ANNEX 3: REQUIREMENTS

1. Functional Requirements

FUNCTIONAL REQUIREMENT ID	FUNCTIONAL REQUIREMENT NAME	FUNCTIONAL REQUIREMENT DESCRIPTION	FUNCTIONAL REQUIREMENT RELATED TEST	RELATED BUSINESS REQUIREMENT ID	RELATED BUSINESS REQUIREMENT NAME	RELATED BUSINESS REQUIREMENT DESCRIPTION
PUS_FUR_0001	Receive Data	The system must be able to receive data.		PUS_BUS_0001	Receive Proof Request	The CCO must be able to receive a proof request, which can either be an endorsement request or a registration request. It includes the step to validate the format of the request and the data of the proof request.
				PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
				PUS_BUS_0015	Receive Proof Presentation Notification	The Customs must be able to receive a proof presentation notification. It includes the step to validate the format of the notification and the data of the proof presentation notification.
PUS_FUR_0002	Validate Data	The system must validate if the data conforms to its associated Rules & Conditions.		PUS_BUS_0001	Receive Proof Request	The CCO must be able to receive a proof request, which can either be an endorsement request or a registration request. It includes the step to validate the format of the request and the data of the proof request.
				PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
				PUS_BUS_0015	Receive Proof Presentation Notification	The Customs must be able to receive a proof presentation notification. It includes the step to validate the format of the notification and the data of the proof presentation notification.

PUS_FUR_0003	Identify If IE Is Valid	The system must identify if the IE is valid or not.		PUS_BUS_0001	Receive Proof Request	The CCO must be able to receive a proof request, which can either be an endorsement request or a registration request. It includes the step to validate the format of the request and the data of the proof request.
				PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
				PUS_BUS_0015	Receive Proof Presentation Notification	The Customs must be able to receive a proof presentation notification. It includes the step to validate the format of the notification and the data of the proof presentation notification.
PUS_FUR_0004	Register Data	The Customs Officer must be able to register data.		PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
				PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
				PUS_BUS_0024	Manage Documentary Controls	CCO and PCO must be able to examine the endorsement request, the presentation notification and the supporting documents - the necessary particulars in the endorsement request and the presentation notification and the availability and content of the supporting documents.
PUS_FUR_0005	Exchange Data	The system must exchange data with the PC or AI with an IE.		PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
				PUS_BUS_0004	Accept or Not Accept Proof Request	The CCO must be able to reject the request, due to invalid format of the request message or the data of the request, or to accept a proof request. This involves notifying the declarant.
				PUS_BUS_0012	Accept or Not Accept Proof Presentation	The Customs must be able to reject the

					Notification.	presentation of the notification, due to invalid format of the proof presentation notification message or the data of the notification, or to accept a proof presentation notification. This involves notifying the declarant.
				PUS_BUS_0013	Notify About Proof Validity	The CCO must be able to notify declarant about the validity of the proof.
				PUS_BUS_0014	Notify about Proof Usage	The PCO must be able to notify declarant about the usage or non-usage of the proof.
				PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
				PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
				PUS_BUS_0024	Manage Documentary Controls	CCO and PCO must be able to examine the endorsement request, the presentation notification and the supporting documents - the necessary particulars in the endorsement request and the presentation notification and the availability and content of the supporting documents.
				PUS_BUS_0026	Notify about Proof Archiving	The CCO must be able to notify declarant about the archiving of the proof, in case the validity date has expired.
PUS_FUR_0006	Record Data	The system must record the data using the unique identifier.		PUS_BUS_0001	Receive Proof Request	The CCO must be able to receive a proof request, which can either be an endorsement request or a registration request. It includes the step to validate the format of the request and the data of the proof request.
				PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
				PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0010	Perform Risk Analysis At Competent Customs Office	The CCO must be able to perform a risk analysis and interpret the result of this risk analysis.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.

				PUS_BUS_0019	Perform Risk Analysis At Presentation Customs Office	PCO must be able to perform a risk analysis and interpret the result of this risk analysis.
				PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
				PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
				PUS_BUS_0024	Manage Documentary Controls	CCO and PCO must be able to examine the endorsement request, the presentation notification and the supporting documents - the necessary particulars in the endorsement request and the presentation notification and the availability and content of the supporting documents.
				PUS_BUS_0025	Retrieve Proof to Archive	The CCO must be able to retrieve expiring proofs, using a specific expiry date.
PUS_FUR_0007	Identify Type of Request	The system must identify the type of request: - Endorsement request; or - Registration request.		PUS_BUS_0001	Receive Proof Request	The CCO must be able to receive a proof request, which can either be an endorsement request or a registration request. It includes the step to validate the format of the request and the data of the proof request.
PUS_FUR_0008	Identify Requested Validity Period	The system must identify if the requested validity period is more than 90 days or not.		PUS_BUS_0003	Register Proof	The CCO must be able to register proof, which can either be an endorsement request or a registration request. It includes the steps to assign a master reference number (MRN) and to calculate the expiry date.
PUS_FUR_0009	Issue a Master Reference Number	The system must issue a unique Master Reference Number.		PUS_BUS_0003	Register Proof	The CCO must be able to register proof, which can either be an endorsement request or a registration request. It includes the steps to assign a master reference number (MRN) and to calculate the expiry date.
PUS_FUR_0010	Calculate Expiry Date for Validity	The system must calculate the date upon which the validity expires, which is the default of 90 days following the date of receipt, or a specific validity period.		PUS_BUS_0003	Register Proof	The CCO must be able to register proof, which can either be an endorsement request or a registration request. It includes the steps to assign a master reference number (MRN) and to calculate the expiry date.
PUS_FUR_0011	Exchange Data with Central Repository	The system must exchange data with the Central Repository.		PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update

						proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
				PUS_BUS_0025	Retrieve Proof to Archive	The CCO must be able to retrieve expiring proofs, using a specific expiry date.
PUS_FUR_0012	Present Data	The system must present data to the user. This is a read only activity.		PUS_BUS_0013	Notify About Proof Validity	The CCO must be able to notify declarant about the validity of the proof.
				PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
PUS_FUR_0013	Search for Proof of Union Status Data	The system must search in the Central Repository for Proof of Union Status data using the MRN of the Proof.		PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
PUS_FUR_0015	Generate Printable SRD	The system must generate a printable SRD.		PUS_BUS_0003	Register Proof	The CCO must be able to register proof, which can either be an endorsement request or a registration request. It includes the steps to assign a master reference number (MRN) and to calculate the expiry date.
PUS_FUR_0017	Identify if Proof is Valid to be Used	The system will not allow any further action for a specific Proof if: a. For a T2L or T2LF Document the status returned by the central repository is "Already Used" or "Expired" or "Does not Exist" and b. For a Customs Goods Manifest the status returned is either "Expired" or "Does not Exist".		PUS_BUS_0008	Identify If Proof Is Valid for Use	Customs must identify if proof is valid for use.
PUS_FUR_0018	Identify if National Risk Analysis is to Be Consulted	The system must be able to identify if a National Risk Analysis System will be consulted.		PUS_BUS_0010	Perform Risk Analysis At Competent Customs Office	The CCO must be able to perform a risk analysis and interpret the result of this risk analysis.
PUS_FUR_0019	Identify Competent Member State for Risk Analysis	The system must be able to identify the competent Member State that will perform a national		PUS_BUS_0010	Perform Risk Analysis At Competent Customs Office	The CCO must be able to perform a risk analysis and interpret the result of this risk analysis.

		risk analysis. The Member State will be identified based on the CCO (Proof endorsement) or on the PCO (Proof presentation).			
			PUS_BUS_0019	Perform Risk Analysis At Presentation Customs Office	PCO must be able to perform a risk analysis and interpret the result of this risk analysis.
PUS_FUR_0020	Exchange Data with Competent Member State	The system must be able to exchange data with the Competent Member State.	PUS_BUS_0010	Perform Risk Analysis At Competent Customs Office	The CCO must be able to perform a risk analysis and interpret the result of this risk analysis.
			PUS_BUS_0019	Perform Risk Analysis At Presentation Customs Office	PCO must be able to perform a risk analysis and interpret the result of this risk analysis.
PUS_FUR_0021	Identify if Risk is Determined	The system must be able to identify if risk is determined.	PUS_BUS_0010	Perform Risk Analysis At Competent Customs Office	The CCO must be able to perform a risk analysis and interpret the result of this risk analysis.
			PUS_BUS_0019	Perform Risk Analysis At Presentation Customs Office	PCO must be able to perform a risk analysis and interpret the result of this risk analysis.
PUS_FUR_0023	Record Expiry of Time Limit to Complete Endorsement	The system must identify if the timer for automatic processing of endorsement request has expired.	PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
PUS_FUR_0024	Identify if Requested Validity Period is Longer than 90 Days	The system must identify if the requested validity is longer than the default value of 90 days.	PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
PUS_FUR_0026	Record Expiry of Time Limit to Complete Proof Usage Registration	The system must identify if the timer for Proof usage registration has expired.	PUS_BUS_0007	Update Proof Information	Customs must update proof information.
PUS_FUR_0027	Submit T2L/F Endorsement/Registration Request to Certify Union Status of Goods	The PC or AI must be able to submit an T2L/F Endorsement/Registration Request to the CCO, in order to certify the Union Status of goods declared in the form of T2L/F data.	PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0028	Retrieve Information	The system must	PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised

	from UCC EORI2	automatically populate the fields related to the Person Requesting a Proof of Union Status/Representative /Consignor/Person Presenting the Goods based on the relevant EORI record in UCC EORI2 system.				Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0029	Validate Commodity Codes – Combined Nomenclature Codes from TARIC system	The system must automatically validate the provided Commodity Codes – Combined Nomenclature Codes against TARIC system.		PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0030	Mass Upload of Goods in Request	The PC or AI must be able to add multiple goods with the use of a mass upload from file (e.g Excel file) functionality.		PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0031	Identify if relevant control is to be or has been performed	The system must be able to identify if relevant control is to be or has been performed.		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
PUS_FUR_0032	Identify Control Results at Departure	The system must identify the control results. The result of the control may be "A1 – Satisfactory", "P2 – Different goods" or "P3 – Non-union goods".		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
PUS_FUR_0033	Submit T2L/T2LF Corrected Endorsement Request to Certify Union Status of Goods	The PC must be able to submit a corrected T2L/F Endorsement Request to the CCO, in order to certify the Union status of goods declared in the form of T2L/F data.		PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0034	Identify if Endorsement is Confirmed	The system must identify if the endorsement is confirmed.		PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90

						days is requested.
PUS_FUR_0035	Identify if Extended Validity Period is Confirmed	The system must identify if the requested extended validity period is confirmed or not.		PUS_BUS_0002	Check Conditions for Endorsement	The CCO must be able to verify whether the goods declared in the proof request have Union status. It includes the step to check the validity date, when another period than 90 days is requested.
PUS_FUR_0036	Exchange Data with National Proof of Union Status Systems and Other National Systems	The system must exchange data with National Proof of Union Status Systems and Other National Systems.		PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
				PUS_BUS_0014	Notify about Proof Usage	The PCO must be able to notify declarant about the usage or non-usage of the proof.
				PUS_BUS_0026	Notify about Proof Archiving	The CCO must be able to notify declarant about the archiving of the proof, in case the validity date has expired.
PUS_FUR_0037	Identify if Request is Received from a National Proof of Union Status System / Other National System	The system must identify if the source of the request is a National Proof of Union Status System / Other National System or not.		PUS_BUS_0006	Retrieve Proof	The CCO must be able to retrieve proof, using an MRN. It includes the step to identify whether the expiry date of the proof has expired.
				PUS_BUS_0007	Update Proof Information	Customs must update proof information.
				PUS_BUS_0011	Store or Update Proof in Central Repository	CCO and PCO must be able to store or update proof particulars and all related information (e.g MRN, usage information, etc.) allowing the provision of proof of existence, validity status and all necessary data for monitoring and reporting.
PUS_FUR_0038	Submit T2L/T2LF Presentation Notification to Register Proof Usage	The EO at Arrival must be able to submit a T2L/T2LF Presentation Notification to the PCO, in order to register proof usage information..		PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0039	Identify Control Results at Arrival	The system must identify the control		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.

		results. The result of the control may be "A1 – Satisfactory", "P2 – Different goods", "P4 - Missing goods" or "P5 – Excess goods".				
PUS_FUR_0040	Identify if Proof is to be Used	The system must identify if the Proof is to be used.		PUS_BUS_0007	Update Proof Information	Customs must update proof information.
PUS_FUR_0041	Submit Request to get Updated T2L/T2LF Proof Information	The Economic Operator must be able to submit a Request for updated T2L/T2LF Proof information to the Competent Customs Office. The request may concern only the status or the full data of a T2L/T2LF Proof.		PUS_BUS_0009	Trader Interface	The Person Concerned and the Authorised Issuer must be able to use either an EU harmonized trader interface or the national system.
PUS_FUR_0042	Retrieve Proofs to be Archived	The system must automatically retrieve the Proofs that must be archived. A Proof must be archived if its validity date has expired and it has not been yet presented to a PCO.		PUS_BUS_0025	Retrieve Proof to Archive	The CCO must be able to retrieve expiring proofs, using a specific expiry date.
PUS_FUR_0043	Identify if Proofs for Archiving Have Been Retrieved	The system must automatically identify if there are Proofs that must be archived.		PUS_BUS_0025	Retrieve Proof to Archive	The CCO must be able to retrieve expiring proofs, using a specific expiry date.
PUS_FUR_0046	Identify if T2L/T2LF Proof Information Request Concerns Full Data	The system must identify if a T2L/T2LF Proof Information request shall return only the status of the Proof or the full data.		PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
PUS_FUR_0047	Identify if T2L/T2LF Proof Information Request is Initiated by a Customs Office	The system must identify if a T2L/T2LF Proof Information request has been initiated by a Customs Officer or an EO.		PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details

PUS_FUR_0048	Identify if User has Access to the Proof	The system must identify if a user has Access to a Proof. If the user is an EO, he/she must be indicated in the T2L/T2LF Proof data as "Person requesting a Proof of customs Union goods" or "Person presenting a Proof of customs Union goods" or "Representative". If the user is a Customs Officer his Customs Office must be indicated in the T2L/T2LF Proof data.		PUS_BUS_0008	Identify If Proof Is Valid for Use	Customs must identify if proof is valid for use.
				PUS_BUS_0022	View Proof	The Economic Operator must be able to retrieve an existing proof to view its details
PUS_FUR_0049	Identify if All Proofs Have Been Archived	The system must automatically identify if there are Proofs that must be archived.		PUS_BUS_0007	Update Proof Information	Customs must update proof information.
PUS_FUR_0050	Identify if supplementary documents are requested	The system must be able to identify if supplementary documents are requested.		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
				PUS_BUS_0024	Manage Documentary Controls	CCO and PCO must be able to examine the endorsement request, the presentation notification and the supporting documents - the necessary particulars in the endorsement request and the presentation notification and the availability and content of the supporting documents.
PUS_FUR_0051	Identify if physical control is performed	The system must be able to identify if physical control is to be performed.		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
PUS_FUR_0052	Record Expiry of Time Limit to Perform Relevant Control	The system must identify if the timer for the completion of the relevant control has expired.		PUS_BUS_0020	Perform Controls	CCO and PCO must be able to perform controls based on risk analysis information.
PUS_FUR_0053	Identify if Proof was	The system must		PUS_BUS_0014	Notify about Proof Usage	The PCO must be able to notify declarant

	Created by a National Proof of Union Status System	identify if the Proof was created by a National Proof of Union Status System or by the Central PoUS system.				about the usage or non-usage of the proof.
				PUS_BUS_0026	Notify about Proof Archiving	The CCO must be able to notify declarant about the archiving of the proof, in case the validity date has expired.
PUS_FUR_0054	Identify Member State Involved in the Creation of the Proof	The system must be able to identify the Member State that was involved in the creation of the Proof. The Member State will be identified based on the CCO.		PUS_BUS_0014	Notify about Proof Usage	The PCO must be able to notify declarant about the usage or non-usage of the proof.
				PUS_BUS_0026	Notify about Proof Archiving	The CCO must be able to notify declarant about the archiving of the proof, in case the validity date has expired.
PUS_FUR_0055	Generate Archiving Reference Number	The system must generate a unique reference number for each instance of the archiving process.		PUS_BUS_0025	Retrieve Proof to Archive	The CCO must be able to retrieve expiring proofs, using a specific expiry date.
PUS_GFR_0001	Print Proof of Union Status	The user (Economic Operator or Customs Officer) must be able to print a Proof of Union Status.				
PUS_GFR_0002	Notify Customs Officer About New Tasks or Notifications	The system must notify (e.g. email alert) the customs officer each time a new task or notification is received by a Customs Office.				
PUS_GFR_0003	Communicate Unavailability	A communication mechanism must exist to inform all the concerned parties about the unavailability of the system.				
PUS_GFR_0004	Change Language	The user must be able to change the language of the PoUS system.				

PUS_GFR_0005	Attach Additional Documents	The user (Economic Operator or Customs Officer) must be able to attach additional documents when submitting/registering information.	
PUS_GFR_0006	Query Proof of Union Status	The Economic Operator must be able to query his own Proofs of Union Status and the Customs Officer must be able to query the Proofs of Union Status where his MS is involved.	

Table 1: Functional Requirements

2. Non-Functional Requirements

2.1. Access Control and Connectivity Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_ACC_0004	Password	Password shall not be stored as a clear-text.	
PUS_ACC_0005	Reverse Proxies	The TA must provide support for deploying into environments making use of HTTP reverse proxies. This includes such things as proper handling of absolute URLs (e.g. in redirects) and page expiration for dynamic content.	
PUS_ACC_0006	Single Authentication	The PoUS system shall authenticate the users once and grant access for any subsequent business operations within the same session in a transparent manner (i.e. not requesting every time the user credentials).	
PUS_ACC_0007	Identical Behaviour	The behaviour of the PoUS system must be identical whether direct or proxy connection exists between the client or IT system, and the CDCO, independently of the number of proxy or reverse proxy servers participating in the communication.	
PUS_ACC_0008	HTTP Proxy for Outbound HTTP Requests	The PoUS system must be capable of using HTTP proxy for outbound HTTP requests.	
PUS_ACC_0009	External Access	The PoUS system might be accessible to external users and external IT systems, only through an additional security layer, for example provided by HTTP reverse proxies services.	
PUS_ACC_001	Access Authentication	Every interaction with the PoUS system, must take place under identification, authentication and authorisation control. – The identification establishes the user or IT system identity; – The authentication validates the user credentials; – The authorisation determines: which users or IT systems have access to what function; which users or IT systems have access to what data. The PoUS system shall not allow a user to login by bypassing the identification and authentication procedures.	
PUS_ACC_0010	Type of Users	The following type of users of the PoUS system, must be supported: – MS users; – MS IT systems; – Trade users; – EC users; – EC IT systems; – Administrator users.	
PUS_ACC_0011	IAM	The TA must support DG TAXUD's approved IAM	

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
		solutions.	
PUS_ACC_0012	Pluggable Authentication	Pluggable authentication and authorisation providers must be supported in order to integrate with future IAM solutions.	
PUS_ACC_0013	Access Paths	Depending on the user type, the following access paths to the PoUS system must be supported: – EC users and EC IT systems access CDCO only via the EC internal network or CCN; – MS users and MS IT systems access CDCO only via the CCN; – Trade users access CDCO through the EU Customs Trader Portal web user interface with synchronous HTTPS requests over the internet. There is no direct access to the CDCO itself from the Internet.	
PUS_ACC_002	CCN Access	When the PoUS system and the Central Repository are accessed through the CCN, the authentication and access control must be based on user information available via the CCN. The CDCO must avoid re-authenticating CCN users, unless absolutely necessary. The identity of the user must be made available to the CDCO for auditing or additional authorisation purposes.	
PUS_ACC_003	Security Checks	The security checks and operations shall be distinguished from the business operations and logic. The security policy should be easily modifiable without affecting the business operations. The security policy consists of the security measures related to identification, authentication and authorisation.	

Table 2: Access Control and Connectivity Requirements

2.2. Audit Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_AUD_0001	Audit Trail of Data Exchanges Availability	The audit trail of all data exchanges over the CCN between the MS IT systems and the Central Repository must be available for at least 5 years.	
PUS_AUD_0002	Audit Trail of Data Changes Availability	'The data of Proof of Union status must remain available in the PoUS system and the Central Repository for 5 years after the expiry of the proof.	
PUS_AUD_0004	CCN Audit Trail	The PoUS system and the Central Repository must keep an audit trail of all data exchanges over the CCN: what kind of exchange, who initiated it, when the exchange took place and whether it was successful.	
PUS_AUD_0005	Business Statistics	The Central Repository must allow that a number of business statistics are extracted. The exact scope of these business statistics are to be defined by B1. Proposal:	

		Number of Proofs (total and per MS)	
		Number of Retrieved Proofs (total and per proof)	
		Number of endorsed proofs (total and per MS)	
		Number of registered proofs (total and per MS)	
PUS_AUD_0006	Audit trail of Data Changes	The PoUS system must keep an audit trail of all data changes: what data was affected, the kind of changes (creation, update or deletion), who applied the changes and when. In case of an update, the initial and the new state of the changed data must also be recorded. In case of a delete, there is a difference between a logical deletion and a physical deletion. For physically deleted data, the audit trail shall only contain a limited set of data: the reference of the deleted record, who deleted it and when. For the logical deletion, the whole data record is audited. The auditing component must support both modes.	

Table 3: Audit Requirements

2.3. Availability Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_AVA_0001	Availability	TA must support applications that have wide range of availability requirements. Maximum availability that application might require and hence architecture have to enable is 99% for 24/7 period. Initial accepted application availability is 99.9% during business hours and 98% outside business hours, and it should evolve to target availability 99.9% 24/7 by means of infrastructure changes, no TA changes should be needed.	
PUS_AVA_0002	Failure Containment	The PoUS system and the Central Repository must be designed in a way so that it does not need periodic maintenance that results in significant downtime. In case of failure of one component the TA must minimise the effect on other components which are not directly related to the failed component (failure containment).	
PUS_AVA_0003	Failure of Database	The PoUS system and the Central Repository must guarantee the following after a failure of database: – no loss of transactional data; – business data must remain in consistent state; – immediate availability of database to process new requests after a failure; – no impact on application server components, i.e. transparent failover is required.	
PUS_AVA_0005	Backup and Restore Procedures	The TA components must be capable of integrating with backup and restore procedures. The preferred solution is the current infrastructure provider backup/restore.	
PUS_AVA_0006	Failure of a Batch Service	The PoUS system must guarantee the following after a	

		failure of a batch service:	
		– no batch jobs should be lost;	
		– recovery mechanism for batch jobs that were in progress at the moment of a failure. This might be either automated or manual process.	
PUS_AVA_0007	Failure of HTTP Communication of CCN	The PoUS system must guarantee the following after a failure of HTTP communication over CCN: – Ability to process a new request right after a failure; – Continued processing of all user requests that may have been initiated before a failure, i.e. transparent failover to another application server is required, without need to re-login and re-submit of the request; – Failover and/or load balancing of this component must be transparent to the CCN.	
PUS_AVA_0008	Failure of Asynchronous CCN Communication Component	The PoUS system must guarantee the following after a failure of the asynchronous CCN communication component: – no message should be lost; – CCN messages and JMS messages must remain in a consistent state; – no duplicate delivery of the same message after a failure; – ability to process queued CCN messages right after a recovery; – continued reprocessing of CCN messages that were in progress at the moment of a failure, i.e. failed messages need to be re-processed.	
PUS_AVA_0009	Fault Tolerance	The PoUS system must be fault tolerant, i.e. be able to continue functioning and remain in consistent state when single component fails.	
PUS_AVA_0010	New Requests Right after Failure	The PoUS system must guarantee the ability to process new requests right after a failure.	
PUS_AVA_0011	Ability to Recover by Resubmitting Failed Request	The PoUS system must guarantee at the presentation and web service layers the ability to recover by resubmitting the failed request by the end user, right after a failure.	
PUS_AVA_0013	Hot Deployment Support	The TA must provide means for application hot deployment support, meaning that installation of a new application version will not result in application down time.	
PUS_AVA_0014	Application Deployment Rollback	The TA must provide means for application deployment rollback.	
PUS_AVA_0015	Downtime during Deployment	Downtime during the deployment of a new application version must be minimal. The allowed downtimes are CDCO specific and depend on application availability requirements.	
PUS_AVA_0016	Presentation Layer	The PoUS system must guarantee at the presentation layer the continued processing of all user requests that may have	

		been initiated before the failure, i.e. transparent failover is required, without a need to re-login and re-submit of the request.	
PUS_AVA_0017	Asynchronous Layer	At the asynchronous layer the PoUS system must guarantee the following after a failure: – no message should be lost; – ability to process queued messages right after a failure; – continued processing of messages that were in progress at the moment of a failure, i.e. failed messages need to be re-processed.	
PUS_AVA_12	Minimal Manual Intervention in Recovery	After a partial or a total failure of an internal or external component the PoUS system must be able to recover. The manual intervention must be minimal.	

Table 4: Availability Requirements

2.4. Data Integrity Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_INT_0001	Data Consistency	The PoUS system must preserve the consistency of all data. All data must be stored persistently using transactions.	
PUS_INT_0002	Protection against Data Modification and Loss of Data during Transfer	The PoUS system must protect the data against modification and loss during transfer between the client part and the server part and when exchanging data with other systems.	
PUS_INT_0003	Loss of Messages	Loss of messages is not allowed between the PoUS system, the Central Repository and the national systems or between CDCOs. Messages must be delivered exactly once. Due to CCN and the client, it is possible to receive duplicate messages which should be handled by the application (e.g. by creating idempotent business operations or detecting and intercepting duplicates).	
PUS_INT_0004	Access Rights	An MSA must not be able to change the data provided by another MSA. This implies that competent customs office will have read- and write access, while the Presentation Customs office will only have read- access.	
PUS_INT_0005	Data Availability	The data must be available for all proofs in force and for a period of at least 3 years after expiry.	
PUS_INT_0006	Administrator Inspection	The messages that could not be processed must be available to the administrator for inspection. After the inspection the administrator can decide to retry or discard the message.	

Table 5: Data Integrity Requirements

2.5. Implementation Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_IMP_0001	DG TAXUD Development Process	The development process of DG TAXUD must be followed.	
PUS_IMP_0002	DG TAXUD Testing Process	The testing process of DG TAXUD must be followed.	
PUS_IMP_0003	High Level of Testability	TA should strive to reach a high level of testability.	
PUS_IMP_0004	Integration on Test Environment and Automated Test Execution	A continuous integration practice must be applied for the CDCO installation on the test environment and automated test execution.	
PUS_IMP_0005	Smoke Test Scenarios	Smoke test scenarios must be 100% automated.	
PUS_IMP_0006	Unit Testing	CDCO unit tests must be run during delivery package build and unit test report must be automatically generated. Unit test coverage goal is application specific, but it should be avoided setting goals lower than 80%.	
PUS_IMP_0007	Regression Functional Test Scenarios	Regression functional test scenarios must be 100% automated. There might be exceptions on the CDCO level, due to automation complexity which needs to be agreed on case by case level.	
PUS_IMP_0008	Automated Build of Delivery Package	Build of the delivery package must be fully automated and include following steps: – a source code and other artefacts checkout from the source control system; – a source code build; – a delivery package creation. Ideally, it must be possible to automatically test the package (i.e. verify that it is possible to create installation from the delivery).	
PUS_IMP_0009	Installation Package	As a result of CDCO build, installation package must be produced. The Installation package contains artefacts ready to be installed on an environment.	
PUS_IMP_0010	Automated Installation Procedure	The CDCO installation procedure must be fully automated.	
PUS_IMP_0011	Re-use of Installation Procedure	The same CDCO installation procedure must be used for integration test, FAT, preSAT, SAT, and production environments.	
PUS_IMP_0012	Delivery Package of Release	As a result of new application release, a delivery package must be produced. The delivery package includes application source code, all third party libraries and additional files required to build installation package. It also contains all application documentation. The structure of the delivery package must be common across applications.	
PUS_IMP_0013	Identification of Exact Version	It must be possible to identify the exact version (including hot fix) of the CDCO during the whole deployment lifecycle:	

		– a delivery package; – an installation package; – a deployed application.	
PUS_IMP_0014	Availability of Necessary Environments	All necessary environments to support testing required during build and test phases must be available. Including the following: – Build & unit test environment - is to be used by developers for doing their testing or for doing a continuous integration and a unit test automation; – Integration test environment - is to be used by the testing team to perform the internal testing activities before moving to FAT testing; – FAT environment - is to be used by the testing team for FAT testing activities with DG TAXUD; – Reference environment - is to be used by development and test teams to do simulations in case of receiving incidents from production to analyse. It thus must always be in line with the release in production including patch / hot fixes and must have regular updates of business data from production; – Performance environment - is to be used by the testing team for performance related testing activities.	

Table 6: Implementation Requirements

2.6. Infrastructure Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_INF_0001	Security and Confidentiality of Traffic	The security and confidentiality of the traffic between the client part and the server part of the PoUS system and Central Repository must be ensured by Common Communication Network (CCN) and by the EC's internal network.	
PUS_INF_0002	Traffic between PoUS System/Central Repository and National Systems	All traffic between the PoUS system/Central Repository and the national systems must be performed through the CCN or through the EC's internal network.	
PUS_INF_0003	Communication Trade - CDCO	All communications between the traders part and the CDCO system shall be made through the EU Customs Trader Portal IT Application which will be the main electronic interface containing both the user interface and necessary services required by the PoUS processes.	

Table 7: Infrastructure Requirements

2.7. Installability Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_INS_0001	Continuous Integration Practice	Continuous integration practice must be applied for CDCO	

		installation package build.	

<div align="center">Table 8: Installability Requirements</div>

2.8. Interface Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_ITF_0001	Interface with CS/RD2	The PoUS system must interface with the CS/RD2 to retrieve all reference data in the form of Code Lists and Authorities. This will avoid duplication of data.	
PUS_ITF_0002	Interface with National Proof systems	The PoUS system must interface with the national systems responsible for the management of Proof of Union Status.	
PUS_ITF_0003	Interface with EOS-AEO	The PoUS system must be able to interface with the EOS-AEO system. AEO certificate numbers submitted by economic operators will be automatically validated against the EOS-AEO system. The acquisition point for AEO authorisation data will be the EOS-AEO system and the reference point for these data will be CRS.	
PUS_ITF_0004	Interface with Customs Decisions System	The PoUS system must have an interface with the Customs Decision System to check whether declared authorisations: - match with the declarant; - match with the declared goods; - are valid; - are active.	
PUS_ITF_0005	Interface with EOS-EORI	The PoUS system must be able to interface with the EORI-EOS system to retrieve the details of the economic operator. Furthermore, EORI numbers submitted by economic operators will be automatically validated against the EOS-EORI system. The acquisition point for economic operator data will be the EOS-EORI system and the reference point for these data will be CRS.	
PUS_ITF_0006	Interface with National Risk Systems	The PoUS system must interface with the National Risk System of the respective MS.	
PUS_ITF_0007	Interface with TARIC	The PoUS system must interface with TARIC to retrieve the reference data regarding goods nomenclature, excise duties and free circulation. This will avoid duplication of data.	
PUS_ITF_0008	Interface with Notification of Arrival, Presentation Notification and Temporary Storage	The PoUS system must interface with national systems related to Notifications of Arrival, Presentation Notifications (PN) and Temporary Storage (TS).	
PUS_ITF_0009	Interface with EUCTP	The PoUS system must interface with the EU Customs Trader Portal, through a separate PoUS Specific Trader Portal module corresponding to the PoUS back-office application. The EU Customs Trader Portal is the unique online access point for the traders of the European Union to all DG-TAXUD trader related applications. The PoUS system is the application to which the Customs Officers have access and from where they can handle the requests	

		presented by the traders in the EU Customs Trader Portal (through the PoUS STP module).	
PUS_ITF_0010	Access CDCO Functions	The CDCO functions must be accessible: • to the online users through a light Web client • also a part of them should be exposed as web-services All involved roles (traders, MS, etc.) should be able to access functions through both type of interfaces. During the technical implementation it shall be decided for each type of access which functions it shall cover.	
PUS_ITF_0011	Interface with CRS Repository	The PoUS system must interface with CRS repository to retrieve the details of the authorisations delivered in the EU in close relation with the Customs Decisions System. The CRS repository will also be used by the PoUS system in order to retrieve the latest EORI details of Economic Operators and Representatives.	

Table 9: Interface Requirements

2.9. Logging Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_LOG_0001	Technical Logs Availability	Technical logs must be available for configurable periods of time.	
PUS_LOG_0002	Dump Messages	TA must provide possibility to dump the messages. There is no need to filter messages based on the origin or type, all exchanged messages are dumped.	
PUS_LOG_0003	Centralised Storage for Logs	The logging component must support centralised storage for logs.	
PUS_LOG_0004	Technical Logging	The TA must provide logging component that can be used by any CDCO for technical logging. It must be possible to customise logging on the CDCO level.	
PUS_LOG_0005	Authentication Log	The PoUS system must provide possibility to log all authentication or authorisation attempts whether they are successful or not.	

Table 10: Logging Requirements

2.10. Monitoring Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_MON_0001	IIntegration with External Monitoring Component	The PoUS system must enable integration with the external (infrastructure provider) monitoring component currently used at DG TAXUD.	
PUS_MON_0002	Metrics	The following metrics must be reported: – Common metrics exposed by the application server such as CPU load, heap usage, IO activity, JMS Queue (number of pending messages), JDBC data sources (number of free	

		connections), number of threads;	
		– Health checks where components should check that they are able to perform the necessary functions. The TA must provide framework to simplify implementation of health checks on the component level. Exact checks are component specific and should be defined at design time of the component.	
		The frequency should be defined under the context of TATAGng.	

<div align="center">Table 11: Monitoring Requirements</div>

2.11. Ownership of Assets Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_OOA_0001	Data Ownership	The TA must support the notion of a data ownership. The TA must provide a mechanism for (dis)allowing data access based on the current user identity and data ownership information (the specific rules are CDCO-specific). Business data kept in (or created in) the central application on behalf of a party, belong to that party. Owner is holding the responsibility of the data quality. The EC is normally owner of all reference data, while an MS is normally owner of all business data originating from those MS. See below specific requirements related to ownership of assets: - The reference data are owned by DG TAXUD and can only be changed by DG TAXUD users; - The data exchanged between the PoUS system and the MSs are owned by the MS that created them; - The data related to the proof and to its expiry are owned by the MS of the issuing customs authority and can only be changed by users of the IT system of that MS; - The list of competent customs authorities of each MS is owned by the respective MSs and can only be changed by users or IT systems of that MS.	
PUS_OOA_0002	Data Masking Strategies and Techniques	Data masking strategies and techniques must be used for production data before they are sent for use in non-production environments. Data masking strategies and techniques will obscure or depersonalize specific data within a database table or a flat file ensuring data security is maintained and sensitive customer information is not leaked outside of authorised environments. The data masking algorithms are applied across multiple tables, applications and environments so referential and business integrity will always be maintained. This allows testing and development teams to carry out project work safely and efficiently.	

<div align="center">Table 12: Ownership of Assets Requirements</div>

2.12. Performance Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_PER_0001	Performance Requirements	The TA must support applications that have wide range of performance requirements; hence, the TA must ensure that the lowest response times are achievable. The lowest response times are defined as follows: when measured in the standard stress test configuration , CDCO response time with respect to requests from all users shall not exceed 2 seconds. Longer response time periods may be deemed acceptable for some types of operations (e.g., report generation, extractions, and complex queries). Each case of such 'anticipated' longer response time shall be agreed upon and documented as an exception.	

Table 13: Performance Requirements

2.13. Scalability Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_SCA_0001	Horizontally Scaled	The CDCO must be architected to horizontally scale including increased number of users and increased transaction and data volume without changing technical architecture (the underlying infrastructure architecture will probably change). The amount of messages exchanged via CCN increases 30% annually. This statement does not imply that the architecture must support 30% annual increase because messages are distributed across applications, environments, etc. But it indicates that the architecture must be scalable.	
PUS_SCA_0002	Allow Additional Servers	The architecture must allow adding additional servers during maintenance periods without any impact to application code or deployment scripts.	
PUS_SCA_0003	Split Messages that Exceed Size	The PoUS system must be able to split messages sent to the CCN if a size limit is exceeded. The size limit is equal to the CCN or NA message size limit, depending which limit is lower.	
PUS_SCA_0004	Maximum Size of Messages Exchanged via CCN	The PoUS system must be designed to support maximal size of messages exchanged via CCN queues. This is a configurable value, so there should be no dependency on the current maximal size of the message.	

Table 14: Scalability Requirements

2.14. Security & Data Protection Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_SEC_0001	Compliance with Directive 95/46/EC	TA must provide support to applications in order to	

		comply with the TEMPO security policy; see [TMP-REF-SDLC]. Compliance with the TEMPO security policy implies that the CDCO and the data exchanged between the CDCO and the national IT systems complies with the applicable directives, regulations and decisions related to security and data protection: – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;	
PUS_SEC_0002	Compliance with Council decision No 2001/264/EC	TA must provide support to applications in order to comply with the TEMPO security policy; see [TMP-REF-SDLC]. Compliance with the TEMPO security policy implies that the CDCO and the data exchanged between the CDCO and the national IT systems complies with the applicable directives, regulations and decisions related to security and data protection: – Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;	
PUS_SEC_0003	Compliance with Regulation (EC) No 45/2001	TA must provide support to applications in order to comply with the TEMPO security policy; see [TMP-REF-SDLC]. Compliance with the TEMPO security policy implies that the CDCO and the data exchanged between the CDCO and the national IT systems complies with the applicable directives, regulations and decisions related to security and data protection: – Council decision No 2001/264/EC of 19 March 2001 adopting the Council's security regulations;	
PUS_SEC_0004	Compliance with Commission decision C(2006)	TA must provide support to applications in order to comply with the TEMPO security policy; see [TMP-REF-SDLC]. Compliance with the TEMPO security policy implies that the CDCO and the data exchanged between the CDCO and the national IT systems complies with the applicable directives, regulations and decisions related to security and data protection, i.e.: – Commission decision C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission	
PUS_SEC_0005	Modern Standards and Best Practices	The PoUS system shall be secured in accordance with best practices for the concerned platform, including at least immunity against the OWASP top 10 vulnerabilities.	

Table 15: Security & Data Protection Requirements

2.15. Software Architecture Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_SAR_0001	TATAFng Compliant	The architecture must be compliant with the technical architecture framework [TATAFng] of the Customs CDCOs of DG TAXUD.	
PUS_SAR_0002	TSOAP Compliant	The PoUS system must be deployable to DG TAXUD SOA Platform. This implies among others the use of the following technology · Oracle WebLogic Fusion Middleware · Oracle RAC database	
PUS_SAR_0003	CDCO Applications	All the developed applications will be of type CDCO.	

Table 16: Software Architecture Requirements

2.16. Usability Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_USE_0001	Several Users Work Simultaneously	The central database must allow several users to work simultaneously, while guaranteeing coherence.	
PUS_USE_0002	User Interface Uniformity	User Interface should be uniform for the end users (not necessary for administrators).	
PUS_USE_0003	Textual Data	It must be possible to enter textual data in the interactive client any present or future official language of the EU using [UTF-8] encoding.	
PUS_USE_0004	No Translation or Transliteration	No translation or transliteration will be provided by the system.	
PUS_USE_0005	Community Languages	The user interface will be available in English but must support the option to be translated in order to be available in all the official languages of the EU. Provisions must be made to allow the localisation of the user interface in any future official language of the EU using Unicode Transformation Format 8 [UTF-8] encoding. New languages should be deployed without system downtime.	

Table 17: Usability Requirements

2.17. Volumetric Requirements

REQUIREMENT ID	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	RELATED TEST
PUS_VOL_0001	Number of Proofs Retrieved per Day	The PoUS system (or Central Repository) must support up to 25000 retrievals of proofs per day	
PUS_VOL_0002	Number of New Proofs Stored per Day	The PoUS system (or Central Repository) must support up to 5000 new proofs stored in the central repository per day.	

PUS_VOL_0003	Graceful Degradation	When the volumetric requirements are exceeded, the performance of the PoUS system and Central Repository must 'gracefully' degrade.	
PUS_VOL_0004	Number of Customs Users	The PoUS system must support up to 55.000 Customs users. Customs users consist of users using the national or central implementation, or DG TAXUD users.	
PUS_VOL_0005	Number of Concurrent Customs Users	The PoUS system must support up to 1.000 (e.g. 20) concurrent Customs users, i.e. the system must be able to process up to 1.000 (e.g. 20) simultaneous requests from the Customs users. Customs users consist of users from MS and from DG TAXUD.	
PUS_VOL_0006	Number of Economic Operator Users	The PoUS system must support up to 500.000 (e.g. 500 000) economic operator users.	
PUS_VOL_0007	Number of Concurrent Economic Operator Users	The PoUS system must support up to 2.000 (e.g. 200) concurrent economic operator users, i.e. the system must be able to process up to 2.000 (e.g. 200) simultaneous requests from the Economic Operator Users.	
PUS_VOL_0008	Growth Rate	The PoUS system should support an entity growth rate of at least 10% (e.g. 20%) per year.	

Table 18: Volumetric Requirements