Technical rules

Technical requirements and procedures for the certification of Digital Procurement Platforms

Version 1.0 of 1 June 2023

AGID | Via Liszt, 21 – 00144 Rome | protocollo@pec.agid.gov.it | www.agid.gov.it | Tel. 06 85264.1

Summary

Introduction

Legislative Decree No 36 of 31 March 2023, published in Official Gazette No 77 of 31 March 2023 (hereinafter the Code) provides, pursuant to Article 26(1) thereof, that the Agency for a Digital Italy (hereinafter AGID), in agreement with ANAC and the Prime Minister's Office, the Department for the Digital Transformation, must establish, by means of its own measure, the technical requirements for digital procurement platforms referred to in Article 25 of the Code, as well as the compliance of such platforms with the provisions of Article 22(2).

In the context of the same measure, pursuant to Article 26(2) of the Code, the AGID is also required to establish the procedures for the certification of digital procurement platforms.

Pursuant to Article 106(3) of the Code and with reference to distributed ledger technologies referred to in Article 8*b*, paragraph 1, of Decree-Law No 135 of 14 December 2018, converted, with amendments, by Law No 12 of 11 February 2019, these Technical Rules lay down the characteristics of platforms for the management of guarantees operating using distributed ledger technologies.

These Technical Rules are adopted in implementation of Part II of Book I of the Code on the Digitalisation of the Life Cycle of Public Contracts, the provisions of which aim to reduce the time needed to prepare tenders, simplify procedures and reduce disputes, helping to improve the overall administrative efficiency and administrative burden on companies by encouraging wider participation by them, and go beyond the provisions of Ministerial Decree No 148 of 12 August 2021.

The digitalisation of the life cycle of public procurement contracts is based on compliance with the principles and provisions of the Digital Administration Code (CAD) referred to in Legislative Decree No 82 of 7 March 2005, and on the training, acquisition and management of natively digital documents through digital infrastructure platforms and services enabling the life cycle management of public contracts and digital procurement platforms, which make up the national digital procurement ecosystem referred to in Article 22 of the Code.

These Technical Rules **may** be updated to take into account the evolution of both the Italian and European regulatory framework and the reference technological standards.

1. Scope

1.1 Subjective scope

These Technical Rules are issued pursuant to Article 26(1) of the Code, in accordance with the provisions of the Digital Administration Code (CAD) referred to in Legislative Decree No 82 of 7 March 2005, and the three-year plan for information technology in public administration, drawn up by the AGID and adopted by Prime Minister's Decree pursuant to Article 14a(2)(b) of the CAD.

The addressees of these Technical Rules are:

- Owners of digital procurement platforms, as referred to in Article 25 of the Code;
- Operators of such digital procurement platforms;
- Platform Operators, for the management of guarantees, operating using distributed ledger technologies referred to in Article 106(3) of the Code.

1.2 Objective scope

This document sets out:

- The technical requirements for digital procurement platforms, divided into three classes:
    - general requirements arising from the provisions of the CAD and general rules as provided for in Article 19(1) of the Code;

    - specific functional requirements explicitly indicated in the Code, with particular reference to Article 22(2), in the activities referred to in Article 21. Paragraph 1;
    - requirements for interoperability with digital infrastructure platforms and services enabling the life cycle management of public contracts, as referred to in Article 23, and in particular with the National Public Procurement Database (BDNCP), referred to in Article 62a of the CAD and kept by the ANAC.
- The procedures for the certification of digital procurement platforms.
- The characteristics of distributed ledgers used in guarantee management platforms.

2. References and acronyms

2.1 Document reading notes

In line with the ISO/IEC Directives, Part 2, and the practices of European standardisation bodies in the drafting of technical standardisation documents, this document uses the verbal forms “**must**”, “ **must not**”, “**should**”, “**should not**”, “**may**”, and the adjective “**optional**”, as described below:

- **must** or **must not** indicate an obligation;
- **should** or **should not** indicate a recommendation, for which it is required to understand and evaluate the implications in case alternative approaches are chosen;
- **may** or the adjective **optional** indicate a choice.

2.2 References to Legislation

The following are the acts that make up the main reference legal framework, at a national and European level, of this document.

[CAD] Legislative Decree No 82 of 7 March 2005 on the “Digital Administration Code”; NOTE – Legislative Decree 82/2010 is also known by the abbreviation “CAD”.

[EU Directives] European Public Procurement Directives: **1. 2014/23/EU** on the award of concession contracts, **2. 2014/24/EU** on public procurement, **3. 2014/25/EU** on procurement by entities operating in the water, energy, transport and postal services sectors.

[Code] Legislative Decree No 36 of 31 March 2023 “Code of public contracts implementing Article 1 of Law No 78 of

21 June 2022, delegating powers to the Government in the field of public contracts", transposing the 2014 European Directives.

[eIDAS] electronic IDentification Authentication and Signature – Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC – aims to provide a European legal basis for the trust services and electronic identification means of EU Member States.

[GDPR] REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2.3 Reference guidelines and technical rules

The following are the Guidelines issued by the AGID pursuant to Article 71 of the CAD and other regulatory documentation, which are also referred to indirectly in this document. The AGID Guidelines are available on the agency's website at the following address: https://www.agid.gov.it/it/linee-guida, where related updates are also published as a result of technological evolution or the need to adapt to the reference legislation.

[LG_DOC_INF] Guidelines on the formulation, management and storage of computer documents and related attachments.

[LG_PDND_INTER] Guidelines on the technological infrastructure of the National Digital Data Platform for the interoperability of database information systems

[LG_SIC_INTER] Technological Guidelines and Standards for the Security of Interoperability through Information System APIs

[LG_INTER_TEC]	Guidelines on the Technical Interoperability of Public Administrations
[ST_eDGUE]	Technical specifications for the definition of the Italian electronic ESPD “eDGUE-IT”
[RT_SPID]	REGULATION on SPID Technical Rules
[AVVISI_SPID]	DECISION NO 16/2016 on the Publication of “Notifications” on technical procedures concerning the Public System for the Management of Digital Identity (SPID)
[LG_OPENID]	OpenID Connect Guidelines in the SPID
[FICEP]	FICEP Project -Italian eIDAS node – Notice No 1-2018 – Notes for the deployment of the eIDAS LOGIN in Public Administrations
[LOA]	SPID – Public Digital Identity System – Notice No 04-2018 – Minimum service levels for homogeneous functionality
[DET_CLOUD]	ACN Directorial Decree with Ref. No 5489 of 08/02/2023 for the transition of digital infrastructure and services https://www.acn.gov.it/documents/DeterminazioneCloud__20230208_def_signed.pdf
[QUAL_CLOUD]	Directorial Decree with Ref. No 29 of 02/01/2023 https://www.acn.gov.it/DecretodirettorialeQualificazioneServiziCloud2genn23DEFsigned.pdf
[REG_CLOUD]	REGULATION on minimum levels of security, processing capacity, energy saving and reliability of digital infrastructure for PA and quality, security, performance and scalability characteristics and the portability of cloud services for public administration,

	the methods of migration and the methods of qualification for cloud services for public administration
[LG_DATI]	National GUIDELINES for the enhancement of public information assets https://www.dati.gov.it/linee-guida-valorizzazione-patrimonio-informativo-pubblico
[RACC_TLS]	Decision No 471 of 5 November 2020 – Adoption of the AgID Recommendations on the Transport Layer Security (TLS) standard
[LG_OPENDATA]	Open Data Guidelines | Guidelines laying down technical rules for the implementation of Legislative Decree No 36, as amended and supplemented, of 24 January 2006 on the openness of data and the reuse of public sector information (italia.it) Available in the public consultation version on Docs Italia
[LG_ACCESS]	Guidelines on the accessibility of IT tools
[LG_SITI]	Design guidelines for PA websites and digital services https://docs.italia.it/italia/design/lg-design-servizi-web/it/versione-corrente/index.html

2.4 Terms and definitions

The ACRONYMS that will be used in these Technical Rules are set out below:

[PA]	Public administration.
[SA]	Contracting authority and, where applicable under the Code, the granting entity.
[CdC]	Central purchasing body.
[EO]	Economic operator.
[CEN]	European Committee for Standardisation (one of the standardisation bodies recognised in Europe, see Annex I to Regulation (EU) No 1025/2012).

[BDNCP] National public procurement database, as referred to in Article 62a of the CAD.

[PDND] National Digital Data Platform, as referred to in Article 50b of the CAD.

The following definitions are set out for the purposes of these Technical Rules:

[Digital procurement platform] or **[Platform],** pursuant to Article 25 of the Code, a set of interconnected and interoperable services and IT systems, used by contracting authorities and granting entities to carry out one or more activities in the life cycle of public contracts (usually programming, design, publication, awarding and execution), and for interaction with the BDNCP.

[Digital Procurement Platform Component] The software component IT service or system of a Digital Procurement Platform and such that it meets both of the following conditions:

a) the component is used by at least one contracting authority and one granting entity;

b) the component carries out one of the activities provided for in Article 22(2) of the Code or interacts with the BDNCP.

[Platform Owner] or **[Producer]** A public or private legal entity which owns the rights, even if non-exclusive, of at least one essential component of the Platform and which makes available, including through contracts and agreements, develops and maintains the software of the Platform in accordance with the requirements of the Code and these Technical Rules and submits it for certification by the AGID pursuant to Article 26(2) of the Code, with the methods specified in these Technical Rules.

[Platform Operator] or**[Operator]** A public or private legal entity responsible for the operation of an application of the Platform in accordance with these Technical Rules, coinciding with or appointed by an SA,

which guarantees the functioning, security and protection of personal data.

[System Administrator] or [ADS] The physical person entrusted by the Operator with the task of overseeing the management and maintenance of the Platform and its use in compliance with data protection and security requirements.

[User] A physical person authorised to use the platform according to a specific application profile.

[Application profile] the set of information related to the application privileges of a platform user that allows you to define, based on the declared role that you fulfil within your organisation, the set of competent activities for each activity in the life cycle of the contract.

[Operators of guarantee management platforms] A private or public legal entity responsible for the management of distributed ledger-based platforms, provided for in Article 106(3) of the Code to enable the management of guarantees.

[PDND interoperability] The technological interoperability infrastructure referred to in paragraph 3 of Article 50b of the CAD.

[Register of certified platforms] The Register provided for by Article 26(3) of the Code. These Regulations identify the following three sections constituting the Register of Certified Platforms:

- The section of the components of the Digital Procurement Platform that have obtained certification in the manner provided for in these Technical Rules, also called, in short, the Certified Products Section;
- The section of Authorised Operators: public or private legal entities authorised to manage the applications of the Digital Procurement Platform;
- The section of Compliant Platforms: Digital Procurement Platforms that have obtained the “Declaration of Platform Compliance”.

[Declaration of Platform Compliance]: a document certifying that a given Digital Procurement Platform:

- consists of components (products) certified in accordance with these Technical Rules;
- that these components are installed in accordance with the Manufacturer's instructions;
- that the Platform has been successfully subjected to the PDND's "client user" behaviour functionality tests.

The Declaration of Platform Compliance is issued by the Operator of an Authorised Platform.

2.5 Reference standards

The data standards and schemas to which these Technical Rules refer derive from the direct application of European legislation. The standardisation activity in the field of eProcurement is carried out at a European level within the European Committee for Standardisation (CEN) to ensure consistency and close adherence to European directives, introducing or maintaining levels of regulation corresponding to the minimum levels required by the directives.

In particular, reference is made to the standards developed, or currently being developed, by the following CEN Technical Committees:

- CEN/TC 440 "Electronic Public Procurement";
- CEN/TC 434 "Electronic Invoicing".

The Platforms **should** comply with these standards as a means of supporting compliance with the requirements of European legislation, also in view of its expected evolution.

3. Platform requirements

3.1 General principles and subdivision into classes of requirements

The AGID plans and coordinates the administrations' activities for the use of information and communication technologies, through the drafting and monitoring of the Three-Year Plan for Information Technology in Public Administration, which establishes the objectives and identifies the main interventions for the development and management of the information systems of all public administrations including contracting authorities and granting entities (SAs).

The AGID Guidelines referred to in Article 71 of the CAD govern in detail certain components of the PA's information system (e.g. development and accessibility to digital services, security, document management, platforms, databases, internal interoperability and cross-border interoperability) to which digital procurement platforms are also subject.

The Code regulates public procurement contracts and concessions. In accordance with Article 19(1), SAs shall ensure the digitisation of the life cycle of contracts in accordance with the principles and provisions of the CAD, guarantee the exercise of digital citizenship rights and operate in accordance with the principles of technological neutrality, transparency, protection of personal data and IT security.

SAs shall use Digital Procurement Platforms to carry out the procedures for awarding and executing public contracts (Article 25(2) of the Code) in accordance with these Technical Rules.

In the event that SAs do not have their own digital procurement platform, they shall "... *make use of platforms made available by other contracting authorities or granting entities, central purchasing bodies or aggregators, regions or autonomous provinces that in turn* ***may*** *use a system operator that ensures the operation and security of the platform*." (Article 25(3) of the Code).

The technical requirements of digital procurement platforms **must** be met, in relation to their respective roles, both by Platform Owners and Platform Operators, and are divided into three classes:

1. general requirements (Class 1) arising from compliance with the principles and provisions of the CAD or other generally applicable legislation, as specified in paragraph 3.2;
2. functional requirements of the life cycle of contracts pursuant to the Code (Class 2), divided into two subclasses:
    a. general functional requirements (Class 2-a), specified in paragraph 3.3.1;
    b. specific functional requirements (Class 2-b) specified in paragraph 3.3.2;
3. interoperability requirements (Class 3) specified in paragraph 3.4.

Class 2 and 3 requirements are subject to certification in accordance with Article 26 of the Code.

Figure 1 shows the actions carried out in each of the digital life cycle activities of the contracts referred to in Article 21.

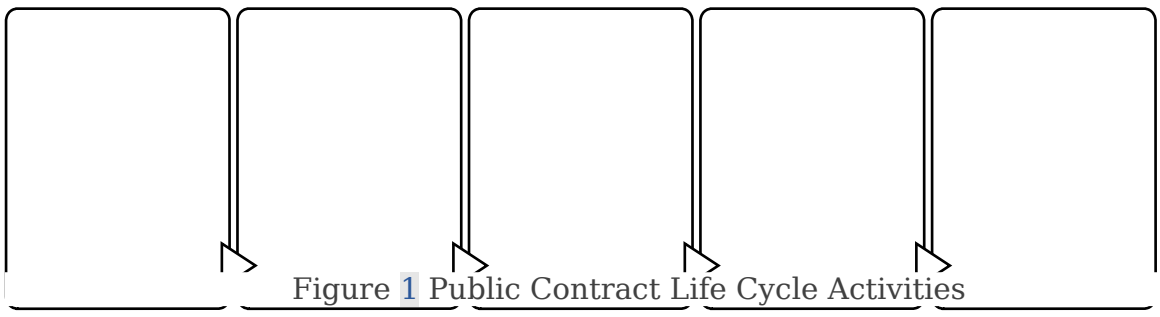

Figure 1 Public Contract Life Cycle Activities

Figure 2 presents a synopsis of the specific functional requirements (Class 2-b) and interoperability requirements (Class 3).

Public contract life cycle activities (Article 21(1) of the Code)	Requirements for digital platforms and services (Article 22(2) of the Code)						
	a) Drafting or acquisition of documents in a native digital format	b) publication and transmission of data and documents to the BDNCP	c) electronic access to tender documentation	d) presentation of the ESPD in a digital format and interoperability with the FVOE	e) submission of tenders	f) opening and storing the tender dossier digitally	g) technical, accounting and administrative control of contracts during the execution and management of guarantees
Planning	Class 2-b	Class 3	Class 2-b	NO	NO	NO	NO
Design	Class 2-b	NO	Class 2-b	NO	NO	NO	NO
Publication	Class 2-b	Class 3	Class 2-b	Class 2-b (ESPD)	Class 2-b	Class 2-b	Class 3
Awarding	Class 2-b	Class 3	Class 2-b	Class 3 (FVOE)	NO	Class 2-b	Class 3
Execution	Class 2-b	Class 3	Class 2-b	Class 3 (FVOE)	NO	Class 2-b	Class 3

Figure 2 synopsis of the specific functional requirements (Class 2-b) and interoperability requirements (Class 3)

In particular:

- The planning activity involves sending the necessary information to the BDNCP in relation to the three-year plan;
- The design activity involves the preparation of documentation for each of the scheduled tenders;
- The publication activity includes, inter alia, the creation of the tender dossier and making available the public tender documentation to the EOs and other interested parties;
- The awarding includes the execution of the procedure for selecting economic operators. At this stage the formal communications between the SA and EO take place, and the tender is submitted, evaluated and awarded, with all the consequent communications between the Platform and the central infrastructure of the BDNCP;
- The execution activity involves the sending to the BDNCP of the data and information collected by the platforms during the contractual execution activity (e.g. Work Progress Reports, contractual changes, testing, etc.).

3.2 Requirements arising from CAD provisions and general standards (Class 1)

Class 1 requirements derive from compliance, primarily, with the principles and provisions of the CAD and other applicable general rules.

[3.2-1] Platform Owners and Operators **must** comply with the following regulatory requirements:

- [3.2-1.1] the provisions on IT security, in particular those laying down the minimum requirements set out in Annex B of the Regulation referred to in Article 33f(4) of Decree-Law No 179 of 18 October 2012, converted, with amendments, by Law No 221 of 17 December 2012 issued by the AGID, as amended and supplemented, and the further provisions of the National Cybersecurity Agency issued with reference to the aforementioned Regulation;
- [3.2-1.2] Legislative Decree No 36 of 24 January 2006 with regard to the data and information to be managed and made available in an open format;
- [3.2-1.3] Law No 4 of 9 January 2004 with regard to simplifying the access of users and, in particular, of persons with disabilities to IT tools.

[3.2-2] Platform Owners and Operators **must** also comply with at least the following AGID Guidelines:

- [3.2-2.1] Guidelines on the training, management and storing of IT documents issued by the AGID pursuant to the CAD;
- [3.2-2.2] Guidelines on the accessibility of IT tools issued by the AGID pursuant to Law No 4 of 9 January 2004.

[3.2-3] Platform Owners and Operators **must**:

- [3.2-3.1] continuously monitor the publication of standards, guidelines and technical rules in order to ensure compliance

with the rules applicable to the platforms and services they provide;

- [3.2-3.2] operate in line with standards and best practices such as ISO/IEC 20000-1, ISO 9001:2015 and ISO/IEC 27001; any certifications, whose scope is consistent, **may** be a supporting means of proof of compliance with the provisions herein.

[3.2-4] Platform Operators **must**:

- [3.2-4.1] use only Platforms to which the AGID Certificate has been issued in accordance with Article 26(2) of the Code and included in the appropriate register kept by the ANAC, in accordance with paragraph 3 of the same article;
- [3.2-4.2] Configure and manage the platforms in accordance with Chapter 5 of these Technical Rules and the instructions provided by the Owner.

[3.2-5] In the event that the Platform Owner and Operator are the same entity, an internal organisational separation **must** be guaranteed, enabling the assigning of the responsibilities identified in the Technical Rules to the roles of Operator and Owner.

3.3 Functional requirements of the digital life cycle of contracts (Class 2)

Class 2 requirements are functional requirements that, in relation to the Platforms, establish compliance with the requirements of the Code and, in any case, in compliance with the principles and provisions on the digitisation of public contracts.

3.3.1 General functional requirements (Class 2-a)

3.3.1.1 Digital access to the platform

[3.3.1.1-1] The platform **must** allow the identification of users through the SPID and CIE electronic identification mechanisms.

[3.3.1.1-2] The platform **must** enable the electronic identification of users also through other mechanisms, in accordance with current legislation. In particular, for European users, the platform **should** use the functionality of the Italian eIDAS node [FICEP].

[3.3.1.1-3] The additional authentication mechanisms referred to in [3.3.1.1-2] made available by the platform **must** be classified by the Owner according to its own assessment, with respect to the guarantee level definitions of the ISO/IEC 29115 standard (LoA2, LoA3 or LoA4).

[3.3.1.1-4] The platform **must** ensure the uniqueness of the identified entity regardless of the electronic identification mechanism used.

[3.3.1.1-5] The electronic identification of the user **must** be guaranteed at the time of access and shall remain valid until the end of the working session (e.g. possible integration with the entity's single sign-on system) without prejudice to compliance with security requirements.

3.3.1.2 Registration, profiling and delegation

[3.3.1.2-1] The platform **must** provide a profiling system that makes it possible to associate an application profile with individual users of the respective organisations: Contracting Authority, Economic Operator, Platform Operator.

[3.3.1.2-2] The platform **must** make it possible to associate the minimum level of guarantee required to individual application functions or logical aggregations thereof.

[3.3.1.2-3] The platform **must** provide, in relation to the Contracting Authority, an application profile for the RUP role, as referred to in Article 15 of the Code, and **should** make available functions for the creation and deletion of additional profiles with specific delegations in relation to the management of the life cycle

of contracts and, in particular, to access to the FVOE in order to check the requirements of the EO.

[3.3.1.2-4] The platform **must** provide, where applicable, application profiles for the roles of Execution Director or Works Director, Ordering Point, Investigation Point, Committee Chairperson, **must** make it possible to associate the same user with different roles and **may** make available functions for creating and deleting additional application profiles.

[3.3.1.2-5] The platform **must** allow the Operator, and **may** allow the RUP or its delegate, to know the detail of each application profile attributed to each user according to their role, in particular the privileges associated with each application role for each activity in the life cycle of the contract, and all user-profile associations.

[3.3.1.2-6] The platform **must** provide, with regard to the Economic Operator, an application profile for the role of legal representative or its delegate and **may** make available the creation and deletion of additional application profiles.

[3.3.1.2-7] The platform **must** provide, with regard to the Operator, the platform’s system administrator (ADS) application profile and **may** make available the creation and deletion of additional application profiles with specific administrative functions identified by the Operator.

3.3.1.3 Traceability

[3.3.1.3-1] The platform **must** manage a system Register, consisting of one or more logs, that guarantees the registration of each access (user and application profile) of significant events in relation to the life cycle of the contract.

[3.3.1.3-2] For each event registered in the system Register, the platform **must** contain the date and time and, where applicable in the context of the event, the identification data of the physical or

legal entity or device that caused the event, the individual operation carried out with the information necessary for its contextualisation, the IP address of origin and other information deemed useful.

[3.3.1.3-3] The platform **must** guarantee the unalterability of the system Register and the possibility of verifying its integrity.

[3.3.1.3-4] The platform **must** produce extracts from the system Register with the information collected for each individual procedure and attach this extract to the relevant tender dossier. The Platform must produce extracts from the Register relating to a time period determined by the System Operator, and possibly governed by the contractual agreement referred to in paragraph 5.1.

[3.3.1.3-5] Platforms **must** have the ability to maintain the information in the system Register for two years, unless otherwise agreed with the SA in the contractual agreement referred to in paragraph 5.1.

3.3.1.4 Digital communications

[3.3.1.4-1] The platform **must** manage the communications and information exchanges referred to in the Code, implementing a specific area of communication between the SA and EO in relation to the procedure. With regard to this area:

- [3.3.1.4-1.1] the platform **must** track every sending and receiving event in the system Register;
- [3.3.1.4-1.2] the platform **must** store any communication in the tender dossier.

[3.3.1.4-2] The platform **must** allow contracting authorities to include in the tender dossier any communications between the EO and SA on communication channels other than the platform,

including by mail and certified mail, tracing the operation in the system Register.

[3.3.1.4-3] The platform **must** explicitly state to all users involved where communications relevant to the procedure take place and request the necessary consents.

[3.3.1.4-4] The platform **may** provide for additional notification mechanisms by clearly indicating which channel produces the communication effects.

3.3.2 Specific functional requirements (Class 2-b)

3.3.2.1 a) Drafting or acquisition of documents in a native digital format

[3.3.2.1-1] The platform **must** ensure the drafting or acquisition of documents in a native digital format in all the activities of the life cycle of the contract provided for in the synoptic framework, in compliance with paragraph 2.1.1 (formation of the computer document) of the Guidelines on the formulation, management and storage of computer documents [LG_DOC_INF], Annex 2 to those guidelines in relation to formats and Annex 5 in relation to metadata.

[3.3.2.1-2] The platform **must** declare to the user the maximum size and formats of the files.

[3.3.2.1-3] The platform **may** indicate format limitations for security reasons, e.g. in relation to executable codes.

[3.3.2.1-4] The platform **must** allow the acquisition of documents with an electronic signature or seal. Failure to recognise a specific form of signature or seal **must** not prevent the acquisition of the document.

[3.3.2.1-5] The platform **must** specify for which formats, as part of compliance with the requirement [3.3.2.1-4], it validates electronic signatures and seals.

[3.3.2.1-6] The platform **must** provide clear indications of the reason in case of non-acceptance of the acquisition of a document (e.g. exceeding the size limit, signature validation error, etc.).

[3.3.2.1-7] The platform **may** make available API interfaces with which to exchange data, for the purpose of document acquisition, subject to compliance with the requirements of access (par. 3.3.1.1) and profiling (par. 3.3.1.2).

3.3.2.2 c) Electronic access to tender documentation

[3.3.2.2-1] The platform **must** make available data and information that it collects or generates in the various activities of the tender life cycle within the constraints of the Code.

[3.3.2.2-2] The platform, before authorising access to data and information relating to tender documentation, **must** carry out the following checks:

- [3.3.2.2-1.1] identify the entity requesting access, in compliance with the requirements of paragraph 3.3.1.1. Digital access to the platform;
- [3.3.2.2-1.2] associate any application profiles and delegations valid for that entity at the time of access, in compliance with the requirements of paragraph 3.3.1.2. on registration, profiling and delegation;
- [3.3.2.2-1.3] verify the access rights in relation to valid profiles/delegations and the activity that the entity may perform in compliance with the limitations provided by the Code;
- [3.3.2.2-1.4] track all accesses, in accordance with the requirements of section 3.3.1.3 Traceability.

[3.3.2.2-3] If parts of the tender are redacted pursuant to Article 36 of the Code, the platform **must** manage the link to the non-redacted documents and the corresponding access rights.

Note: the requirements of this paragraph shall apply in conjunction with those of paragraph 3.3.2.5 “f) Opening and storing of the tender dossier digitally”.

3.3.2.3 d) Presentation of the ESPD in a digital format

[3.3.2.3-1] The platform **must** ensure the drafting or acquisition of the ESPD as referred to in Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 in the publication of the tendering procedure in the format defined by the AGID guidelines based on the structured XML format in accordance with the ESPD-EDM data model ver. 2.1.1 defined by the European Commission.

3.3.2.4 e) Presentation of tenders

[3.3.2.4-1] The platform **must** provide the EO with templates and forms for formulating the bid or with functions for the acquisition of tender documents.

[3.3.2.4-2] The platform **may** make available API interfaces for acquiring the tender documentation in addition to the provisions of [3.3.2.4-1], without prejudice to compliance with the requirements for access (par. 3.3.1.1) and profiling (par. 3.3.1.2).

[3.3.2.4-3] The platform **must** provide tracking functions relative to the moment of acquisition.

[3.3.2.4-4] The platform **must** make confidential (not readable) the contents of the documents that make up the offer preventing the readability of the content to anyone, until the opening date set for tender bids.

[3.3.2.4-5] The platform **must** enable the acquisition of additions or adjustments to the tender, in the cases provided for by the Code.

[3.3.2.4-6] The platform **must** enable the grouping of the documents that compose the tender into logical sets, called Envelopes, and **must** manage at least Envelopes with the documents that constitute the technical offer, the economic offer and the administrative documentation.

[3.3.2.4-7] The platform **must** allow the opening of the Envelopes of the administrative documentation, the technical offer and the economic offer separately.

[3.3.2.4-8] The platform **must** make it possible to associate the application profile enabling this function with the entity formally authorised to open the Envelopes.

[3.3.2.4-9] After each Envelope is opened, the platform **must** only allow access to the contents of the Envelope to formally authorised entities.

[3.3.2.4-10] The platform **must** track in the system Register:

- [3.3.2.4-10.1] the allocation and deletion of application profiles allowing the opening of Envelopes;
- [3.3.2.4-10.2] the allocation and deletion of application profiles that allow access to the content of each Envelope after its opening with an indication of the entity to which the profile relates;
- [3.3.2.4-10.3] the opening of each Envelope and each access to its content with an indication of the entity to whom those events relate.

[3.3.2.4-11] The platform **must** make it possible to distinguish between the entities who have the right to open the “Envelopes” and access their contents and the right to manage/process the system Register respectively, without prejudice to the unalterability of the system Register.

3.3.2.5 f) Opening and storing the tender dossier digitally

[3.3.2.5-1] The platform **must** prepare the information necessary for compliant storage of the tender dossier according to the Guidelines on the formulation, management and storage of computer documents and attachments thereto.

[3.3.2.5-2] The platform **must** prepare the mandatory metadata for the tender documentation in accordance with Annex 5 “Metadata” of the aforementioned Guidelines, with the exclusion of metadata that depend on the classification plan and related plan for the organisation of document aggregations adopted by the contracting authority pursuant to Article 64 of Presidential Decree No 445 of 28 December 2000, Consolidated Text on administrative documentation.

[3.3.2.5-3] In order to enable the Contracting Authority to correctly identify documents and aggregations consistent with its plan for the organisation of document aggregations, the platform **must** acquire the unique identification codes related to the tender dossier, through interaction with infrastructure services referred to in requirement [3.4-5], in particular [3.4-5.1], which constitute persistent identifiers within the meaning of the Guidelines set out in requirement [3.2-2.1]:

- [3.3.2.5-3.1] Procurement ID;
- [3.3.2.5-3.2] CIG.

[3.3.2.5-4] The platform **must** allow the generation, display and exportation of the dossier at any time during the life cycle of the contract, within the limitations indicated in reference to section 3.3.2.2 “c) Electronic access to tender documentation”.

[3.3.2.5-5] The platform **must** enable the insertion and extraction of documents or sets of documents formulated outside the platform.

[3.3.2.5-6] The platform **may** make available API interfaces for the functions required by the requirements [3.3.2.5-4], subject to the limitations set out therein and compliance with the requirements for access (section 3.3.1.1) and profiling (par. 3.3.1.2).

[3.3.2.5-7] The platform **must** allow the cancellation of the tender dossier following a request by the RUP. This function **must** provide for a strong control mechanism. For example: confirmation by both the RUP and the ADS or a role of the Operator expressly delegated for this function.

[3.3.2.5-8] The events referred to in [3.3.2.5-4], [3.3.2.5-5], [3.3.2.5-6] and [3.3.2.5-7] **must** be tracked in the system Register.

3.4 Interoperability requirements (Class 3)

Class 3 requirements concern interoperability aspects through PDND interoperability, referred to in paragraph 2 of Article 50b of the CAD, including the preparatory activities for the registration of the IT systems involved, authentication and authorisation between them carried out through PDND interoperability, and integration with the enabling infrastructure services of the ANAC, referred to in the provision issued by that Authority pursuant to Article 23(5) of the Code (hereinafter referred to as “ANAC e-services”) and subject to Article 22(2) of the Code, letters b), d) and g).

[3.4-1] The platform **must** comply with the Public Administrations Interoperability Model (MoDI) defined by the “Guidelines on the Technical Interoperability of Public Administrations” [LG_INTER_TEC] and the “Technological Guidelines and Standards for the Security of Interoperability through Information System APIs” [LG_SIC_INTER] and based on the Interoperability Technology Infrastructure (PDND interoperability) referred to in paragraph 2 of Article 50b of the CAD in accordance with the “Guidelines on the technological infrastructure of the National

Digital Data Platform for the interoperability of information systems and databases" [LG_PDND_INTER].

[3.4-2] The platform **must** identify the natural person performing operations on the platform involving the use of ANAC e-services. Identification **must** be done via SPID or CIE, or other electronic identification means issued under an electronic identification scheme included in the list published by the Commission in accordance with Article 9 of the [eIDAS] Regulation.

[3.4-3] The platform **must** make requests to ANAC e-services by applying the models provided for in the "Guidelines on the Technical Interoperability of Public Administrations" [LG_INTER_TEC], in order to indicate at least the user performing operations on the platform and the level of guarantee associated with the digital identity of that user.

[3.4-4] If the requested ANAC e-service provides, for a specific operation, evidence of the need for a higher level of guarantee than that stated by the platform in relation to the user performing operations, the platform **must** re-identify the user by ensuring for the new identification a level of guarantee at least equivalent to that required to authorise the operation.

[3.4-5] The platform, by interacting with ANAC e-services retrieved via PDND interoperability, **must**:

- [3.4-5.1] in planning and publishing activities, create the contract and acquire the relevant identification codes associated with it;
- [3.4-5.2] ensure the transmission of the data and documents necessary for updating the BDNCP (Article 22(2)(b) of the Code);
- [3.4-5.3] ensure interoperability with the FVOE (Article 22(2)(d) of the Code) by managing the request and retrieving the documents necessary for verification by the SA;

- [3.4-5.4] in publishing, awarding and executing activities, manage the transmission of information and related documentation in support of technical, accounting and administrative control of contracts during the execution and management of guarantees (Article 22(2)(g) of the Code).

4. Certification

4.1 AGID certification

The certification process of digital procurement platforms aims to define a clear and precise baseline of legal, security, functional and technical requirements that platforms **must** comply with in order to ensure reliability, security, the uniformity of operations and in order to increase the quality of the services provided.

The basic legal requirements are laid down in national laws and EU directives on public procurement (see in particular Articles 22, 53 and Annex IV of Directive 2014/24/EU).

The certification of platforms shall cover functional requirements of the digital life cycle of contracts (Class 2 requirements referred to in paragraph 3.3) and the interoperability requirements (Class 3 requirements referred to in paragraph 3.4) and is a tool allowing the SA to adopt only compliant digital procurement platforms. Platform certification is a tool to support compliance with national requirements and with provisions of EU Directives, and to implement best practices.

The governance model of the certification process takes into account national and EU public procurement legislation, existing procurement practices and existing markets and enables monitoring of platform compliance with the requirements set out in Chapter 3 of these Technical Rules.

The certification process defined in these Technical Rules concerns the requirements set out in sections 3.3 (Class 2) and 3.4 (Class 3) and provides for:

- the definition and publication by the AGID of an **operational model** supporting certification, consisting of a checklist of the requirements to be met and describing the procedural and operational processes;
- the use of conformity assessment bodies referred to in Regulation (EC) No 765/2008 accredited as test laboratories or certification bodies, which will operate in the field;
- the issuance of the certificate on the basis of the compliance reports received and the supervision of the correct application of the operational model by the AGID.

The operational model checklist is modular, to allow the certification of Platforms that implement only some of the activities of the digital life cycle of public contracts, and is inclusive of all technical requirements subject to AGID certification (Class 2 and 3), identifying for each requirement the criteria that must be met.

The operational model is published by the AGID with its own provision, in agreement with the ANAC and the Prime Minister's Office – Department for Digital Transformation, following these Technical Rules and provides in relation to the interoperability requirements (Class 3) the execution of the functionality tests defined in the checklist in an environment other than that of operation (sandbox) outside the PDND authentication, with the qualification environment provided by the ANAC.

The operational model and, in particular, the checklist contained therein, is used by Platform Owners to support a process of **self-assessment of the conformity of the product with these technical rules**. The request for certification, in the form of an application to be submitted to the AGID in the manner defined in the operational model, is based on self-assessment and is assessed by the AGID for the purpose of certification of the platform or its components.

The operational model also provides for the ways in which the Owner **must** submit the certification application.

The operational model also sets out the process of transitioning from the first application, based on self-assessment, to the use of conformity assessment bodies accredited in accordance with Regulation (EC) 765/2008. The possible scenarios are:

- use of Test Laboratories (accreditation according to ISO/IEC 17025);
- use of Certification Bodies (accreditation according to ISO/IEC 17065).

The AGID shall communicate to the ANAC each time a certification is issued, updated or revoked the data necessary to identify the Owner, the Platform and its version to allow the ANAC to manage the Register of Certified Platforms referred to in Article 26(3) of the Code, in the Certified Products Section.

The AGID shall also communicate to the ANAC the information relating to the Platform Operators, in order to allow ANAC to update the Register in the Authorised Operators section.

5. Operator requirements and declaration of conformity

5.1 Operator Requirements

The Platform Operator **must** operate in accordance with the provisions of these Technical Rules.

The Operator **may** coincide with the Contracting Authority (SA). Otherwise, the relationship between the Operator and SA **must** be regulated by a contractual agreement between the Parties, which regulates the formal assumption of responsibility by the Operator for the activities carried out and related to the life cycle of public contracts.

The contractual agreement between the Parties also regulates the levels of quality in order to establish the services offered to users of the Platform and support services.

In the event that the Platform provides for access with credentials issued by the SA through a process defined by the latter (see requirement [3.3.1.1-2]) other than, for example, SPID and CIE, the contractual agreement **must** provide for the acceptance of responsibility by the SA to correctly carry out the recognition of the users to whom these credentials are associated.

If the Platform integrates with the SA's Identity and Access Management (IAM) system, the contractual agreement **must** provide for the assumption of responsibility by the SA to operate its IAM system correctly.

The Operator **must** perform the following activities:

- enable users and/or delegates through the functions referred to in paragraphs 3.3.1.1 and 3.3.1.2;
- manage the Platform in relation to activities related to the provision of services and communications to users;
- manage tracking activities through the functions referred to in paragraph 3.3.1.3;
- carry out activities of anonymization and/or aggregation of all acquired and managed data, as well as make available such data in an open format according to the procedures provided for by the CAD;
- monitor the functioning of the platform to support the improvement and evolution of the platform (analysis, research and development).

In each of these activities, the Operator **must** ensure the protection of the personal data processed, in compliance with national and EU law. The Operator **must** reduce the processing of personal data strictly to what is necessary to pursue the purposes underlying the individual processing activities and, consequently, be able to prove, in compliance with the principle of accountability, that the personal data are relevant, necessary and not excessive in relation to the purpose pursued.

The Operator **must** prepare an impact assessment on the protection of personal data and if necessary consult the Italian Data Protection Authority pursuant to Articles 35 and 36 of the GDPR.

With regard to the processing whose ownership is identified by the Operator, the latter **must** issue, through the Platform, a specific policy pursuant to Articles 12, 13 and 14 of the GDPR.

The Operator **must** take appropriate organisational measures to guarantee data subjects' exercise of their rights.

In the provision of the services and functionalities provided by the platform, the Operator **may** make use of third parties, duly appointed as

data processors in accordance with the procedures set out in Article 28 of the GDPR.

In this case, the Operator **must** prioritise suppliers located in the national territory and the European Union. Where this is not possible, the Operator **may** make use of data controllers located in third countries, who offer sufficient guarantees to implement technical and organizational measures appropriate to the security of the processing and the protection of the data subject, in compliance with the legislation.

The Operator **must** instruct data processors on the need to store personal data within the European Union where providers are unable to offer sufficient guarantees to ensure effective compliance with Chapter V of the GDPR in respect of technical and organisational measures adequate for the security of processing and the protection of the data subject.

In accordance with Recital 83 and Article 32 of the GDPR and in compliance with the principle of accountability, the Operator **must** implement any appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Such security measures shall include at least:

- “in transit” and “data at rest” encryption and where possible the anonymization of personal data;
- the ability to ensure, on a permanent basis, the confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to promptly restore the availability and access of personal data in the event of a physical or technical accident.

5.2 Declaration of Platform Compliance

This section governs the process leading to certifying the compliance of a Digital Procurement Platform with the requirements identified in this Regulation. The basic steps of the process are as follows:

- Recognition of the Operator authorised to issue Declarations of Platform Compliance;
- Accession of the authorised Operator to the PDND platform;
- Provision of a Procurement Platform by an authorised Operator;
- Configuration and testing of the Platform in the role of “PDND Client User” of the ANAC e-services;
- Carrying out of the interoperability test;
- Issuance of the “Declaration of Platform Compliance” by the authorised Operator.

[5.2-1] For the purpose of identifying authorised Operators, the Owner of certified platform components **must** communicate to the AGID the following information and updates thereto relating to each Operator using its platform:

- [5.2-1.1] the Operator’s identification data;
- [5.2-1.2] the version of the platform and certified essential components used;
- [5.2-1.3] the digital domicile of the Operator.

The AGID shall communicate to the ANAC the information relating to authorised Operators referred to in requirement [5.2-1], in order to allow the ANAC to update the Register of Certified Platforms, in the Authorised Operators section.

[5.2-2] The Platform Operator, at the time of the first platform configuration, **must**:

- [5.2-2.1] request the activation of the accession procedure on the PDND (as defined in Chapter 5 of the [LG_PDND_INTER]) as an ANAC e-service user;
- [5.2-2.2] request the use of ANAC e-services in the PDND **test** environment, in the role of User (as defined in Chapter 8 of the [LG_PDND_ITER]), for all ANAC e-services;

- [5.2-2.3] following acceptance of the request referred to in point [5.2-2.2] by the ANAC, carry out the “risk analysis regarding the protection of personal data” in the PDND **test** environment (as defined in Chapter 9 of the [LG_PDND_ITER]) with regard to the purpose referred to in paragraph 3 of Article 23 of the Code;
- [5.2-2.4] register as an “PDND Client User” in the PDND **test** environment;
- [5.2-2.5] carry out a compliance test with regard to the BDNCP interoperability requirements;
- [5.2-2.6] after obtaining a positive result for the tests referred to in [5.2-2.5], issue a “Declaration of Platform Compliance”, which certifies the use of certified products, correct installation thereof and that the functionalities of the PDND “client user” have been tested;
- [5.2-2.7] request the use of ANAC e-services in the PDND **exercise** environment, in the role of User (as defined in Chapter 8 of the [LG_PDND_ITER]), for all ANAC e-services;
- [5.2-2.8] following acceptance of the request referred to in point [5.2-2.7] by the ANAC, carry out the “risk analysis regarding the protection of personal data” in the PDND **exercise** environment (as defined in Chapter 9 of the [LG_PDND_ITER]) with regard to the purpose referred to in paragraph 3 of Article 23 of the Code;
- [5.2-2.9] register as an “PDND Client User” in the PDND **exercise** environment.

If the Operator is already compliant with the PDND, the requirement [5.2-2.1] is considered already fulfilled.

The AGID shall communicate to the ANAC the Declarations of Platform Compliance received from authorised Operators, in order to allow the ANAC to update the Register of Certified Platforms, in the

section of the Platforms that have obtained the Declaration of Compliance.

6. Guarantee management platforms

6.1 Scope and definitions

This Chapter lays down the characteristics with which the distributed ledgers used in the context of guarantee management platforms referred to in Article 106(3) of the Code (hereinafter referred to in short as “guarantee platforms”) must comply and refers to:

- the definition of “distributed ledger technologies” in Article 8b(1) of Decree-Law No 135 of 14 December 2018, converted, with amendments, by Law No 12 of 11 February 2019;
- the definitions in technical standard EN ISO 22739.

SAs shall use guarantee platforms through the portals of such platforms or through MoDI-compliant APIs, where applicable.

6.2 Requirements for distributed ledgers

[6.2-1] Guarantee platforms **must** ensure the protection of the personal data processed, in compliance with national and EU law and, more specifically:

- [6.2-1.1] guarantee platforms **must not** store personal data on distributed ledgers, except as specified in [6.2-1.2];
- [6.2-1.2] it is permitted to store personal data on the distributed ledgers on which the guarantee platforms are based under the following conditions that **must** all be met:
    - the distributed ledgers on which they are based are permissioned;
    - all rights under current legislation can be guaranteed to data subjects;

- in accordance with current legislation, all operators of guarantee platforms that process personal data are appointed as data processors and data subjects shall be informed of such processing.

[6.2-2] Guarantee platforms **must** store on distributed ledgers the hash value of the guarantees, both in the final version and in any intermediate versions, and **must** use hash functions that according to the ETSI TS 119312 technical specification are to be considered usable for a period of at least 6 years. The final version of the guarantee is the guarantee issued and signed digitally as provided for in Article 106(3) of the Code.

[6.2-3] The guarantee platforms **must** allow data subjects to verify the validity of the guarantee electronically to anyone in possession of a computerised duplicate or its hash value. Note: electronic validity means the technical validation of the guarantee certificate, because it is not the responsibility of guarantee platforms to verify the civil validity of this guarantee.

[6.2-4] Guarantee platforms **must** meet general Class 1 requirements as applicable.

[6.2-5] Guarantee platforms **must** meet any of the following conditions:

- [6.2-5.1] the distributed ledgers on which they are based **must** implement a “permissioned” or “permissioned distributed ledger technology system” and **must** ensure that the writing of the guarantee issued in the distributed ledgers is under the control of one of the entities allowed to issue guarantees pursuant to Article 106(3) of the Code. The electronic identification of such entities **must** have a significant or high level of guarantee with reference to the eIDAS Regulation; or

- [6.2-5.2] the writing of the guarantee issued in the distributed ledgers is made by means of a smart contract that **must** ensure that this operation is possible only by a person allowed to issue guarantees pursuant to Article 106(3) of the Code who is authorised to write in the distributed ledger, after electronic identification with a significant or high level of guarantee with reference to the eIDAS Regulation.

[6.2-6] In accordance with the DNSH principle, guarantee platforms **should** evaluate the use of energy-efficient consensus mechanisms.

In relation to the processing of personal data, the provisions set out in paragraph 5.1 shall apply to the entities operating the guarantee platforms.

7.
Entry into force and transitional rules

1. In accordance with Article 225(2) of the Code, the provisions of these Technical Rules shall become effective from 1 January 2024.
2. With effect from 1 January 2024, Circular No 3 of 6 December 2016 containing "*Additional Technical Rules to ensure the exchange and sharing of data between telematic purchasing and negotiating systems*", adopted by the AGID in implementation of Article 58(10) of Legislative Decree No 50 of 18 April 2016, is repealed with the exception of Chapter 5 "Interconnection of the systems involved".
3. The technical specifications for the definition of the Italian electronic ESPD "*eDGUE-IT* ", issued by the AGID on 30 July 2021 as an annex to Circular No 3/2016, remain in force, subject to possible amendments and additions, until the adoption by the AGID of guidelines transposing the new ESPD-EDM data template published by the Publications Office of the European Union.
4. These Technical Rules shall be updated as the current national and European regulatory framework changes and/or as a result of technological or architectural developments, in the same manner in which they are issued.