An application of the Agency for Digital Italy guidelines and CSA Star self-assessment: A Docustar case study

Pierluigi Calabrese, Paola Lunalbi, Vincenzo Ribaudo, Saverio Crisafulli, Antonio Ruoto, Vito Santarcangelo, Diego Sinitò, Carlo Bonelli, Giuseppe Stella

1. Introduction

The digital documents play a predominant role in the production of business and public administration documents; they are created through telematic tools and, in the same way, they are stored, with the aim of guaranteeing a better efficiency and lower costs of business and public authority processes, definitively replacing the use of paper.

Consequently comes the problem of uniformly regulating the way in which this documents are produced and stored, to guarantee their integrity and authenticity, so is enacted the Digital Administration Code (CAD) with the function of regulating, among other things, the validity and the effectiveness of public administration's informatic documents; subsequently, the "Agenzia per l'Italia Digitale" (AgID) adopted initial guidelines aimed precisely at giving technical application to the rules of the CAD and establishing the procedures for the production, management and storage of digital documents by public administration's and private entities.

In 2020, AgID issued new guidelines in this regard, with the aim of updating the technical rules on the formation, registration, management and storage of digital documents in application of the CAD, bringing together all the various provisions and guidelines on the subject in a single text containing, precisely, all these rules.

The structure and objectives of these AgID guidelines will be outlined below, followed by a presentation of Docustar, the platform developed by Stella All in One for managing access to digitalised versions of business documents in compliance with the General Data Protection Regulation (GDPR), and certified ISO 27001:2013.

2. AgID guidelines

AgID's guidelines have the dual purpose of updating the current technical rules under article 71 of the Digital Administration Code (CAD), concerning the formation, protocol, management and storage of computerised documents, and of incorporating all the technical rules and circulars on the subject into a single guideline.

The general purpose of these guidelines is to simplify the entire process of managing computerised documents through an overall vision that aggregates within a single guideline all the subjects that were previously regulated separately, highlighting the functional interdependencies between the various phases of document management, from the moment of formation to its permanent preservation.

Six documents are also attached to the guidelines, and form an integral part of them. Among these we can find the one on file formats that can be used for the formation of digital documents (annex 2) and the one on metadata related to the same documents (annex 5): with regard to usable files, the digital formats that documents must have are identified from among those used by the different software known today, such as .doc, .docx, .pdf; with regard to metadata, on the other

Pierluigi Calabrese, Stella All in One Srl, Italy, luigi@dittastella.it
Paola Lunalbi, Stella all in one Srl, Italy, paola@dittastella.it
Vincenzo Ribaudo, iInformatica Srl, Italy, vincenzo@iinformatica.it
Saverio Crisafulli, iInformatica Srl, Italy, saverio@iinformatica.it
Antonio Ruoto, iInformatica Srl, Italy, antonio@iinformatica.it
Vito Santarcangelo, iInformatica Srl, Italy, vitho87@hotmail.it, 0000-0003-4971-8788
Diego Sinitò, iInformatica Srl, Italy, diego@iinformatica.it, 0000-0002-5044-0050
Carlo Bonelli, Keylogic Srls, Italy, c.bonelli@keylogic.it
Giuseppe Stella, Stella All in One Srl, Italy, giuseppe@dittastella.it, 0000-0002-5967-5446

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Pierluigi Calabrese, Paola Lunalbi, Vincenzo Ribaudo, Saverio Crisafulli, Antonio Ruoto, Vito Santarcangelo, Diego Sinitò, Carlo Bonelli, Giuseppe Stella, *An application of the Agency for Digital Italy guidelines and CSA Star self-assessment: A Docustar case study*, © Author(s), CC BY 4.0, DOI 10.36253/979-12-215-0106-3.45, in Enrico di Bella, Luigi Fabbris, Corrado Lagazio (edited by), *ASA 2022 Data-Driven Decision Making. Book of short papers*, pp. 257-262, 2023, published by Firenze University Press and Genova University Press, ISBN 979-12-215-0106-3, DOI 10.36253/979-12-215-0106-3

hand, we identify the minimum set of information relating to the file/document that must be associated with the file itself, such as the ID, the producer, the date, the title, the subject, etc.

The management of digital documents is characterised by a process consisting of three distinct phases, which we will now look at in detail: the formation, management and preservation of the document.

The first aspect on which the guidelines are based deals with the formation of an electronic document, identifying four different ways in which an electronic document must be created to be considered valid:

- the creation of the document through software or cloud services that are qualified and able to guarantee that documents are produced in formats that allow interoperability between systems;
- the acquisition of an electronic document by telematic means or by storage device or the creation of a copy of an analogue document by scanning it and subsequent acquisition on an electronic medium, or the direct acquisition of an electronic copy of an analogue document;
- the storage of information in digital format on a storage device resulting from computer transactions or processes or from the submission of data via modules or forms made available to the user;
- The generation or grouping, also automatically, of a set of data or records, from one or more databases, according to a predetermined logical structure and stored in static form.

The digital document produced must be identified in a unique and persistent manner. As far as public administration is concerned, the guidelines require that identification take place by means of the document's registration, whereas in the case of any documents that are not registered, identification is entrusted to the functions of the computerised document management system. An identification system other than protocol is envisaged, which can be used as an alternative to the former by associating the document with a cryptographic fingerprint based on hash functions that are considered cryptographically secure. Subsequently, the document must be rendered unalterable: to achieve this, it is established that the document is stored on a computer medium in a digital format that cannot be altered in its access, management and preservation. The operations that must be performed to guarantee the immodifiability and integrity of the computer document are also established within the guidelines for each of the types of computer document formation set forth.

With regard to the computerised administrative document, the same rules apply as for the ordinary computerised document, with the difference that the immodifiability and integrity of this type of document can also be achieved through its registration in the entity's protocol register or in the other registers, directories, lists, archives or data collections that are contained in the entity's computerised document management system, and by the fact that the computerised file of the administrative document is associated with the set of metadata provided for protocol registration and those for classification and storage.

The guidelines then go on to regulate the stage of managing the computerised document, establishing the technical rules, criteria and specifications of the information that must be complied with when recording computerised documents. Each public administration must appoint a document management manager, as well as a document management coordinator, who have legal, IT and archiving skills. The computerised registration of documents is carried out through the application of electronic data attached or connected to the computer document that serve to uniquely identify it. Once the registration is completed, the document will be identified with the set of data in electronic format. The protocol registration, therefore, is made up of the set of metadata applied to the documents received or sent by the public administration (PA) that are stored in the protocol registry and that are associated in a permanent and unmodifiable form, a registry that must ensure that each protocol operation performed is traced, historicized and

attributed to the operator who performed it; in particular, it must be ensured that the information (subject, sender and addressee of a registered document) cannot be modified, nor cancelled, and that the only information that can be modified is that relating to internal administration assignment and classification. All modification or cancellation operations must be historicised and always visible. In addition, the system used for filing must be developed in compliance with the cyber security provisions of the guidelines, which must guarantee the unambiguous identification and authentication of users, the guarantee of access to resources only to users who are authorised and/or to groups of users according to the definition of appropriate profiles, the permanent tracking of any event of modification of the information processed and the identification of its author, sending the daily record of the protocol for the previous day to the filing system, through transmission methods that guarantee the unchangeability of the content.

Finally, the guidelines regulate the digital document preservation system, establishing that the computerised document management system must transfer closed computer files and closed computer series to the preservation system, transferring them from the current archive or from the deposit archive, and computer files and series that have not yet been closed, transferring the computer documents they contain according to the specific needs of the institution, with particular attention to the risks of technological obsolescence. The function of the preservation system is to guarantee the preservation of computerised documents and computerised administrative documents with the relevant metadata, as well as computerised document aggregations (i.e. files and series) and computer files with the relevant metadata until the eventual discarding of such computer files, through the adoption of rules, procedures and technologies in such a way as to guarantee the characteristics of authenticity, integrity, reliability, readability and retrievability of the same. In addition, the preservation system must have functions and requirements to ensure that it is possible to access the preserved documents for the entire period laid down in the owner's preservation plan and in current legislation, or for a longer period that may be agreed between the parties.

The guidelines also identify the subjects that play roles in the preservation process: the owner of the preservation object; the producer of the deposit package; the authorised user; the preservation manager and the preserver. In the public administration, the role of preservation manager is entrusted to an internal manager or official identified by the owner of the preservation object, who has legal, IT and archiving skills, or to a person outside the body, provided that he or she has the required skills and is a third party with respect to the owner of the preservation object, the preserver. His task is to define and implement the policies of the preservation system and to manage it independently under his responsibility: in particular, he defines the preservation policies and the functional requirements that the preservation system must have, manages the preservation process and ensures its constant compliance with the law, generates and signs the deposit report, monitors the proper functioning of the preservation system, carries out the periodic check, at least every five years, of the integrity and legibility of the documents contained in the preservation system, provides for the duplication or copying of computer documents as the technological context evolves, and prepares the necessary measures to ensure the physical and logical security of the preservation system.

The guidelines also provide the formation and adoption of a preservation manual (to be published on the institutional website), an IT document that specifically identifies the organisation, the subjects involved and their roles, as well as the operating model, a description of the process and the architectures and infrastructures used, the security measures adopted and all other information useful for managing and verifying the operation of the preservation system.

3. Analysis of solutions on AgID Cloud Marketplace

In order to carry out an analysis of the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) services qualified with AgID, we used the open data database of the Cloud Marketplace, taking advantage of the datasets obtained and analysing the

solutions of service offered on the marketplace, by year and by category.

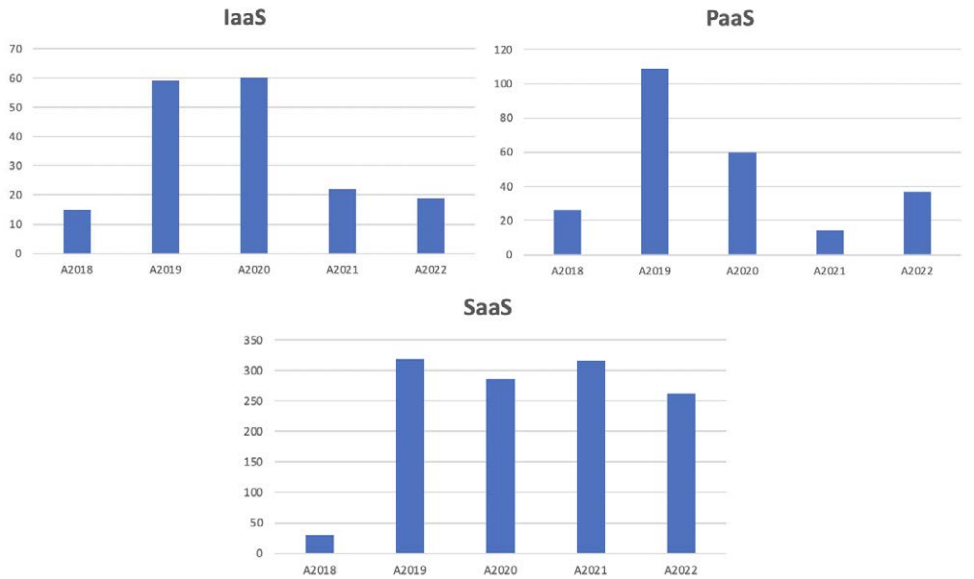

Figure 1. IaaS, PaaS and SaaS services on marketplace per year

The analysis carried out shows a greater presence of IaaS services within the marketplace in the two-year period 2019-20 (34%) as well as for PaaS services in 2019 (44%); it is also important the figure for SaaS, with an exponential growth from 2018 (2%) to 2019 (26%) that has remained constant over the years. This trend gives us evidence of how it has become necessary, as of 1 April 2019, for these services to be qualified by AgID and published in the Cloud Marketplace so that they can be acquired by public administrations.

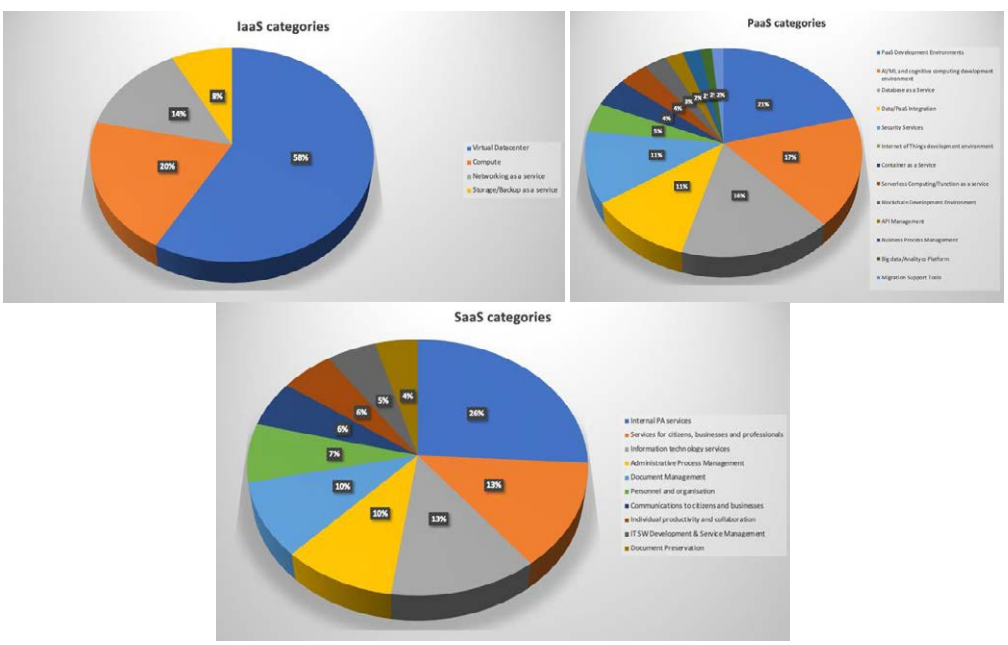

Figure 2. IaaS, PaaS and SaaS services on marketplace by category

An analysis by category, on the other hand, shows us that 58% of the IaaS services present on the market is related to virtual data centres, while in the case of PaaS services we find a 21% of PaaS development environments, 17% AI/ML and cognitive computing development environments, 16% database as a service environments, while a small slice (only 3%) concerns blockchain development environments. With regard to SaaS, most of the software relates to internal PA services (26%); 10% of the software on the marketplace relates to document management software, while only 4% of the software relates to document preservation software.

It is therefore clear that IaaS and PaaS services are the clear minority, given the considerable costs and above all the requirements involved, with mainly large accredited players starting out (such as IBM, Amazon, Oracle, Microsoft and Google), while SaaS services, for which it is sufficient to rely on an accredited Cloud Service Provider (CSP), are increasing.

4. Case study: Docustar

In order to be in perfect compliance with the requirements of the AgID guidelines, innovative SME Stella All in One Srl designed and developed the Docustar software, implementation of the new DRM-related industrial privative technique and in compliance with ISO 27001 no. 102020000032405 entitled 'Method for digital document rights management for digitisation, archiving and destruction for ISO27001 compliance' and Cloud Security Alliance (CSA) STAR Cloud Assessment. The latter is a free tool and registry that documents the security controls provided by different cloud computing services, thus helping users assess the security of the cloud providers they currently use or are considering to use.

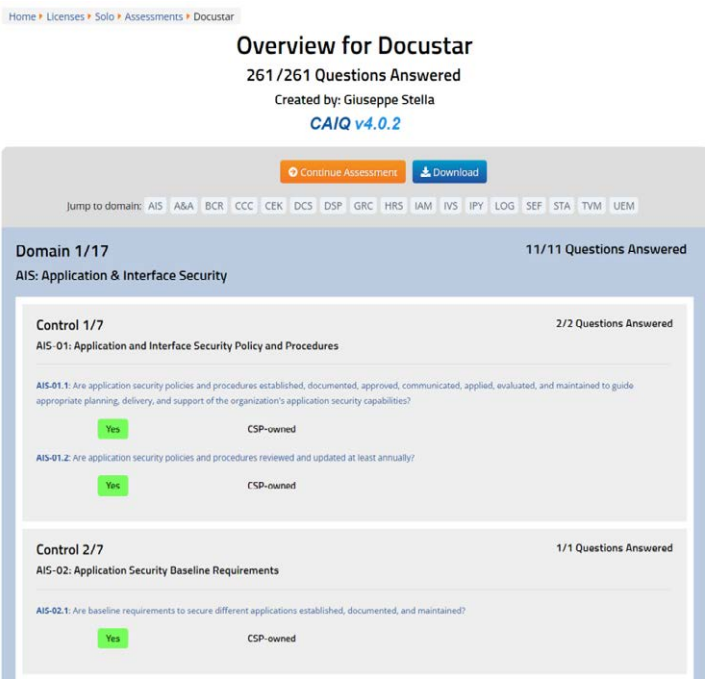

Figure 3. Overview for Docustar in CAIQ questionnaire

Observance of the RID paradigm (confidentiality, integrity and availability) and the related information security compliance is the object of the entire Docustar project. In fact, each document, in addition to being profiled and encrypted, is the subject of an appropriate workflow that traces each access to the system, the individual document request and the access to the resource, in order to guarantee appropriate confidentiality in the access and management of information resources.

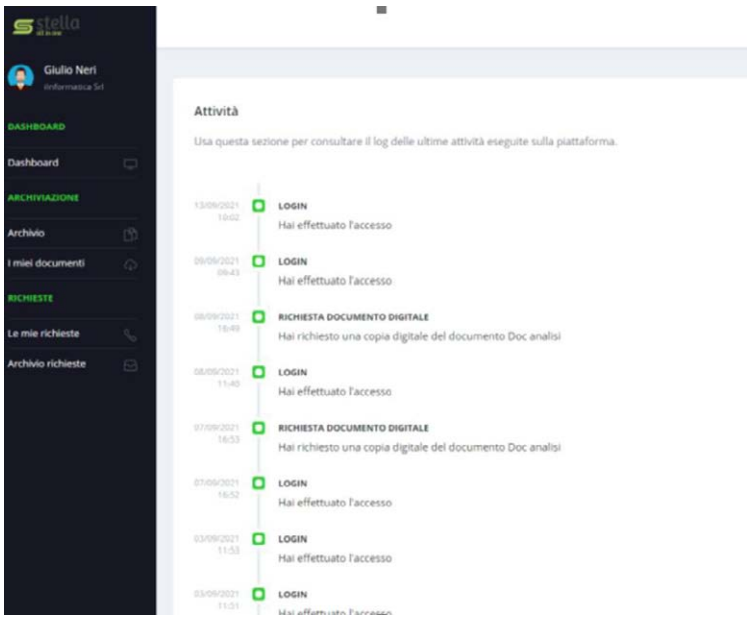

Figure 4. Docustar activities

5. Conclusions

This paper described the rigorous standards introduced at the Italian national level to regulate digital documents and document preservation and provided in Docustar a possible solution for complying with the relevant requirements set out, combined with a revolutionary document workflow approach with time-based Digital Rights Management (DRM). Docustar is a SaaS solution that confirms the potentiality of these applications that aims to improve PA services following AgID requirements compliance. This innovative approach that combines DRM within SaaS document management application opens the door to a new concept of data and file confidentiality by further enhancing the security of information exchanges in the cloud.

References

Calder, A (2009). Information Security based on ISO 27001/ISO 27002. Van Haren.

Lisi, A. (2009). The Digital Administration Code in Italy: Light and Shade. Curentul Juridic, The Juridical Current, Le Courant Juridique 1, pp. 57-63.

Phattanateeradej, C., Twittie S. (2016). Storage and search tool for cloud provider security information in CSA STAR. 13th International Joint Conference on Computer Science and Software Engineering (JCSSE). IEEE.

Ziming, L. (2008). Paper to digital: Documents in the information age. ABC-CLIO.

Voigt, P., Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International.

Diamantopoulou, V., Tsohou, A., Karyda, M. (2019). General Data Protection Regulation and ISO/IEC 27001: 2013: Synergies of activities towards organisations' compliance. International Conference on Trust and Privacy in Digital Business. Springer, Cham, pp 94–109.