



2024 Meeting of UN/LOCODE Advisory Group

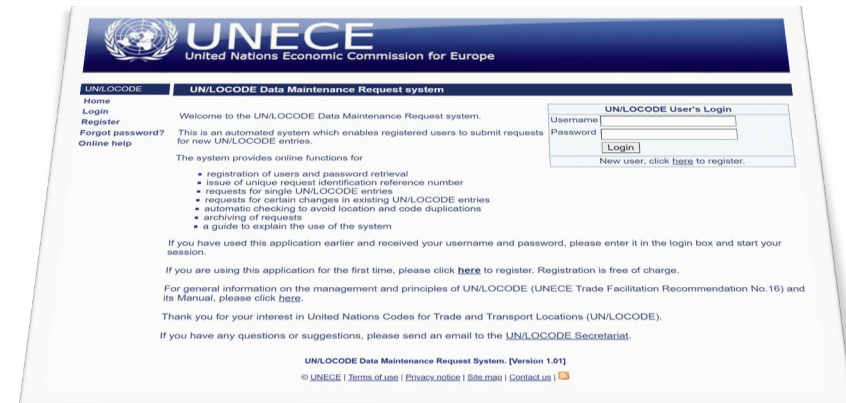
UN/LOCODE Task Force Subgroup 4 Report
Testing of the new re-engineered online DMR application

UN/LOCODE Advisory Group
Hapag-Lloyd AG, Ballindamm 25 Hamburg Germany
16 - 17th April, 2024



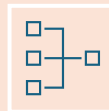
Overview of the presentation:

1. Scope of the group
2. Summary of achievements, activities and discussions
 - Assessments and technical steps.
 - The work plan and what was completed.
3. Recommendations
4. Conclusions





The UN/LOCODE Task Force – Subgroup 4, established in September 2023, initially focused on testing the updated UN/LOCODE Web Frontend Application. Its mandate expanded to include technical exploration for the sustainable development of the UN/LOCODE ecosystem.



UN/LOCODE system consists of three sub-systems: Entry Portal (Subsystem 1), Validation (Subsystem 2), and Directory Publication (Subsystem 3). Subsystem 1 was flagged for cybersecurity non-compliance, posing a threat.



OICT/ISU recommended fixing the critical cybersecurity issues and migrating the entire application to meet modern security standards to meet future expectations.



The UN/LOCODE Task Force – Subgroup 4 meetings were held virtually with 9 to 15 experts from public, private, and NFPs, including technical and policy officers, software developers, and other stakeholders.









The current UN/LOCODE system, including its IT web interface, was developed almost two decades ago. Since then, IT systems, including cyber security needs have evolved considerably. This resulted in a situation where the UN/LOCODE web interface (i.e., the web-based online Data Maintenance Request application), was flagged by the Office of Information and Communications Technology (OICT) as non-compliant with UN cyber security requirements, and the rest of the system has not been audited. This was reflected in the UNECE Executive Secretary Compact assessment for 2021 as well as in para. 24 of [UNLOCODE-AG/2022/INF.2](#).

The system comprises of three (3) sub-systems:

Subsystem 1 – DMR Submission (Entry Portal), Subsystem 2 – DMR Validation, and Subsystem 3 – Directory Publication.

- All three (3/3) of the major critical cybersecurity issues have been fixed, and a few improvements have been implemented.
- UAT Testing and the OICT Cybersecurity Audit passed successfully.
- UNECE is currently filling out the documents to request the security audit of the system.

Issues with the current system can be categorized as:

Critical Cyber Security Vulnerabilities	
Data Quality and Validation Errors	
User Friendliness	
Outdated Business Logic, Workflow and Technical Source Code	

● HIGH ● MEDIUM ● LOW ● LOWEST

21/04/2024

<https://apps.unece.org/unlocode/>



Priority	Importance	Category	Sub-Category	Fix / Functionality	Impact Page(s)	Component(s)	Estimated time for Dev and Test (Days)	Comments
1	Critical	Security	SQL Injection	replace all in-line SQL code with the use of database stored procedures	all pages	web database	14	
2	Critical	Security	user credentials	store the user password as hash (with a salt) in the database. Passwords cannot be retrieved (user will have to create a new password)	register edit user profile forgot password	database	5	
3	Critical	Security	user credentials	enforce password policy (i.e., complexity rules)	register edit user profile forgot password	web database	6	Passwords cannot be retrieved (user will have to create a new password)
4	Critical	Security	Multi-factor authentication	user email multi-factor authentication (verify user's email by user entering emailed random code and system verify it before allowing registration/login/editing user profile)	login register edit user profile	web	6	
5	Improvements	Security	website authentication	add ability to have asp.net forms authentication so that website pages are only accessible if user is authenticated its also possible restrict access of folders via web.config	all pages	web	2	this can be done on web with form-based authentication or directly on web server by Hakan
6	Improvements	Security	Error Handling	Any errors from the system (database and web) should not display the actual (sql) error in the web browser. Browser should only display the fact that an error occurred and display an error internal ID. The actual error and its details should be stored in a database table (internalID, user, time stamp and technical error message).	login logout new DMR Request request DMR change previous history edit user profile register user online help forgot password	database web	5	
7	Improvements	Security	etrade user on database	set proper database server permission for the etrade user (in sql server)	N/A	database	3	The specific permission are to be set directly on database by Hakan. Etrade user should not be able to view the list of databases, nor the list of tables at a min
8	Improvements	Data Quality/Validation	latitude and longitude	add leading zero when necessary, based on expected format	new DMR request	web database	3	





UN/LOCODE Application Re-engineering

- Two Factor Authentication
- Password Security and Complexity
- Hashing and Encryption
- Data Quality - Client-side form field validation
- Testing and Deployment
- UN OICT Cybersecurity Audit Report



Future perspectives – UN/LOCODE Ecosystem

- Peer evaluation of the UN/LOCODE subsystems
- UI Wireframes of proposed changes
- Functional Improvements
 - Integrate interactive geolocation identification
 - Bulk submission template/interface
 - Enhanced Field Validation
- Workflow (DMR submission, maintenance and publications)
- Realtime data exchange (API, SSRS or other web services)
- Complete solution (one-application)





Establishment of the UN/LOCODE Task Force – Subgroup 4 permanently as an Ad hoc Group.



Drafting of a UN/LOCODE ecosystem roadmap towards the development of a complete UN/LOCODE application.



Pilot the implementation of the use of GitHub for UN/LOCODE data lifecycle (DMR submission, Maintenance, and Publication).



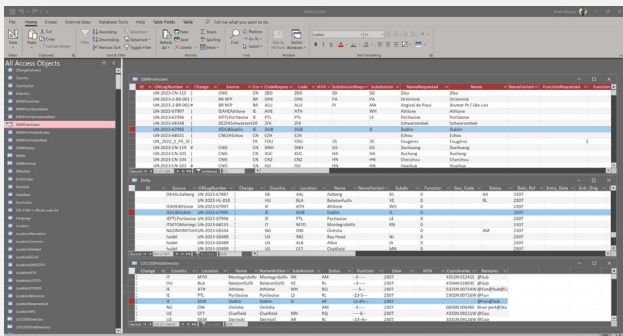
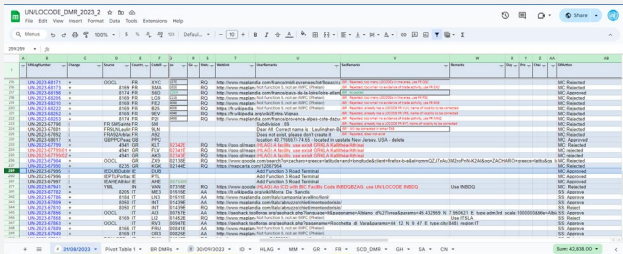
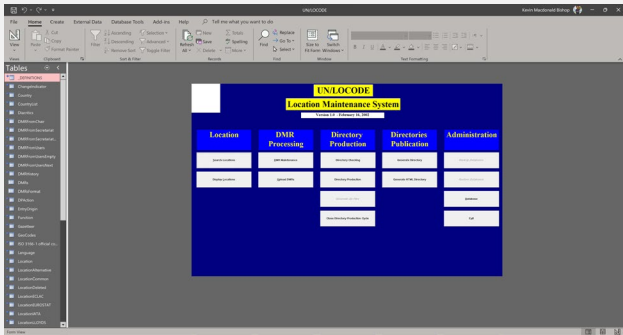
Re-explore the possibility of in-kind contributions of technical assistance to solve critical software issues in the UN/LOCODE subsystems.





- The identification of cybersecurity vulnerabilities prompted comprehensive remediation efforts, presenting us with opportunities to enhance the system and procure crucial resources.
- The recommendations from UN/LOCODE Advisory Group – Subgroup 4 provide a clear actions and options for advancing and evolving the UN/LOCODE ecosystem further.
- Developing an action plan (roadmap) and actively implementing decisions (technical recommendations of Subgroup 4) will contribute significantly to the sustainable growth of the UN/LOCODE ecosystem.





Issue with the UN/LOCODE subsystem 3

The application is not processing function change indicated by the pipe symbol "**|**" or correctly processing **| vs ;** (Further what I found is that when the change request is indicated by the pipe symbol "**|**" the request is correctly processed.)

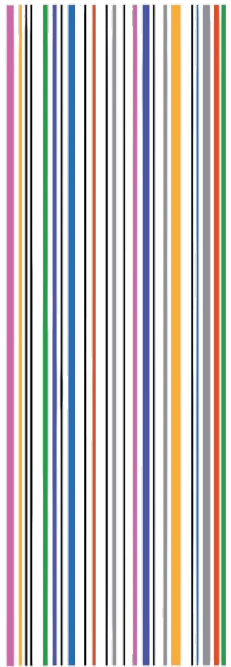
For example: DUB – Dublin request for change denoted by "**|**" in the DMR
 GOOGLE EXCEL SHEET -> IMPORTED INTO THE ACCESS DATA TABLE
"DMRFromUsers" – on post-processing "UploadRequestsToDMRTTable()" to change function to +3+5 it doesn't process, thus appending the table columns "Function Requested and Function".

There is possibly some trimming or conversion of "|**" to "**;**" ??? – DMRFromUsers Data Table contains both occurrences of the symbol.**

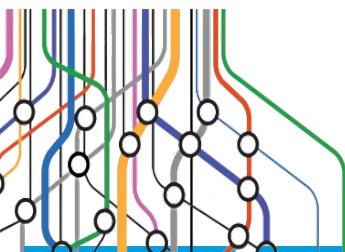
Next steps:

- Create a testing environment with clean data
- Rewrite the function code





UN / CEFAC



[UN/CEFACT website](#)



[UN/LOCODE](#)

CONTACT

**Economic Cooperation and Trade Division
United Nations Economic Commission for Europe
Palais des Nations, CH-1211, Geneva 10, Switzerland
Email: uncefact@un.org**



 A graphic consisting of two overlapping speech bubbles. The front bubble is pink and contains the text "Q&A" in white. The back bubble is yellow.

UN/LOCODE Application Re-engineering

Current UN/LOCODE System Workflow

