SECOM Test Project

Test report

Draft version

Content

[1 SECOM Test Project 6](#_Toc68092769)

[1.1 Purpose and expected outcome 6](#_Toc68092770)

[1.2 General 6](#_Toc68092771)

[1.3 Examples of questions 7](#_Toc68092772)

[1.4 Overview of Test Objectives 8](#_Toc68092773)

[1.5 Overview of Test Cases 9](#_Toc68092774)

[2 Observations 10](#_Toc68092775)

[3 Testbed 13](#_Toc68092776)

[3.1 General 13](#_Toc68092777)

[3.2 Testbed A 13](#_Toc68092778)

[3.2.1 Description 13](#_Toc68092779)

[3.2.2 Functionality in the testbed 14](#_Toc68092780)

[3.3 Testbed B 15](#_Toc68092781)

[3.3.1 Description 15](#_Toc68092782)

[3.3.2 Functionality in the testbed 15](#_Toc68092783)

[3.3.3 Requirements and input 15](#_Toc68092784)

[3.4 Testbed C 16](#_Toc68092785)

[3.4.1 Description 16](#_Toc68092786)

[3.4.2 Functionality in the testbed 16](#_Toc68092787)

[4 Test Case 1 - Data protection (signing) of unclassified data 18](#_Toc68092788)

[4.1 Description 18](#_Toc68092789)

[4.1.1 Test objectives 18](#_Toc68092790)

[4.1.2 Acceptance Criteria 18](#_Toc68092791)

[4.1.3 Test Scenarios 18](#_Toc68092792)

[4.1.4 Test Environment 18](#_Toc68092793)

[4.1.5 Test tools 18](#_Toc68092794)

[4.1.6 Test data 18](#_Toc68092795)

[4.1.7 Test procedure 18](#_Toc68092796)

[4.2 Test results and discussions 20](#_Toc68092797)

[4.3 Conclusions and Recommendations 21](#_Toc68092798)

[5 Test Case 2 - Data protection of classified data (signing and encryption) 22](#_Toc68092799)

[5.1 Description 22](#_Toc68092800)

[5.1.1 Test objectives 22](#_Toc68092801)

[5.1.2 Acceptance Criteria 22](#_Toc68092802)

[5.1.3 Test Scenarios 22](#_Toc68092803)

[5.1.4 Test Environment 22](#_Toc68092804)

[5.1.5 Test tools 22](#_Toc68092805)

[5.1.6 Test data 22](#_Toc68092806)

[5.1.7 Test procedure 22](#_Toc68092807)

[5.2 Test results and discussions 23](#_Toc68092808)

[5.3 Conclusions and Recommendations 23](#_Toc68092809)

[6 Test Case 3 – SECOM PKI 24](#_Toc68092810)

[6.1 Description 24](#_Toc68092811)

[6.1.1 Test objectives 24](#_Toc68092812)

[6.1.2 Acceptance Criteria 24](#_Toc68092813)

[6.1.3 Test Scenarios 24](#_Toc68092814)

[6.1.4 Test Environment 24](#_Toc68092815)

[6.1.5 Test tools 24](#_Toc68092816)

[6.1.6 Test data 24](#_Toc68092817)

[6.1.7 Test procedure 24](#_Toc68092818)

[6.2 Test results and discussions 25](#_Toc68092819)

[6.3 Conclusions and Recommendations 25](#_Toc68092820)

[7 Test Case 4 – Exchange large data 26](#_Toc68092821)

[7.1 Description 26](#_Toc68092822)

[7.2 Targeted questions 26](#_Toc68092823)

[7.3 Test Functionality 26](#_Toc68092824)

[7.4 Test Variables 26](#_Toc68092825)

[7.5 Testbed 26](#_Toc68092826)

[7.6 Test Sequence 26](#_Toc68092827)

[7.7 Test results and discussions 29](#_Toc68092828)

[7.8 Conclusions and Recommendations 29](#_Toc68092829)

[8 Test Case 5 – Exchange compressed data 29](#_Toc68092830)

[8.1 Description 29](#_Toc68092831)

[8.1.1 Test objectives 29](#_Toc68092832)

[8.1.2 Acceptance Criteria 29](#_Toc68092833)

[8.1.3 Test Scenarios 29](#_Toc68092834)

[8.1.4 Test Environment 29](#_Toc68092835)

[8.1.5 Test tools 30](#_Toc68092836)

[8.1.6 Test data 30](#_Toc68092837)

[8.1.7 Test procedure 30](#_Toc68092838)

[8.2 Test results and discussions 31](#_Toc68092839)

[8.3 Conclusions and Recommendations 31](#_Toc68092840)

[9 Test Case 6 – Closed loop communication 32](#_Toc68092841)

[9.1 Description 32](#_Toc68092842)

[9.1.1 Test objectives 32](#_Toc68092843)

[9.1.2 Acceptance Criteria 32](#_Toc68092844)

[9.1.3 Test Scenarios 32](#_Toc68092845)

[9.1.4 Test Environment 32](#_Toc68092846)

[9.1.5 Test tools 32](#_Toc68092847)

[9.1.6 Test data 32](#_Toc68092848)

[9.1.7 Test procedure 32](#_Toc68092849)

[9.2 Test results and discussions 33](#_Toc68092850)

[9.3 Conclusions and Recommendations 33](#_Toc68092851)

[10 Test Case 7 – Subscribe to data 34](#_Toc68092852)

[10.1 Description 34](#_Toc68092853)

[10.1.1 Test objectives 34](#_Toc68092854)

[10.1.2 Acceptance Criteria 34](#_Toc68092855)

[10.1.3 Test Scenarios 34](#_Toc68092856)

[10.1.4 Test Environment 34](#_Toc68092857)

[10.1.5 Test tools 34](#_Toc68092858)

[10.1.6 Test data 34](#_Toc68092859)

[10.1.7 Test procedure 34](#_Toc68092860)

[10.2 Test results and discussions 35](#_Toc68092861)

[10.3 Conclusions and Recommendations 35](#_Toc68092862)

[11 Test Case 8 – Service information 36](#_Toc68092863)

[11.1 Description 36](#_Toc68092864)

[11.1.1 Test objectives 36](#_Toc68092865)

[11.1.2 Acceptance Criteria 36](#_Toc68092866)

[11.1.3 Test Scenarios 36](#_Toc68092867)

[11.1.4 Test Environment 36](#_Toc68092868)

[11.1.5 Test tools 36](#_Toc68092869)

[11.1.6 Test data 36](#_Toc68092870)

[11.1.7 Test procedure 36](#_Toc68092871)

[11.2 Test results and discussions 37](#_Toc68092872)

[11.3 Conclusions and Recommendations 37](#_Toc68092873)

[12 Test Case 9 – Service status 38](#_Toc68092874)

[12.1 Description 38](#_Toc68092875)

[12.1.1 Test objectives 38](#_Toc68092876)

[12.1.2 Acceptance Criteria 38](#_Toc68092877)

[12.1.3 Test Scenarios 38](#_Toc68092878)

[12.1.4 Test Environment 38](#_Toc68092879)

[12.1.5 Test tools 38](#_Toc68092880)

[12.1.6 Test data 38](#_Toc68092881)

[12.1.7 Test procedure 38](#_Toc68092882)

[12.2 Test results and discussions 39](#_Toc68092883)

[12.3 Conclusions and Recommendations 39](#_Toc68092884)

[13 Test Case 10 - Cyber Security Review 40](#_Toc68092885)

[13.1 Description 40](#_Toc68092886)

[13.2 Targeted questions 40](#_Toc68092887)

[13.3 Test Functionality 40](#_Toc68092888)

[13.4 Test Variables 41](#_Toc68092889)

[13.5 Testbed 41](#_Toc68092890)

[13.6 Test Sequence 41](#_Toc68092891)

[13.7 Test results and discussions 41](#_Toc68092892)

[13.7.1 Observations 41](#_Toc68092893)

[13.8 Conclusions and Recommendations 41](#_Toc68092894)

[14 Test Case 11 – White list and access request 42](#_Toc68092895)

[14.1 Description 42](#_Toc68092896)

[14.1.1 Test objectives 42](#_Toc68092897)

[14.1.2 Acceptance Criteria 42](#_Toc68092898)

[14.1.3 Test Scenarios 42](#_Toc68092899)

[14.1.4 Test Environment 42](#_Toc68092900)

[14.1.5 Test tools 42](#_Toc68092901)

[14.1.6 Test data 42](#_Toc68092902)

[14.1.7 Test procedure 42](#_Toc68092903)

[14.2 Test results and discussions 43](#_Toc68092904)

[14.3 Conclusions and Recommendations 43](#_Toc68092905)

[15 Test Case 12 – Service Discovery 43](#_Toc68092906)

[15.1 Description 43](#_Toc68092907)

[15.2 Targeted questions 44](#_Toc68092908)

[15.3 Test Functionality 44](#_Toc68092909)

[15.4 Test Variables 44](#_Toc68092910)

[15.5 Testbed 44](#_Toc68092911)

[15.6 Test Sequence 46](#_Toc68092912)

[15.7 Test results and discussions 46](#_Toc68092913)

[15.8 Conclusions and Recommendations 46](#_Toc68092914)

[16 Test Case 13 – Exchange of several different payloads 46](#_Toc68092915)

[16.1 Description 46](#_Toc68092916)

[16.1.1 Test objectives 46](#_Toc68092917)

[16.1.2 Acceptance Criteria 46](#_Toc68092918)

[16.1.3 Test Scenarios 46](#_Toc68092919)

[16.1.4 Test Environment 46](#_Toc68092920)

[16.1.5 Test tools 47](#_Toc68092921)

[16.1.6 Test data 47](#_Toc68092922)

[16.1.7 Test procedure 47](#_Toc68092923)

[16.2 Test results and discussions 48](#_Toc68092924)

[16.3 Conclusions and Recommendations 48](#_Toc68092925)

[17 ANNEX A Participant (SMA) 49](#_Toc68092926)

[17.1 Planning 49](#_Toc68092927)

[17.1.1 Schedule 49](#_Toc68092928)

[17.1.2 Input 49](#_Toc68092929)

[17.2 APPENDIX SECOM Test Project SMA Report 50](#_Toc68092930)

[18 ANNEX B Participant (Saab) 50](#_Toc68092931)

[18.1 Planning 50](#_Toc68092932)

[18.1.1 Schedule 50](#_Toc68092933)

[18.1.2 Input 50](#_Toc68092934)

[18.2 APPENDIX SECOM Test Project SAAB Report 51](#_Toc68092935)

[19 ANNEX C Participant (StormGeo) 52](#_Toc68092936)

[19.1 Planning 52](#_Toc68092937)

[19.1.1 Schedule 52](#_Toc68092938)

[19.1.2 Input 52](#_Toc68092939)

[19.2 APPENDIX SECOM Test Project StormGeo Report 52](#_Toc68092940)

# SECOM Test Project

## Purpose and expected outcome

The purpose is to challenge the IEC 63173-2 SECOM standard draft and provide feedback to WG17. The purpose is also to get more experience and example data of actually implementing the standard.

The expected outcomes from the project are

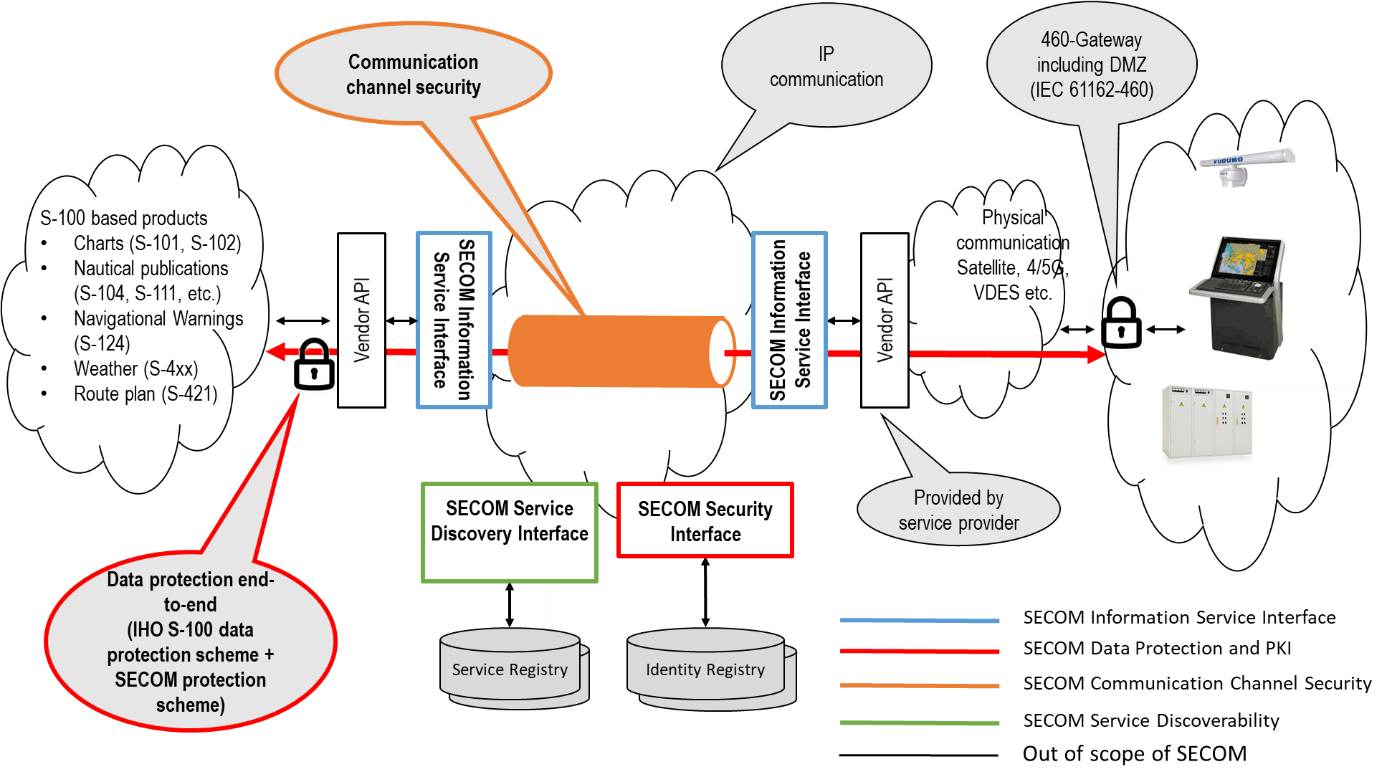
* feedback with recommendations to WG17 for improvement and stabilizing the SECOM standard. Completeness, Correctness, Consistency
* demonstrator, but not the primary goal
* example data and example commands, (tbd which example data that is of later use)
* bonus if the outcome is data and even a “simulator” or “reference service” that can support “Test methods and expected result” clauses and how a party can test if their equipment is compliant with SECOM

## General

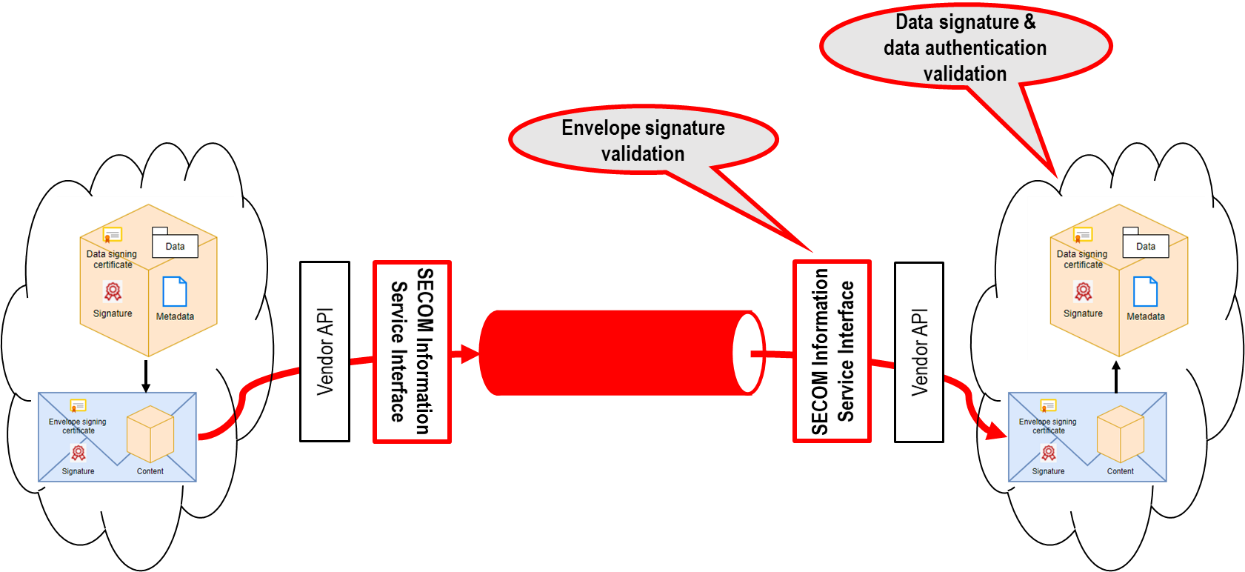
SECOM standard is expected to be as standalone as possible, yet aligned with other standards. And standalone means here that a user shall be able to implement secure exchange and communication of S-100 based products based on the IEC 63173-2 SECOM standard document.

SECOM specifies service interfaces (APIs) for data exchange, data protection measures to enable secure communication and interfaces for service discoverability. SECOM is applicable for S-100 based products but also other data (payload) formats are supported i.e. SECOM is generally independent of which data type is exchanged.

SECOM contains several parts or components that are needed to achieve secure exchange, but different parties will implement different parts/components into their product, and by nature an exchange involves at least two parties where one is sending and one is receiving, and in many cases the roles changes during an interaction and most parties will most likely need to implement the SECOM as both sender and receiver (provider and consumer of information).



Description of below figure…TBD



## Examples of questions

1. How does the signing request to SECOM PKI work?
2. What are the SECOM requirements for the asymmetric keys in PKI?
3. What are the SECOM requirements for the encryption key
4. How exchange the encryption key?
5. How use keys from e.g. PRIMAR with SECOM solution?
6. How relate keys for signing data to keys for TLS encryption? E.g. for a ship, for a VTS.
7. Shall SECOM Communication Channel Security and service authentication be based on TLS and X.509 Certificates or OpenID, HMAC or other standard using the HTTP Headers instead?
8. What are the requirements, and are the met, on SECOM Service Discovery Interface?

## Overview of Test Objectives

The following Test Objectives have been identified as candidates for SECOM Test Project.

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Objective** | **Description/ rationale** | **SECOM solution** | **Test case(s)** |
| 1. Message integrity | Ensures the complete message is unchanged between SECOM services | Envelope signing | 1 |
| 1. Data integrity\* | Data integrity ensures the data transmitted is accurate and consistent | Data signing | 1 |
| 1. Transport confidentiality | Ensure communication channel protection between SECOM services | Channel encryption (TLS) | 1, 2 |
| 1. Data protection | Data protection ensures information is confidential except for the intended recipient | Data encryption (AES) | 2 |
| 1. Service identity | Support SECOM service identification | Service certificate authentication (X.509 PKI) | 1, 3 |
| 1. Client identity\* | Support client identification | End user client certificate authentication (X.509 PKI) | 1, 3 |
| 1. Client authorization | Facilitate client access to information | Service authorization | 11 |
| 1. Bandwidth optimization | Minimize size of data package sent to reduce required bandwidth | Data compression (GZIP, Deflate) | 5 |
| 1. Large message transfer | Facilitate large message transfer i.e. message sizes > 350 kB | Link to data facilitated by interfaces Upload Link, Get By Link | 4 |
| 1. Closed loop communication | Notification of message received/ read etc. to ensure dialogue between end-user applications. | Acknowledgement message (acknowledgement interface) | 6 |
| 1. Service discoverability | Search for services by means of service metadata. In order to locate relevant services for consumption. | Service registry lookup (Search Service interface) | 12 |
| 1. Information push | Share information by uploading data to a service | Service interface to receive uploaded information (Upload interface) | 2 |
| 1. Information pull | Retrieve information by downloading data from a service | Service interface to retrieve information (Get interface) | 1 |
| 1. Subscribe to data | Subscribe to information to receive subsequent updates | Service interfaces for Subscription request, remove & notify | 7 |
| 1. Service information | To facilitate information wrt service accepted payloads and endpoints | Service capability interface | 8 |
| 1. Service condition | Contextual service status to check service operation. | Ping interface for checking last interactionTime with end user application and SECOM service status | 9 |
| 1. Payload agnostic service | Caters for exchanging payloads of different types | To be investigated | 13 |

\* Data integrity and client identity test objectives are only relevant if SECOM PKI is used for end user client certificates.

## Overview of Test Cases

The following Test Cases have been identified to cover previously described test objectives.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test Case** | **Name** | **Interface** | **Document Reference** | **Test objects** | **Testbed target** |
| Test Case 1 | Data protection of unclassified data (signing) | Upload | 5.7.2, 6, 7.3 | 1, 2, 3, 5, 6, 13 | Testbed B |
| Test Case 2 | Data protection of classified data (signing and encryption) | Get, EncryptionKey | 5.7.2, 6, 7.3, 7.4, 7.5 | 1, 2, 3, 4, 5, 6, 12 | Testbed B |
| Test Case 3 | SECOM PKI |  | 8 |  | Testbed B |
| Test Case 4 | Exchange Large Data | Upload Link, Get By Link | 5.6.4 + 5.6.8 | 9 | Testbed B |
| Test Case 5 | Exchange compressed data | Upload | 7.2 | 8 | Testbed B |
| Test Case 6 | Closed loop communication | Acknowledgement | 5.7.4 | 10 | Testbed B |
| Test Case 7 | Subscribe to data | Subscription request, remove & notify | 5.7.10, 5.7.11, 5.7.12 | 14 | Testbed B |
| Test Case 8 | Service information | Capability | 5.7.13 | 15 | Testbed B |
| Test Case 9 | Service status | Ping | 5.7.14 | 16 | Testbed B |
| Test Case 10 | Cyber Security Review |  | 4 + 6 + 7 + (5) |  | Testbed B |
| Test Case 11 | White list and access request |  | 5 + Annex D/E | 7 | Testbed B |
| Test Case 12 | Service Discovery | Search Service | 9 | 11 | Testbed B |
| Test Case 13 | Exchange several different types of payloads | Capability, Upload, Get | ? | 17 | Testbed C |

# Observations

| Num | Ref number | Observation | Found when … | Consequence/Proposal | Reference in SECOM Document |
| --- | --- | --- | --- | --- | --- |
| 001 | SMA-001  STT-001 | Converting signature to HEX may add carriage return signs, but it can also be on one line  Today not described in SECOM | Building Testbed A | 1. affects the JSON or XML 2. affects interoperability   Need to be described in SECOM. | 7.3 Data Protection |
| 002 | STT-002 | Data may need padding if shorter than signing key  Today not described in SECOM |  |  | 7.3 Data Protection |
| 003 | SMA-002 | SECOM v20xx is missing description of what to sign.  Q: What if the data is compressed? converted to Base64? Encrypted?  Shall the original data file always be signed? Or shall the file prepared for transfer be signed? | Building Testbed A | The different alternatives is elaborated in 4.7.1 Discussion: What shall be signed? | 7.3 Data Protection  5 Information Service Interface |
| 004 | SMA-003 | Update Link and Get By Link is not well defined in the document | Building Testbed B and the swagger file | Impact on the swagger file | Interface Upload Link and Get By Link |
| 005 | SMA-004 | It may be a security risk to exchange a URL to any external storage/web page | Building Testbed B and the swagger file | One approach could be that instead of uploading a URL, an identifier is uploaded, and then Get can be used to retrieve the object attached to the identifier. | Interface Upload Link and Get By Link |
|  | SMA-006 | Should both ResponseObject and Error ResponseObject be defined for every REST interface? | Building Testbed B and the swagger file | Removed when moved to Specification part.  But it may need to be defined for the REST design of the interface. |  |
|  | SMA-007 | Many identifiers in the different service interfaces makes it messy. | Building Testbed B and the swagger file | Propose to clean up and make consistent, and remove unnecessary identifiers. |  |
|  | SMA-008 | What shall the REST operation be named for Upload and Get now when we removed the type of message in the URL? Object, Message | Building Testbed B and the swagger file |  |  |
|  | SMA-009 | When data is incorporated in JSON object, such as in UploadObject, it tricky to restore the data exactly to match the original, hence difficult to verify the signature. |  |  |  |
|  | SMA-010 | Is it necessary/beneficial to exchange a filename as well? If the data is compressed into a ZIP-file you need to open and see the files inside before handle it further. |  |  |  |
|  | SMA-011 | Currently the UploadObject contains a SECOM\_SecurityMetadata object based on S-100. Another alternative would be to always exchange an ExchangeSet ZIP containing the necessary metadata to verify the signature, filename etc. |  | This requires however a stable S-100 to finalize SECOM.  The metadata is always used in GET and ACK. |  |

# Testbed

## General

Three testbeds, called Testbed A, Testbed B and Testbed C, have been defined for this project. The functionality and connectivity is increased in each testbed.

The first step (Testbed A) is local implementation and email for connectivity.

Second step (Testbed B) is still local implementations with local services as intermediate step. Perhaps this testbed will be the closest design for the Test methods described in SECOM.

Third step (Testbed C) is local implementation connected through services and internet with adequate protection according to SECOM.

## Testbed A

### Description

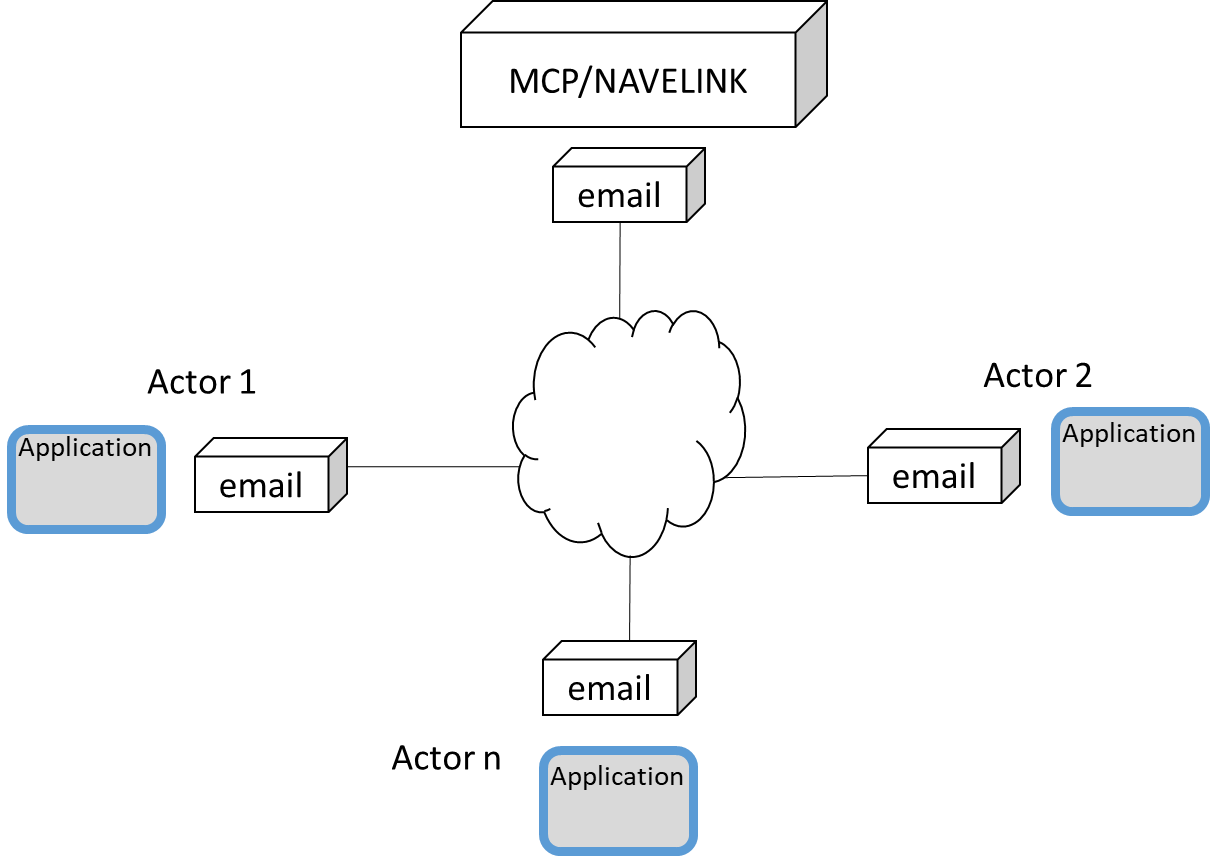
The purpose with testbed A is to test SECOM Data Protection Scheme.

**PKI in the testbed**

The approach is to use MCP and Navelink as far as possible as PKI system. Where SECOM goes beyond MCP/Navelink, manual commands using e.g. openssl need to be used.

* SMA creates a Service ID called “SECOM SMA Test Service ID” and issues certificate for that entity. The public certificate (Download the public part) is then emailed to Saab.
* Saab creates a Service called SECOM-SAAB and issues certificate for that entity. The public key/certificate is then emailed to SMA.

MCP/Navelink cannot today provide all public keys to other than user within same organization, hence public keys between organizations need today be mail around.



### Functionality in the testbed

The following functionality is required in the testbed:

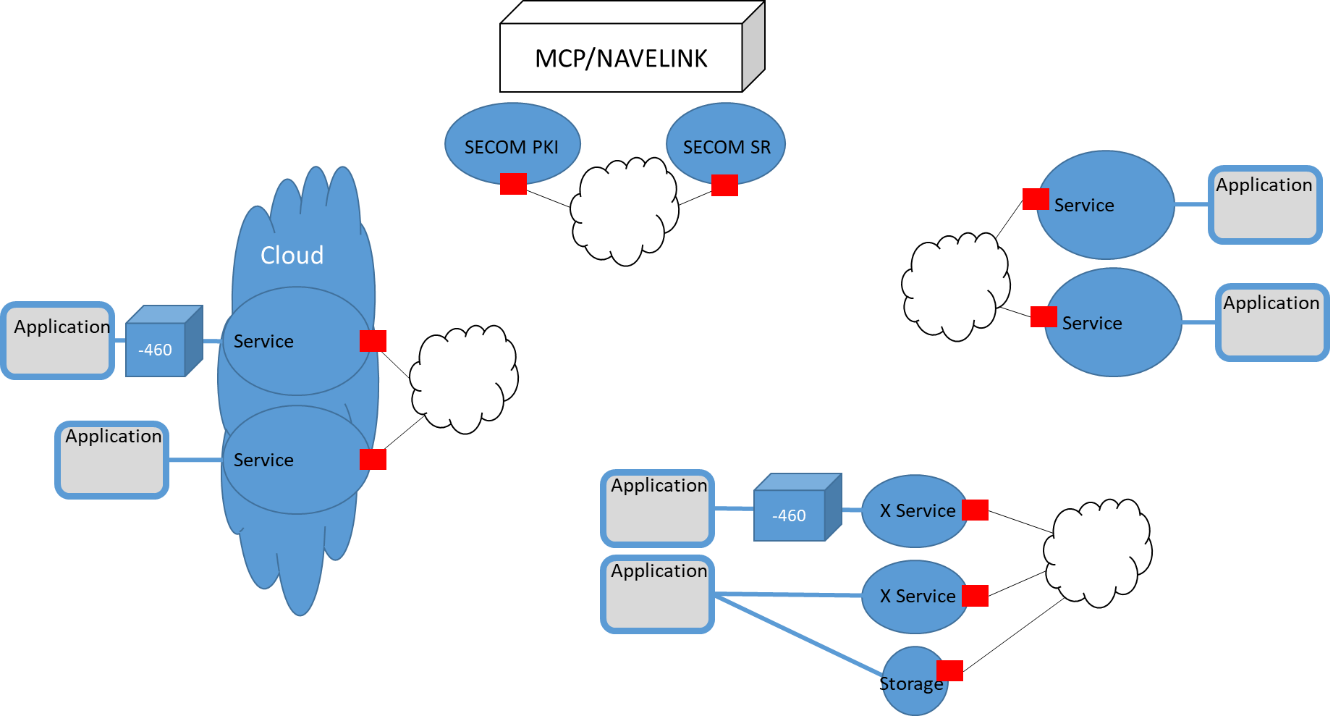
1. Create Signature on a payload
   * Calculate checksum according to SECOM (S-100)
   * Encrypt checksum with own private key
2. Exchange payload and SECOM\_ExchangeMetadata objects
3. Verify signature
   * Retrieve public keys for claimed identity
4. Encrypt payload
   * Generate secret key
   * (compress data)
   * Encrypt data
5. Compress data
6. Exchange secret key
   * Encrypt secret key (RSA or ECC, diffie-hellman or similar)
   * Sign secret key
7. Decrypt payload
   * Receive secret key
   * Verify signature
   * Decrypt secret key
   * Decrypt data
   * (uncompress data)
8. Uncompress data

## Testbed B

### Description

The purpose with Testbed B is to test SECOM Data Protection in combination with SECOM transport security and SECOM service interface within each partners own environment.

Testbed B is an intermediate test bed before achieving Testbed C, but also a “plan B” if firewalls and connection between partners for some reason fails.



### Functionality in the testbed

See Testbed C for list of functionality.

This testbed might be the testbed closest to what can/will be used in Test methods in SECOM.

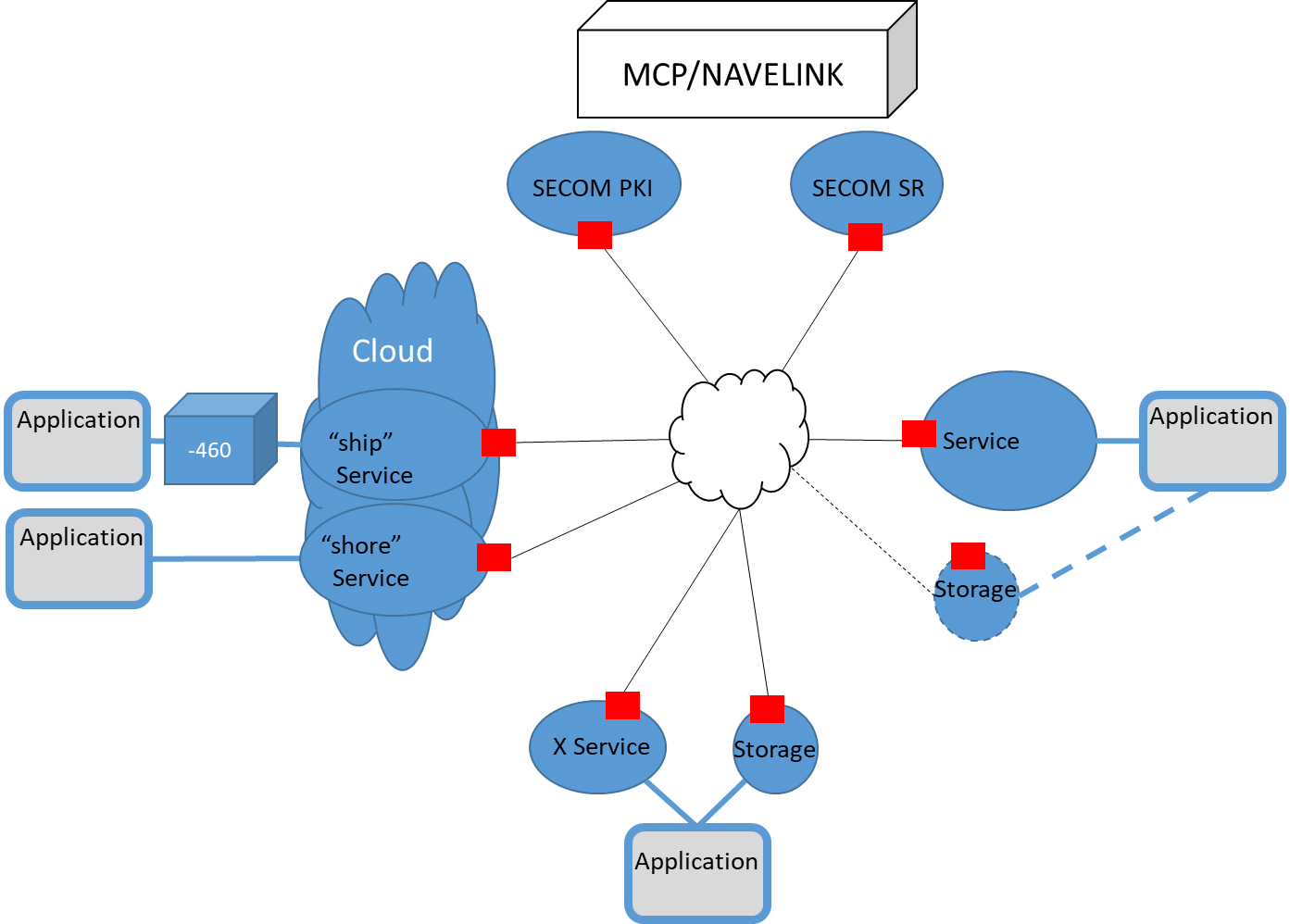
### Requirements and input

* IEC 63173-2 SECOM
  + Annex X: OpenAPI (swagger)

## Testbed C

### Description

The purpose with Testbed C is to test SECOM Data Protection in combination with SECOM transport security and SECOM service interface and connections across different organizations networks.



### Functionality in the testbed

The following functionality is required in the testbed:

1. *Create Signature on a payload*
   * *Calculate checksum according to SECOM (S-100)*
   * *Encrypt checksum with own private key*
2. *Exchange payload and SECOM\_ExchangeMetadata objects*
3. *Verify signature*
   * *Retrieve public keys for claimed identity*
4. *Encrypt payload*
   * *Generate secret key*
   * *(compress data)*
   * *Encrypt data*
5. *Compress data*
6. *Exchange secret key*
   * *Encrypt secret key (RSA or ECC, diffie-hellman or similar)*
   * *Sign secret key*
7. *Decrypt payload*
   * *Receive secret key*
   * *Verify signature*
   * *Decrypt secret key*
   * *Decrypt data*
   * *(uncompress data)*
8. *Uncompress data*
9. Expose (provide) deployed and consumable service interface   
   **OBS! Discuss which interfaces that need logic.**
   * Upload
   * Upload Link
   * Get Summary
   * Get
   * Get by Link
   * Acknowledgement
   * Subscribe
   * Remove subscription
   * Subscription notofication
   * Request Access
   * Access Notification
   * Capability
   * Ping
   * EncryptionKey
10. Consume service interface
11. Transport Security and Service Authentication
    * Encrypt traffic
    * Authenticate client in service call
    * Decrypt traffic
12. Send Sign request
    * Create signing request
    * Call SECOM PKI Signing Request (secure, authentication)
13. Search for service to consume
14. SECOM PKI: Provide Public Keys
15. SECOM PKI: Handle Signing request
    * Authentication
    * Handle Signing request and store Public Key
16. SECOM Service Registry: Handle search request for service

# Test Case 1 - Data protection (signing) of unclassified data

## Description

The test case focus on exchange of unclassified signed data, and the verification and authentication of the signature.

### Test objectives

* Message integrity
* Data integrity
* Transport confidentiality
* Service identity
* Information push

### Acceptance Criteria

Message integrity verified by comparing calculated envelope signature with the corresponding received signature.

Data integrity can be validated providing the end-user application public certificate is issued by SECOM PKI. In other cases the data integrity has to be validated in the end-user application which out of scope for SECOM.

Transport confidentiality verified by establishing an encrypted channel using SECOM PKI issued SSL host certificates.

Service identity verified against SECOM PKI using provided “client” certificate received in TLS session.

Information push achieved by a successful data uploaded.

### Test Scenarios

Actor A shall send one data object (XML) to Actor B. Actor A decides that the information is unclassified. The data is encapsulated into an UploadObject ready to be exchanged as body to a SECOM Upload Service Interface.

### Test Environment

Testbed B

### Test tools

OpenSSL, Notepad++

### Test data

Steps to prepare **unclassified** and **uncompressed** data.

The data in this example is one RTZ.

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
| Select data file |  | data-1.rtz |
| Convert to Base64 | openssl base64 -A -in data-1.rtz -out data-1.rtz.base64 | data-1.rtz.base64 |
| Select Private Key |  | PrivateKey\_SECOM\_SMA\_Test\_Service\_ID.pem |
| Create signature using original data file (data-1.rtz) | openssl dgst -sha256 -sign PrivateKey\_SECOM\_SMA\_Test\_Service\_ID.pem data-1.rtz > data-1.rtz.sig | data-1.rtz.sig |
| Convert signature to HEX | xxd -u -ps -c 120 data-1.rtz.sig > data-1.rtz.sig.hex | data-1.rtz.sig.hex |
| Select Public Certificate for the data object |  | Certificate\_SECOM\_SMA\_Test\_Service\_ID.pem |
| Select envelope public certificate |  | EnvelopeCertificate.pem |
| Set other metadata values for the Envelope Object |  | Envelope.json |
| Sign envelope |  | Envelope.sig |
| Add envelope signature to upload object |  |  |
| Create Upload Object in JSON |  | UploadObject-1.json |
| SECOM A | | |
| Add client certificate Actor A |  |  |
| Verify receiver host certificate SECOM B | Check certificate against SECOM Pki | True/false |
| Create TLS |  | Encrypted channel established |
| Consume Actor B SECOM Api Upload | POST URL/v1/object?parameters {body} : return |  |

**RECEIVER**

Verify Signature(s) and restore data

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
| Receive … |  | UploadObject deserialized |
| Authenticate sender | Verify client cert for Actor A from TLS against SECOM Pki | True/false |
| Parse envelope |  | uploadObject.Envelope |
| Convert to byte[] |  | Envelope[] |
| Authenticate data and claimed public key | Verify envelope signature | True/false |
| Store(inform Actor B OEM) incoming object |  | UploadObject-1.json |
| Actor B | | |
| Parse and store data from object |  | data.rtz.base64 |
| Parse and store signature from object |  | data.sig.hex |
| Restore signature from HEX | xxd -r -u -ps data.sig.hex > data.sig | data.sig |
| Parse and store public certificate from object |  | publicCert.pem |
| Identify Root Certificate through the Thumbprint |  | mc-ca-chain\_staging.pem |
| Verify Certificate | openssl verify -CAfile mc-ca-chain\_staging.pem publicCert.pem > publicCert.pem.verification | publicCert.pem.verification |
| Extract public keys from certificate | openssl x509 -in publicCert.pem" -pubkey -noout > publicCert\_key.pem" | publicCert\_key.pem |
| Restore data from Base64 to original | openssl base64 –A -d -in data.rtz.base64 -out data.rtz | data.rtz |
| Verify signature i.e. compare signature with original data file | openssl dgst -sha256 -verify publicCert\_key.pem -keyform pem -signature data.sig data.rtz > data.sig.verification | Verified OK |
| Compare received data with restored data | Open received data.rtz and restored data.rtz (Notepad++ Compare Plugin) | Received data unchanged |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

|  |  |  |  |
| --- | --- | --- | --- |
| **Step** | **Test comments** | **Conclusions** | **Outcome** |
| Set other metadata values for the Envelope Object | Attribute data type values might differ in various OS/ languages. | There is a need to agree on attribute data types used in SECOM to ensure interoperability. | Introduce S100 basic data types to have a common description. |
| Sign envelope | Signature not consistent in different implementations | Order for attributes important when creating the EnvelopeObject to be signed. | Added an ordering column in the EnvelopeObject |
| Create Upload Object in JSON | Conversion of keys to JSON format is implementation specific. | The conversion of keys to JSON need to be agreed upon. | Minify keys to create a uniform way of sending keys in JSON format. To secure interoperability in different OS. |
| Receive … | Deserialization issue, not consistent between different implementations | Attribute data type issue and ordering important to be able to verify signature at the receiving end. | Added an ordering column in the EnvelopeObject |

## Conclusions and Recommendations

|  |  |  |  |
| --- | --- | --- | --- |
| **Acceptance criteria** | **Solution** | **Conclusions** | **Recommendations** |
| Message integrity | Envelope signature creation and verification | Depends on OS and implementation for consistency between services. | Introduce envelope metadata attribute ordering, commonly defined data types and rules for serialization of JSON uploadObject. |
| Data integrity | Data signature creation and verification | If created in SECOM PKI this can be validated in the SECOM service instance. | Introduce ordering for attributes in the DigitalSignatureValueObject. |
| Transport confidentiality | TLS using PKI issued SSL certificates | Can be an issue if SSL certificates are self-signed, hence not possible to use in certain implementations (Azure). | Suggest to use official CA issued certificates. |
| Service identity | Received service instance “client” certificate | Mutual authentication on service instance level by using exchanged SECOM PKI certificates. | Important to agree beforehand on entities in certificate information for “Subject distinguished name” for authentication purposes. |
| Information push | Upload interface | Response code if total base 64 encoded message exceeds web server maximum message size missing. | Introduce response code 413 / message if uploaded message > maximum message size (350 kB). |

# Test Case 2 - Data protection of classified data (signing and encryption)

## Description

The test case focus on exchange of classified signed data, and the verification and authentication of the signature.

Publish and get encrypted data

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 3 – SECOM PKI

## Description

The test case focus on exchange of classified signed data, and the verification and authentication of the signature.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 4 – Exchange large data

## Description

* What to sign?
* Different protection schemes for each layer
* Sign ZIP file with signed data files

## Targeted questions

## Test Functionality

## Test Variables

The following test variables in this test case have been identified:

* Data type and packaging
* Packaging of exchange metadata

## Testbed

## Test Sequence

* Description: Test exchange of large data e.g. grib data and ENC encrypted with S-63 procedure (Primar) (SECOM task 2020-03)
* Purpose:

Verify that SECOM interface is suitable for large data

**Use Case**

Actor 1 wants to send large data block (>10MB) to Actor 2.

Actor 1 creates temporary storage, loads it with data and retrieves a link to it

Actor 1 sends (uploads) the link to Actor2

Actor 2 retrieves the data using the link

Actor 1 deletes the data after X minutes/hours

**Discussions**

Q: What is the Temporary Storage?

FTP?

Webserver with file?

Q: What security is required?

Open? (and refer to Data Encryption if classified data?)

FTP login?

Certificates from SECOM PKI?

OpenID/token from SECOM PKI?

Sequence - Exchange large data

Last modified 2020-04-14



1. Sequence - Exchange large data





1. Sequence diagram for Upload Link to classified data

## Test results and discussions

This chapter contains the common results and discussions around the test case. For each individual participants result see the Annexes in end of this document.

## Conclusions and Recommendations

Missing HTTP response code added

Filter attribute added

# Test Case 5 – Exchange compressed data

## Description

The test case focus on exchange of compressed data.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 6 – Closed loop communication

## Description

The test case focus on notification of messages received/ read etc.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 7 – Subscribe to data

## Description

The test case focuses on subscription to information for receiving subsequent updates of information.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 8 – Service information

## Description

The test case focus on information with regards to service information i.e. accepted payloads, endpoints etc.

Test cases for; upload, uploadLink, get, getByLink, getSummary, subscription, access and encryptionKey dependant on provided payload and version.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 9 – Service status

## Description

The test case focus on retrieving the contextual status of a service.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# Test Case 10 - Cyber Security Review

## Description

This test case is performed as a review of the SECOM document. If possible, the changes and variables made and recommended during the SECOM Test Project is also reviewed.

## Targeted questions

* Review of the SECOM security solution as a whole
  + Overall description (Clause 4) of the SECOM standard
  + Overall solution of SECOM Data Protection (Clause 7)
  + Overall solution of SECOM Transport Security (Clause 6)
  + Data protection and Transport security applied on/in SECOM Information Service (REST)
* Review of specific issues
  + How exchange the secret key if SECOM Data Protection scheme is used instead of IHO and Permits?
  + What requirements does the exchange of the secret key put on the algorithm used in asymmetric keys used mainly for signing data? Will it work the same with ECC keys as for RSA keys? Or are there different procedures required for the encryption of the secret key?
  + Shall SECOM handle Nonrepudiation?
  + Is there a security risk with the Acknowledgement procedure described?
  + Exchange the digital signature in service defined attribute, PERMIT.xml, S100\_DatasetDiscoveryMetadata, S100\_CatalogueMetadata or in SECOM\_ServiceExchangeMetadata?
  + How shall the signature be transferred?
  + Which SECOM service interfaces requires signature on the payload (all interfaces that includes payload…)?
  + How ensure authentication in those interfaces that do not exchange payload and its signature?
  + Shall SECOM describe which identity to use for signing data versus service authentication (signing transport?
  + Should SECOM support session based interaction a'la S-100/Offis examples, or MMS style in MCP?
  + Shall SECOM describe Service Authentication as normative?
  + Shall SECOM Communication Channel Security be based on TLS and Certificates or OpenID/HMAC or similar?
  + Is it/will it be accepted to mandate the use of Client Certificates from SECOM PKI?
  + Should/Shall SECOM also mandate use of host certificate from SECOM PKI? Which then becomes a selfsigned certificate? Will it work in reality?

## Test Functionality

N/A

## Test Variables

N/A

## Testbed

N/A

## Test Sequence

N/A

## Test results and discussions

This chapter contains the common results and discussions around the test case. For each individual participants result see the Annexes in end of this document.

### Observations

| Num | Ref number | Observation | Consequence/Proposal | Reference in SECOM Document |
| --- | --- | --- | --- | --- |
| 001 |  |  |  |  |

## Conclusions and Recommendations

# Test Case 11 – White list and access request

## Description

The test case focus on client access and client identity together with functions for white listing services.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

Fine granular organizationstructure, access on organizational level

Servicecertificate as a basis for access control which means attributes in the certificate would limit the granularity possible for access

# Test Case 12 – Service Discovery

## Description

The test case focus on service instance discovery.

The main purpose is to challenge

* 9 SECOM Service Discoverability.
  + Service Discovery Interface definition file (Swagger)

## Targeted questions

* Fixed search parameter in interface, or dynamic query with key:value pair with recommended list of search parameters.

## Test Functionality

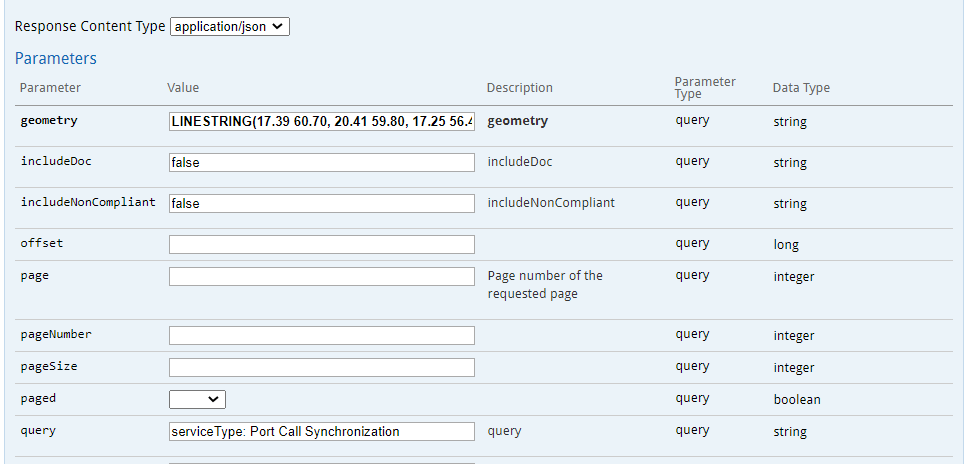
## Test Variables

## Testbed

Example 1: geometry combined with serviceType search

**REQUEST**

Search for services with provided geometry inside service coverage area and service type “Port Call Synchronization”.



Figur 1 - Request find service with geometry and query

https://serviceregistry.navelink.org/api/\_searchGeometryWKT/serviceInstance?geometry=LINESTRING(17.39%2060.70%2C%2020.41%2059.80%2C%2017.25%2056.43)&includeDoc=false&includeNonCompliant=false&query=serviceType%3A%20Port%20Call%20Synchronization

**RESPONSE**



Figur 2 - Response from service registry

Example 2: Search with AND/ OR condition

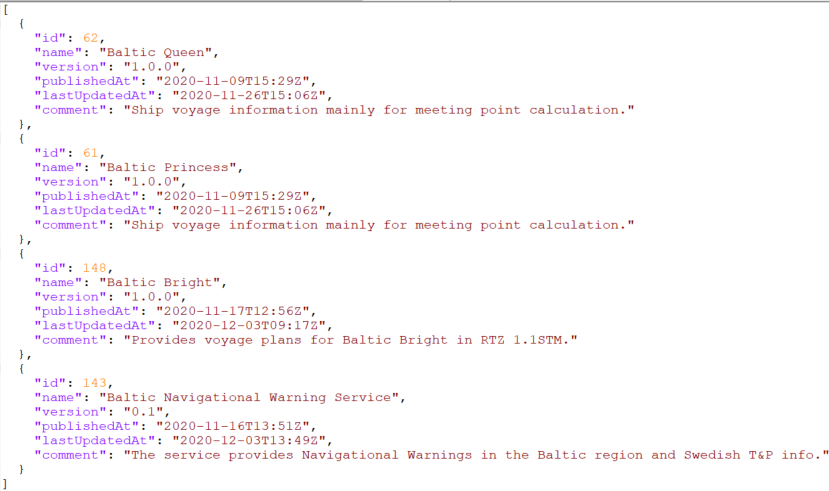
**REQUEST**

Search for services with specific IMO and MMSI OR services with name containing “Baltic”.

Query = (imo: 9443255 AND mmsi: 276779000) OR name: Baltic

https://serviceregistry.navelink.org/api/\_search/serviceInstance?includeDoc=false&includeNonCompliant=false&query=(imo%3A%209443255%20AND%20mmsi%3A%20276779000)%20OR%20name%3A%20Baltic

**RESPONSE**



Figur 3 - Response from service registry

## Test Sequence

## Test results and discussions

This chapter contains the common results and discussions around the test case. For each individual participants result see the Annexes in end of this document.

## Conclusions and Recommendations

# Test Case 13 – Exchange of several different payloads

## Description

The test case focus on exchanging payloads of different types.

### Test objectives

TBD

### Acceptance Criteria

TBD

### Test Scenarios

TBD

### Test Environment

TBD

### Test tools

TBD

### Test data

TBD

### Test procedure

**SENDER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| Actor A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| SECOM A | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**RECEIVER**

|  |  |  |
| --- | --- | --- |
| **Step** | **Commands** | **Result** |
| SECOM B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Actor B | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Test results and discussions

This chapter contains the common results and discussions around the test case.

TBD

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Test comments | Conclusions | Outcome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Conclusions and Recommendations

TBD

# ANNEX A Participant (SMA)

## Planning

* (Mikael) Implement Testbed A
  + Implement exchange of unclassified signed data (messages such as RTZ, S-421, S-124)
  + Implement exchange of classified signed data (messages such as RTZ, S-421, S-124)
  + Implement exchange of large classified data (big data as GRIP data, ENC data)
* (Mattias) Implement Testbed B with functionality as Ship and service provider
  + Implement core of Testbed A
  + Implement exchange of large classified data (big data as GRIP data, ENC data)
  + Implement SECOM Information Service Interface
    - Upload
    - tbd
  + Implement SECOM Data Protection
* Implement Testbed C
* Figure out how SECOM PKI and SECOM Discovery can be realized using MCP or Navelink

### Schedule

See PP for detailed schedule

* + Meetings
  + Work
  + Vacation
  + Milestones

### Input

Input will be located on ProjectPlan (<https://service.projectplace.com/>)

* IEC 63173-2 SECOM Document
  + Annex A REST openAPI/swagger (Mattias 10/7)
* S-100 ed 4 (<http://s100.iho.int/S100/home/s100-introduction>)
* Excel SECOM Tool (command line)
  + openssl, xxd, 7zip commands
* .NET, library (discuss with Mattias and Peter)
* Access to MCP (<https://management.maritimecloud.net/#/apply>)
* or, Access to Navelink (<https://www.navelink.org/enrolment-form/>)
* Testdata (RTZ, S-421, S-4xx etc)
  + RTZ\_v1.1STM.xsd
  + S421.xsd ?
  + S41x.xsd?
* Document references
* Schedule

## APPENDIX SECOM Test Project SMA Report

<placeholder for separate document with Participant report>

# ANNEX B Participant (Saab)

## Planning

* Implement Testbed A
  + Implement exchange of unclassified signed data (messages such as RTZ, S-421)
  + Implement exchange of classified signed data (messages such as RTZ, S-421)
  + Implement exchange of large classified data (big data as GRIP data, ENC data)
* Implement Testbed B with functionality as VTS (shorecenter)
  + Implement core of Testbed A
  + Implement SECOM Information Service Interface
    - Upload
    - tbd
  + Implement SECOM Data Protection
* Implement Testbed C with functionality as Service provider (chart server, route deviation detection)
  + Implement core of Testbed B
  + Implement SECOM Communication channel security (transport security)

### Schedule

See PP for detailed schedule

* + Meetings
  + Work
  + Vacation
  + Milestones

### Input

Input will be located on ProjectPlan (<https://service.projectplace.com/>)

* IEC 63173-2 SECOM Document
  + Annex A REST openAPI/swagger (Mattias 10/7)
* S-100 ed 4 (<http://s100.iho.int/S100/home/s100-introduction>)
* Excel SECOM Tool (command line)
  + openssl, xxd, 7zip commands
* .NET, library (discuss with Mattias and Peter)
* Access to MCP (<https://management.maritimecloud.net/#/apply>)
* or, Access to Navelink (<https://www.navelink.org/enrolment-form/>)
* Testdata (RTZ, S-421, S-4xx etc)
  + RTZ\_v1.1STM.xsd
  + S421.xsd ?
  + S41x.xsd?
* Document references
* Schedule

## APPENDIX SECOM Test Project SAAB Report

<placeholder for separate document with Participant report>

# ANNEX C Participant (StormGeo)

## Planning

* Implement Testbed C

Reference IEC 63173-2 SECOM document

* Implement core of Testbed B
  + Implement exchange of unclassified signed data (messages such as RTZ, S-421)
  + Implement exchange of classified signed data (messages such as RTZ, S-421)
  + Implement SECOM Information Service Interface
    - Upload
    - tbd
  + Implement SECOM Data Protection
  + Implement SECOM Communication channel security (transport security)

### Schedule

See PP for detailed schedule

* + Meetings
  + Work
  + Vacation
  + Milestones

### Input

Input will be located on ProjectPlan (<https://service.projectplace.com/>)

* IEC 63173-2 SECOM Document
  + Annex A REST openAPI/swagger (Mattias 10/7)
* S-100 ed 4 (<http://s100.iho.int/S100/home/s100-introduction>)
* Excel SECOM Tool (command line)
  + openssl, xxd, 7zip commands
* .NET, library (discuss with Mattias and Peter)
* Access to MCP (<https://management.maritimecloud.net/#/apply>)
* or, Access to Navelink (<https://www.navelink.org/enrolment-form/>)
* Testdata (RTZ, S-421, S-4xx etc)
  + RTZ\_v1.1STM.xsd
  + S421.xsd ?
  + S41x.xsd?
* Document references
* Schedule

## APPENDIX SECOM Test Project StormGeo Report

<placeholder for separate document with Participant report>