Annex 1 – Functional and Technical requirements

System: NCTS 5

FUNCTIONAL REQUIREMENTS SPECIFICATION

The existing trans-European New Computerised Transit System (NCTS) must be aligned with the new requirements of the Convention on Common Transit (CTC) and with the new requirements defined in the Union Customs Code (UCC).

According to the Delegated Act and Implementing Act (DA / IA) as well as CTC, the current system "NCTS Phase 4" must evolve on business level and on data level.

Reference documents for detailed functional specification are:

1. **Latest versions of:**
   FUNCTIONAL TRANSIT SYSTEM SPECIFICATION – NCTS ADDENDUM (REF: FSS-NCTS)
   FSS-UCC NCTS Section I-BUSINESS PROCESS THREADS FOR CORE BUSINESS-SfA-v5.30.or later
   FSS-UCS NCTS Section II-BUSINESS PROCESS THREADS FOR GUARANTEE MANAGEMENT-SfA-v5.30.or later
2. **Latest version of EU Customs Functional Requirements BPM Report for New Computerised Transit System (NCTS) (REF: SC22-QTM007, Ver.7.0 or later)**

NOTE: The main goal of the "Functional Transit System Specification" (FTSS) [R4] is to provide – next to the Functional Requirements Report – a document that the intended readership is already familiar with. This document aims to identify the scope of the New Computerised Transit System (NCTS) and to provide detailed description of its functional specification. It is also intended to serve as a stable baseline for the NCTS detailed technical specification (see 'Technical Transit System Specification' [TSS-TSP-SYS]) DDNTA [R7].

3. **Latest version of Design Document for National Transit Application (DDNTA) (REF: DDNTA-Main Document-5.15.0-SfA-v1.00 or later)**

Applicable to every National Transit Application and must be considered as a **mandatory** for all implementation and verification activities.

The purpose of the DDNTA document is:

- *To state **unambiguously what** needs to be developed. This will be achieved by specifying the sequences of Information Exchanges to be supported, as a number of message exchange protocols, the State Transition Diagrams and the detailed structure and building rules of these Information Exchanges.*
  Regarding the Message Exchange Protocols and the State Transition Diagrams, this volume will also define any Transitional Message Exchange Protocols (Transitional scenarios) for NCTS in case they are different from Message Exchange Protocols in Post Transitional phase.

- *To define **how** the Information Exchanges, have to be performed and transported between the National Transit Applications. The message formatting as well as the transport mechanisms are described in the DDCOM volume.*

*NCTS-P5 L4 BPMs [R10] has been used as a basis for the production of DDNTA. However, a substantive re-structuring of data structures and messages has been implemented which **resulted from the changes** defined in the ANNEX B of UCC-DA and ANNEX B of UCC-IA [***Error! Reference source not found.***]. Moreover, further analysis, elaboration and refinement has been performed for the business processes to specify their IT implementation reducing complexity, aligning with operational practices and legal provisions.*

It should be noted that for the (mandatory) Information Exchanges (Information Exchanges in the Common Domain), DDNTA should therefore be considered as an applicable document, while for the category of (Recommended, Strongly Recommended or Optional) Information Exchanges, DDNTA should only be considered as a guideline with recommendations.

*The Functional System Specifications for NCTS-P5 [***Error! Reference source not found.***] and L4 BPMs for NCTS [***Error! Reference source not found.***] will be revisited in alignment to the latest amendment of UCC legal provisions and the Technical Specifications following their approval. Consequently, **DDNTA prevails in case of contradiction**.*

RfC-List.31 and all the next scheduled RfC's until the contract warranty expiry date

The major process threads are described and depicted through **scenarios, time sequence diagrams and state transition diagrams in DDNTA** – Main Document:

CORE FLOW (CFL)

T-TRA-CFL-M-001-Standard Transit Procedure (overview)

SPECIFIC SCENARIOS AT OFFICE OF DEPARTURE (DEP)

Declaration Lodged Prior to Presentation of Goods

T-TRA-DEP-A-003-Transit presentation notification valid

T-TRA-DEP-A-002-Correction of the pre-lodged declaration prior to presentation of goods

T-TRA-DEP-E-004-Transit presentation notification not valid

T-TRA-DEP-E-005-Cancellation of the pre-lodged declaration prior to presentation of goods

T-TRA-DEP-A-001-Simplified procedure at departure

T-TRA-DEP-E-012-Rejection of transit declaration

Amendment of Transit Declaration

T-TRA-DEP-A-014-Declaration amendment accepted

T-TRA-DEP-E-015-Declaration amendment rejected

T-TRA-DEP-M-006-Control by Office of Departure with release for transit

Minor Discrepancies Found During Control

T-TRA-DEP-A-007-Positive release request with release for transit

T-TRA-DEP-A-008-Negative release request
T-TRA-DEP-E-009-Release request rejected

T-TRA-DEP-A-011-Transit Movement is released for transit

T-TRA-DEP-A-020 - 'Open' ATR Response C_ATR_RSP (IE115) is closed

Movement is not released for Transit

T-TRA-DEP-A-010-Control by Office of Departure with release for transit refused
T-TRA-DEP-A-013-Release for transit refused due to guarantee registration failure

Departure Specific Safety and Security

Departure Activity
Safety and Security Risk Analysis when Declaration Amendment is Requested
T-TRA-DEP-A-021-Release for transit refused for safety and security reasons

Invalidation of Transit Declaration

T-TRA-DEP-A-016-Invalidation request by the Holder of the Transit Procedure before release for transit
T-TRA-DEP-A-017-Invalidation request by the Holder of the Transit Procedure after release for transit
T-TRA-DEP-A-018-Invalidation of a transit declaration before release for transit when declaration data is electronically unavailable
T-TRA-DEP-A-019-Invalidation of a transit declaration after release for transit

SPECIFIC SCENARIOS AT OFFICE OF TRANSIT (TRT)

Formalities at Office of Transit

T-TRA-TRT-A-003-Control by Office of Transit with Passage Confirmed
T-TRA-TRT-A-004-Control by Office of Transit with Passage Not Confirmed
T-TRA-TRT-A-010-Transit Declaration having Office of Destination being also Office of Transit

Diversion at Office of Transit

T-TRA-TRT-A-002-Diversion at Office of Transit accepted
T-TRA-TRT-A-001-Diversion at Office of Transit rejected

Formalities Prior to Exit of Goods at Customs Office of Exit for Transit

T-TRA-TRT-A-005-Movement arrives at declared Office of Exit for Transit
T-TRA-TRT-A-007- Movement allowed to leave the Security Area
T-TRA-TRT-A-006-Movement stopped at Customs Office of Exit for Transit

Diversion at Office of Exit for Transit

T-TRA-TRT-A-008-Diversion at Customs Office of Exit for Transit – Movement is allowed to leave the Security Area
T-TRA-TRT-A-009-Diversion at Customs Office of Exit for Transit – Movement stopped at the border of Office of Exit for Transit

SPECIFIC SCENARIOS AT OFFICE OF DESTINATION (DES)

T-TRA-DES-M-001-Arrival notification valid
T-TRA-DES-A-004-Simplified procedure at destination
T-TRA-DES-A-011-Manual closure at Departure based on alternative proof
T-TRA-DES-A-006-Unloading Permission Received – Unloading Remarks
T-TRA-DES-E-007-Unloading remarks rejected
T-TRA-DES-E-003-Rejection of arrival notification

Control of the Goods at Destination

T-TRA-DES-A-008-Major Discrepancies found during control at the Office of Destination – Resolved before the expiration of resolution timer
T-TRA-DES-A-013-Major Discrepancies found during control at the Office of Destination – Major Discrepancies are confirmed – Recovery to be started

T-TRA-DES-A-012-Major Discrepancies found during control at the Office of Destination – Resolved after the expiration of resolution timer

Diversion at Office of Destination

T-TRA-DES-A-009-Diversion at Office of Destination accepted

T-TRA-DES-A-010-Diversion at Office of Destination rejected

SPECIFIC SCENARIOS FOR INCIDENTS "EN ROUTE" (INC)

T-TRA-INC-M-001-Capturing movement information at Office of Incident Registration

T-TRA-INC-A-003-Office of incident registration allows transit movement to continue its journey

T-TRA-INC-A-002-Transit Movement does not continue-Office of Incident Registration becomes Actual Office of Destination

POSSIBLE EXCEPTIONS IN THE COMMON DOMAIN (EXCEPTIONS OF MESSAGE SEQUENCING IN THE COMMON DOMAIN) (EXC)

T-TRA-EXC-M-001-Query movement information

T-TRA-EXC-A-007-Status request/response

T-TRA-EXC-A-002-AAR missing

T-TRA-EXC-A-003-ATR missing

T-TRA-EXC-A-004-NCF not received

T-TRA-EXC-A-005-AXR Record missing

T-TRA-EXC-A-006-Notification leaving security area not received

T-TRA-EXC-A-008-Deviation from the Binding Itinerary at Actual Office of Transit - Movement is allowed Diversion after registering the Incident

EXPORT FOLLOWED BY TRANSIT (EFT)

Core Flow of the Export followed by Transit

T-TRA-EFT-M-001-Core flow of the export followed by transit - External transit

T-TRA-EFT-M-002-Core flow of the export followed by transit - Internal transit (Appropriate Office of Destination)

T-TRA-EFT-M-003-Core flow of the export followed by transit - Internal transit (Inappropriate Office of Destination)

Lodgement of Transit Declaration having Export as Previous Procedure

T-TRA-EFT-E-004-Lodgement of transit declaration having export as previous procedure - Negative response from Office of Exit (before acceptance)

T-TRA-EFT-A-005-Lodgement of Transit Declaration having Export as Previous Procedure - Unknown Export MRN and Positive IE503 (before acceptance)

Amendment of the Transit Declaration for the Export Followed by Transit

T-TRA-EFT-A-006-Amendment of transit declaration having export as previous procedure – Positive Response from AES

T-TRA-EFT-E-007-Amendment of transit declaration having export as previous procedure – Negative Response from AES

Example business scenarios of allocation and amendment of the Export MRNs referenced in the transit Movement

Scenario A - Initial Cross-Check & Allocation of the Export MRNs with the Transit Declaration

Scenario B - Amendment of the Transit Declaration that references Export MRNs

Export followed by Transit – Destination Control Results are received from the Office of Destination

T-TRA-EFT-A-010-Transit movement having export as previous procedure - Control results from destination indicate major discrepancies - Dispatch of control results information to Office of Exit

T-TRA-EFT-A-011-Transit movement having export as previous procedure - Departure notifies Office of Exit for the initiation of Recovery
T-TRA-EFT-A-012-Manual closure at Departure based on alternative proof - Export is previous procedure

Transit Movement having Export as Previous Procedure is invalidated or not released for transit

T-TRA-EFT-A-008-Invalidation of transit declaration having export as previous procedure - Before release for transit
T-TRA-EFT-A-009-Transit movement having export as previous procedure is not released for transit

NCTS GUARANTEE MANAGEMENT (GMN)

CHECK GUARANTEE INTEGRITY (GUI)

T-GMN-GUI-M-001-Check guarantee integrity

REGISTRATION OF GUARANTEE USAGE (GUR)

T-GMN-GUR-M-001-Registration of guarantee usage

GUARANTEE RELEASE (GUF)

T-GMN-GUF-M-001-Credit of Reference Amount
T-GMN-GUF-M-002-Release of a Guarantee
T-GMN-GUF-M-003-Release of a Guarantee after resolution of major discrepancies in the destination control results

CANCELLATION OF GUARANTEE USAGE (GUC)

T-GMN-GUC-A-005-Cancellation of the national guarantee registration usage due to the failure of the international guarantee registration usage
T-GMN-GUC-A-008-Cancellation of the international guarantee registration usage due to the failure of the national guarantee registration usage
T-GMN-GUC-A-006-Cancellation of guarantee registration usage due to a transit declaration invalidation request submitted by the holder of the transit procedure before release for transit
T-GMN-GUC-A-007-Cancellation of guarantee registration usage due to the invalidation of transit declaration after release for transit

NCTS HANDLE ENQUIRY & RECOVERY

T-ENR-ENQ-Handle Enquiry (ENQ)

T-ENR-ENQ-M-001-Status Request with Arrival Processing Resumed
T-ENR-ENQ-A-002-Sufficient information–Enquiry with arrival processing resumed
T-ENR-ENQ-A-003-Sufficient information–Enquiry response with “Return Copy”
T-ENR-ENQ-A-004-Sufficient information–Enquiry with duplicate movement
T-ENR-ENQ-A-005-Sufficient information–Enquiry with movement unknown at Destination–Holder of the transit procedure contacted
T-ENR-ENQ-A-006-Insufficient information–Alternative proof and movement closed
T-ENR-ENQ-A-007-Insufficient information – Movement closed–Enquiry cancelled
T-ENR-ENQ-A-008-Insufficient information–Enquiry started–Recovery started
T-ENR-ENQ-A-009-Insufficient information–Holder of the transit procedure provides negative response
T-ENR-ENQ-A-010-Enquiry in the case of suspected fraud
T-ENR-ENQ-A-011-Cancellation of Enquiry request
T-ENR-ENQ-A-012-Exchange of additional information

T-ENR-REC-Handle Recovery (REC)

T-ENR-REC-M-001-Early Recovery in Special Cases
T-ENR-REC-A-008-Recovery Initiation on Incident occurrence
T-ENR-REC-A-002-Recovery at Destination – Destination's Recovery request accepted
T-ENR-REC-A-003-Recovery at Departure – Destination's Recovery request rejected
T-ENR-REC-A-004-Recovery at other country – Transfer of competency
T-ENR-REC-A-005-Recovery at Departure – Other Country's Recovery Request Rejected – No Transfer of Competency
T-ENR-REC-A-006-Recovery at Departure – Departure Recovery Request Sent to Other Country Rejected
T-ENR-REC-A-007-Recovery at other country–Departure Recovery request sent to other country accepted

New Process

Incidents during movement of goods under a transit operation (Art. 305 of the UCC IA/ Article 44 Appendix I, Convention) - New process and new customs office role for handling the "incidents en route".

This customs office will be competent for recording the incidents that occurred during the movement of goods into the electronic transit systems. In case of incidents during the movement of goods, a carrier presents the goods together with the MRN to the nearest customs authority in whose territory the means of transport is located or, if the legislation does not require such presentation, provides relevant information concerning the type of incident and the MRN to that customs authority.

Main Process

Clearly, all of above mentioned process threads are inter-dependent, e.g. the processing of a Transit movement crossing a frontier will happen after the processing at departure. The 'link' between those two processes is the journey of the consignment from the Customs Office of Departure to the Customs Office of Destination via Offices of Transit. The major item of the core business is that NCTS delivers data for Safety and Security risk analysis and communicates the results of risk analysis and control results between the offices concerned.

The movement is initiated. Thereafter, the Holder of the Transit Procedure receives the NCTS Accompanying Document or MRN of Transit Declaration in an electronically readable format and the vehicle with the consignment goes to the first Customs Office of Transit (if any).

The following might happen not at all or several times. The consignment arrives at a Customs Office of Transit where the processing of crossing a frontier occurs. Afterwards, the consignment leaves either to the next Customs Office of Transit, or to its destination.

Normally, the consignment arrives at destination. The goods are presented to the Customs Office of Destination which processes the arrival. Once the arrival processing is complete, the Customs Office of Departure writes-off the movement.

In case the Customs Office of Departure does not receive any feed-back about the arrival of the movement within the expected period, an enquiry procedure is started. Depending on the result of the enquiry, taxes and duties might be collected. In all cases, sooner or later, the movement is written-off.

INTEGRATION WITH OTHER SYSTEMS, SUPPORTING APPLICATIONS AND REFERNCE DATA

NCTS5 system integration in NATIONAL DOMAIN

- Guarantee Management system
- National authorisations for customs procedures Reference System
- Temporary storage
- Import module
- Export module
- LDAP authorisation system for CARNM users
- Trader autorisation system za external users
- Risk Analisys system
- EORI and TIN numbers reference data
- CS/RD2 reference data
- TARIC data
- Reporting system or BI- Business Intelligence

NCTS5 system integration in COMMON (EU) DOMAIN

- CCN adapter – connectivity module for EU communication network using CSI protocol (API)
- CS/MIS2 – business statistics
- ieCA – Information exchange Conversion Application

TECHNICAL AND NON-FUCTIONAL REQUIREMENTS

This chapter describes the high-level technical requirements of the NCTS5 system. The aim is to provide the reader with a global view of the system, to clarify the required system architecture, and to categorise the main technical elements of the system. **Detailed technical and non-functional requirements MUST be specified in the initial stages of the system implementation project**.

Globalisation and Localisation

The requirements for globalisation, localisation, regional settings, and Unicode support are given in the last version of DDCOM document as follows:

- Unicode compliance according DDCOM latest version (NCTS5 must support UTF-8 for XML messages)
- Support for the Macedonian, Albanian and English Language and regional settings (date, time, currency and number format, and other regional and cultural conventions at national level)

Regarding the connection to the Common Domain:

- NCTS5 has to support only UNOC as the default character set in all data-items (non-language sensitive text fields and numeric fields) in EDIFACT messages.
- NCTS5 has to support UNOC, UNOD or UNOF as the character set in all language-sensitive text fields in EDIFACT messages or UTF-8 for XML messages.
- NCTS5 has to be able to convert (transliterate) the character sets of the EDIFACT messages (namely UNOC, UNOD and UNOF) or XML messages (UTF-8) into the character set(s) used internally in the system.

Introduction and Principles

The technical solution of the NCTS5 system must be based on the following key principles:

- Scalability:
  The system should support an initial capability of 1000 concurrent users.

  The following information provides some very broad volumetric for peak and average processing days:

  Daily transactions peak at around 2pm to 4pm. During the peak hour the number of transactions reaches 200 transit transactions per hour.

  The average amount of daily transactions is 1500 transit transactions per day.

  To cope with larger numbers of users, or increased calculation complexity, the system should also be able to scale with only configuration changes or/and additional hardware.

- Availability:
  The system is considered to be mission critical application. NCTS5 availability will be measured on a monthly level. Minimum availability shall be 99.58% during the first three months of operations, and 99,85% after the third month. Maximum length of failure period during the working hours is 3 hours in the first three months of operations, and 1 hour after the third month.and thus should be 99.99% available. CARNM will assume planned downtimes of 2 hours per week

  In case NCTS5 fails or is shut down for maintenance, incoming messages must be queued.

  NCTS5 must support Fallback procedure, e.g. to support processing of unprocessed documents, in case of unavailability of the system, as records in Fallback procedure.

- Performance:
  The system should provide acceptable system response times. The response time of the systems should not exceed 1 second except when communications with external or sub systems take place; however it’s possible for some reports the response time to be more than 1 second.

- Architecture:
  NCTS5 must be a web enabled n-tier based application system.

- Graphing Capabilities – The system is not required to initially implement graphical representation of data with rich user interaction. Still it can be extended to include it.
- Interfacing:
  The system should be able to interface with existing systems using API, Web services and ODBC interfaces.

- Configurability and extensibility:
  NCTS5 system building blocks will be identified and built to support strong extensibility and configurability of the application.

Architectural Assumptions

The following are the assumptions made in defining the architecture of the proposed solution:

- All components of the hardware and the application will be made available within the CARNM data centre.
- Standard data centre equipment such as backup (and restore) infrastructure, monitoring and management environment etc. will be made available within the CARNM data centre.
- The recommended hardware configuration will be based on the fact that the application and database servers will be hosting NOT only the NCTS5 application and the resources could be shared across different systems/applications.
- Users of the system are part of one domain or are part of mutually trusted domains.

Service-Oriented Architecture

Service-Oriented Architecture (SOA) is defined as "the policies, practices, and frameworks that enable application functionality to be provided and consumed as sets of services published at a granularity relevant to the service consumer. Services can be invoked, published and discovered, and are abstracted away from the implementation using a simple, standards-based form of interface."

NCTS5 architecture must be compliant with the above definition of SOA. Web-services protocols will be "standards-based form of interface" for NCTS5. The NCTS5 functionality that is deemed to be of interest to other applications from within CARNM, from the External Domain (including Governmental Domain), will be exposed at appropriate granularity levels via standards-based interfaces. New software applications (even in the next 10 or 20 years) will be able to consume these services and integrate with NCTS5 since their interfaces are based on standards and are not proprietary.

The system should allow CARNM to decide on the level of granularity of the functionality that it will expose by means of Web Services to the External Domain.

Technology solution

The system needs to be designed so that all transactions between trade operators and the Customs administration can be performed via network, using the single-window to access the available on-line services for citizens and companies.

Incremental Model for the software lifecycle

The Incremental model is expected to be used for the software lifecycle.

LOGICAL ARCHITECTURE AND COMPONENTS OF THE SOLUTION

Logical Architecture Summary

Logical architecture for the NCTS5 solution should be built on Presentation, Business, Data Persistence, and Integration tier.

Integration Tier

During its implementation and introduction at CARNM will have to integrate with a number of existing systems at National Domain. During the accession of North Macedonia to the EU, NCTS5 will need to integrate with a number of applications from the Common Domain.

For all software systems from the National Domain, Common Domain, External Domain and Other Government Agencies that NCTS5 needs to be capable of interfacing with, **NCTS5 must provide Service Interfaces and Service gateways**. Integration tier is separate from the implementation of the other tiers: integration with additional software systems and removal of existing integration with software systems will have no implications on the implementations of the other tiers.

Presentation Layer

The presentation layer will provide the application's user interface. NCTS5's user interface (UI) will be browser-based. The presentation layer can be further split into two sub-layers: Server presentation layer and Client presentation layer.

Business Logic Tier

Business logic includes all business rules, data validation, manipulation, processing, and security for NCTS5. The Business Logic Tier enables NCTS5 to separate the business logic and rules from the data or presentation tier. This tier also allows the components to be written once and reused multiple times to serve multiple clients and systems, both internal and external. In accordance to the proposed principle of in-depth security, Business Logic Tier is responsible for enforcing security.

Database Tier

The data tier will consist of an RDBMS database hosted on the database server and will capture and preserve the data of the system. This will be independent of other tiers and the data access components would interface with the database and provide the necessary data to the business tier.

INFRASTRUCTURE AND UTILITY SERVICES

NCTS5 will contain following infrastructure services: Monitoring and logging, Exception management, Authentication and Authorisation, Caching, Configuration, Localisation, Auditing.

Utility services

The utility services logic is accessible by all applications of the NCTS5 System. Following services are foreseen:

- A message storage service allowing storing information, under the form of an XML message, to be fetched later by a correspondent. The service must also allow retrieving this stored message. The system must be capable to keep/store and manage messages in Queue system (e.g. during and after unavailability of the system)
- A mechanism allowing a user to perform a query, possibly generate a report from the result, and to download the result or the report later on.

Reporting Services

NCTS5 must provide to the end-users a number of predefined frequently used reports in the customs domain. CARNM also suggests a reporting tool to be used to enable the ad-hoc creation of reports in NCTS5.

Reports will be available in a variety of formats: Portable Data Format (PDF), Postscript (PS), MS Word, and MS Excel at the very least.

Version management and work packages

Development of NCTS5 as a project, during and after their implementation, must be realized, supported and managed with Versioning - the creation and management of multiple releases of a system, all of which have the same general function but are improved, upgraded or customized.

Backup & restore

NCTS5 system must provide the capability for Backup and Restore. Backup operation can be either manually initiated by operations support staff or automatically performed at regular pre-determined basis as specified by the operation support staff. The backup tools available or/and integrated into the NCTS5 Technical environment (Hardware, RDBMS, System software) could be used. The backup tools available and/or integrated into the NCTS5 technical environment and the technical environment itself will be provided by CARNM.

Archiving

The archiving function allows dividing the state of the application in two partitions between which no data integrity constraints exist. After the archiving operation the first partition of the information is no longer available on-line. It has been removed from the database and saved on another durable storage. This partition is archived. The second partition is still available on-line. The criterion for the division is the validity date of the information. All data no longer valid after the date of archiving is archived.

The archived partition is saved in a format independent of the technical format of the information in the database. The objective is to allow the archived partition to be loaded again in the database

later. At this moment, the structure of the database may have changed but it must always be possible to load the archived data.

Having abovementioned, Data older than pre-defined period should be archived in a different database or different database scheme. CARNM should have access to this data through the different ways (application and/or reports) included in NCTS5.

Implementation of NCTS 5 must be in accordance with the applicable Law regarding the electronic signature, electronic documents, archiving
(ref URL:https://www.mioa.gov.mk/?q=en/documents/legislation)

Exception Management

Exception management consists of catching, throwing, publishing and logging the run-time errors generated by the system. All the errors will be trapped by the specific components where the error originated and will be passed on to the exception management component for publishing and logging. Once the error is trapped, this component will decide on the criticality of the error, log it in event log accordingly and publish a useful error message to the user.

Performance Monitoring

The NCTS5 system must be capable for monitoring of the performance of the application. The business components must trigger the system processes to log the response times and other parameters for each of the functionalities. This should help administrators to make decisions about the state of the system.

Auditing strategy

NCTS5 will provide functionality to log selected changes to a selected set of its entities. Auditing components will be responsible for storing all the required audit related information. Auditing components will record user identity, date and time of change, and the changed data. Auditing can be enabled or disabled on a per-entity basis in NCTS phase 5 at application configuration time. At the same time, for an audited entity, auditing can be further enabled or disabled on a field level.

Domains of the NCTS phase 5

The domains define clear interfaces between the actors involved and divide the responsibility. NCTS phase 5, from system point of view, must support operations on the following domains: External Domain (including governmental domain), the National Domain and the Common Domain.

National Domain

This covers the relationship between the Customs Offices at country level and national system – NCTS5. This domain is under the sole responsibility of the national customs administration concerned.

External Domain (including governmental domain)

This covers the relationship between the national customs administration and traders. This domain is under the sole responsibility of national customs administration concerned. Within the External Domain, traders interact with their national customs administration, which is the body responsible for specifying and setting up the interfaces for them.

For the purpose of data capture by the respective customs office four methods should be considered:

- EDI – Electronic Data Interchange (XML),
- DTI – Direct Trader Input,
- Internet application,
- Data capture by the respective customs office.

Governmental domain covers electronic integrated processes with other government agencies involved in the transit formalities

Common Domain

The NCTS5 shall cover the common transit of goods transported from one contracting party of the Convention on a common transit procedure via or into another contracting party – EU or EFTA country (direct transit). The NCTS5 shall also cover the common transit of goods transported from one contracting party of the Convention on a common transit procedure through third country (neither EU nor EFTA country) via or into another contracting party – EU or EFTA country (indirect transit).

Modes of operation

NCTS5 has to support the existence of at least four environments:

- One production environment
- One test environment
- One training environment
- One development environment

The production, test, training, and development environments must be logically disjoint and independent.

Test application and data, training application and data, development application and data, and production application and data must be separated from each other. On the other hand, the

synchronization of other environments with the production to the level of control of business and technical rules must be implemented and enabled.

It could be possible to switch between the production, testing, training, and development context.

Test environment will be used for testing of a working version of NCTS5 and testing data. Organisations (software developers) from External domain will use the testing environment to test their applications.

Graphical User Interface (GUI)

The graphical interface of the NCTS5 has to meet the following requirements, among others:

The system should have a transparent, legible and easy to navigate GUI. User interface must meet key parameters such as: ergonomic, resistant to user errors, with incorporated filtering mechanism, drop down lists, special on-screen operations and response to end users

Security

Users:

The users of the system should be divided on two groups – Internal Users and External Users.

The internal users are the customs officers involved in the process of the transit processing (National Domain). The internal users will be authenticated in the system by providing username and password. The electronic certificate can be used for user authentication too.

The external users are the users from the External Domain, namely, declarants which lodge customs declaration electronically in the system, employees of other government agencies, or applications from economic operators and other government agencies which consume the web services provided by NCTS5. The e.xternal users can be authenticated in the system with username and password, electronic certificate or both.

Additional information for every system user can be kept in the system.

A link should be established in the system between the external users that represent a juridical person (operator) and their respective juridical person.

A link should be established in the system between the internal users and their customs office and department.

There should be a possibility for activation / deactivation of a user profile. This will allow system administrators respectively to allow / forbid given user(s) to access the system.

The usernames should be unique in the system. It should not be possible to have two different users (system users) with the same username no matter if they belong to the same or different domains.

Access Rights, Roles and Security:

The system should keep a list of predefined access rights (privileges) of Customs officers. For traders we have a authorisation for e-communication with customs authorities. Every access right allows the execution of a given operation or usage of a particular resource in the system. The system should hide the interface elements which lead to an execution of an operation (for example loading of data, executing a business process, saving data modifications and so on) when the user is not in the possession of the privilege responsible for that particular operation.

The system should support manageable user roles of Customs officers. The roles are composed of access rights. A user with the corresponding access rights (system administrator) can add, delete and modify user roles. One or more roles should be assigned to every user in the system.

The system will authorize a user to execute a given action or use particular data if the user is in a role that contains the access right defined (responsible) for this particular action or data.

The authorization for the external users to use certain customs regimes or electronic certificates is decided based on information from the Authorization sub-application. The visibility of user interface elements and the possibility for execution of certain functions could also be realized with the access rights and user roles.

The system must ensure the sound SingleSignOn mechanism within application.

Authentication and Digital Certificates:

User authentication can be done with (i) username and password, and (ii) digital certificates.

For the external domain it is strongly recommended that digital certificates are used for user authentication.

Implementation of NCTS 5 must be in accordance with the applicable Law regarding the electronic documents and services, electronic signature and archiving.
(ref URL:https://www.mioa.gov.mk/?q=en/documents/legislation)

Detailed Security, Monitoring, Auditing and Logging requirements will be defined in the initial phase of project implementation.

Common Domain Security Requirements

This section provides the additional security requirements for NCTS phase 5 in order to enable the specific requirements related to Common Domain:

The Contractor should consider that eCustoms Security Policy principles must be implemented as stated in the ‘eCustoms TES Security Plan’ document.