	
	Valid To	
	State (Active/Damaged/Destroyed/Expired Inactive/Lost/Stolen)	
	IdentifierInfoList	Type (Card/**Biometric**/Keyfob/PIN)
		Value Encoding (Base64, Decimal, Hex, String)
		Value – **CBEFF Record**
	CardComponentList	Type
		ValueEncoding
		Value

2. Common Biometrics Exchange Format Framework (CBEFF)

2 .1 Prerequisites: Biometric Organization Registration

Prior to starting the biometrics integration, the PSIA mandates that all organizations be registered with the International Biometrics Identity Association (IBIA) as a Biometric Organization. This registration will assign an organization identifier to your organization. The identifier that is allocated to your organization is used in all CBEFF records that contain information from your biometrics organization. This allows the receiver of the CBEFF record to identify the organization from where the biometric data originated.

To register as a biometrics organization, go to https://www.ibia.org/cbeff/iso

To check if your organization as has already been registered with the IBIA go to https://www.ibia.org/cbeff/iso/biometric-organizations. This site will show you the organization identifier in both hexadecimal and decimal format.

2 .2 CBEFF Specification

The full details of the CBEFF specification can be found in the ISO Biometric Standard 19785-1-2015 document. At the time of writing this document, the version in use was ISO/IEC 19785-1 (Second Edition 2015-08-01). The PSIA are not licensed to provide the full CBEFF, only the PLAIBiometric derivative. To purchase a copy of the full specification document go to https://www.iso.org/standard/66179.html

2 .3 Supported CBEFF structures

PLAIBiometric supports only the Simple and Complex BIR structures as defined in the CBEFF standard.

1. **Simple BIR structure**: Usually only contains a single biometric record (e.g. 2 iris images, or a set of 4 fingerprint images of right hand) per CBEFF structure, because it only has a single Standard Biometric Header (SBH) that describes the data.
2. **Complex BIR structure**: Contains multiple and tiered levels of the SBH to allow for all biometrics belonging to a single credential holder to be transmitted in on CBEFF record. This allows for multiple records of the same modality (e.g. Left and Right IRIS and 10 fingerprints) and well as multiple modalities such as Fingerprint, Face, Iris, and Palm Vein. This is of value when a manufacturer supports multiple modalities of biometrics that cannot be described in a single SBH.
3. **Multiple CBEFF BIR structure**: Allows for the aggregation of multiple CBEFF credentials into a single record and is therefore not suitable for PLAI currently.

The multiple CBEFF BIR structure is **NOT** supported as part of the PSIABiometrics profile.

2 .4 Data Flow and resolution

1. When a new biometric record is created, the PLAI Agent will be notified and it will distribute the record to all listening systems that has implemented the PSIABiometrics profile. Each system receiving a CBEFF record will be responsible for processing the message to determine if the record is relevant to that biometric system. Examples of non-relevant data:
    a. A fingerprint system receives a CBEFF record containing data from an Iris system, it will discard the information it receives as it has no relevance to a fingerprint system.
    b. A fingerprint system receives proprietary templates from a different fingerprint system, it would ignore these messages.
2. To facilitate conflict resolution the PLAIBiometric information being sent regarding the CBEFF record contains a Created Date and Last Updated Date as part of the CredentialInfo. (Refer to Area Control Specification; Section 1.12)
3. The PLAIBiometric extension provides no mechanism for biometric deduplication or duplication detection.

2 .5 Biometric Organization Specific Identifiers

The CBEFF record has many fields that are specific to a biometric manufacturer. Examples of these fields include:

- BDB_capture_device_type
- BDB_capture_device_subtype
- CBEFF_BDB_format_type
- CBEFF_BDB_comparison_algorithm_type

- CBEFF_BDB_feature_extraction_algorithm_type
- CBEFF_BDB_compression_algorithm_type
- CBEFF_BDB_PAD_technique
- CBEFF_BDB_product_type
- CBEFF_BDB_quality_algorithm_type

The PSIA does not require that you register these fields with the IBIA but does **recommend** that you register them with the PSIA. These identifiers will be included as an Annex to this document for other manufacturers to interface with. An online representation of these will also be available at https://psialliance.org.

2 .6 CBEFF Validation Tools and development tools

The PSIA does not provide any tools to validate a CBEFF structure. The following tool can be downloaded to determine the validity of your CBEFF record. https://www.nist.gov/itl/computer-security-division/biometrics-resource-center-website/nistitl-conformance-test-suite.

There are also pay ware SDK's available that simplify the creation of the CBEFF record. PSIA do not endorse any vendors implementation and biometric vendors are responsible for the entirety of their compliant PLAI Adapters. Here are some examples of these SDK's:

https://www.aware.com/biometrics/nistpack/

http://www.netxsolutions.co.uk/impexlibrary.aspx

https://www.lakotasoftware.com

Note: The PSIA has not tested any of the SDK's mentioned above. It still remains the responsibility of the integrator to ensure the validity of the CBEFF record.

3. Biometric Standards

Interoperability is critical when sharing biometrics between disparate biometric systems for interoperability it is important to be conscientious on the type of biometric information being sent and the formatting of biometric records. The below is an informative list and is meant to be understood as recommended best practices for biometric interoperability.

3 .1 Biometric format standard representations

PSIA strongly encourage the use of standards based biometric formats. At the time of this publication Table 1 contains a list of standard published specifications. The below are industry formats that are open-standard and non-supplier specific formats for interoperability between biometric brands.

Biometric Modality	**RAW formats (e.g. Images)**	**PROCESSED formats (e.g. Minutiae extracted template data)**

Iris	640c480 8-bit greyscale data structure	ISO/IEC 19794-6:2011: IMAGE_TYPE_VGA, PNG or JPEG2000 (lossy and lossless) image type
Face	JPEG BMP	ISO/IEC 19794-5:2011: Full Frontal Image Type, JPEG or BMP
Fingerprint	WSQ (Preferred) PNG JPEG RAW	ISO19794-2 ISO19794-2; 2011 ANSI INCITS 378

Table 1 – Biometric Capture Standards