Document ID	
0167	
Appendix to	

Title				
Navelink release Notes 0.12.1				
Issued by	*Unit*	*Date*	*Issue*	*Project number*
Navelink		2021-06-21	1	
Approved by		*Classification*		
Anders Wendel		Consortium Unclassified Released Public		

Navelink scheduled maintenance window for v0.12.1 upgrade of Navelink environments

Navelink v0.12.1 upgrade

We have scheduled a maintenance window at 2021/08/23 between 13:00-17:00 CET for upgrading Navelink development and test environment to version 0.12.1. You will not be able to work in the system during parts of this period (please follow navelink.org for precise timings).

Preliminary, we have scheduled a maintenance window at 2021/08/27 between 13:00-17:00 CET for upgrading Navelink operational environment to version 0.12.1. Further notice will follow.

After the upgrade

Please verify system functionality after each of the upgrades, in case of any issues contact us at info@navelink.org and we will assist you.

Navelink v0.12.1 Upgrade plan

- 2021/08/23 13:00-17:00 CET Upgrade Navelink Development environment v0.12.1

- 2021/08/23 13:00-17:00 CET Upgrade Navelink Test environment v0.12.1.

- 2021/08/27 13:00 CET *Upgrade Navelink Operational environment v0.12.1

* If no issues have been discovered between 2021/08/23-2021/08/26 on Navelink DEV and TEST v0.12.1, the OPERATIONAL environment will be upgraded as well.

Document ID	
0167	
Appendix to	

Title				
Navelink release Notes 0.12.1				
Issued by	*Unit*	*Date*	*Issue*	*Project number*
Navelink		2021-06-21	1	
Approved by		*Classification*		
Anders Wendel		Consortium Unclassified Released Public		

Navelink Release Notes v0.12.1

PKI

- Changed extracting certificate from HTTP header to conform with the new default behaviour of how NGINX escapes the certificate

Keycloak SPI Providers

- When converting certificates to tokens non-human attributes like IMO number, etc., are now also added to token
- Align extracting certificate from HTTP header to conform with how NGINX escapes certificates
    - All occurrences of $ssl_client_cert in NGINX config should be replaced with $ssl_client_escaped_cert

Identity Registry

- Made issue certificates with server generated key pairs an optional feature which is disabled by default
- Align extracting certificate from HTTP header to conform with how NGINX escapes certificates
    - All occurrences of $ssl_client_cert in NGINX config should be replaced with $ssl_client_escaped_cert
- The role of any non-human entity now always defaults to the lowest possible role

Portal

- Implemented functionality for generating certificate signing requests which are then used to get certificates from the MIR
    - Implemented optional generation of a PKCS#12 keystore based on the issued certificate
- When issuing a new certificate for an entity the user is given a choice of whether to use the above mentioned features for getting the certificate or to use the "old" method of letting the ID registry generate the key pair and certificate

	Document ID	
	0167	
	Appendix to	

Title				
Navelink release Notes 0.12.1				
Issued by	*Unit*	*Date*	*Issue*	*Project number*
Navelink		2021-06-21	1	
Approved by		*Classification*		
Anders Wendel		Consortium Unclassified Released Public		

- Fixed bug where closing a modal dialogue would not act as expected

Service Registry

- No changes

Additional information

Root certificates can be found:

Public Root Certificate Dev

PEM format for Linux/Curl
https://api.dev.navelink.org/trust-chain.pem
Java Keystore format (password is "changeit")
https://api.dev.navelink.org/trust-chain.jks
Zip-file with .cer filer for easy import in Windows Certificate Store
https://api.dev.navelink.org/trust-chain.zip

Public Root Certificate Test

PEM format for Linux/Curl
https://api.test.navelink.org/trust-chain.pem
Java Keystore format (password is "changeit")
https://api.test.navelink.org/trust-chain.jks
Zip-file with .cer filer for easy import in Windows Certificate Store
https://api.test.navelink.org/trust-chain.zip

Public Root Certificate Operational

PEM format for Linux/Curl
https://api.navelink.org/trust-chain.pem
Java Keystore format (password is "changeit")
https://api.navelink.org/trust-chain.jks
Zip-file with .cer filer for easy import in Windows Certificate Store
https://api.navelink.org/trust-chain.zip