Version 1.3 – 30 November 2020

This publication has been co-funded by the eInvoicing 2018 call of the Connecting Europe Facility (CEF) programme under the SCALES Project 2018-IT-IA-0053.

Version 1.3 – 30 November 2020

Editors: Andrea Caccia (UNINFO) and Daniele Tumietto (UNINFO), with contributions from Alessandro Mastromatteo and Matilde Ratti.

Experts from the UNI/CT 522 "eBusiness and financial services" and UNI/CT 523 "Blockchain and technologies for distributed ledger management" Commissions contributed to the document, as well as SCALES project partners: AgID, UNINFO, Infocert, Polimi - Politecnico di Milano, Consorzio Dafne.

Version 1.3 – 30 November 2020

Table of Content

1 FOREWORD

The SCALES 2018-IT-IA-0053 project is a project funded by the "eInvoicing 2018" call of the Connecting Europe Facility (CEF) programme in which AgID - Agenzia per l'Italia Digitale, coordinator of the mixed public/private consortium composed of UNINFO Politecnico di Milano, InfoCert and DAFNE Consortium participates.
The aim of SCALES is to design and implement a digital supply chain architecture enabling value-added services for businesses and public administrations:

- the DLT-RegRep (Register-Repository) model and
- the Once only principle,

creating a data ecosystem that facilitates the relationship between customers, suppliers, regulators and financial actors, and enabling the development of value-added services (VAS).
When using e-Invoicing, the supplier does not send the invoice, but makes it available to the customer and the control authorities on his SCALES node.
The SCALES architecture adopts technologies based on distributed ledgers (Distributed Ledger Technologies, DLT) and is designed in a multi-chain perspective so as to depend as little as possible on specific DLT implementations. The implemented model ensures that only the authorised party has access to the document or to a specific subset of metadata.
The owner has complete control over who accesses the data and for what reason, as well as being certain of the identity of the person accessing the data.

The model has advantages in terms of performance, scalability and data protection.

The SCALES model has numerous advantages in terms of:

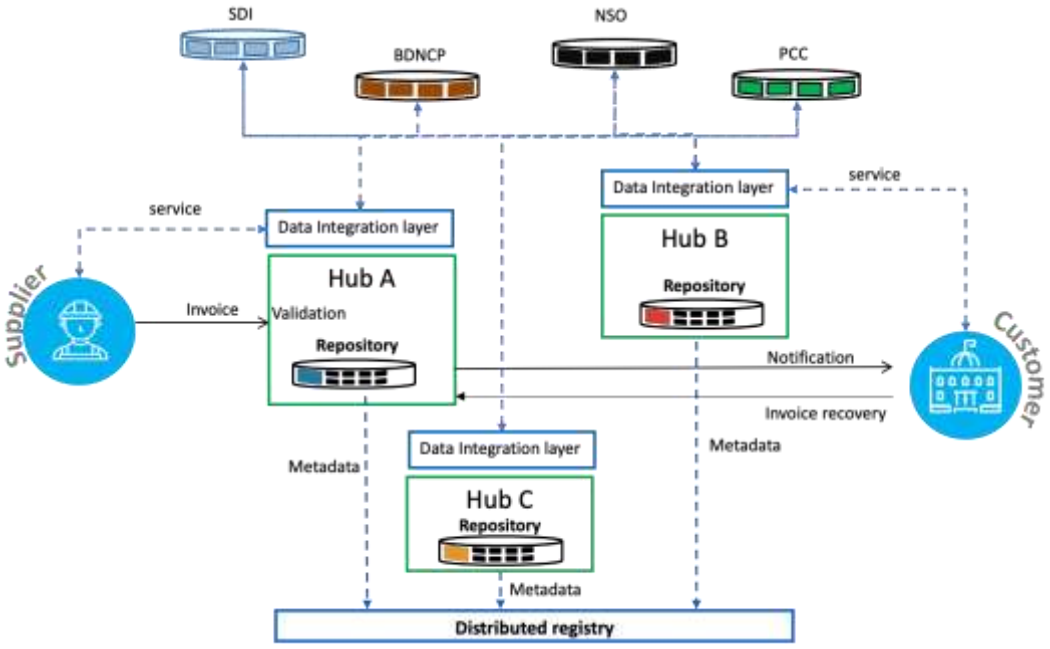
- performance,
- scalability,
- data protection.

The SCALES architecture has been designed with specific attention to the processing of personal data and compliance with Regulation 679/2016/EU, the so-called GDPR regulation.

Specific analysis and attention was paid to the order cycle and, in particular, to e-invoicing seen from a transnational perspective and therefore based on the European e-invoice standard defined by EN 16931-1:2017.

A vertical use case in healthcare was also developed, involving pharmaceutical companies, distributors and depositories.

The uniqueness of the e-Invoice object-document is guaranteed at logical level, i.e. both seller and buyer are present in SCALES and access the same object, and its updates as a consequence of the VAS intervention in the process.

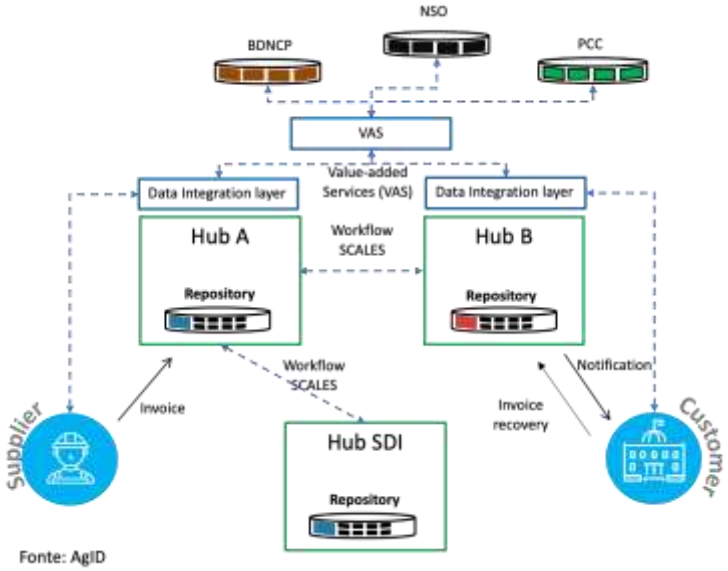


Basic logical architecture of the SCALES project

Finally, SCALES has been designed to also allow the integration of control and monitoring systems such as:

- Interchange System (SDI),
- Credit Certification Platform (CCP),
- National Data Bank for Public Contracts (BDNCP),
- Node for Sending Purchase Orders of Public Administrations (NSO),

as providers of value-added services (VAS) who may not participate in the network with their own node, but according to the following logical scheme



SCALES logic diagram

2 THE SCALES PROJECT - SUPPLY CHAIN ARCHITECTURE LEADING TO ENHANCED SERVICES

2.1 WHAT IS SCALES?

The objective of SCALES is to design and implement a digital supply chain architecture that is an enabler of value-added services (VAS) for businesses and public administrations.

The SCALES architecture adopts distributed ledger technologies (DLT) and is designed with a multi-chain perspective, adopting solutions compliant with personal data processing and Regulation (EU) 2016/679 (GDPR).

Particular analysis and attention have been paid to:

- the order cycle,
- the electronic invoicing, with a transnational perspective,
- the adoption of the European e-Invoice standard EN 16931-1:2017.

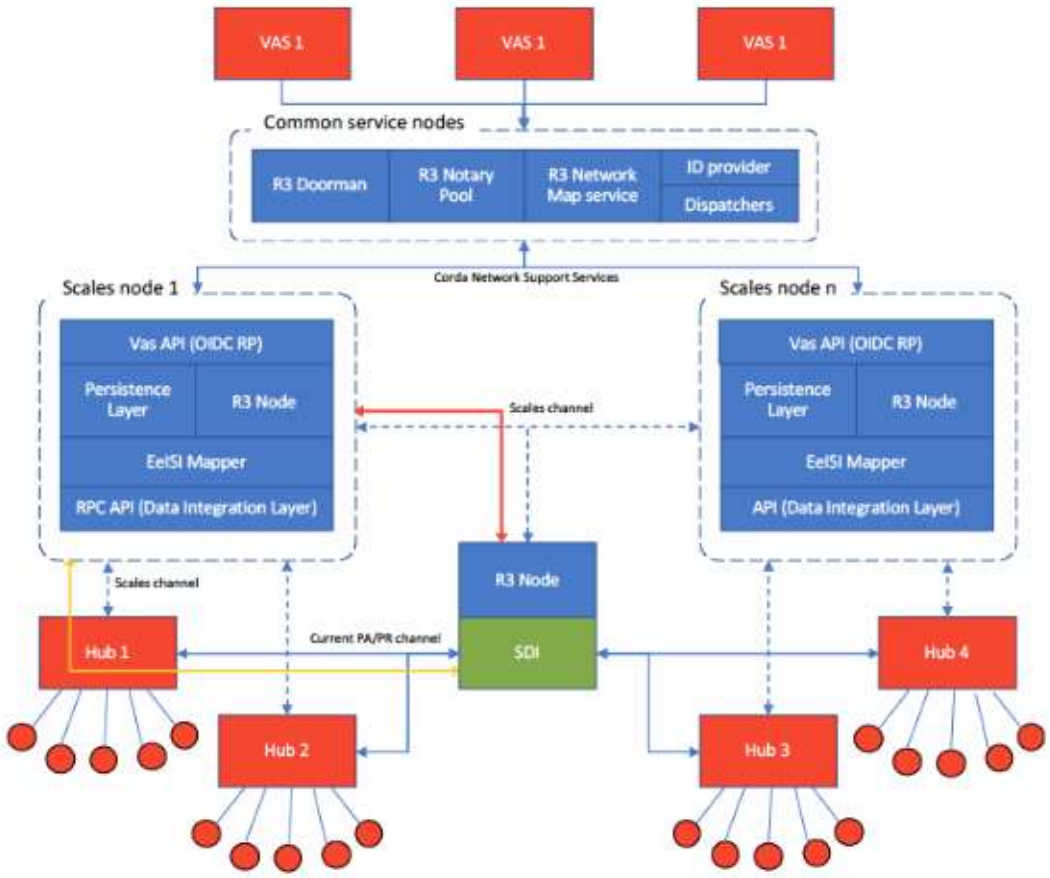
A vertical use case in healthcare was developed, involving pharmaceutical companies, distributors and depositories.

The e-Invoice is considered as a single document at logical level, therefore both seller and buyer in SCALES access the same data, and its updates, resulting from the interaction with VAS value added services.

The objectives of this project are:

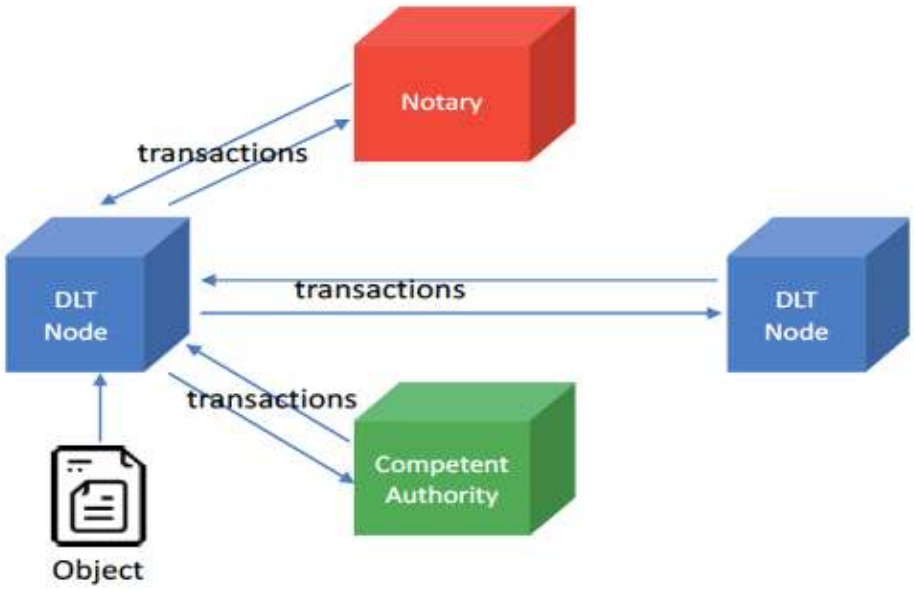
- design, analysis and implementation of an architecture for eProcurement systems involved in the supply execution phase;
- implementation of services addressed to SMEs for a complete adoption of EN 16931 "*Semantic data model of the core elements of an electronic invoice*" and its ancillary documents, with a specific focus on digital transformation in the post-award environment in B2G and B2B contexts;
- integration of e-Invoicing functionalities into existing eProcurement platforms, extending the results obtained in the previous eIGOR (2015-EU-IA-0050) and EeISI (2017-IT-IA-0150) actions;
- implementation of innovative digital services for the supply chain based on distributed repositories and DLT technologies, targeting different market sectors and vertical development in the health sector;
- dissemination activities to facilitate and promote further adoption of EN 16931 in national and cross-border contexts in all business sectors, both public and private.

SCALES logically implements the Distributed Registry-Repository model and the Once Only principle, creating a data ecosystem that facilitates the relationship between customers, suppliers and regulators and enables the development of value-added services:



The decentralised approach of the SCALES architecture also takes into account that:

- the **digital object** is created on a specific node of the DLT network and is visible only to the node that created it and to all the nodes of the counterparts involved in a given workflow;
- the **workflow is distributed** among several nodes, where each node participates through a transaction guaranteed by DLT;
- the only node that has **ownership of the data** is the source node, where the data have been loaded. All other nodes, involved in the workflow, participate by obtaining the data from the source node, processing it and signing their own transaction to advance the workflow;
- the **Competent Authority** node checks the correctness of the data within its competence;
- the **Notary node** guarantees via DLT the last step of the workflow, in order to avoid the repetition of the workflow on the same data instance (**double spending**);
- the system **complies with the GDPR - General Data Protection Regulation** (Eu) 2016/679', as further detailed in section 3.3.



For the development of SCALES the following assumptions were considered:

- standardised storage is a service external to SCALES, which could be provided by one or more VAS;
- once the archiving period has expired, the e-Invoice is deleted from the repository and the following metadata is retained:
    - Unique invoice ID,
    - Invoice imprint,
    - VAS data present, if any.

The development of SCALES, given its purpose, did not take into account a number of services that a generalised platform could implement of which some possible features are exemplified:

- integration into standardised storage nodes;
- the parametric management of the archiving period (other than storage in accordance with the law) of an electronic invoice, which could be modulated between a few months and a few years;

- the determination of the length of the storage period should be a matter for both the transferor and the transferee, who should be able to decide this "policy" according to their own needs (it could therefore be different for transferor and transferee for the same invoice);
- the archiving of an e-Invoice is done according to the active archiving parameter for each of the counterparts and, once the e-Invoice is issued, the archiving period for that invoice should not be changed;
- The transferor and transferee should always be able to request the immediate cancellation of an e-invoice, which can be accepted according to existing agreements and provisions.

3 AN OVERVIEW OF BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES (DLT)

Distributed Ledger Technologies (DLT) are technologies that enable the operation and use of an add-only ledger, shared among a set of nodes and synchronised between them using a consensus mechanism. While in distributed databases, all nodes have a copy of the database and can consult it but must pass through a central entity (or multiple validators) to modify the data, with distributed ledger technologies, instead, changes to the ledger are governed by consensus algorithms. The registry can therefore be read and modified independently by individual nodes.

Specific algorithms are used to achieve consensus between different versions of the ledger, even if they are updated independently by network members. In addition to consensus algorithms, DLT and Blockchain also make widespread use of cryptography to ensure the security and immutability of the shared ledger. Blockchain is a technology belonging to the DLT family whose distributed ledger is structured as an add-only sequence of blocks containing transactions or references to them. These blocks are confirmed, i.e. accepted by the validating nodes according to a consensus algorithm, and organised in a chain through cryptographic links.

In addition, Blockchain and DLT are the technologies behind the Internet of Value, which is the set of applications and platforms based on networks of digital and non-digital nodes linked by trust relationships that transfer value through a system of algorithms and cryptographic rules that allows consensus to be reached on changes to a distributed ledger by tracking the transfer of value through unique digital tokens.

3.1 THE EVOLUTION OF TECHNOLOGY: PAST AND PRESENT

Blockchain and DLT are increasingly attracting media attention and are considered among the most interesting digital trends for the coming years. Blockchain technology is a relatively recent invention, dating back just over 10 years to the creation of Bitcoin and cryptocurrencies.

Indeed, the innovative idea of a virtual, decentralised, p2p currency emerged as we know it today in 2008, when Satoshi Nakamoto's white paper was published. However, Bitcoin was soon associated with the illicit market, snubbed by banks and the media and considered a niche product.

At the same time, legislators have developed a conflicting approach towards cryptocurrencies. In some cases, Bitcoin was considered a currency, while in others it was prohibited or not recommended. Despite the discouraging picture, other platforms were created, based on the same founding principles as Bitcoin, but extending its scope of use, for example Ethereum, Corda, Hyperledger.

In 2016 something changed, suddenly the Blockchain was all over the media as one of the potentially revolutionary and disruptive technologies of the future. The media attention,

however, has always been closely linked to cryptocurrencies, rather than the technology behind them.

The boom phase of the cryptocurrency market, characterised by rapid growth in capitalisation in 2017, was suddenly followed in 2018 by a sharp drop in their value: the so-called Cryptowinter.

However, there has been no winter for Blockchain, which, if anything, is enjoying another spring, as it continues to mature and evolve, gaining strong interest from companies around the world.

So why is this technology attracting so much attention?

What is the real innovation introduced by Blockchain?

It is the achievement of the effective integration of established technological solutions (such as cryptography, hash functions, distributed systems) to create an irreproachable transfer of 'value', independent of central guarantors and potentially anonymous.

The revolutionary significance lies in this paradigm shift that may lead to the creation of the Internet of Value: a system that allows the exchange of valuable goods without intermediaries and in a programmable way using so-called smart contracts.

However, the technology is not yet fully mature, and there is much confusion and exploitation surrounding what it can and cannot do.

3.2 THE PILLARS OF THE INTERNET OF VALUE: SOME DEFINITIONS AND TECHNICAL CHARACTERISTICS

Blockchain and DLT are the technologies behind the Internet of Value, i.e. systems that allow value to be exchanged over the Internet as easily as we exchange information.

DLT systems are distinguished by three basic characteristics: the type of network, the consensus mechanism and the register structure.

Depending on the type of network, systems can be permissioned, i.e. systems where users have to register and identify themselves in order to be authorised to access; or permissionless, where anyone can access, without the need for authorisation.

The consensus mechanism varies according to the type of system. In permissioned systems, consensus is simpler: when a node proposes the addition of a transaction, its validity is checked and if approved by the majority of nodes, it can be added to the register.

In permissionless systems, on the other hand, consensus algorithms are more complex (based for example on Proof of work or Proof of Stake) to ensure that a malicious individual cannot create numerous fictitious identities to influence the registry update process.

The third feature of DLT systems is the structure of the ledger. In Blockchain solutions the ledger is structured as a chain of blocks containing multiple transactions and the blocks are linked to each other using cryptography (as is the case in Bitcoin or Ethereum platforms). In other solutions, the ledger consists of Tangle, where transactions are processed in parallel (for example Iota) or even other cases where the ledger is created by a chain of transactions (for example Ripple).

Blockchain systems also allow users to carry out transfers, or more generally, transactions. These transactions can be simple or more complex, depending on the level of programmability allowed by the platform. For example, the Ethereum platform allows the creation and management of smart contracts.

Finally, the last feature of blockchain systems is that there is a unique asset to be transferred, which can be a cryptocurrency or a token.

The numerous platforms enabling the Internet of Value share the following characteristics:

- Disintermediation, platforms facilitate the management of transactions without an intermediary, i.e. without the presence of trusted central entities;
- Decentralisation, information is recorded by distributing it over several nodes to ensure information security and system resilience;
- Log immutability, once data have been written to the log they can no longer be changed without the consent of the network;
- Transparency of the register: the content of the register is transparent and visible to all;
- Traceability of transfers, each item represented on the register can be traced back to its exact origin;
- Programmability, it is possible to schedule certain actions to be performed when certain criteria are met. Smart contracts, defined by Nick Szabo as "a set of promises, specified in digital form", including protocols within which parties fulfil these promises", are a fundamental element of some platforms;
- Digitisation, data are converted to digital format.

In the 2016-2017 period, it seemed that Blockchain solutions could solve countless problems and increase efficiency in many processes. Several companies, stimulated only by media hype, started to develop projects and experiments without fully understanding how the technology could really bring value. Efforts to apply Blockchain and DLT to unsuitable use cases have brought little benefit, and the technology itself has been blamed, rather than its concrete application.

For this reason, the Blockchain & Distributed Ledger Observatory, through the analysis of numerous use cases, has identified some variables that must be taken into account when assessing the suitability of Blockchain and DLT for a given project. In particular, Blockchain and DLT are particularly suitable when there are a large number of participants who do not trust each other (lack of trust) and need a shared system that can ensure that all copies of the shared ledger are updated in the same way, in the absence of a third party. Furthermore, it is important that these participants need to share information, i.e. it is useful to make a certain piece of information visible to a large number of parties, or they need to transfer assets between them, where it can be guaranteed that an asset is distinguishable and unique and therefore not replicable (uniqueness of the asset). The asset may be natively digital or easily digitised (digitisation).

Blockchain and DLT can also be applied to platforms that allow certain actions to be scheduled to be performed when certain conditions are met through the use of smart contracts (variable programmability).

Finally, Blockchain and DLT can be fully and properly exploited if the participants consider as a main objective that the shared information remains immutable and cannot be tampered with.

It is not necessary that all conditions are fully applicable, nor all at the same time. However, the more conditions are present, the more advantageous the implementation that a solution based on Blockchain and DLT can bring.

3.3 BLOCKCHAIN USAGE TYPES AND DLT-REGREP MODEL

Projects using blockchain and DLT can be classified according to their use.

Notarisation, for example, includes projects that use the distributed ledger of an existing blockchain to record the date of a document and the fact that it has not been modified over time (timestamp).

The mechanism is provided by the use of hash functions that allow a fingerprint (a fixed-length alphanumeric code) to be created from an entire document or database, which can then be shared on the blockchain.

Other projects use smart contracts and exploit existing networks and their programmability features to digitise processes and create decentralised applications (DAPs).

Then there are projects that exploit existing cryptocurrencies to enable the exchange of value between actors who do not know each other, in the absence of trust. In these projects, the presence of a unique asset within the platform becomes crucial. These three categories mainly use existing platforms.

On the contrary, there are some projects that are based on new platforms created ad hoc.

This is the case with Distributed Ledger Permissioned and Distributed Ledger Permissionless.

These projects envisage the creation of a network of nodes and an immutable and distributed register where information is shared between numerous actors in the absence of mutual trust. This model, which does not require any third party or even mutual trust between the counterparties, is known as the Zero Corner Model (ZCM) to distinguish it from the classic 2-sided models, i.e. with direct transactions, which are only possible if all the parties trust each other, 3-sided, i.e. with transactions via a service provider playing the role of a third party, which is possible if the counterparties trust the same service provider, or 4-sided, i.e. with the presence of a service provider trusted by each of the parties and a common rule to which all service providers adhere. The zero-sided model (ZCM) can be implemented through a DLT-based network and the distributed ledger, if the latency typical of DLT-based solutions can be neglected, represents the only shared copy of the information.

This also allows processes to be digitised and the programmability of smart contracts to be exploited, without introducing unique assets to manage transfers.

Assuming that the same information is available at the same time to each actor that has the right to access it, in a DLT-based network there is always a latency, dependent on its implementation, necessary to reach consensus among its nodes.

A shared ledger for e-invoices, and the supply chain in general, has no need for real-time transactions, and a typical DLT implementation is adequate for most cases, although the suitability of a specific DLT should be assessed on a case-by-case basis.

Some, or all, of the corporate data may be stored outside a DLT using registry-repository services such as, for example, OASIS RegRep[1], the use of which becomes necessary in cases where the immutability properties of a DLT are unsuitable, as may be necessary for full compliance with privacy rules (see Chapter 5 for specific details) or if there are reasons of commercial confidentiality with respect to the information handled.

In the case of SCALES, its DLT network implements a DLT-RegRep model and the information contained in the shared registry is linked to the data in the RegRep-based registry-repository to ensure its integrity and authenticity.

A DLT should therefore:

- provide a resilient infrastructure to cost-effectively manage the expected volume of documents and data;
- provide a platform to support the implementation of requirements, in terms of e-Invoicing and eProcurement services, related workflows and information access control.

The following are some requirements to be considered when designing a DLT implementing a ZCM:

- adoption of a DLT-based model that adopts the Once Only principle, extending the concept to all the different actors. It can be referred to as Provide Data Once Principle (PDOP);
- the parties do not send documents, but make them available to stakeholders and tax authorities;
- document metadata are stored in DLT and only accessible by authorised users, while DLT itself ensures their integrity;
- because of the immutability characteristic of DLTs, special care should be taken to avoid personal data being present in the clear in a DLT, so appropriate solutions such as encryption, anonymisation ... should be considered;
- implement better data control and protection, scalability and performance than the centralised hub architecture. Privacy requirements can be met by respecting the principle of '*need-to-know*' access to information;
- the use of common standards is essential, as, for example, the development of EN 16931:2017 has been crucial for the interoperability, with possible reuse, of the information contained in electronic invoices.

The following documents were developed during the project:

- **Report on Blockchain and DLT technologies**
  POLIMI conducted research on Blockchain and DLT technologies applicable to the supply chain and the national e-invoicing process.
  The analysis addressed the application of a DLT-based architecture to the stages of the order cycle.

[1] http://docs.oasis-open.org/regrep/regrep-core/v4.0/os/regrep-core-overview-v4.0-os.html

- **Solution design**
  The Solution design document, developed by Infocert, defines the general architecture of the SCALES network, taking into account the results of the state of the art analysis on DLT technology and the requirements of the Italian eInvoicing infrastructure (B2B and B2G) and end-to-end eProcurement systems.

- **New Service Framework**
  POLIMI conducted a survey on the supply of value-added services by existing supply chain ecosystems.
  Case studies will be produced to identify the criticality of existing services and the appetite of enterprises for new services.

- **Feasibility study on eProcurement systems**
  AgID has coordinated the feasibility study for the adoption of the SCALES architecture by national eProcurement systems including SDI. On the basis of the results of this study it is AgID's intention to update the AgID Circular 3/2016 that defines the additional technical rules for the interoperability of eProcurement systems pursuant to art.58 paragraph 10 of the Legislative Decree 50/2016 "Public Contracts Code", in order to facilitate the adoption of architectures based on DLT and BC on the SCALES model by national eProcurement systems.
  In particular, the study analysed the following aspects considered critical for the adoption of distributed ledger and blockchain technologies by eProcurement systems and by public administration systems in general:
    - Governance
    - Interoperability
    - Scalability
    - Performance
    - Verifiability
    - Integrity
    - Security
    - Privacy (GDPR)
    - Smart contracts (legal and non-legal)
    - Identity management

- **Software components**
  The software components of the SCALES architecture, developed by Infocert, will be published on Github under the EUPL licence to facilitate their adoption and reuse by public administrations and private sector companies.

- **Services for the health sector**
  DAFNE Consortium has developed a series of value-added services (VAS) aimed at NHS providers by exploiting the potential of SCALES with possible integration into national monitoring systems (SDI, NSO and PCC).

3.4 GENERAL OPERATING MODEL OF SCALES

For the correct management of privacy, the solution adopted was to keep the DLT node separate from the persistence layer, so that the digital object (such as an invoice) can be totally or partially erased (for example for any sensitive data present) while preserving the transactions that involved the digital object.

The service agreement defines the time for which the object remains stored on the node holding it.

Preservation could be carried out by the node where the digital object is placed in the node, in a manner unrelated to the operation of SCALES.

The system is not tied to compliance with 'electronic storage', the latter being an independent obligation from the Interchange System and solely the responsibility of the taxpayer under current tax law.

In any case, the token has a dual owner, so in case of deletion, both must be informed and decide independently on the deletion, bearing in mind that both have an independent responsibility with respect to compliance obligations.

There are three users of the invoice: sender, recipient and third party.

User histories may or may not be compatible, in which case a choice must be made:

- when the sender asks to delete a document, the recipient must be able to continue to access the document;
- automatic deletion may occur for both parties after a period of time defined in the service agreement, generally coinciding with the retention period provided for in the applicable tax legislation;
- each party must be able to access its own documents (active/passive) for the purpose of sending them for preservation;
- in the case of a third party involved in a transaction, the document can be verified by means of the fingerprint remaining on the document, thus allowing access to the data by the third party even if the sender and recipient have 'deleted' the document;
- the document can only be permanently deleted after the sender, the addressee and any third parties no longer have access to the document by automatic or voluntary deletion;
- any partial deletion of the document must be propagated to all nodes where the document is stored.

4 RESEARCH CONDUCTED BY POLITECNICO DI MILANO OSSERVATORIO DIGITALE B2B

4.1 THE ROLE OF THE B2B DIGITAL OBSERVATORY

The Osservatorio Digitale B2b is part of the Osservatori dell'Innovazione Digitale (Digital Innovation Observatories) of the Scuola di Management of the Politecnico di Milano, which aims to raise awareness in all the main areas of digital innovation through a team of almost 100 professors, researchers and analysts working in over 40 different Observatories on all the key issues of Digital Innovation in companies, including SMEs, and in the public sector.

The research of the Osservatorio Digitale B2b was conducted as a contribution to the SCALES Project. In particular, the role of the Osservatorio Digitale B2b was aimed at:

- develop survey-based research to define the uptake and interest of companies in various activities, while understanding the impact of e-invoicing on the automation of some of these services;
- define a service framework and an improvement roadmap on which to focus in order to invest in the digitisation of these activities.

4.2 THE MAIN RESULTS

The Observatory carried out a CATI survey, targeting both Italian SMEs and large enterprises, with a representative sample of the Italian business population, with ex ante and ex post weighting of the sample and results. The overall analysis highlighted some fundamental concepts:

- Large companies focus more on management control, dealing with a wider complexity in terms of suppliers and customers. On the other hand, SMEs are more focused on financial management, having also less need and urgency to manage their upstream value chain.
- In general, e-Invoicing has not yet been perceived in an advanced way within the supply chain: so far only the benefits of the activities directly impacted by the obligation are exploited, while there is no investment aimed at integrating it into more comprehensive digital processes. The relational and ecosystem dimension is therefore missing. Investments in automation are oriented towards activities that tend to be time-consuming, where the company has direct visibility of the time spent and the time that could be saved. In addition, the willingness to invest in automation activities already at a medium level shows that many companies are still in the process of digitisation: after the initial investments, the company perceived the efficiency and effectiveness improvements linked to automation, thus confirming further future investments for a further evolutionary step. Most companies, on the other hand, show that they have not yet implemented a long-term vision: there is probably no process viewpoint, so a specific framework is needed to understand where improvements introduced by digitisation would have an impact.
- When investing in a new business management system, large companies attach great importance to easy integration with existing systems.
  This is because, being large companies, the software, management and database systems are often well integrated and well adapted to the needs and processes of the company

itself, which therefore wants to maintain the same level of efficiency with subsequent add-on systems.
Another key feature for large enterprises is the facilitation of relations with domestic customers/suppliers, with the aim of optimising flows within their supply chain. In this context, the introduction of e-Invoicing can certainly have a positive impact.
On the other hand, for SMEs, preferences are more widespread.
In particular, it should be considered that among the characteristics of the new systems, the facilitation of relations with domestic customers and suppliers and those with foreign customers and suppliers have almost equal weight.

- However, it should be emphasised that the pharmaceutical sector shows a greater awareness and readiness to perceive the improvements linked to e-Invoicing, particularly in relation to those activities that characterise supply chain relationships (vendor and customer rating) and those relating to the analysis of internal processes (process mining).

The data therefore show that the market is not yet ready and has not yet managed to go beyond the obligation, using e-Invoicing to apply digitisation to new business processes, increasing efficiency and effectiveness.

The key aspect is that the use of e-Invoicing and the information it contains must go beyond the administrative area, so that this data can travel further within the company and contribute more to the overall management of the business situation within the supply chain, to create a greater balance in a wider ecosystem.

Maturity is not simply about having efficient administrative processes, but about making sure that the data in e-Invoicing (in a synthetic way) is released in all business units to give a greater contribution to knowledge and decision making, in order to better incorporate it:

- planning processes;
- logistics;
- production;
- marketing....

4.3 THE NEW FRAMEWORK AND ROADMAP OF ACTIVITIES

The Observatory therefore decided to aggregate the individual activities into macro-areas in order to better appreciate the differences between the group of activities and try to prioritise the actions to be taken.

From this, an overall picture emerged of new services that can be implemented and the roadmap shown in the figure below.

Companies need to optimise a few key activities first, in order to obtain results that can then be exploited in several related processes, as shown in the figure.

These are the activities that can reap the most immediate benefits, following the introduction of the eOrder and e-Invoicing obligations.

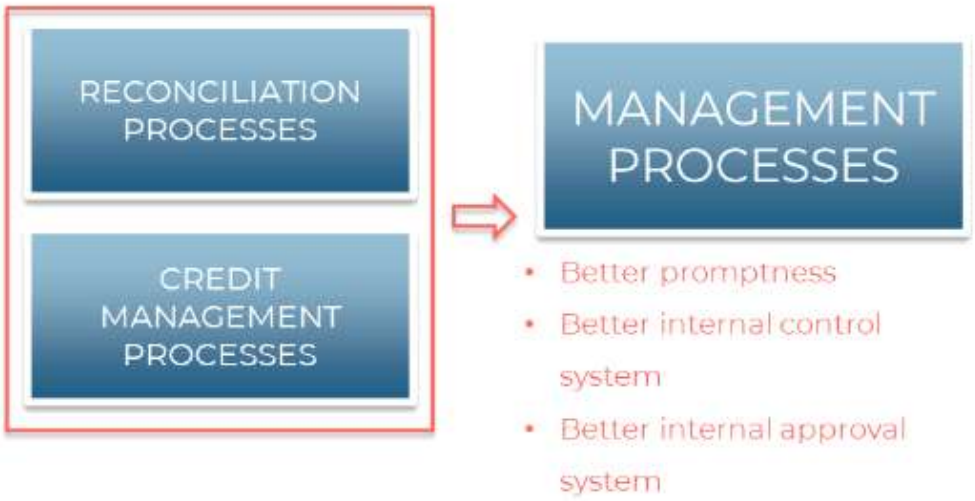
A company can only optimally improve these processes if it has first perfected its reconciliation processes, in particular the amounts received.

Therefore, we focus on these processes and activities as they can lead to improvements and problem solving in other areas.

And then, what should be the next steps?

Which services need to be optimised?

On the basis of the findings of the previous analyses, the research recommended a sequence of the different areas of activity on which to intervene represented in the figure below.



The creation and development of new services can therefore be repeated in a modular manner on the different blocks of the framework.

In this way, the company can make use of the experience already gained during the first steps in optimising reconciliation processes and credit management activities.

4.4 A FURTHER STEP FORWARD: SUPPLY CHAIN FINANCING INSTRUMENTS

As we have outlined, the first steps concern the improvement of the company's internal processes, in particular those related to financial and management activities.

Once these steps have been completed, the company can then focus its optimisation efforts on two different paths:

- on activities related to the internal value chain (purchasing, operations, marketing & sales);
- on their supply chain activities, in particular with regard to supply chain financing instruments, see figure below.

5 REGULATION (EU) 2016/679 AND REFERENCE PRACTICE UNI/PDR 43:2018

5.1 REGULATION (EU) 2016/679.

The purpose of the new European Data Protection framework is to create a coherent and harmonised EU-wide system for the protection of personal data. It was presented by the Commission on 25 January 2012 and finally approved by the Parliament and the Council on 27 April 2016. The final texts of the measures were published in the Official Journal of the European Union on 4 May 2016 (L 119).

The current legal framework for the protection of personal data in Europe and Italy is represented by:

- General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) published in the Official Journal of the European Union on 4 May 2016, entered into force on 24 May 2016, became effective on 24 May 2018)
- General Data Protection Directive - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- Legislative Decree No. 81 of 30 May 2018 Implementing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

This legal framework serves to:

- create a uniform legal framework, but in many areas allow or refer to derogating legislation of the Member States,
- contemplate the possibility or need for specific regulations at national level in certain areas left to the national laws of EU Member States,
- maintain the basic concepts governing the roles of owners and managers,
- affects and increases the responsibilities of data controllers and data processors,
- affects the role and powers of national supervisory authorities.

The most important principles of adaptation, integration and margins of flexibility contained in the following recitals of Regulation (EU) 2016/679 are reported:

Recital 8 - Where this Regulation provides for specifications or limitations of its rules under the law of the Member States, Member States may, to the extent necessary for the sake of consistency and to make the national provisions understandable to the persons covered, incorporate elements of the Regulation into their national law;

Recital 9 - Although its objectives and principles remain valid today, Directive 95/46/EC has not prevented the fragmentation of the application of personal data protection across the Union, nor eliminated legal uncertainty or the widely held public perception that in particular online operations pose risks to the protection of individuals;

Recital 10 - This Regulation provides for a margin of manoeuvre for Member States to specify the rules, with regard to the processing of "sensitive data", as regards processing for the performance of a lawful obligation and for the performance of a task carried out in the public interest or in the exercise of official authority.

In this sense, the regulation does not exclude that the law of the Member States lays down more precisely the conditions under which processing is lawful;

Recital 11 - Effective protection of personal data throughout the Union presupposes the reinforcement and detailed regulation of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers to monitor and enforce compliance with data protection rules and equivalent sanctions for infringements in the Member States.

The **principle of Accountability is an** important innovation because it introduces the shift from form to substance. Indeed, the data controller is responsible for complying with the principles applicable to the processing of personal data that can prove it ('accountability'), and the most important references are contained in the following Recitals:

- 42 Consent,
- 69 Legitimate interest of the proprietor,
- 74 Empowerment,
- 77 Security of treatment,
- 78 Privacy by design,
- 81 Data processor,
- 82 Register,
- 84 DPIA and
- 85 Data breach.

The characteristics of decentralisation, immodifiability and persistence of the TLD must be assessed and coordinated with the provisions on the protection of personal data dictated by EU Regulation no. 679/2016 - GDPR, aimed at regulating the hypotheses of centralised processing of the same data. As is known, in fact, such legislation imposes a series of obligations on the

data controller, which must be identified from time to time. Consequently, any processing of personal data carried out by means of the system in question must comply with the fundamental principles set out in the GDPR (principle of lawfulness of the processing, principle of privacy by design and of privacy by default, etc.) and must be based on the assumptions of legitimacy of the processing set out in Articles 6 and 9. In fact, a system based on DLT that operates with personal data falls within the scope of the data protection legislation and must therefore meet several legal requirements. Specifically, further critical profiles may concern:

- **immodifiability of the information** entered in the blockchain in the event that personal data relevant to privacy have also been acquired; relationship with the right to be forgotten with the possibility of requesting the deletion of the data pursuant to Article 17 GDPR: this is, however, not an absolute right as it is mitigated, for example, by the presence of a public interest or the occurrence of the cases dictated by paragraph 3 of Article 17 GDPR (exercise of the right to freedom of expression and information; fulfilment of a legal obligation; reasons of public interest in the public health sector; archiving in the public interest, scientific or historical research or statistical purposes; ascertainment of the right to privacy, scientific or historical research or statistical purposes; verification of the existence of the right to be forgotten). 17 GDPR (exercise of the right to freedom of expression and information; fulfilment of a legal obligation; reasons of public interest in the public health sector; archiving in the public interest, for scientific or historical research or for statistical purposes; establishment, exercise or defence of a right in court);

- **guarantee of the right of** rectification, pursuant to Article 16 GDPR, of any inaccurate personal data: to be achieved through the request for data correction coming from all the participants in the blockchain and subsequent subscription of the data thus amended;

- compliance with the **right to data portability** (Art. 20 GDPR) through the possibility of rendering personal data to the applicant in an electronic format that is interoperable with systems other than the original blockchain.

In any case, knowledge of data protection principles is the basis for '*implementing appropriate technical and organisational measures*': in detail, Article 25 GDPR provides for the principle of ***Privacy by Design and by*** *Default,* i.e. '*data protection by design and protection by default*'. This is a general obligation according to which: "'*taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, and taking into account risks of varying likelihood and severity to the rights and freedoms of natural persons represented by the processing, both at the time of determining the means of processing and at the time of processing itself*', the data controller '*shall implement appropriate technical and organisational measures, such as pseudonymisation, to implement effectively the principles of data protection, such as minimisation, and to build the necessary safeguards into the processing to meet the requirements of this Regulation and to protect the rights of data subjects*'.

In light of the principles of **Privacy by Design and by Default,** therefore, the data controller must ensure that it puts in place '*appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed by default*'. In this sense, '*this obligation applies to the amount of personal data collected, the scope of processing, the storage period and accessibility*.' This means that such '*measures shall ensure that, by default, personal data are not made accessible to an indefinite number of*

natural persons without the intervention of the natural person'. Finally, a certification mechanism is foreseen in this area, which '*may be used as an element to demonstrate compliance with the requirements*' mentioned above.

Principles of data protection and related risks

The implementation of a DLT or Blockchain system cannot therefore disregard, when it contains personal data, the principles of privacy by design at an early stage. The principles to be considered, identified in Article 5 GDPR, are:

(i) *purpose limitation*: data collected and processed must fulfil a predefined purpose and therefore have a specified, explicit and legitimate purpose, to be further processed in a way that is not incompatible with that purpose. *Ad hoc* purposes distinct from those initially established for the further processing of personal data are contrary to this fundamental principle of data protection. Consequently, the re-use of personal data for a purpose not initially foreseen is contrary to the purpose limitation principle.

If the purpose limitation principle is not respected, the data could be processed in a way contrary to the information given in the notice that the data subject received at the time of sharing;

(ii) *accuracy*: the principle requires data controllers to ensure that personal data are '*accurate and, where necessary, kept up to date'. If* not, they must be '*erased or rectified' without* delay. In other words, if the data are inaccurate, they must be rectified. In DLT-based systems, the ability to delete or rectify inaccurate data poses specific problems due to the distributed functionality and immutability property. However, if the only purpose of the application is to document the occurrence of a fact at a certain point in time (by combining a piece of data with a time stamp, thus not attempting to describe the current state of affairs), there does not seem to be any criticality in relation to the principle of accuracy;

(iii) *Data minimisation and retention limitation: minimisation is the collection and* processing of a limited amount of data; such data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Data may be minimised from the source (i.e. at the time of collection) or reduced to what is strictly necessary if imported from an existing source. Supervisory authorities may verify that technical and organisational measures are taken that are proportionate to the risk to the data subject. Failure to minimise data increases the risk to the rights and freedoms of the data subject. It is therefore recommended that a DLT-based system be designed to consider the data minimisation requirement at the initial design stage, in accordance with the principle of *privacy by design*;

(iv) *Confidentiality and integrity*: according to recital 39, of the GDPR Personal data must '*be processed in a way that ensures appropriate security and confidentiality, including to prevent unauthorised access to or use of personal data and the equipment used for processing*'. Ensuring this principle requires both the knowledge of what data must not be disclosed to third parties and the application of appropriate technical and organisational measures to safeguard the data from disclosure. In DLT-based systems potentially all or many nodes could be aware of personal data. It is therefore necessary

to strike a balance between the visibility of some data to keep the system functional and distributed and the application of technical measures to safeguard personal data from unauthorised access;

(v) *transparency:* this is a fundamental principle of data protection. The GDPR requires that data processing be carried out in a fair and transparent manner. The obligation to inform the data subject is a corollary of the obligation to be transparent about the processing of their data. Data subjects must be fully informed of the relevant aspects of the processing (e.g. from whom the data are collected for what purposes, how long the data are stored, who might possibly receive such data, what rights are applicable to them, how to enforce such rights etc.). The risk that could result from not complying with the transparency principle is that the purpose and scope of the data processed on the DLT network is not communicated. Efforts should therefore be made to clarify these aspects with informative content that is accessible and presented to the intended audience.

Further requirements

Additional requirements under the GDPR Regulation that should characterise any processing of personal data include:

1) ***right to be forgotten*** *(Article 17 GDPR)*: the right to erasure of personal data without undue delay is technically possible on a single computer from a technical point of view. Implementing this right in a DLT-based system is relatively more difficult because deletion on the computer of a single node does not result in deletion throughout the network. Although some technical measures have been proposed to delete specific transaction content from a DLT, this is highly dependent on the existence of an enforceable *governance* mechanism that allows deletion '*without undue delay*' at the request of a data subject;

2) ***immutability of records***: Article 17(3) GDPR governs exemptions from the obligation to erase data at the request of the data subject. If a DLT-based system is able to comply with one of these exemptions, the immutability feature of a DLT network may be justified and allowed;

3) ***right of rectification*** *(Art. 16 GDPR)*: when data is incorrect, the data subject has the right to request rectification. In DLT-based systems, it is not entirely clear whether the requirement is met with further data entry, correcting incorrect information without complete deletion of the previous data. Even if information or transactions can be invalidated with the newly added blocks, anyone can view incorrect data. Even if this technical solution were sufficient, its implementation would still represent a significant obstacle to compliance with this requirement;

4) ***right to data portability*** *(Art 20 GDPR)*: the right to data portability allows a data subject to request from a data controller, in a structured, commonly used and machine-readable format, the personal data concerning him or her that has been provided. As data portability is primarily an answer to a problem that arises in closed-format systems, it can be solved more easily in DLT-based systems if common interoperability standards are applied;

5) ***information to be provided to data subjects*** *(Articles 13 and 14 GDPR)*: data controllers are required to inform data subjects about the processing of personal data relating to them.

In DLT-based systems, this can present aspects of uncertainty, as the role of the data controller is difficult to identify;

6) ***automated decision-making*** *(Art. 22 GDPR)*: the data subject has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar way. The aim of Article 22 GDPR is precisely to establish high safeguards for fully automated decision-making processes that have legal consequences for the data subject. Although applications relying on DLT networks often implement highly automated processes (e.g. *smart contracts*), it strongly depends on the individual use case whether this functionality constitutes a decision falling within the scope of Article 22 GDPR. The controller shall implement appropriate measures to safeguard the rights and freedoms of the data subject and their legitimate interests, at least the right to obtain human intervention.

7) ***data minimisation*** *(Article 5(1)(c) GDPR)*: in a DLT-based system, one of the possible ways of promoting compliance with the principle of data minimisation may be to pseudonymise the data with the use of *hash* functions. In the case of a DLT network that guarantees data immutability, data minimisation must be taken into account already during the development process, since subsequent modification is technically difficult, if not impossible, due to the intrinsic characteristics of DLTs;

8) ***data subject's right of access*** *(Art. 15 GDPR)*: the data subject has the right to obtain from the controller confirmation as to whether or not personal data relating to him or her are being processed, and if so, to obtain access to the personal data. Compared to a centralised system, it might be even easier for the data subject to access the necessary information in a transparent DLT-based system. However, applying this right in a distributed network might present technical difficulties that need to be addressed by *governance* methods.

The SCALES project, in order to allow a flexible and privacy-compliant implementation, has adopted the DLT-RegRep model, which on the one hand makes it possible to exploit the immutability guarantees of a DLT network to guarantee the integrity of transactions and information, and on the other allows, through a registry-repository service (RegRep), to comply with regulatory requirements while maintaining control over the information, as described in more detail in paragraph 3.3.

The above has also seen the issuing of applicable standards for **certifications** which can be divided into:

REGULATED CERTIFICATIONS,
based on Laws, Regulations, Directives.
Certification is based on compulsory compliance with the regulations set out in State Laws and European Union Regulations or Directives.

VOLUNTARY CERTIFICATIONS
which are technical rules of private origin.
The choice to adhere to certification is entirely voluntary, as it is not established by law.
Certifications are therefore based on reference or technical standardisation documents.

Some certifications are based on the ISO/IEC 17065 accreditation standard schemes such as:

- **UNI/PdR 43.2:2018** - Guidelines for the management of personal data in the ICT environment according to Regulation (EU) 2016/679 (GDPR) - Requirements for the protection and conformity assessment of personal data in the ICT environment**;**
- The proprietary certification scheme **ISDP©10003:2015** developed by INVEO, prior to the entry into force of Regulation (EU) 2016/679.

ISO has issued **ISO/IEC 27701:2019** Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines that can be used for the certification of the management system of any entity that processes personal data.
Work is underway within **CEN/CENELEC/JTC 13/WG 5** to write a standard based on ISO/IEC 27701 to enable its use within certification schemes based on **ISO/IEC 17065** as required by Article 43 of the GDPR for certifications issued under Article 42.
The certification of professional profiles in the field of data protection is possible under Law 4/2013 according to the **UNI 11697** standard, which defines the figures of:

- Data Protection Officer,
- Privacy Manager,
- Privacy verifier,
- Privacy Specialist.

With regard to the certifications in the field of privacy, we believe it is appropriate to recall what is written in the joint statement of the Privacy Guarantor and ACCREDIA[2]: "in *order to correctly address the activities carried out by the various stakeholders in this area - that at the moment the certifications of persons, as well as those issued in the field of privacy or data protection that may be issued in Italy, although they may constitute a guarantee and act of diligence towards stakeholders of the voluntary adoption of a system of analysis and control of the principles and standards of reference, under current legislation cannot be defined as "complying with Articles. 42 and 43 of Regulation 2016/679", as the "additional requirements" for the purposes of accreditation of certification bodies and the specific certification criteria have yet to be determined.*"

5.2 UNI/PDR 43:2018

The UNI/PdR 43:2018 (in Italian Prassi di Riferimento) "*Guidelines for the management of personal data in the ICT environment according to EU Regulation 679/2016 (GDPR)*" was developed by the Table "Privacy management processes in the digital environment", under the coordination of UNINFO, which works in the field of information technologies and their applications.

The reference practice consists of two sections:

[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723

- **UNI/PdR 43.1** 'Management and monitoring of personal data in the ICT environment'.
- **UNI/PdR 43.2** "Requirements for the protection and conformity assessment of personal data in the ICT environment.

Section 1 provides guidelines for the definition and implementation of processes concerning the processing of personal data by electronic means (ICT), according to European Regulation 679/2016 and current legislation.
Section 2 provides an appropriate set of requirements that enables organisations, in particular SMEs, to comply with the European and national regulatory framework in an effective way, and to demonstrate this compliance and effectiveness also through a certification route.
Only UNI/PdR43.2 can be used for certification activities.

What does it mean to be certified?

It means having a compliant planning and proper management with regard to:

- Risk Management for personal data,
- Implementation plan for the 'protection of Personal Data',
- PIA - Privacy Impact Assessment,
- Consent of the person concerned,
- Innovative operational tools,
- Protection by design and by default,
- Treatment records,
- Economic aspects and synergies,
- Data Breach,
- Role of the Data Protection Officer.

6 ANNEXES

6.1 TERMS & DEFINITIONS

- ITU: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf
- ISO: https://www.iso.org/obp/ui#home
- UNCEFACT: https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf , Annex II.

6.2 SOURCES TO BE TAKEN INTO ACCOUNT

- Dl 135/2018 Art. 8 ter https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135!vig=
- Blockchain - Consultazione pubblica "Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain" https://www.mise.gov.it/index.php/it/consultazione-blockchain#documento
- Linee guida modello Interoperabilità https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/bozza/doc/doc02cap07.html
- Regolamento eIDAS https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32014R0910&from=ES#d1e2942-73-1-
- REGULATION (EU) 2018/1724 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 2 October 2018 "establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L.2018.295.01.0001.01.ENG
- Circolare Accredia su eDelivery eIDAS https://www.accredia.it/app/uploads/2020/03/CircolaretecnicaDC05-2020.pdf
- Blockchain and the General Data Protection Regulation https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRSSTU%282019%29634445
- Study on blockchains. Legal, governance and interoperability aspects – Study https://op.europa.eu/en/publication-detail/-/publication/c7d71ce2-5782-11ea-8b81-01aa75ed71a1/language-it
- JRC Report "Blockchain Now And Tomorrow - Assessing Multidimensional Impacts of Distributed Ledger Technologies" https://ec.europa.eu/jrc/en/facts4eufuture/blockchain-now-and-tomorrow
- EU Blockchain Observatory and Forum reports https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRSSTU%282019%29634445
- PEPPOL Continuous Transaction Controls Project, Tax clearance and reporting models. https://peppol.eu/wp-content/uploads/2019/09/20191105-Hoddevik-on-Peppol-André-Hoddevik.pdf
- PEPPOL CTC project Reference Group presentation, May 20, 2020

6.3 TECHNICAL STANDARDS AND INTERNATIONAL RECOMMENDATIONS

ISO/TC 307 Blockchain and distributed ledger technologies
(https://www.iso.org/committee/6266604.html)

- ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary
- ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
- ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
- ISO/CD TR 23245.2 Blockchain and distributed ledger technologies — Security risks, threats and vulnerabilities
- ISO/CD 23257.3 Blockchain and distributed ledger technologies — Reference architecture
- ISO/CD TR 23576 Blockchain and distributed ledger technologies — Security management of digital asset custodians

- DIN SPEC 4997 (PAS) Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology
https://www.din.de/en/innovation-and-research/din-spec-en/business-plans/wdc-beuth:din21:303231492

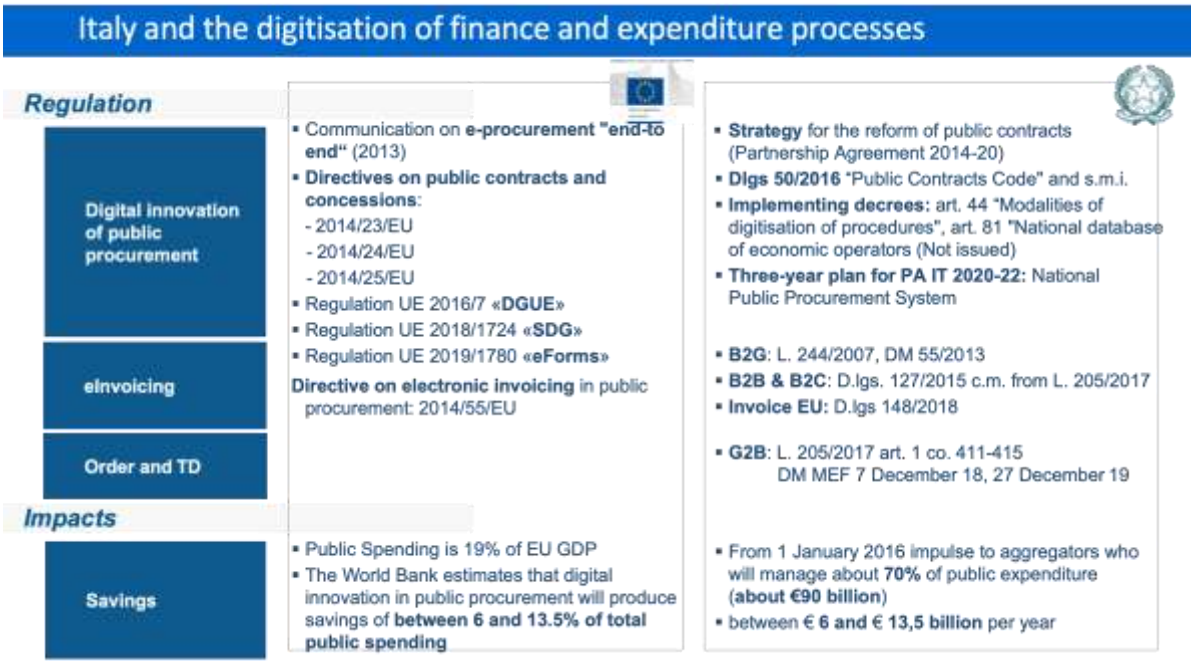
- PAS 333:2020 PAS 333:2019, Smart Legal Contracts – Specification
https://standardsdevelopment.bsigroup.com/projects/2018-03267#/section

- ESI Policy and security requirements
  - ETSI EN 319 401
https://www.etsi.org/deliver/etsien/319400319499/319401/02.02.0020/en319401v020200a.pdf
  - ETSI EN 319 521
https://www.etsi.org/deliver/etsien/319500319599/319521/01.00.0020/en319521v010000a.pdf

- UNCEFACT
  - Transport, Trade Logistics and Trade Facilitation, Seventh session: Trade facilitation and transit in support of the 2030 Agenda for Sustainable Development
https://unctad.org/system/files/non-official-document/cimem7p16_Lance%20Thompson_en.pdf

6.4 DIRECTIVE 2014/55/EU ON ELECTRONIC INVOICING IN PUBLIC PROCUREMENT

e-Invoicing is the pivotal point in the process of digitisation of procurement, tax payment, accounting and auditing processes to be achieved through the implementation also of the European standards related to end-to-end e-procurement that are being defined by CEN/TC 434 and CEN/TC 440, which represent a key element to contribute to the sustainable growth objectives indicated by the EU 2020 Strategy with the "*Communication of the European Commission (2013) 453 End-to-end e-procurement for the modernisation of public administration*".



End-to-end e-procurement is not about implementing an IT project that would only replicate paper-based processes; it is an opportunity to radically rethink the way public administration is organised, and this rethinking is also being addressed with state-of-the-art technologies.

Italy considers it essential to achieve compliance with both the European e-Invoice and the PA's digital procurement management process to reduce costs and create new efficiencies and value. Compliance alone does not require a significant overhaul, in fact the PA Invoice format already existed, but the potential for savings lies in the addition of new levels of automation of e-invoice management that also improve both the fight against evasion and VAT fraud. The Directive required the definition of a European standard defining a common semantic model on e-Invoicing and further standardisation documents to improve interoperability at syntax level.

Article 1 of Directive 2014/55 specifies that it applies to e-invoices issued as a result of the performance of contracts to which it applies:

- Directive 2009/81/EC on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security,

- Directive 2014/23/EU on the award of concession contracts,
- Directive 2014/24/EU on public procurement or Directive 2014/25/EU on procurement entities operating in the water, energy, transport and postal services sectors.

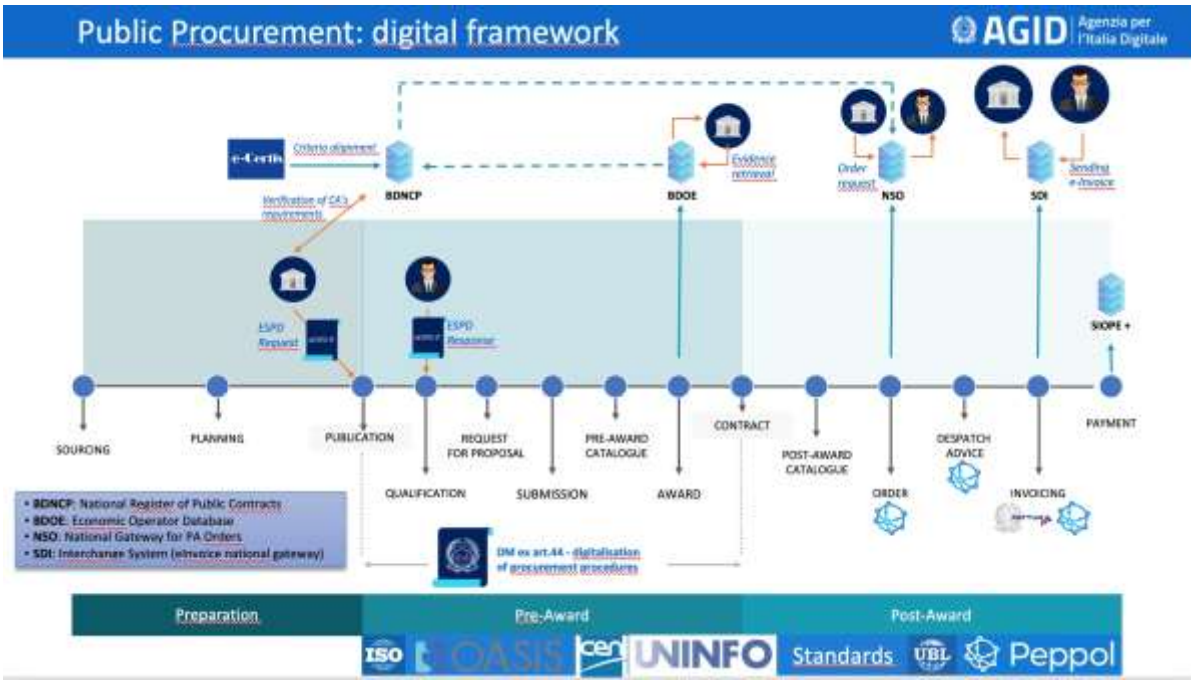
The Directive states that the obligation to receive e-invoices "*shall not apply to e-invoices issued as a result of the performance of contracts within the scope of Directive 2009/81/EC where the award and performance of the contract is declared secret or is subject to special security measures in accordance with the laws, regulations or administrative provisions in force in a Member State, and provided that the Member State has determined that the essential interests involved cannot be secured by less restrictive measures*".

There is an obligation to receive and process, so the supplier will have the option to send e-invoices to the recipient and, in that case, it must be ensured that the invoice is received and processed, resulting in payment or some other possible response from the recipient to the purchaser (integration of information, rejection,...). The Directive does not require suppliers to send e-invoices, but Member States or individual recipients may impose such requirements as part of the adoption of the Directive.

The reception of e-invoices requires one or more solutions at transmission level. Neither the Directive nor the e-invoice standard specify how e-invoices should be transmitted, but the standard provides guidance on the interoperability of e-invoices at transmission level, identifying options and making recommendations. Accepted transmission options can be identified in Member States as part of the national transposition of the Directive.

The standard defines the semantics and syntax (format) of the European e-Invoice, and does not prescribe the transport infrastructure used.

The Directive does not specify how invoices are to be processed. EN 16931-1:2017 specifies which business processes are supported by the standard, which means that a fully EN 16931-1:2017 compliant recipient will receive and process all invoices that require one of the supported processes. The standard does not specify how invoices are to be processed, which leaves it up to the recipient to decide on the level of automation they wish to adopt.



All this to move Italy towards the Digital Single Market through these actions:

- **eProcurement & eInvoicing:** with the transposition of Directives 2014/24/EU and 2014/55/EU, Public Administrations have been allowed to improve administrative efficiency. For companies, access to the Single Market has already led to a reduction in administrative burdens and the automation of document flows, especially in a transnational context (EN 16931);
- **Single Digital Gateway**: with the enactment of EU Regulation 2018/1724, the Single Digital Gateway (Once Only) will facilitate access to the information, administrative procedures and support services needed by citizens and businesses to be active in the Single Market;
- **Free movement of non-personal data**: the introduction of EU Regulation 2018/1807 allows for improved cross-border mobility of non-personal data in the Single Market, with the aim of ensuring access to data by competent national authorities, facilitating data porting between storage and processing service providers;
- **Single Market for Capital**: with Communication COM/2020/66 Aims to promote: an agile data-driven economy; an ecosystem that creates new data-driven products and services; sharing of data between companies; increased publication of public data.

In particular, with Communication COM (2020) 66 of 19 February 2020, the Commission will facilitate the development of common European standards and requirements for public procurement data services.

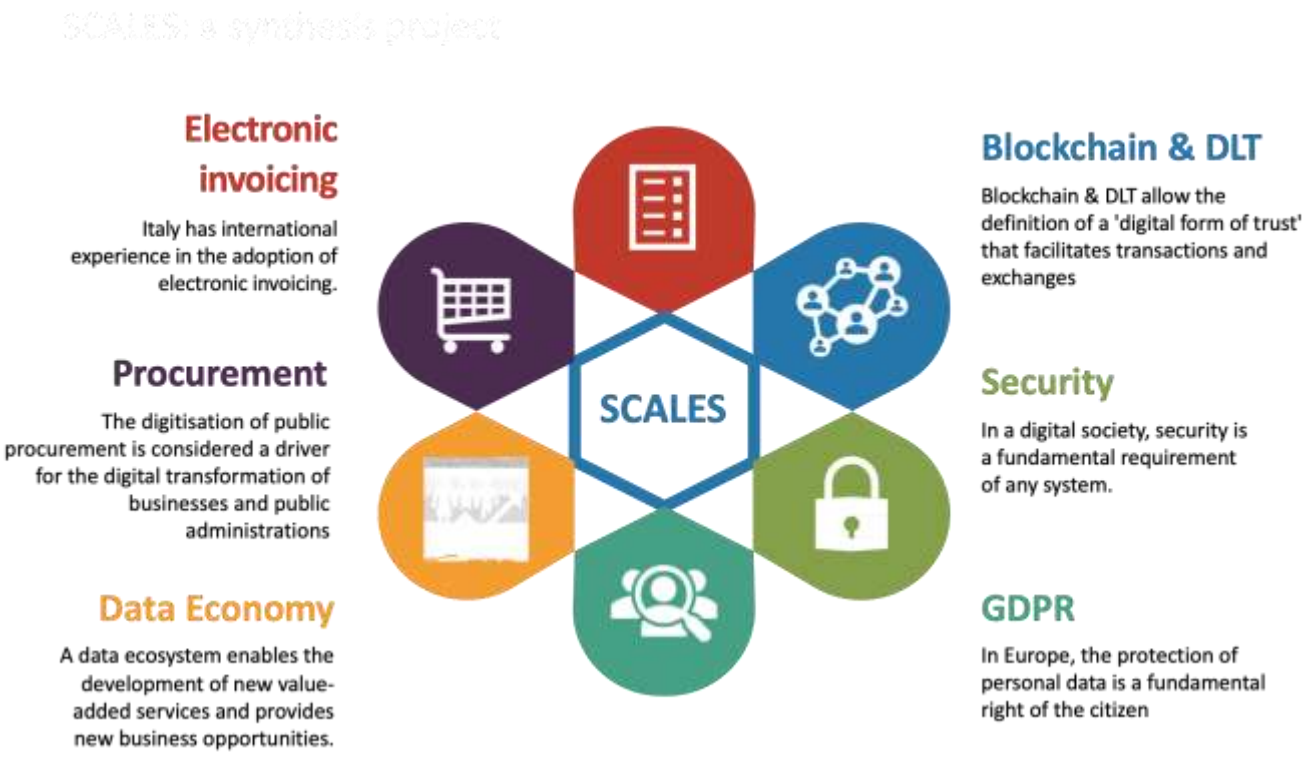
This will enable the EU public sector at European, national, regional and local level to also become a driver for new EU data processing capabilities, instead of being a mere beneficiary of such European infrastructures.

Public procurement data are essential to increase transparency and accountability in public spending, fight corruption and improve the quality of spending.

Currently in the Member States, these data are distributed over several systems and made available in different formats, which does not make them easily usable in real time for strategic purposes. In many cases their quality needs to be improved.

The Commission will develop a procurement data initiative covering both EU (EU datasets such as TED) and national dimensions (Q4 2020) and the initiative will be accompanied by a framework on procurement data governance (Q2 2021).

In this context, SCALES project is positioned as shown in the figure below.



Automation of business processes and tax reporting has evolved independently. In the worst cases tax reporting, financial supply chain and physical supply chain are completely separate silos. In the best cases, companies have integrated the financial and physical supply chain, with buyers and sellers exchanging up to 160 messages.

Globally, we are witnessing an increase in the number of reports required by tax authorities, and information flows to authorities overlap and run in parallel with business process information flows.

The tendency is therefore for the three areas to coincide, creating a single data ecosystem.

- **Tax reporting** with tax authorities, companies with the objectives of controlling evasion, through the collection and control of tax data;
- **Financial supply chain** for companies and financial institutions to finance working capital;
- **Physical supply chain** for companies;
- Objectives: to control and optimise the distribution/supply chain.

6.5 THE EUROPEAN E-INVOICE STANDARD EN 16931:2017

The e-Invoice must comply with the European e-Invoicing standard defined by EN 16931-1:2017.

Contracting authorities must be able to receive and process e-invoices using any of the two syntaxes specified in the syntax list (EN 16931-2:2017) in accordance with EN 16931-1:2017.

The European e-invoicing standard was formally published by the European Committee for Standardisation (CEN) in 6 parts together with the technical specifications and supporting technical reports between June and October 2017.

The e-invoice standard published by CEN represents a semantic data model of the essential elements of an e-invoice: it is not traceable to a specific format, but is a model that allows the essential content of an invoice to be described, the core semantic model, ensuring that the data model complies with Directive 2006/112 EC (VAT Directive) and the VAT rules of the individual Member States as well as their primary legislation.

Together with the semantic data model, the technical specification TS 16931-2:2017 was published, which contains the list of syntaxes.

The requirement to support multiple syntaxes has raised many questions in CEN/TC 434, of an operational and cost nature, in relation to the interests, investments, of specific member states and communities.

The Commission's standardisation request only contained qualitative requirements, and there was much discussion as to whether:

- limit the list to 1 or 2 syntaxes or take a broader approach,
- limit the basic technology to XML or include EDIFACT.

After detailed analysis, CEN/TC 434 decided to include the following syntaxes in the technical specification TS 16931-2:

- ISO/IEC 19845:2015 / OASIS Universal business language (UBL v2.1)
- UN/CEFACT Cross Industry Invoice XML (in sub-part 4).

The official support of UN/EDIFACT was considered essential in view of its wide use in the private sector, but it is emphasised that it is optional.

The complete EN 16931 series is composed as shown in the table below.

Name	Number	Type
Semantic data model of the essential elements of an electronic invoice	EN 16931-1: 2017	European standard
List of syntaxes in accordance with EN 16931-1	CEN/TS 16931-2: 2017	Technical specification
Methodology for syntactic mappings of essential elements of an e-Invoice	CEN/TS 16931-3-1: 2017	Technical specification
Syntactic mappings for invoices and credit notes ISO/IEC 19845 (UBL 2.1)	CEN/TS 16931-3-2: 2017	Technical specification
Syntax mappings for UN/CEFACT XML Cross Industry Invoice D16B	CEN/TS 16931-3-3: 2017	Technical specification
Syntactic mappings for UN/EDIFACT INVOIC D16B	CEN/TS 16931-3-4: 2017	Technical specification
Guidelines on interoperability of e-invoices at transmission level.	CEN/TR 16931-4: 2017	Technical report
Guidelines on the use of sectoral or national extensions in conjunction with EN 16931-1, methodology to be applied in the real environment.	CEN/TR 16931-5: 2017	Technical report
Result of verification of EN 16931-1 against its practical use by the end user	CEN/TR 16931-6: 2017	Technical report

6.6 THE SERVICES OFFERED BY THE REVENUE AGENCY FOR ISSUING, STORING ELECTRONIC INVOICES

The obligation to store active and passive electronic invoices governed by the Ministerial Decree of 17 June 2014 "*Procedures for fulfilling tax obligations relating to electronic documents and their reproduction on different types of media*", as referred to in Article 21(5) of Legislative Decree no. 82/2005, is in addition to the other compulsory fulfilments provided for by civil and tax regulations for VAT taxable persons in relation to storage.

With Provision 89757 of 30 April 2018, the Italian Revenue Agency communicated that all VAT taxable persons resident, established or identified in Italy can adhere, through an online service, to a specific service agreement and take advantage, free of charge, of the regulation-compliant storage service for all electronic invoices issued or received by the operator through the Interchange System.

With the subsequent Measure 524526 of 21 December 2018, the Revenue Agency intervened to resolve the critical issues reported by the Data Protection Authority, incorporating the solutions that emerged in the work of the joint technical roundtable between the Ministry of Finance, the Revenue Agency and the Data Protection Authority. The document amended the measures previously issued by the Director of the Revenue Agency, introducing changes to the storage system as well. Taxpayers had 60 days, starting on 3 May, to decide whether to join the Italian Revenue Agency's storage system, log on to the Fatture e Corrispettivi (invoices and receipts) portal and confirm their intention to activate the service that enables electronic invoices to be stored. For those who join, there is always the possibility of revocation, to be made through the portal. At the end of the transitional period, the Revenue Agency will delete

the electronic invoices stored during the first six months of the document's life in its version 2.0.

With Provision no. 311557/2020 of the Director of the Revenue Agency, the deadline for subscribing to the service, which is now possible until 28 February 2021, has been postponed once again, as implementation activities are still underway to incorporate the regulatory provisions of Decree-Law no. 124/2019. Only invoice data will be maintained for the planned institutional activities of assistance and automated control, until the deadline for any assessments - i.e. by 31 December of the eighth year following the year in which the reference declaration was submitted - has expired. With this intervention at the end of the transitional period, the Revenue Agency has set up the storage system according to the indications of the Guarantor.

The relationship between taxpayer and Revenue Agency

Analysing the Revenue Agency documentation, a first issue to reflect on concerns the roles and responsibilities of two distinct figures: the **Preservation Officer** and the **Preservation Service Officer**.

The **Preservation Officer is** indicated as the person responsible for all the activities listed in article 7, paragraph 1 of the technical rules of the storage system (DPCM 3/12/2013). This role requires precise technical and IT skills and is not merely formal in nature.

According to the Service Agreement, the taxpayer accepts the role of Responsible for the Storage of invoices for which he requests the preservation to the Revenue Agency (art. 1 D.lgs. 127/2015) entrusting the storage of his electronic invoices through a partial delegation to the Revenue Agency art.6, co. 6 DPCM 3/12/2013).

The **officer in charge of the preservation service is** identified by the Revenue Agency and is the person who defines and implements the overall policies of the preservation system and governs its management, in relation to the organisational model described in the Preservation Service Manual.

It follows from the above that:

- the responsibility for the proper storage of documents remains with the taxpayer;
- the Revenue Agency acts as the taxpayer's proxy.

The relationship between the taxpayer and the party delegated to carry out the preservation process was analysed by the Revenue Agency in Resolution 161/E of 09 July 2007, which states that: "in all *cases where the taxpayer entrusts, in whole or in part, the preservation process to a third party, he will continue to be answerable to the tax authorities for the proper keeping and preservation of accounting records and all tax-relevant documents*".

Any failures by the person in charge of the preservation cannot be used against the tax authorities to justify irregularities or errors, so failures by the tax authorities would not be enforceable against them, but only against the taxpayer.

Documents stored

By accessing the "Data relevant for VAT purposes" section of their private area, taxpayers can view in readable format the xml files of invoices sent and received through the Interchange System, save the xml file in their own archive, save the metadata of the xml file sent or received in their own archive.

The storage proposed by the Revenue Agency service only concerns invoices issued and received in xml format.

The duration of the preservation service

The Revenue Agency Service expressly provides for a 15-year retention period. This is an issue to be particularly careful about, as 'commercial' preservation systems have contractual conditions that vary depending on the pricing policy of the individual registrar, and should be carefully assessed according to the needs of each company or professional.

The storage service offered by the Revenue Agency is a useful tool for those who have few invoices to issue and receive.

But those who need to have an archiving system integrated with management procedures, verifying accounting records formed on the basis of digital documents transmitted and received, need to rethink their administrative processes, digitising them to achieve economic savings and greater compliance with current regulations.