|  |  |
| --- | --- |
|  | Moving Picture, Audio and Data Coding by Artificial Intelligencewww.mpai.community |

|  |  |
| --- | --- |
|  |  |
| **N728** | 2022/06/22 |
| **Source** | AIF-DC |
| **Title** | MPAI-AIF Use Cases and Functional Requirements WD1.3 |
| **Target** | MPAI Members |

[1 Introduction 1](#_Toc101799298)

[2 Use Cases 2](#_Toc101799299)

[3 Terms specific to MPAI-AIF V2 2](#_Toc101799300)

[4 Functional Requirements 3](#_Toc101799301)

[5 References 4](#_Toc101799302)

[5.1 Normative References 4](#_Toc101799303)

[5.2 Informative References 4](#_Toc101799304)

[Annex 1 – MPAI-wide terms and definitions 5](#_Toc101799305)

[Annex 2 - Notices and Disclaimers Concerning MPAI Standards (Informative) 8](#_Toc101799306)

[Annex 3 – The Governance of the MPAI Ecosystem (Informative) 10](#_Toc101799307)

# Introduction

In recent years, Artificial Intelligence (AI) and related technologies have been applied to a broad range of applications, have started affecting the life of millions of people and are expected to do so even more in the future. As digital media standards have positively influenced industry and billions of people, so AI-based data coding standards are expected to have a similar positive impact. Indeed, research has shown that data coding with AI-based technologies is generally *more efficient* than with existing technologies for, e.g., compression and feature-based description.

However, some AI technologies may carry inherent risks, e.g., in terms of bias toward some classes of users. Therefore, the need for standardisation is more important and urgent than ever.

The international, unaffiliated, not-for-profit MPAI – Moving Picture, Audio and Data Coding by Artificial Intelligence Standards Developing Organisation has the mission to develop *AI-enabled data coding standards*. MPAI Application Standards enable the development of AI-based products, applications and services.

As a part of its mission, MPAI has developed standards operating procedures to enable users of MPAI implementations to make informed decision about their applicability. Central to this is the notion of Performance, defined as a set of attributes characterising a reliable and trustworthy implementation.

For the aforementioned reasons, to fully achieve the MPAI mission, Technical Specifications must be complemented by an ecosystem designed, created and managed to underpin the life cycle of MPAI standards through the steps of specification, technical testing, assessment of product safety and security, and distribution.

In the following, Terms beginning with a capital letter are defined in Table 1 if they are specific to this Standard and in Table 2 if they are common to all MPAI Standards.

The MPAI Ecosystem is fully specified in [1]. It is composed of:

* MPAI as provider of Technical, Conformance and Performance Specifications.
* Implementers of MPAI standards.
* MPAI-appointed Performance Assessors.
* The MPAI Store which takes care of secure distribution of validated Implementations.

Figure 1depicts Version 1 of the MPAI-AIF Reference Model under which Implementations of MPAI Application Standards and user-defined MPAI-AIF conforming applications operate.

An AIF Implementation allows execution of AI Workflows (AIW), composed of basic processing elements called AI Modules (AIM).



*Figure 1 – The AI Framework (AIF) Reference Model and its Components*

MPAI Application Standards normatively specify Syntax and Semantics of the input and output data and the Function of the AIW and the AIMs, and the Connections between and among the AIMs of an AIW.

In particular, an AIM is defined by its Function and data, but not by its internal architecture, which may be based on AI or data processing, and implemented in software, hardware or hybrid software and hardware technologies.

MPAI defines Interoperability as the ability to replace an AIW or an AIM Implementation with a functionally equivalent Implementation. MPAI also defines 3 Interoperability Levels of an AIW executed in an AIF:

*Level 1 –* Implementer-specific and satisfying the MPAI-AIF Standard.

*Level 2 –* Specified by an MPAI Application Standard.

*Level 3 –* Specified by an MPAI Application Standard and certified by a Performance Assessor.

MPAI offers Users access to the promised benefits of AI with a guarantee of increased transparency, trust and reliability as the Interoperability Level of an Implementation moves from 1 to 3. Additional information on Interoperability Levels is provided in Annex 3.

# Scope of this document

This document specifies the functional requirements of the planned MPAI-AIF V2 standard, an extension of the MPAI-AIF V1.1 standard designed to add a security infrastructure to the AI Framework standard of [2] so that AIF V2 Components can access security services provided by a security infrastructure.

MPAI-AIF V2 will be developed by the MPAI *AI Framework Development Committee* (AIF-DC).

# Terms specific to MPAI-AIF V2

*Table 1* defines the Terms used in this document whose first letter is capital*.* The Terms of MPAI-wide applicability are defined in Table 2.

*Table 1 – Terms and definitions*

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Attestation Service | A mechanism for software to prove its identity. The goal of attestation is for a party to prove to a remote party that its operating system and application software are intact and trustworthy. The remote party trusts that attestation data is accurate because it is signed by a Trusted Platform Module (TPM) whose key is certified by the Certification Authority (CA). |
| Certification Authority | A trusted entity that manages and issues security certificates and public keys that are used for secure communication in a public network. |
| Crypto Engine | A self-contained, redundant cryptographic module designed to be integrated into devices. |
| Root of Trust | (RoT) A source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, RoT schemes generally include a hardened hardware module. |
| Threat Model | The result of a procedure for optimising application, system or business process security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent or mitigate the effects of threats to the system. |
| Trusted Service | Any of Attestation Service Trusted Communication Service, Trusted Communication Service, and Trusted Storage Service |
| Trusted Communication Service | Any service provided for the purpose of secure transmission of data without regard to the transmission protocol employed, whether or not the transmission medium is public or private. |
| Trusted Platform Module | A specialised hardware and embedded software that is designed to secure hardware with integrated cryptographic keys. |
| Trusted Storage Service | A service providing protected (encrypted) persistent storage. |

# Functional Requirements

AIF V1 is based on the assumption that the whole AI Framework runs in a Trusted Zone without specifying any trusted service that an implementer should follow.

AIF-V2 intends to identify specific trusted services to support the implementation of a Trusted Zone meeting a set of functional requirements by enabling AIF Components to access trusted services via APIs as defined in *Table 1*, such as:

1. Encryption Service.
2. Attestation Service.
3. Trusted Communication Service.
4. Trusted AIM Model Services
5. Trusted AIM Storage Service
6. AIM Security Engine.

Figure 2 represents the Reference Model of MPAI-AIF V2.



Figure 2 - Reference Model of MPAI-AIF V2

The MPAI-AIF V2 standard extends the functionalities specified in the MPAI-AIF V1 standard. Specifically, to enable the following functionalities, the following is required:

1. The AIF Components shall access high-level implementation-independent Trusted Services API to handle:
	1. Encryption Service.
	2. Attestation Service.
	3. Trusted Communication Service.
	4. Trusted AIM Storage Service including the following functionalities:
		1. Initialisation (secure and non-secure flash and RAM)
		2. Read/Write.
		3. De-initialisation.
	5. Trusted AIM Model Services including the following functionalities:
		1. Secure and non-secure Model Storage.
		2. Model Update.
		3. Model Validation.
	6. AIM Security Engine including the following functionalities:
		1. Model Encryption.
		2. Model Signature.
		3. Model Watermarking.
2. The AIF Components shall be easily integrated with the above Services.
3. The AIF Trusted Services shall be able to use hardware and OS security features already existing in the hardware and software of the environment in which the AIF is implemented.
4. Application developers shall be able to select the application’s security either or both by:
	1. Level of security that includes a defined set of security features for each level.
	2. Developer-defined security, i.e., a level that includes a developer-defined set of security features.
5. The specification of the AIF V2 Metadata shall be an extension of the AIF V1 Metadata supporting security with either or both standardised and developer-defined levels.

MPAI welcomes the submission of use cases and their respective threat models.

# References

## Normative References

MPAI-AIF V2 will normatively reference the following documents:

1. The Governance of the MPAI Ecosystem (MPAI-GME), https://mpai.community/standards/mpai-gme/.
2. Technical Specification: AI Framework (MPAI-AIF) V1.1, <https://mpai.community/standards/mpai-aif/>.

## Informative References

1. https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/bare.pdf

# Annex 1 – MPAI-wide terms and definitions

The Terms used in this standard whose first letter is capital and are not already included in *Table 1* are defined in Table 2*.*

*Table 2 – MPAI-wide Terms*

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Access | Static or slowly changing data that are required by an application such as domain knowledge data, data models, etc. |
| AI Framework (AIF) | The environment where AIWs are executed. |
| AI Module (AIM) | A processing element receiving AIM-specific Inputs and producing AIM-specific Outputs according to according to its Function. An AIM may be an aggregation of AIMs. |
| AI Workflow (AIW) | A structured aggregation of AIMs implementing a Use Case receiving AIW-specific inputs and producing AIW-specific inputs according to its Function. |
| AIF Metadata | The data set describing the capabilities of an AIF set by the AIF Implem­enter. |
| AIM Metadata | The data set describing the capabilities of an AIM set by the AIM Implem­enter. |
| Application Programming Interface (API) | A software interface that allows two applications to talk to each other |
| Application Standard  | An MPAI Standard specifying AIWs, AIMs, Topologies and Formats suitable for a particular application domain. |
| Channel | A physical or logical connection between an output Port of an AIM and an input Port of an AIM. The term “connection” is also used as a synonym. |
| Communication | The infrastructure that implements message passing between AIMs. |
| Component | One of the 9 AIF elements: Access, AI Module, AI Workflow, Commun­ication, Controller, Internal Storage, Global Storage, MPAI Store, and User Agent. |
| Conformance | The attribute of an Implementation of being a correct technical Implem­entation of a Technical Specification. |
| Conformance Tester | An entity authorised by MPAI to Test the Conformance of an Implementation. |
| Conformance Testing | The normative document specifying the Means to Test the Conformance of an Implementation. |
| Conformance Testing Means | Procedures, tools, data sets and/or data set characteristics to Test the Conformance of an Implementation. |
| Connection | A channel connecting an output port of an AIM and an input port of an AIM. |
| Controller | A Component that manages and controls the AIMs in the AIF, so that they execute in the correct order and at the time when they are needed. |
| Data | Information in digital form. |
| Data Format | The standard digital representation of Data. |
| Data Semantics | The meaning of Data. |
| Device | A hardware and/or software entity running at least one instance of an AIF. |
| Ecosystem | The ensemble of the following actors: MPAI, MPAI Store, Implementers, Conformance Testers, Performance Testers and Users of MPAI-AIF Im­plementations as needed to enable an Interoperability Level. |
| Event | An occurrence acted on by an Implementation. |
| Explainability | The ability to trace the output of an Implementation back to the inputs that have produced it. |
| Fairness | The attribute of an Implementation whose extent of applicability can be assessed by making the training set and/or network open to testing for bias and unanticipated results. |
| Function | The operations effected by an AIW or an AIM on input data. |
| Global Storage | A Component to store data shared by AIMs. |
| Identifier | A name that uniquely identifies an Implementation. |
| Implementation | 1. An embodiment of the MPAI-AIF Technical Specification, or
2. An AIW or AIM of a particular Level (1-2-3).
 |
| Internal Storage | A Component to store data of the individual AIMs. |
| Interoperability | The ability to functionally replace an AIM/AIW with another AIM/AIW having the same Interoperability Level |
| Interoperability Level | The attribute of an AIW and its AIMs to be executable in an AIF Implementation and to be: 1. Implementer-specific and satisfying the MPAI-AIF Standard *(Level 1)*.
2. Specified by an MPAI Application Standard (*Level 2)*.
3. Specified by an MPAI Application Standard and certified by a Performance Assessor (*Level 3)*.
 |
| Knowledge Base | Structured and/or unstructured information made accessible to AIMs via MPAI-specified interfaces |
| Message | A sequence of Records. |
| Normativity | The set of attributes of a technology or a set of technologies specified by the applicable parts of an MPAI standard. |
| Performance | The attribute of an Implementation of being Reliable, Robust, Fair and Replicable. |
| Performance Assessment | The normative document specifying the procedures, the tools, the data sets and/or the data set characteristics to Assess the Grade of Performance of an Implementation. |
| Performance Assessment Means | Procedures, tools, data sets and/or data set characteristics to Assess the Performance of an Implementation. |
| Performance Assessor | An entity authorised by MPAI to Assess the Performance of an Implementation in a given Application domain |
| Port | A physical or logical communication interface of an AIM. |
| Profile | A particular subset of the technologies used in MPAI-AIF or an AIW of an Application Standard and, where applicable, the classes, other subsets, options and parameters relevant to that subset. |
| Record | Data with a specified structure. |
| Reference Model | The AIMs and theirs Connections in an AIW. |
| Reference Software | A technically correct software implementation of a Technical Specific­ation containing source code, or source and compiled code.  |
| Reliability | The attribute of an Implementation that performs as specified by the Application Standard, profile and version the Implementation refers to, e.g., within the application scope, stated limitations, and for the period of time specified by the Implementer. |
| Replicability | The attribute of an Implementation whose Performance, as Assessed by a Performance Assessor, can be replicated, within an agreed level, by another Performance Assessor. |
| Robustness | The attribute of an Implementation that copes with data outside of the stated application scope with an estimated degree of confidence. |
| Scope | The domain of applicability of an MPAI Application Standard. |
| Service Provider | An entrepreneur who offers an Implementation as a service (e.g., a recommendation service) to Users. |
| Specification | A collection of normative clauses. |
| Standard | The ensemble of Technical Specification, Reference Software, Conformance Testing and Performance Assessment of an MPAI application Standard.  |
| Technical Specification | (Framework) the normative specification of the AIF.(Application) the normative specification of the set of AIWs belon­ging to an application domain along with the AIMs required to Im­plem­ent the AIWs that includes:1. The formats of the Input/Output data of the AIWs implementing the AIWs.
2. The Connections of the AIMs of the AIW.
3. The formats of the Input/Output data of the AIMs belonging to the AIW.
 |
| Testing Laboratory | A laboratory accredited by MPAI to Assess the Grade of Performance of Implementations.  |
| Time Base | The protocol specifying how AIF Components can access timing information. |
| Topology | The set of AIM Connections of an AIW. |
| Use Case | A particular instance of the Application domain target of an Application Standard. |
| User | A user of an Implementation. |
| User Agent | The Component interfacing the user with an AIF through the Controller |
| Version | A revision or extension of a Standard or of one of its elements. |
| Zero Trust | A cybersecurity model primarily focused on data and service protection that assumes no implicit trust. |

# Annex 2 - Notices and Disclaimers Concerning MPAI Standards (Informative)

The notices and legal disclaimers given below shall be borne in mind when [downloading](https://www.mpai.community/resources/) and using approved MPAI Standards.

In the following, “Standard” means the collection of four MPAI-approved and [published](https://www.mpai.community/resources/) documents: “Technical Specification”, “Reference Software” and “Conformance Testing” and, where applicable, “Performance Testing”.

Life cycle of MPAI Standards

MPAI Standards are developed in accordance with the [MPAI Statutes](https://mpai.community/statutes/). An MPAI Standard may only be developed when a Framework Licence has been adopted. MPAI Standards are developed by especially established MPAI Development Committees who operate on the basis of consensus, as specified in Annex 1 of the [MPAI Statutes](https://mpai.community/statutes/). While the MPAI General Assembly and the Board of Directors administer the process of the said Annex 1, MPAI does not independently evaluate, test, or verify the accuracy of any of the information or the suitability of any of the technology choices made in its Standards.

MPAI Standards may be modified at any time by corrigenda or new editions. A new edition, however, may not necessarily replace an existing MPAI standard. Visit the [web page](https://mpai.community/resources/) to determine the status of any given published MPAI Standard.

Comments on MPAI Standards are welcome from any interested parties, whether MPAI members or not. Comments shall mandatorily include the name and the version of the MPAI Standard and, if applicable, the specific page or line the comment applies to. Comments should be sent to the MPAI Secretariat. Comments will be reviewed by the appropriate committee for their technical relevance. However, MPAI does not provide interpretation, consulting information, or advice on MPAI Standards. Interested parties are invited to join MPAI so that they can attend the relevant Development Committees.

Coverage and Applicability of MPAI Standards

MPAI makes no warranties or representations of any kind concerning its Standards, and expressly disclaims all warranties, expressed or implied, concerning any of its Standards, including but not limited to the warranties of merchantability, fitness for a particular purpose, non-infringement etc. MPAI Standards are supplied “AS IS”.

The existence of an MPAI Standard does not imply that there are no other ways to produce and distribute products and services in the scope of the Standard. Technical progress may render the technologies included in the MPAI Standard obsolete by the time the Standard is used, especially in a field as dynamic as AI. Therefore, those looking for standards in the Data Compression by Artificial Intelligence area should carefully assess the suitability of MPAI Standards for their needs.

IN NO EVENT SHALL MPAI BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

MPAI alerts users that practicing its Standards may infringe patents and other rights of third parties. Submitters of technologies to this standard have agreed to licence their Intellectual Property according to their respective Framework Licences.

Users of MPAI Standards should consider all applicable laws and regulations when using an MPAI Standard. The validity of Conformance Testing is strictly technical and refers to the correct implementation of the MPAI Standard. Moreover, positive Performance Assessment of an implementation applies exclusively in the context of the [MPAI Governance](https://mpai.community/governance/) and does not imply compliance with any regulatory requirements in the context of any jurisdiction. Therefore, it is the responsibility of the MPAI Standard implementer to observe or refer to the applicable regulatory requirements. By publishing an MPAI Standard, MPAI does not intend to promote actions that are not in compliance with applicable laws, and the Standard shall not be construed as doing so. In particular, users should evaluate MPAI Standards from the viewpoint of data privacy and data ownership in the context of their jurisdictions.

Implementers and users of MPAI Standards documents are responsible for determining and complying with all appropriate safety, security, environmental and health and all applicable laws and regulations.

Copyright

MPAI draft and approved standards, whether they are in the form of documents or as web pages or otherwise, are copyrighted by MPAI under Swiss and international copyright laws. MPAI Standards are made available and may be used for a wide variety of public and private uses, e.g., implementation, use and reference, in laws and regulations, and standardisation. By making these documents available for these and other uses, however, MPAI does not waive any rights in copyright to its Standards. For inquiries regarding the copyright of MPAI standards, please contact the MPAI Secretariat.

The Reference Software of an MPAI Standard is released with the [MPAI Modified Berkeley Software Distribution licence](https://mpai.community/about/licence/). However, implementers should be aware that the Reference Software of an MPAI Standard may reference some third party software that may have a different licence.

# Annex 3 – The Governance of the MPAI Ecosystem (Informative)

**Level 1 Interoperability**

With reference to Figure 1, MPAI issues and maintains a standard – called MPAI-AIF – whose components are:

1. An environment called AI Framework (AIF) running AI Workflows (AIW) composed of inter­connected AI Modules (AIM) exposing standard interfaces.
2. A distribution system of AIW and AIM Implementation called MPAI Store from which an AIF Implementation can download AIWs and AIMs.

A Level 1 Implementation shall be an Implementation of the MPAI-AIF Technical Specification executing AIWs composed of AIMs able to call the MPAI-AIF APIs.

|  |  |
| --- | --- |
| Implementers’ benefits | Upload to the MPAI Store and have globally distributed Implementations of* AIFs conforming to MPAI-AIF.
* AIWs and AIMs performing prop­rietary functions executable in AIF.
 |
| Users’ benefits | Rely on Implementations that have been tested for security. |
| MPAI Store’s role | * Tests the Conformance of Implementations to MPAI-AIF.
* Verifies Implementations’ security, e.g., absence of malware.
* Indicates unambiguously that Implementations are Level 1.
 |

**Level 2 Interoperability**

In a Level 2 Implem­entation, the AIW must be an Implementation of an MPAI Use Case and the AIMs must con­form with an MPAI Applicati­on Standard.

|  |  |
| --- | --- |
| Implementers’ benefits | Upload to the MPAI Store and have globally distributed Implementations of* AIFs conforming to MPAI-AIF.
* AIWs and AIMs conforming to MPAI Application Standards.
 |
| Users’ benefits | * Rely on Implementations of AIWs and AIMs whose Functions have been reviewed during standardisation.
* Have a degree of Explainability of the AIW operation because the AIM Func­tions and the data Formats are known.
 |
| Market’s benefits | * Open AIW and AIM markets foster competition leading to better products.
* Competition of AIW and AIM Implementations fosters AI innovation.
 |
| MPAI Store’s role | * Tests Conformance of Implementations with the relevant MPAI Standard.
* Verifies Implementations’ security.
* Indicates unambiguously that Implementations are Level 2.
 |

**Level 3 Interoperability**

MPAI does not generally set standards on how and with what data an AIM should be trained. This is an important differentiator that promotes competition leading to better solutions. However, the performance of an AIM is typically higher if the data used for training are in greater quantity and more in tune with the scope. Training data that have large variety and cover the spec­trum of all cases of interest in breadth and depth typically lead to Implementations of higher “quality”.

For Level 3, MPAI normatively specifies the process, the tools and the data or the characteristics of the data to be used to Assess the Grade of Performance of an AIM or an AIW.

|  |  |
| --- | --- |
| Implementers’ benefits | May claim their Implementations have passed Performance Assessment. |
| Users’ benefits | Get assurance that the Implementation being used performs correctly, e.g., it has been properly trained. |
| Market’s benefits | Implementations’ Performance Grades stimulate the development of more Performing AIM and AIW Implementations. |
| MPAI Store’s role | * Verifies the Implementations’ security
* Indicates unambiguously that Implementations are Level 3.
 |

**The MPAI ecosystem**

The following 

 is a high-level description of the MPAI ecosystem operation applicable to fully conforming MPAI implementations:

1. MPAI establishes and controls the not-for-profit MPAI Store.
2. MPAI appoints Performance Assessors.
3. MPAI publishes Standards.
4. Implementers submit Implementations to Performance Assessors.
5. If the Implementation Performance is acceptable, Performance Assessors inform Implementers and the MPAI Store.
6. Implementers submit Implementations to the MPAI Store tested for Confor­mance and security.
7. Users download and use Implementations, and submit experience scores.



*Figure 3 – The MPAI ecosystem operation*