DLV03.02-Technical requirements overview

Study on functional, technical and semantic interoperability requirements for the single digital gateway (SDG) implementation

10/07/2018

Table of Contents

List of tables

List of figures

Document characteristics

Property	Value
Release date	10/07/2018
Status:	Submitted for Review
Version:	3.0
Authors:	Everis
Reviewed by:	
Approved by:	

Document history

Version	Description	Date
1.0	Document submitted for review	16/05/2018
2.0	Document submitted for review	29/06/2018
3.0	Document submitted for review	10/07/2018

1 Introduction

The present document is the second part of the second deliverable of the project "*Study on functional, technical and semantic interoperability requirements for the single digital gateway implementation*", and aims at identifying the technical requirements necessary to run the different services of the Single Digital Gateway (SDG). The SDG will be aligned with the proposal for a Regulation of 2 May 2017 [COM(2017)256]. The regulation aims at making it easier for EU citizens and businesses who need to navigate regulatory and administrative requirements to access the necessary information, procedures and assistance services online.

The technical requirements have been identified following the business needs analysed in the business processes and sub-processes of the six SDG services[1] and following the Functional requirements[2].

The methodology applied to identify the technical requirements has followed a user-centric approach. From the use and context of usage, groups and categories of requirements have been defined. 18 different categories are grouped in three high level groups, namely, Operation, Revision and Transition. The structure of the document is based on such grouping and categorisation, and a brief description of each of the categories is provided in each one of the chapters.

A total of 191 technical requirements have been identified: 105 in Operation, 45 in Revision, and 33 in Transition.

[1] See: *DLV02.01 – Business processes – Study on functional, technical and semantic interoperability requirements for the Single Digital Gateway implementation.*

[2] See: *DLV03.01 – Functional requirements overview – Study on functional, technical and semantic interoperability requirements for the Single Digital Gateway implementation*

2 Methodology

Technical requirements are vital for the success of SDG. Technical requirements are identified and defined taking into consideration the wide range of users that rely on them, first when developing, then when interacting with the SDG. In the context of the SDG it includes developers, End users, Application Managers, Coordinators and Service Providers –both at EU and national levels–, and other stakeholders that eventually will interact with the gateway.

While functional requirements focus on **what** tasks the system should perform, technical requirements focus on to **who** should use the system –and in which context–. To identify and define technical requirements, major focus is put in the user-centric approach and in the elements that help understand users' needs.

For the purpose of the current document, a user of the SDG is considered as an individual who interacts with the SDG. User interactions, translated into technical requirements, can be grouped into Operation, Revision and Transition:

- **Operation**: User that is using the functionality provided by the system. These requirements are related with basic operation and deal with needs that directly affect the daily operations of the SDG, in other words, how well the system operates;
- **Revision**: User that needs to change source code or data that drives the system. These requirements affects the complete range of the SDG corrective or adaptive maintenance activities (changing source code or data that drive the system);
- **Transition**: User that manages and upkeeps the system. These requirements pertain to the adaptability of the SDG to new environments, its interaction with other systems and its upkeeping.

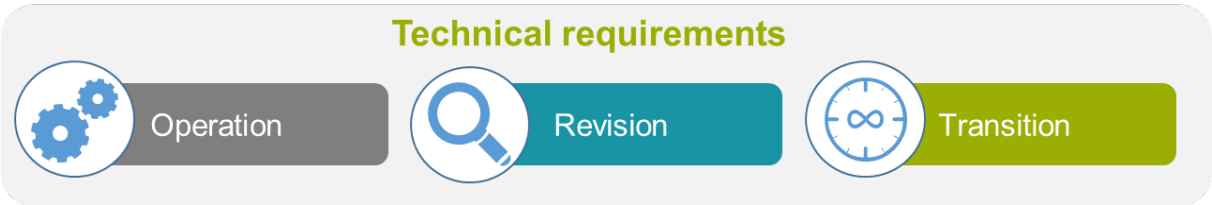

Figure 1: Three groups of Technical requirements

Operation, Revision and Transition are high level groups of technical requirements. As intermediate levels, each group includes different categories that deepen into detailed requirements. The different categories belonging to each group of technical requirements are the following:

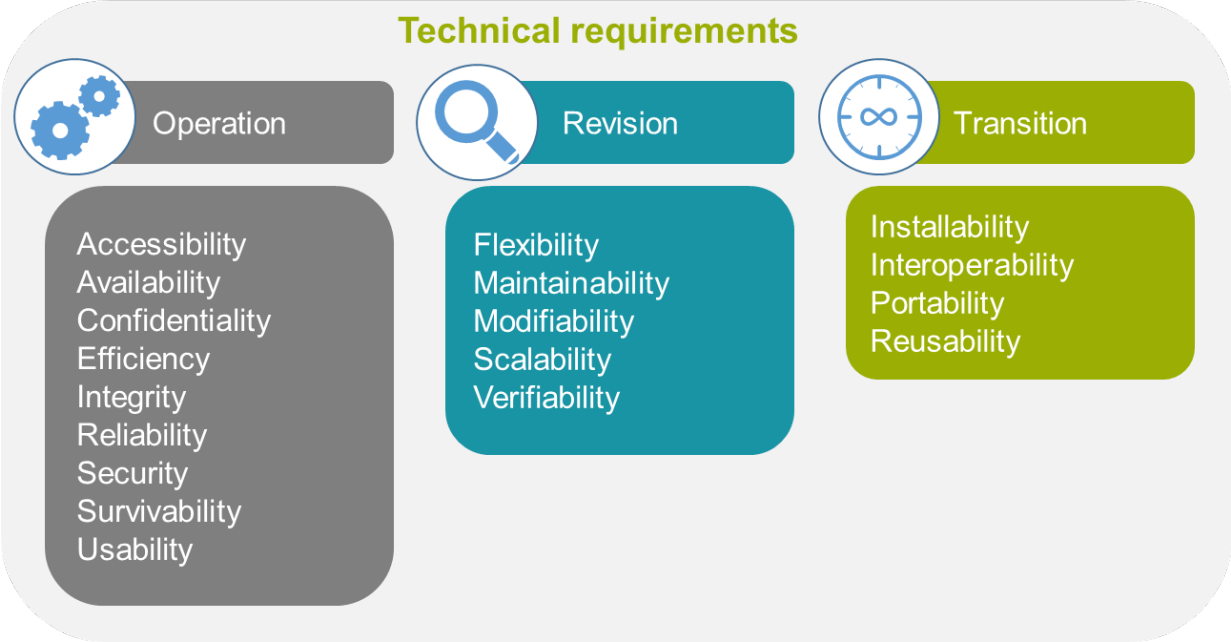

Figure 2: Categories belonging to each group of technical requirements

The structure of the current document is based on such grouping and categorisation, and a brief description of each of the categories is provided in each one of the chapters.

To support the grouping and categorisation, and in order to orient the purpose of each requirement, they are formulated using the following terminology:

- **Shall**: A requirement that must be implemented. It is a requirement that is contractually binding;
- **Should**: Used to indicate a goal which must be addressed by the design team;
- **Will**: Used to indicate a statement of fact, for example when giving a description of something that exists.

All the requirements related with physical infrastructure should be further address and analysed in design phase of the solution.

3 Technical Requirements

3.1 Operation

The technical requirements included in the group "**Operation"** describe the users' needs for the SDG and their expectations on what the system should perform to function correctly. The group "**Operation"** includes nine different categories and defines a total of 105 requirements.

Figure 3: Operation requirements categories

3.1.1 Accessibility

The technical requirements included in the category Accessibility tackle how easily users with the widest range of capabilities can use the SDG interface.

ID	Requirement
TR-OR-01.001	The front-end of the SDG system should comply with Web Content Accessibility Guidelines (WCAG) 2.0[3].
TR-OR-01.002	The system shall be accessible by people with specific vision needs, to the extent that a user shall be able to: • Display the whole user interface in a large font without truncating displayed text or other values; • Use a screen magnifier to magnify a selected part of the screen; • Use a screen reader to read aloud information displayed.
TR-OR-01.003	The system shall be accessible by individuals who are colour blind, to the extent that they shall be able to discern all text and other information displayed by the system as easily as a person without colour blindness. Any meaning conveyed through the use of colour shall also be conveyed by other means discernable by a colour-blind person.

Table 1: Accessibility requirements

[3] https://www.w3.org/TR/WCAG20/

3.1.2 Availability

The technical requirements included in the category Availability tackle how the system is able to function during normal operating times.

ID	Requirement
TR-OR-02.001	The SDG platform should be designed according to high availability principles.
TR-OR-02.002	The system should comply with Tier 2 requirements: • No single point of failure (redundant hardware component, load balancing, support for failover); • Availability (software, hardware, network) of at least 99.75% (or less than 22 hours of unavailability per year).
TR-OR-02.003	The system should incorporate a heartbeat service, which will periodically communicate on the normal work status of the system.
TR-OR-02.004	The system should comply with the following Tier 3 requirements: • Multiple independent distribution paths serving the IT equipment; • The entire IT equipment must be dual-powered and fully compatible with the topology of a site's architecture. As an alternative, it should be connected to a UPS device capable of providing the electricity to power the system.
TR-OR-02.005	System up time should be at least 99.5%.
TR-OR-02.006	Unless the system is non-operational, the system shall present the user with a notification informing them that the system is unavailable.
TR-OR-02.007	The online registration system shall permit backing up of the registration database while other registration activities are going on.

Table 2: Availability requirements

3.1.3 Confidentiality

The technical requirements included in the category Confidentiality tackle how well the SDG system protects sensitive data and allows only authorised access to the data.

ID	Requirement
TR-OR-03.001	The system should comply with the principle that the users should be asked to provide only the information that is absolutely necessary to obtain a service.
TR-OR-03.002	The system should follow the 'privacy-by-design' and 'security-by-design' approaches.
TR-OR-03.003	Catalogue of services will be supported to help others to find reusable resources (e.g. services, data, software, data models).

Table 3: Confidentiality requirements

3.1.4 Efficiency

The technical requirements included in the category Efficiency tackle how well the SDG handles capacity, amount of data and response time. The efficiency requirements should be further analysed and discussed during the design phase of the solution since the physical infrastructure could limit and impact the times presented below.

ID	Requirements
TR-OR-04.001	The system should be able to effectively serve simultaneously: • Up to five system administrators (i.e. Application Managers); • Up to 1.000 active users (i.e. Commission Coordinator, Commission Service Providers, National Coordinators and National Service Providers); • Up to 3.000 read-only users of the general public (i.e. End users).
TR-OR-04.002	Response time of the system should not exceed one second for the execution of 90% of simple queries for at least 700 concurrent active users during normal working hours.
TR-OR-04.003	Response time of the system should not exceed two seconds for the execution of 99% of simple queries for at least 700 concurrent active users during normal working hours.
TR-OR-04.004	Response time of the system should not exceed three seconds for the execution of 90% of complex queries for at least 700 concurrent active users during normal working hours.
TR-OR-04.005	Response time of the system should not exceed five seconds for the execution of 99% of complex queries for at least 700 concurrent active users during normal working hours.
TR-OR-04.006	Response time of the system should not exceed three seconds for the generation of 90% of reports for at least 100 concurrent active users during normal working hours.
TR-OR-04.007	Response time of the system should not exceed five seconds for the generation of 99% of reports for at least 100 concurrent active users during normal working hours.
TR-OR-04.008	Response time of the system should not exceed three seconds for the execution of 90% of document management activities for at least 1.000 concurrent active users during normal working hours.
TR-OR-04.009	Response time of the system should not exceed five seconds for the execution of 99% of document management activities for at least 1.000 concurrent active users during normal working hours.
TR-OR-04.010	At least 20% of the processor capacity and storage space available to the system shall be unused at peak load seasonal periods.
TR-OR-04.011	The system restart cycle should execute completely in less than 60 seconds.

TR-OR-04.012	The system shall be able to process a notification in one second or less, and up to 100 notifications in 15 seconds or less.
TR-OR-04.013	The system shall be able to handle the submission of queries by End users at a minimum rate of 20 per second.
TR-OR-04.014	Any interface between a user and the automated system shall have a maximum response time of two seconds.
TR-OR-04.015	Routine maintenance that is executed while users are active shall not cause a perceptible increase in response time for any function of more than 5% over the response time when no maintenance process is executing.
TR-OR-04.016	The system shall produce a storage capacity warning notification when the 65% capacity threshold is crossed with additional notifications issued thereafter at 5% threshold increments.

Table 4: Efficiency requirements

3.1.5 Integrity

The technical requirements included in the category Integrity tackle how well the data is maintained by the SDG in terms of accuracy, authenticity, and corruption free.

ID	Requirement
TR-OR-05.001	The SDG system should guarantee that links are not provided in duplicate from the same source.
TR-OR-05.002	The SDG system should keep information about the last time a particular page was indexed.
TR-OR-05.003	It should be possible to designate from which system the information is referred to.
TR-OR-05.004	Whenever a change is made to information stored in database, the fact of the change shall be recorded in a database or equivalent technology that is routinely backed up. This is intended to identify changed information in the event of the loss of a disk.
TR-OR-05.005	The SDG system should allow administrators to set up a functionality for archiving, restore data, creation of backup copies, and scheduled maintenance.
TR-OR-05.006	The SDG system should support a functionality allowing the review of archived data and recovery after crashes. When an administrator is using the manual archiving functionality, an appropriate reminder mechanism at determinable time intervals should be in place.
TR-OR-05.007	The SDG system should support a functionality for the automatic creation of a regular backup copy, as well as a backup copy prior to migration of data, new versions, or other critical actions, for the purpose of restoring

	to the last working configuration of the system (including the database, configuration files, etc.).
TR-OR-05.008	The integrity of the system data area should be checked by the internal audit system twice per second; if inconsistencies in the data are detected, the system operation should be disabled.
TR-OR-05.009	The SDG system should register all system events and errors, status of exchanged messages, etc.
TR-OR-05.010	The system log should contain the following data: date, time, system process, type/nature of actions, system error message.
TR-OR-05.011	The SDG system should provide a way to track system events by different criteria: date and time, system process, error number, availability of the system.
TR-OR-05.012	The SDG system should generate a message upon any successful or unsuccessful update of a nomenclature, lists, etc.
TR-OR-05.013	System events should be classified into categories: successful or unsuccessful.
TR-OR-05.014	System events should have a classification for errors by criticality.
TR-OR-05.015	Error messages should be informative and easy to understand. Error messages should be written to error logs to enable these issues to be properly audited and investigated. The system should incorporate all usability heuristics to support ease of navigation and general use of the system, including data entry.
TR-OR-05.016	All errors should have an error code and all error codes should be clearly and correctly described in the administrator's user guide.
TR-OR-05.017	The SDG system should ensure sending, if necessary, of electronic messages to a system administrator or a person authorised by the contracting authority. The setup of parameters necessary for the configuration of certain electronic addresses, such as the message-generating criticality level or type of errors, should be made using the system resources.
TR-OR-05.018	The implementation of the system should follow open standards and use well-known and widely accepted technologies in order to ensure integrity.

Table 5: Integrity requirements

3.1.6 Reliability

The technical requirements included in the category Reliability tackle how well SDG consistently performs specified functions without failure.

ID	Requirement
TR-OR-06.001	The SDG system shall roll back all updates when any update fails to commit.

TR-OR-06.002	The SDG system should flag failures indexing web pages.
TR-OR-06.003	The SDG system should provide a monitoring console or dashboard for system administrators to check the status of the system quickly and easily.
TR-OR-06.004	The SDG system should provide system administrators with a possibility of cancelling the last operations of a user.

Table 6: Reliability requirements

3.1.7 Security

The technical requirements included in the category Security assess how successfully the SDG System is safeguarded against unauthorised access, and deliberate and intrusive fault from internal and external users.

The security requirements should be further analysed and the needs should be further addressed during the design phase of the solution. All the requirements related with the physical infrastructure are facultative and can be used as a checklist in a posterior phase of the project.

ID	Requirement
TR-OR-07.001	The entire SDG platform should be secure in such a way that the level of security is trusted by actors.
TR-OR-07.002	The authentication module should identify the different users accessing the SDG system in a secure and traceable way.
TR-OR-07.003	The SDG system should guarantee that the back office services are only accessible to users with a verified identity.
TR-OR-07.004	The SDG system should guarantee that authenticated users can only access services or data matching their role and access rights.
TR-OR-07.005	The SDG system should use https security certificate.
TR-OR-07.006	The SDG system should guarantee that the data exchanged between actors cannot be intercepted or accessed by a non-authorised third party.
TR-OR-07.007	The SDG system should monitor and record in the system logs all activities performed by users, whether successful or unsuccessful (e.g. attempted but failed logins).
TR-OR-07.008	The SDG system should be tested at least according to OWASP Top 10 Vulnerabilities.
TR-OR-07.009	The SDG system should implement the required firewalls in order to provide a line of defence when external users try to connect to the system from the Internet or other networks.
TR-OR-07.010	The SDG system should implement an Intrusion Detection System, including all necessary agents for all servers.
TR-OR-07.011	The SDG system should provide secure communications between: • The client browser and SDG Platforms;

	• The Central Database Unit and Member States Platforms.
TR-OR-07.012	The SDG system should foresee systematic backup of stored data and servers' configuration, allowing quick and reliable recovery of data in case of an incident resulting in data loss or deterioration.
TR-OR-07.013	The SDG system should provide a Single Sign-On so users can access services on the back-end without any additional authentication.
TR-OR-07.014	The SDG system should implement at least a 3-tier architecture (database, application and presentation tiers).
TR-OR-07.015	The SDG system architecture should be divided into different security zones and contain at least a DMZ and an internal zone.
TR-OR-07.016	The SDG system should foresee embedded security controls.
TR-OR-07.017	The SDG system should be hosted in a physical location with adequate HVAC, access controls, and fire detection and suppression mechanisms.
TR-OR-07.018	The SDG system should protect the user from illogical operations.
TR-OR-07.019	A regular user shall not put the system in disarray by providing data or using the functions in the user interface.
TR-OR-07.020	User authentication should be managed via EU Login.
TR-OR-07.021	All services (except public services) shall be protected using authenticated users and role checks.
TR-OR-07.022	The SDG system shall provide role-based access to its functionalities.
TR-OR-07.023	User groups should be created and maintained. These are not bound to a particular role and access rights but serve only for convenience of the management process of user permissions.
TR-OR-07.024	The SDG system will not allow deletion of users. Only temporary or permanent withdrawal of the access of a user will be allowed.
TR-OR-07.025	The SDG system should allow filtering and sorting of users by different criteria (i.e. by institution, by roles, etc.).
TR-OR-07.026	The SDG system should register in the log all user actions: login to the system, view, search, creation, edit, and deletion of data. In each instance of a data update, a history of changes should be kept (i.e. which user, when and what has changed).
TR-OR-07.027	The SDG system should ensure a reliable mechanism for recording all events related to the system's user management and user permissions.
TR-OR-07.028	The SDG system should support the generation of reports based on the records and according to a pre-defined set of criteria.
TR-OR-07.029	The SDG system should produce a report on user actions containing the following information: date and time of login and logout, work session duration, user data, IP address of the machine, nature/type of actions, and references to completed actions.

Table 7: Security requirements

3.1.8 Survivability

The technical requirements included in the category Survivability tackle how successfully the SDG system continues its functions and recovers in the presence of a system failure.

ID	Requirement
TR-OR-08.001	When an update failure is detected all updates performed during the failed session shall be rolled back to restore the data to pre-session condition.
TR-OR-08.002	All data recovered in a roll-back condition shall be recorded for use in forward recovery under user control.
TR-OR-08.003	The SDG system shall prevent access to failed functions while providing access to all currently operational functions.
TR-OR-08.004	All hardware components of the assembly operation shall be replicated, so that failure of any one hardware component shall not render the assembly operation unavailable to end-users. It shall be acceptable for system performance to be poorer than normal for up to 3 business days following the failure and replacement of a piece of hardware.
TR-OR-08.005	The SDG system should ensure the procedure to check data consistency and the procedure for recovery of partially broken data.

Table 8: Survivability requirements

3.1.9 Usability

The technical requirements included in the category Usability tackle how easily the user is able to learn, operate, prepare inputs and interpret outputs through interaction with the SDG system.

ID	Requirement
TR-OR-09.001	The provided solution should be user-friendly and easy to use.
TR-OR-09.002	The SDG system shall be self-explanatory and intuitive.
TR-OR-09.003	End users with no training shall be able to use the product.
TR-OR-09.004	The SDG platform should be multilingual: it should support the 24 official languages of the EU.
TR-OR-09.005	The SDG system should ensure a high level of integration with spreadsheets and word processors, including copy, cut and paste functions (as a minimum).
TR-OR-09.006	The system should have drag and drop capabilities.
TR-OR-09.007	The SDG system should allow export of Business Intelligence data and report in TXT, CSV and PDF format.
TR-OR-09.008	The SDG system should provide online context-sensitive help facilities and user manual help facilities. The system help feature should assist users in the recognition, diagnosis and recovery of errors.

TR-OR-09.009	The SDG system should include tools such as manuals, tutorials and guidelines.
TR-OR-09.010	The SDG system should allow auto-complete in the form fields.
TR-OR-09.011	The SDG system should allow the description of the field on the forms.
TR-OR-09.012	The user interfaces of the SDG shall have a shared look-and-feel.
TR-OR-09.013	The SDG interface should be responsive.
TR-OR-09.014	The functions in the user interfaces of the different applications shall have consistent names, positions on the page and behaviours.
TR-OR-09.015	Lesser common functions in the user interfaces should have tooltips.
TR-OR-09.016	Using functions on a page in the front-end shall have a near-real-time effect or an indication that its processing is taking place.
TR-OR-09.017	Domain experts not familiar with the application should be able to learn to execute the basic functions of the applications within an hour.
TR-OR-09.018	The SDG system shall provide understandable and actionable feedback for the user in case of error.
TR-OR-09.019	The language used in the mail notifications and communications shall be in the language of preference of the user to who is intended the message.
TR-OR-09.020	The implementation of the system should follow open standards and use well-known and widely accepted technologies in order to ensure ease of use.

Table 9: Usability requirements

3.2 Revision

The technical requirements included in the group **"Revision"** are two folded; on one hand they define the requirements of the SDG that ensure that errors are identified, tackled and addressed. On the other hand, it also defines requirements that ensure the possibilities to easily add and delete functions. The group "**Revision"** includes five different categories and defines a total of 45 requirements.

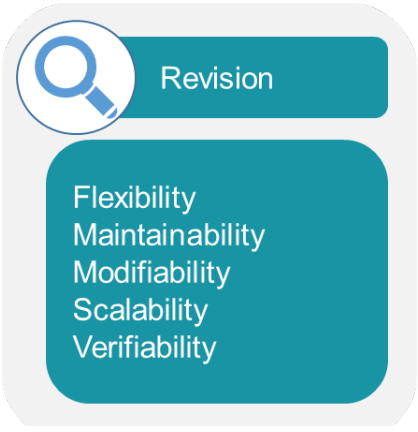

Figure 4: Revision requirements categories

3.2.1 Flexibility

The Flexibility requirements category addresses how easily the SDG can be modified to adapt to different environments, configurations, and user expectations.

ID	Requirements
TR-RR-01.001	Provisions shall be made for the future usage of multiple languages. Provision shall include at least the following:

	• The structure of the data store shall be such that multi-lingual support shall not need additional components neither need to replace existing components, and • A user shall be able to nominate its preferred language when entering information (e.g. search queries).
TR-RR-01.002	No piece of text that might be displayed to a user shall reside in program source code. Every piece of text that a user might see shall be modifiable without changing the source code. That is, no user-visible text will be “hard-coded”.
TR-RR-01.003	The SDG system shall have the ability to include new functionalities by developing and “plugging in” the software developed to support the new method. A new functionality, in order to allow its introduction, shall require the minimum number of changes to the core software of the system.
TR-RR-01.004	The SDG system shall be able to accommodate new Member States without changing the core software system.
TR-RR-01.005	The SDG system shall be able to accommodate new Languages without changing the core software system.

Table 10: Flexibility requirements

3.2.2 Maintainability

The Maintainability requirements category addresses how easily faults in SDG can be found and fixed.

ID	Requirement
TR-RR-02.001	The IT team that will provide maintenance and support to the system should not need to have specific skills.
TR-RR-02.002	The implementation of the SDG system should follow open standards and use well-known and widely accepted technologies in order to ensure interoperability, ease of use, and scalability.
TR-RR-02.003	The SDG system should comply with the open data principle that refers to the idea that all public data should be freely available for use and reuse by others, unless restrictions apply (e.g. for protection of personal data, confidentiality, or intellectual property rights).
TR-RR-02.004	Application Managers should maintain a coherent and complete set of documentation that describe the system in terms of its architecture, design, the implemented functions, data structures and the API's of the various services.
TR-RR-02.005	At least three developers should be able understand the code of the application.
TR-RR-02.006	New developers should be able to learn and contribute to the development of the SDG applications suite after 15 days of study of the documentation and code.
TR-RR-02.007	There should exist a full set of implemented and documented test-cases used for regression testing.
TR-RR-02.008	There should exist an automated test-framework for regression testing in which all the test-cases are executed and on which the applications are tested on a weekly basis during development.
TR-RR-02.009	The test-framework should provide an automated report that can be used to understand the status of the development.
TR-RR-02.010	New versions of the application should be fully tested before the deployment.
TR-RR-02.011	The scripting, querying and programming languages, frameworks, standards, libraries and third party services used in the SDG system should be agreed upon with the Technical Application Manager before they are used in the development.
TR-RR-02.012	Java programming will follow established Java coding conventions.
TR-RR-02.013	Entity names will be in English.
TR-RR-02.014	Comments in code will be in English.
TR-RR-02.015	The SDG system should have business continuity/disaster recovery/backup plans to ensure that digital public services continue to work in a range of situations (e.g. cyber-attacks, failures).

TR-RR-02.016	Monitoring services should be in place to detect problems with disk, memory and CPU issues. In cases of issues, appropriate personnel should be notified and should have procedures to remedy the problem.
TR-RR-02.017	The customer service call centres shall analyse 95% of the problem reports within 2 hours. Items classified as “urgent” shall be repaired within 3 business days in 98% of the reported cases.
TR-RR-02.018	The application development process should have a regression test procedure that allows complete re-testing within 2 business days.
TR-RR-02.019	A developer shall be able to modify existing statements to conform to revised regulations with 48 labour hours or less of development and testing effort.
TR-RR-02.020	A software engineer who has at least one year of experience supporting the SDG system shall be able to add a new product feature, including source code modifications and testing, with no more than one week of labour.
TR-RR-02.021	The SDG system shall not be shut down for maintenance more than once in a 24-hour period.

Table 11: Maintainability requirements

3.2.3 Modifiability

The Modifiability requirements category addresses how easily changes to the SDG can be developed and deployed in an efficient and cost effective manner.

ID	Requirement
TR-RR-03.001	No piece of text that might be displayed to a user shall reside in source code. That is, every piece of text that a user might see should be modifiable without changing the source code.
TR-RR-03.002	A software engineer who has at least one year of experience supporting SDG system shall be able to add a new product feature, including source code modifications and testing, with no more than one week of labour.
TR-RR-03.003	Function calls shall not be nested more than two levels deep in the source code.
TR-RR-03.004	The several functions of the system should be independent so it can be easy to add or remove new functionalities.
TR-RR-03.005	The entire configuration should be available in the database or configuration files, so it is not necessary to change source code in case of a change.
TR-RR-03.006	The SDG system should use Unicode for textual data and separating elements that should be localised from source code or content.

Table 12: Modifiability requirements

3.2.4 Scalability

The Scalability requirements category addresses how well SDG is able to expand its processing capabilities upward and outward to support business growth.

ID	Requirement
TR-RR-04.001	A combination of efficient software architecture, along with sufficient hardware components, should guarantee the scalability of the system.
TR-RR-04.002	The system's logical architecture should be able to sustain at least a 30% increase in transactional load on a yearly basis.
TR-RR-04.003	The system should easily adapt to new requirements imposed by changes in legislation.
TR-RR-04.004	The elapsed duration of time required to produce any report showing information about stored data shall be based upon how much data is presented rather than the total quantity of stored data.
TR-RR-04.005	The SDG system shall be scalable to support unlimited growth in the number of indexed pages and content.
TR-RR-04.006	The SDG system shall be scalable to support unlimited growth in the number of users.
TR-RR-04.007	The SDG system shall be scalable to accommodate its use by an unlimited number of users representing the Member States or European Organisations.
TR-RR-04.008	The implementation of the system should follow open standards and use well-known and widely accepted technologies in order to ensure scalability.

Table 13: Scalability requirements

3.2.5 Verifiability

The Verifiability requirements category addresses the extent to which tests, analysis, and demonstrations are needed to prove that the SDG is function as intended.

ID	Requirements
TR-RR-05.001	The maximum number of test cases to cover testing of any particular source code module shall be 20.
TR-RR-05.002	The design of the SDG shall include software that tests the operating system and the communication links, memory devices, and peripheral devices.
TR-RR-05.003	Software testing will require the use of a test database with data extracted from the production database. This test database will be deleted after successful implementation of the software system.

TR-RR-05.004	All developers on the project shall have identical development environment configurations, and all testers shall have identical quality assurance environment configurations.
TR-RR-05.005	An auditor should be authorised to read all documents in the system related to a particular procedure(s).

Table 14: Verifiability requirements

3.3 Transition

The technical requirements included in the group **"Transition"** refers to the ability of SDG to adapt to its surrounding environment. Technical requirements related to Transition usually are relevant to users who are responsible for managing the upkeep of the system because they relate with aspects such as packaging and compatibility with other systems and the ease of adaptation to changes in the technical environment. The group **"Transition"** includes four categories and defines a total of 33 requirements.

Figure 5: Transition requirements categories

3.3.1 Installability

The Installability requirements category addresses how easily the SDG can be installed, uninstalled, or reinstalled into a target environment.

ID	Requirement
TR-TR-01.001	The installation process shall be convenient and involve the entry of little information by the deployment responsible.
TR-TR-01.002	It shall be possible for the system's main server software to be installed by a competent system administrator who has no previous knowledge of the system or of the third-party products it uses, but who is familiar with the operating system of the machines on which it is to be installed.
TR-TR-01.003	The software shall be installed from a popular portable medium.
TR-TR-01.004	Installing an upgrade shall not modify existing configuration values.
TR-TR-01.005	The software will comply with DIGIT requirements, so that it can be installed on DIGIT premises. The DIGIT requirements are defined in: Service Catalogue - IS Hosting Services - Infrastructure Services Provision DIGIT Directorate - Distribution Data: 15/02/2010 | Version 2.1 Product Catalogue - Version of 13/05/2016
TR-TR-01.006	The software services will be delivered with their hardware requirements.
TR-TR-01.007	New software will be developed in Java and compiled in a WAR file (the exception cases shall be agreed on with the EC).

TR-TR-01.008	The software will be compatible with Tomcat or Weblogic AS.
TR-TR-01.009	New front-end development will be done in Angular2+ and hosted in a WAR file.
TR-TR-01.010	A mechanism should be created for the elimination of temporary files generated by different processes, whereas the parameters for their elimination should be managed by an administrator with system resources.

Table 15: Installability requirements

3.3.2 Interoperability

The Interoperability requirements category addresses how well the SDG is able to couple or facilitate the interface with other systems.

ID	Requirement
TR-TR-02.001	The SDG system shall be able to interface with any HTML (HyperText Markup Language) browser.
TR-TR-02.002	In order to facilitate adoption by public administration, the platform should have a high degree of independence from other applications.
TR-TR-02.003	The platform should be compliant with other recognised European standards.
TR-TR-02.004	New versions of the software should be able to access information from the previous versions.
TR-TR-02.005	Communications with each of the Member State should be through the utilisation of standard protocols.
TR-TR-02.006	Communications will be guaranteed as interoperable through the use of an agreed minimum national service standard (to be defined) for prioritised exchanges of data.
TR-TR-02.007	The implementation of the system should follow open standards and use well-known and widely accepted technologies in order to ensure interoperability.
TR-TR-02.008	Communications will be guaranteed as interoperable through the use of an agreed vocabulary (to be defined) for the exchanges of data.
TR-TR-02.009	Common vocabularies should be used to express the metadata (ISA2 Core Vocabularies, EuroVoc, etc.).
TR-TR-02.010	Consistent attribute naming should be used to deliver data in mutually understood way between all actors in the system.
TR-TR-02.011	Catalogue of services will be supported to help others to find reusable resources (e.g. services, data, software, data models).

Table 16: Interoperability requirements

3.3.3 Portability

The Portability requirements category addresses how easy it will be for the SDG to be transferred from its current hardware or software environment to another environment.

ID	Requirements
TR-TR-03.001	Application specific code will be hidden by using generic API's.
TR-TR-03.002	The SDG system should, apart from installation, have little or no dependencies on the specifics of the OS and the webserver.
TR-TR-03.003	All the code will run on a single version of Java (exceptions to be agreed with DIGIT).
TR-TR-03.004	All timestamps recorded by the transaction processing system shall be in CET (Central European Time) when placed into permanent storage.
TR-TR-03.005	The time zone shall be obvious to the user whenever a time element is displayed.
TR-TR-03.006	The SDG system should be accessible by any web browser.
TR-TR-03.007	It should not be necessary to download or install any software on a computer to use SDG.

Table 17: Portability requirements

3.3.4 Reusability

The Reusability requirements category addresses how easily a portion of the SDG can be converted for use in another software.

ID	Requirement
TR-TR-04.001	The development of a functionality to support the SDG shall be modularised such that it can be reused by other software systems.
TR-TR-04.002	Web applications shall be developed to adhere to HyperText Markup Language (HTML) guidelines and standards.
TR-TR-04.003	All software that runs on a client device shall be written in a prevalent programming language such that the software can be run on a personal computer without having to download a supporting environment.
TR-TR-04.004	It should not be necessary to download or install any software on a computer to use the SDG system.
TR-TR-04.005	The implementation of the SDG system should follow open standards and use well-known and widely accepted technologies in order to ensure reusability.

Table 18: Reusability requirements

4 Annexes

4.1 Acronyms and abbreviations

Term	Description
EC	European Commission
EU	European Union
MS	EU Member States
SDG	Single Digital Gateway
SM	Single Market

Table 19: Acronyms and abbreviations