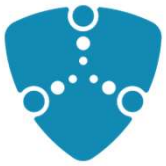


NAVELINK

Issued by	Date
Conceptual team	2023-07-04
Approved by	Classification
	Consortium Unclassified Released Public

Navelink Industry Consortium

HOW-TO Get Public Keys from Navelink

Navelink.org

DocId: 0248
Version: v1.0

HOW-TO Get Public Keys in Navelink

Navelink has now been upgraded with functionality to download public certificates for entities of type Organization, Device, Vessel and Service.

The public certificate contains the public key signed by Navelink and exported in PEM format.

The function follows the Get Public Key defined in SECOM with some minor exceptions.

One purpose may be to download a set of trusted certificates from a trusted source to be used for offline verification of signatures.

Another purpose may be to retrieve receivers public certificate in order to perform a Diffie-Hellman procedure.

Currently it’s open for anyone to use without authentication. Later authentication may be required in order to download the operational certificates. To be discussed.

Get Public Key function

The following HTTPS endpoints has been added in Navelink.

- GET <base URL>/publickey/<mrn>
- GET <base URL>/publickey/<decimal serial number>
- GET <base URL>/publickey/<hex thumbprint in lower case>

Two collection are maintained and possible to download

- GET <base URL>/publickey/pubkey-instances.zip
  Contains all valid public certificates for all registered service instances
- GET <base URL>/publickey/pubkey-vdes.zip
  Contains all valid public certificates for all registered MRN identifiers containing ":vdes:"

Where

- base URL= https://api.dev.navelink.org/v1/publickey/
- base URL= https://api.test.navelink.org/v1/publickey/
- base URL= https://api.navelink.org/v1/publickey/ (not activated yet at this date)

Details

Changes to public certificates are made available every 12th minutes.

- Hence a new issued certificate or a revocation of certificate may take up to 12 minutes before it is available.

If the service is successful, the service returns 200 and all valid certificates in PEM format.
If certificate cannot be found, the service returns 404 Not found.

A request using MRN may result in 0 to many valid certificates in same response.
A request to serial number or thumbprint may result in 0 to 1 valid certificate.

The ZIP-files contains PEM file for each MRN containing all valid certificates for the entity.

Examples

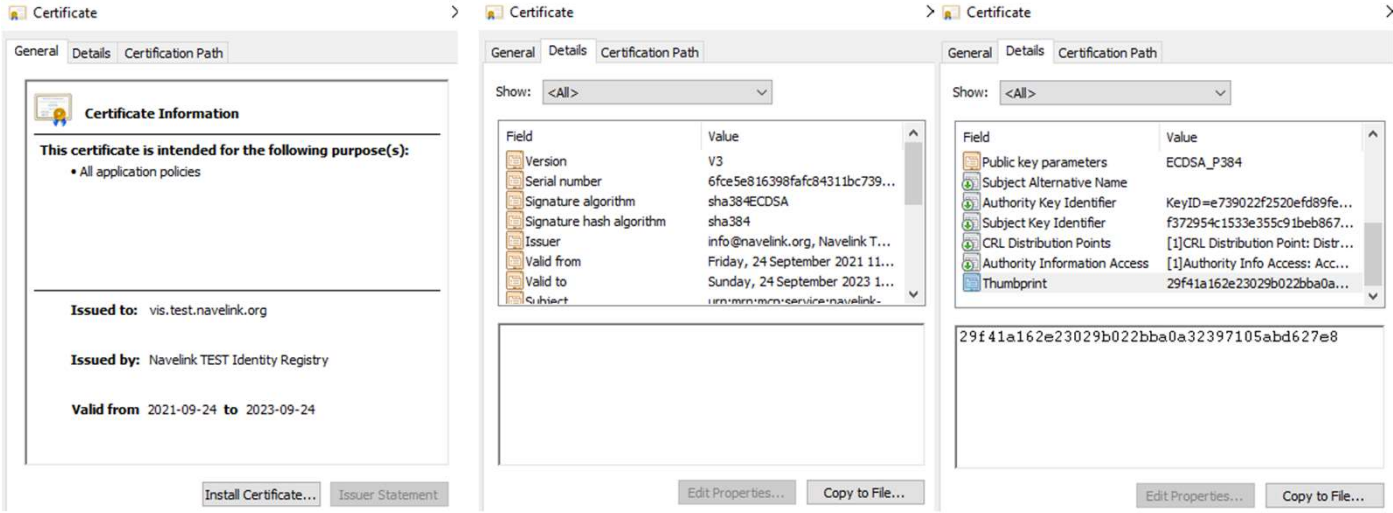
Get Public Key for MRN

GET https://api.test.navelink.org/v1/publickey/urn:mrn:mcp:service:navelink-test:navelink:instance:vis:verificationservice

Response

-----BEGIN CERTIFICATE-----
MIIE0zCCBFmgAwIBAgIUb85egWOY+vyEMRvHOUZZg0I8R94wCgYIKoZIzj0EAwMw
gf4xOzA5BgoJkiaJk/IsZAEBDCt1cm46bXJuOm1jcDpjYTpuYXZlbGluay10ZXN0
Om5hdmVsaW5rLWlkcmVnMQswCQYDVQQGEwJTRTEPMA0GA1UECAwGU3dlZGVuMRAw
DgYDVQQHDAdWw6R4asO2MSUwIwYDVQQKDBxOYXZlbGluayBJbmR1c3RyeSBDb25z
b3J0aXVtMRwwGgYDVQQLDBNOYXZlbGluayBPcGVyYXRpb25zMSgwJgYDVQQDDB9O
YXZlbGluayBURVNUIElkZW50aXR5IFJlZ2lzdHJ5MSAwHgYJKoZIhvcNAQkBFhFp
bmZvQG5hdmVsaW5rLm9yZzAeFw0yMTA5MjQwOTE4MjFaFw0yMzA5MjQwOTE4MjFa
MIHNMQswCQYDVQQGEwJTRTEvMC0GA1UECgwmdXJuOm1ybjptY3A6b3JnOm5hdmVs
aW5rLXRlc3Q6bmF2ZWxpbmsxEDAOBgNVBAsMB3NlcnZpY2UxHjAcBgNVBAMMFXZp
cy50ZXN0Lm5hdmVsaW5rLm9yZzFbMFkGCgmSJomT8ixkAQEMS3Vybjptcm46bWNw
OnNlcnZpY2U6bmF2ZWxpbmstdGVzdDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVy
aWZpY2F0aW9uc2VydmljZTB2MBAGByqGSM49AgEGBSuBBAAiA2IABAYtZ443gGrH
hRTdiZneuEe0zpe1H2hX3lnOrhNgxIVm5M/WtLKeRvlMvWm1PKfJR5zf7GraWG4N
CVAMhkJhxLsqOhsPlZdsggUfi7c8tn/AJbKM6QxNtXQvbPoVsO/ZE6OCAcUwggHB
MIGlBgNVHREEgYAwfolVdmlzLnRlc3QubmF2ZWxpbmsub3JnoGUGFGmDmLzXwJ7w
8MfLqp2AgKqu14oboE0MS3Vybjptcm46bWNwOnNlcnZpY2U6bmF2ZWxpbmstdGVz
dDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVyaWZpY2F0aW9uc2VydmljZTAfBgNV
HSMEGDAWgBTnOQIvJSDv2J/htv1/2L4VoJUUSzAdBgNVHQ4EFgQU83KVTBUz41XJ
G+uGfJdzaur74AgwcwYDVR0fBGwwajBooGagZlZiaHR0cDovL2FwaS50ZXN0Lm5h
dmVsaW5rLm9yZy94NTA5L2FwaS9jZXJ0aWZpY2F0ZXMvY3JsL3Vybjptcm46bWNw
OmNhOm5hdmVsaW5rLXRlc3Q6bmF2ZWxpbmstaWRyZWcwfwYIKwYBBQUHAQEEczBx
MG8GCCsGAQUFBzABhmNodHRwOi8vYXBpLnRlc3QubmF2ZWxpbmsub3JnL3g1MDkv
YXBpL2NlcnRpZmljYXRlcy9vY3NwL3Vybjptcm46bWNwOmNhOm5hdmVsaW5rLXRl
c3Q6bmF2ZWxpbmstaWRyZWcwCgYIKoZIzj0EAwMDaAAwZQIxAM9xcuDdpK4dqv80
LLNNVA2KGLP0eN4bO1jeTakTZ/KwjVZiEw7KlgJ3ju7SYSQyZAlwWyqdVK5GQCe9
vyMtv7LyVre7rpGSDYaJDgNDlsR4y41C4yJj7akDDfehItbbRIM1
-----END CERTIFICATE-----

Opened in Microsoft Certificate Installer it looks like



NAVELINK

Examples

Get Public Key for Certificate Serial Number

GET https://api.test.navelink.org/v1/publickey/638300161656034305135295119391354453166875494366

Response

-----BEGIN CERTIFICATE-----
MIIE0zCCBFmgAwIBAgIUb85egWOY+vyEMRvHOUZZg0I8R94wCgYIKoZIzj0EAwMw
gf4xOzA5BgoJkiaJk/IsZAEBDCt1cm46bXJuOm1jcDpjYTpuYXZlbGluay10ZXN0
Om5hdmVsaW5rLWlkcmVnMQswCQYDVQQGEwJTRTEPMA0GA1UECAwGU3dlZGVuMRAw
DgYDVQQHDAdWw6R4asO2MSUwIwYDVQQKDBxOYXZlbGluayBJbmR1c3RyeSBDb25z
b3J0aXVtMRwwGgYDVQQLDBNOYXZlbGluayBPcGVyYXRpb25zMSgwJgYDVQQDDB9O
YXZlbGluayBURVNUIElkZW50aXR5IFJlZ2lzdHJ5MSAwHgYJKoZIhvcNAQkBFhFp
bmZvQG5hdmVsaW5rLm9yZzAeFw0yMTA5MjQwOTE4MjFaFw0yMzA5MjQwOTE4MjFa
MIHNMQswCQYDVQQGEwJTRTEvMC0GA1UECgwmdXJuOm1ybjptY3A6b3JnOm5hdmVs
aW5rLXRlc3Q6bmF2ZWxpbmsxEDAOBgNVBAsMB3NlcnZpY2UxHjAcBgNVBAMMFXZp
cy50ZXN0Lm5hdmVsaW5rLm9yZzFbMFkGCgmSJomT8ixkAQEMS3Vybjptcm46bWNw
OnNlcnZpY2U6bmF2ZWxpbmstdGVzdDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVy
aWZpY2F0aW9uc2VydmljZTB2MBAGByqGSM49AgEGBSuBBAAiA2IABAYtZ443gGrH
hRTdiZneuEe0zpe1H2hX3lnOrhNgxIVm5M/WtLKeRvlMvWm1PKfJR5zf7GraWG4N
CVAMhkJhxLsqOhsPlZdsggUfi7c8tn/AJbKM6QxNtXQvbPoVsO/ZE6OCAcUwggHB
MIGlBgNVHREEgYAwfoIVdmlzLnRlc3QubmF2ZWxpbmsub3JnoGUGFGmDmLzXwJ7w
8MfLqp2AgKqu14oboE0MS3Vybjptcm46bWNwOnNlcnZpY2U6bmF2ZWxpbmstdGVz
dDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVyaWZpY2F0aW9uc2VydmljZTAfBgNV
HSMEGDAWgBTnOQIvJSDv2J/htv1/2L4VoJUUSzAdBgNVHQ4EFgQU83KVTBUz41XJ
G+uGfJdzaur74AgwcwYDVR0fBGwwajBooGagZIZiaHR0cDovL2FwaS50ZXN0Lm5h
dmVsaW5rLm9yZy94NTA5L2FwaS9jZXJ0aWZpY2F0ZXMvY3JsL3Vybjptcm46bWNw
OmNhOm5hdmVsaW5rLXRlc3Q6bmF2ZWxpbmstaWRyZWcwfwYIKwYBBQUHAQEEczBx
MG8GCCsGAQUFBzABhmNodHRwOi8vYXBpLnRlc3QubmF2ZWxpbmsub3JnL3g1MDkv
YXBpL2NlcnRpZmljYXRlcy9vY3NwL3Vybjptcm46bWNwOmNhOm5hdmVsaW5rLXRl
c3Q6bmF2ZWxpbmstaWRyZWcwCgYIKoZIzj0EAwMDaAAwZQIxAM9xcuDdpK4dqv80
LLNNVA2KGLP0eN4bO1jeTakTZ/KwjVZiEw7KlgJ3ju7SYSQyZAlwWyqdVK5GQCe9
vyMtv7LyVre7rpGSDYaJDgNDlsR4y41C4yJj7akDDfehltbbRIM1
-----END CERTIFICATE-----

Examples

Get Public Key for Certificate Thumbprint

GET https://api.test.navelink.org/v1/publickey/29f41a162e23029b022bba0a32397105abd627e8

Response

-----BEGIN CERTIFICATE-----
MIIE0zCCBFmgAwIBAgIUb85egWOY+vyEMRvHOUZZg0I8R94wCgYIKoZIzj0EAwMw
gf4xOzA5BgoJkiaJk/IsZAEBDCt1cm46bXJuOm1jcDpjYTpuYXZlbGluay10ZXN0
Om5hdmVsaW5rLWIkcmVnMQswCQYDVQQGEwJTRTEPMA0GA1UECAwGU3dlZGVuMRAw
DgYDVQQHDAdWw6R4asO2MSUwIwYDVQQKDBxOYXZlbGluayBJbmR1c3RyeSBDb25z
b3J0aXVtMRwwGgYDVQQLDBNOYXZlbGluayBPcGVyYXRpb25zMSgwJgYDVQQDDB9O
YXZlbGluayBURVNUIElkZW50aXR5IFJlZ2lzdHJ5MSAwHgYJKoZIhvcNAQkBFhFp
bmZvQG5hdmVsaW5rLm9yZzAeFw0yMTA5MjQwOTE4MjFaFw0yMzA5MjQwOTE4MjFa
MIHNMQswCQYDVQQGEwJTRTEvMC0GA1UECgwmdXJuOm1ybjptY3A6b3JnOm5hdmVs
aW5rLXRlc3Q6bmF2ZWxpbmsxEDAOBgNVBAsMB3NlcnZpY2UxHjAcBgNVBAMMFXZp
cy50ZXN0Lm5hdmVsaW5rLm9yZzFbMFkGCgmSJomT8ixkAQEMS3Vybjptcm46bWNw
OnNlcnZpY2U6bmF2ZWxpbmstdGVzdDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVy
aWZpY2F0aW9uc2VydmljZTB2MBAGByqGSM49AgEGBSuBBAAiA2IABAYtZ443gGrH
hRTdiZneuEe0zpe1H2hX3lnOrhNgxIVm5M/WtLKeRvlMvWm1PKfJR5zf7GraWG4N
CVAMhkJhxLsqOhsPlZdsggUfi7c8tn/AJbKM6QxNtXQvbPoVsO/ZE6OCAcUwggHB
MIGlBgNVHREEgYAwfoIVdmlzLnRlc3QubmF2ZWxpbmsub3JnoGUGFGmDmLzXwJ7w
8MfLqp2AgKqu14oboE0MS3Vybjptcm46bWNwOnNlcnZpY2U6bmF2ZWxpbmstdGVz
dDpuYXZlbGluazppbnN0YW5jZTp2aXM6dmVyaWZpY2F0aW9uc2VydmljZTAfBgNV
HSMEGDAWgBTnOQIvJSDv2J/htv1/2L4VoJUUSzAdBgNVHQ4EFgQU83KVTBUz41XJ
G+uGfJdzaur74AgwcwYDVR0fBGwwajBooGagZIZiaHR0cDovL2FwaS50ZXN0Lm5h
dmVsaW5rLm9yZy94NTA5L2FwaS9jZXJ0aWZpY2F0ZXMvY3JsL3Vybjptcm46bWNw
OmNhOm5hdmVsaW5rLXRlc3Q6bmF2ZWxpbmstaWRyZWcwfwYIKwYBBQUHAQEEczBx
MG8GCCsGAQUFBzABhmNodHRwOi8vYXBpLnRlc3QubmF2ZWxpbmsub3JnL3g1MDkv
YXBpL2NlcnRpZmljYXRlcy9vY3NwL3Vybjptcm46bWNwOmNhOm5hdmVsaW5rLXRl
c3Q6bmF2ZWxpbmstaWRyZWcwCgYIKoZIzj0EAwMDaAAwZQIxAM9xcuDdpK4dqv80
LLNNVA2KGLP0eN4bO1jeTakTZ/KwjVZiEw7KlgJ3ju7SYSQyZAlwWyqdVK5GQCe9
vyMtv7LyVre7rpGSDYaJDgNDlsR4y41C4yJj7akDDfehltbbRIM1
-----END CERTIFICATE-----

Examples

Get Public Key collection for Service Instances

GET https://api.test.navelink.org/v1/publickey/pubkey-instances.zip

Response

Application/zip

Get Public Key collection for :vdes: MRN entities

GET https://api.test.navelink.org/v1/publickey/pubkey-vdes.zip

Response

Application/zip

Feedback, Issues and Change Requests

- The Get Public Key by thumbprint differs from SECOM.
  SECOM describes the thumbprint in Base64 format but here we use lower case HEX format as given by OpenSSL and shown in Microsoft Certificate Handler. MCP MIR returns the thumbprint in Base64.
  Need to be discussed what format is best to use.
- No authentication required
  Currently there is no requirement to authenticate yourself for accessing the Get Public Key.
  This may be changed in the final version.
  Need to be discussed further.
- Expired and revoked certificates cannot be downloaded
  Is this an issue?
- Certificates for User entity cannot be downloaded
  Mostly due to GDPR and the possibility to retrieve personal emails etc. in other organizations.
  Is this an issue?
- The VDES certificate collection is based on the MRN sub-namespace :vdes: used by the registrator of the entity.
  This is not a formally agreed requirement but could be stated as a guideline (not documented today).
  The consequence however is that this collection may not be complete if guideline is not followed.