

DEFINITION OF COMIN HUB INTERFACE FOR COMIN CLIENTS

DOCUMENT HISTORY

Version	Date	Description
2.0	27.5.2016	Initial version

TABLE OF CONTENTS

1. INTRODUCTION	4
1.1. LABELS AND SYMBOLS.....	4
2. OPERATION PROCESSING.....	4
2.1. SEND MESSAGE TO ECR GATE.....	4
2.2. RECEIVING AND CONFIRMING OF MESSAGE DELIVERY	6
2.3. OPERATIONS WITH FORMAL ERRORS	9
2.4. OPERATION SEND WITH ERROR ON ECR GATE	10
2.5. LIST OF OPERATIONS.....	11
2.6. DOCUMENTATION OF OPERATIONS AND MESSAGES	11
2.7. LIST OF ERROR CODES IN RESPONSE MESSAGE	11

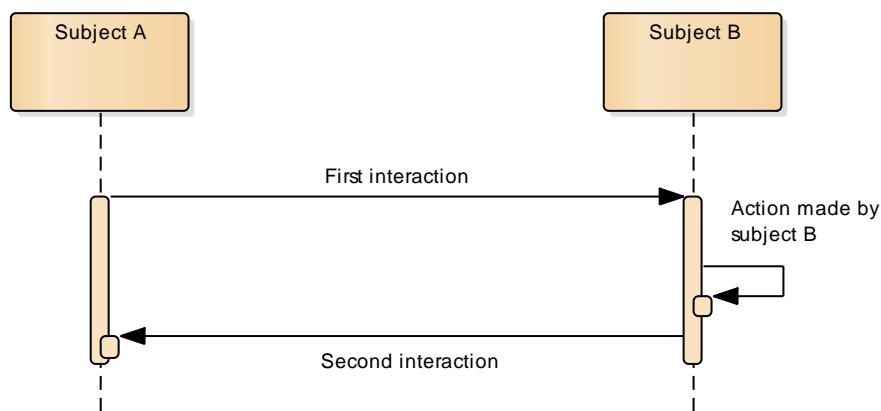
1. INTRODUCTION

Document defines allowed scenarios for message exchange between COMIN client and COMIN Hub. Detailed structure definition and WSDL definition of used web service is in attached ZIP file which is part of this documentation. Structure of messages or WSDL can be changed by release of new version or revision of documentation. Basic documents are published by Czech Customs. Every published revision is obligatory and becomes part of this document.

1.1. LABELS AND SYMBOLS

Sequential diagrams are used for illustration of communication between client and Hub. Its purpose is to describe the sequence of message exchanges.

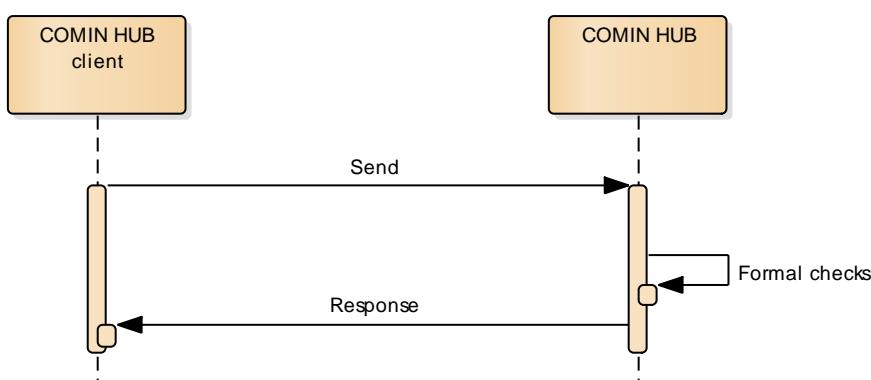
Rectangle or icon on the top side is subject which participates in given situation. Vertical line is time axis. Horizontal lines between objects are mutual interactions in time, arrows show the direction of communication.



2. OPERATION PROCESSING

Operations are realized as web service methods provided by COMIN Hub. Every communication is initialized by COMIN client using standard HTTPS request in synchronous regime request-response.

2.1. SEND MESSAGE TO ECR GATE



Client starts the Send operation and sends data for ECR gateway in form of ECR envelope. Hub makes formal checks and sends affirmative (without Error group) response to client,

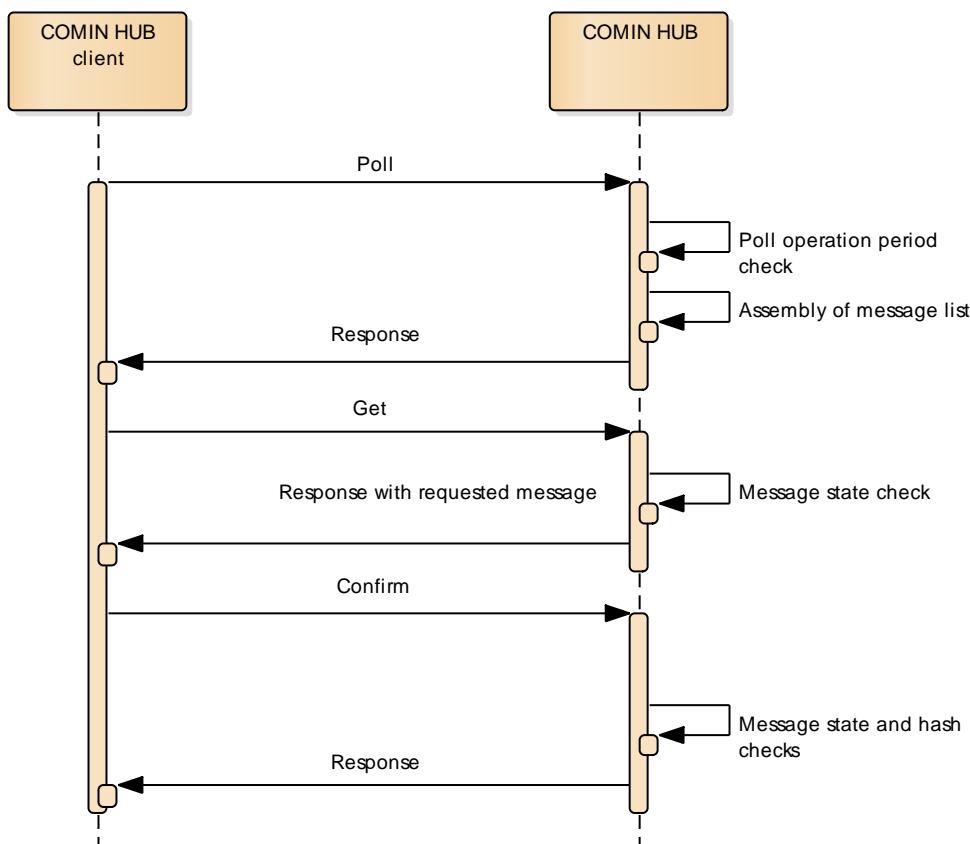
Example of Send operation:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Send xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Send1_0">
      <Authorization CommunicationID="14CZ510000EC00066" Password="password123"/>
      <ClientApplication>
        <Identification>Client</Identification>
        <Version>1.0.0.0</Version>
        <Language>EN</Language>
      </ClientApplication>
      <EcrEnvelope xmlns="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
        <Header EnvelopeGuide="3C3B9358-FB27-40F2-BF90-21AD7EC6CA0D" Domain="NCTS"/>
        <MessageMetadata SecondaryID="ECR_2016052613181769" Type="CZ515A"/>
        <Participants>
          <Participant Role="declarant" Identification="14CZ510000EC00066" ScenarioGuid="668D040F-E3F3-4304-A837-080FA6AD014D" DateAndTime="2016-05-26T13:18:17.36452+02:00" ApplicationName="NCTSClient" ApplicationVersion="2.0"/>
        </Participants>
        <XmlMessage SignatureContext="datacontent">
          <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns="http://www.w3.org/2001/04/xmlenc#">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                  <X509Data>
                    <X509IssuerSerial>
                      <X509IssuerName>E=novak@cs.mfcr.cz, CN=CS test CA, OU=ISL, O=CS, L=Prague, S=Czech Republic, C=CZ</X509IssuerName>
                      <X509SerialNumber>4</X509SerialNumber>
                    </X509IssuerSerial>
                  </X509Data>
                </KeyInfo>
                <CipherData>
                  <CipherValue>HXmnChxgXi201XhQX...</CipherValue>
                </CipherData>
                <EncryptedKey>
                  <KeyInfo>
                    <CipherData>
                      <CipherValue>iHr+pETcHck...</CipherValue>
                    </CipherData>
                  </KeyInfo>
                </EncryptedKey>
              </KeyInfo>
            <EncryptedData>
              <CipherValue>...</CipherValue>
            </EncryptedData>
          </XmlMessage>
        </EcrEnvelope>
      </Send>
    </s:Body>
  </s:Envelope>
```

Affirmative response:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response1_0" xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0" xmlns:extimpl="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
      <OperationSuccessful>1</OperationSuccessful>
    </Response>
  </s:Body>
</s:Envelope>
```

2.2. RECEIVING AND CONFIRMING OF MESSAGE DELIVERY



Client repeatedly makes Poll request (optionally with specified domain, so only messages for given domain are returned). COMIN Hub makes formal checks and check for Poll period. If all checks are OK, it assembles the list of messages with corresponding communication ID for delivery. Message list is sorted by message priority and time. If domain was specified, only messages from specified domain are returned. Maximum number of messages in list is limited - if COMIN Hub has more messages for delivery, only first X messages are returned. Message list is returned to client in form of Response message. Apart from message list the group PollInfo is also returned in this message. It contains period (in seconds) for which the client with given communication ID must wait till the next Poll can be sent to COMIN Hub. Optionally the group Unavailability can be specified (it contains information about planned unavailability - see below).

Example of Poll operation:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <Poll xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Poll1_0">
            <Authorization CommunicationID="14C2510000EC00066" Password="password123"/>
            <ClientApplication>
                <Identification>Client</Identification>
                <Version>1.0.0.0</Version>
            </ClientApplication>
        </Poll>
    </s:Body>
</s:Envelope>

```

Affirmative response in form of Response Message:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>

```

```

<Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response_0"
xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0"
xmlns:extimpl="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
    <Messages>
        <Message>
            <GUID>70936fa6-702a-4c2d-92f5-a05db54e910a</GUID>
            <Domain>NCTS</Domain>
            <Type>CZ906A</Type>
            <SecondaryID>ECR_2016052613181769</SecondaryID>
            <Status>ToDownload</Status>
        </Message>
    </Messages>
    <PollInfo>
        <NextPollIn>10</NextPollIn>
    </PollInfo>
    <OperationSuccessful>1</OperationSuccessful>
</Response>
</s:Body>
</s:Envelope>

```

There are two types of unavailability in COMIN Hub:

1. Type 0 means that ECR gateway will be switched off; during this unavailability client can use only Send and Poll operation. Messages will be queued and sent to ECR gateway after unavailability ends. Use of operations Get and Confirm will result in error.
2. Type 1 means that COMIN Hub will be completely switched off and any attempt of client communication will fail with network-related error.

For given message from list acquired by Poll operation client makes Get operation in which the message ADM001 (enveloped in EcrEnvelope) is sent. This envelope must not be encrypted. All communication domains of ECR gateway are extended with messages ADM001 and ADM002, so ECR envelope for these messages contains the same domain as message which delivery is client requesting. COMIN Hub makes formal checks and then checks the XML signature of included ADM001 message. Operation returns the message Response to the client which contains the requested message in form of ECR envelope.

Order of message downloading (using Get operation) is not important for COMIN Hub, so client can choose to download most important messages first and then the rest.

Example of Get operation:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
    <s:Header>
        <VsDebuggerCausalityData
xmlns="http://schemas.microsoft.com/vstudio/diagnostics/servicemodelsink">uIDPo1Qe5Zu6KuVDqy4HnEoFLKsAAAAA/AdpOFQ7KkCP9ZTsnWLCsvuxO3u
YzMNPyvbd9AJmCQACQAA</VsDebuggerCausalityData>
    </s:Header>
    <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <Get xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Get1_0">
            <Authorization CommunicationID="14CZ510000EC00066" Password="password123"/>
            <ClientApplication>
                <Identification>Client</Identification>
                <Version>1.0.0.0</Version>
            </ClientApplication>
            <EcrEnvelope xmlns="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
                <Header EnvelopeGuid="d5fd64d9-c14e-4c46-aebf-5e409523d178" Domain="NCTS"/>
                <MessageMetadata SecondaryID="ECR_2016052613181769" Type="ADM001"/>
                <Participants>
                    <Participant Role="declarant" Identification="14CZ510000EC00066" ScenarioGuid="d945f9dd-e2d8-429b-af5f-
caf994a31e62" DateAndTime="2016-05-26T13:18:48.1497532+02:00" ApplicationName="Client" ApplicationVersion="1.0.0.0"/>
                </Participants>
                <XmlMessage SignatureContext="datacontent">
                    <Data>
                        <ADM001 xmlns="">
                            <Message>
                                <GUID>70936fa6-702a-4c2d-92f5-a05db54e910a</GUID>
                                <Domain>NCTS</Domain>
                                <Type>CZ906A</Type>
                                <SecondaryID>ECR_2016052613181769</SecondaryID>
                            </Message>
                            <Signature Id="signature-376775319" xmlns="http://www.w3.org/2000/09/xmldsig#">
                                ...
                            </Signature>
                        </ADM001>
                    </Data>
                </XmlMessage>
            </EcrEnvelope>
        </Get>
    </s:Body>
</s:Envelope>

```

Affirmative response in form of Response message with message requested:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response1_0"
      xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0" xmlns:extimpl="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
      <OperationSuccessful>1</OperationSuccessful>
      <EcrEnvelope xmlns="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
        <Header EnvelopeGuid="70936fa6-702a-4c2d-92f5-a05db54e910a" Domain="NCTS"></Header>
        <MessageMetadata Type="CZ906A" SecondaryID="ECR_2016052613181769"></MessageMetadata>
        <Participants>
          <Participant Role="declarant" Identification="14CZ510000EC00066" ScenarioGuid="668D040F-E3F3-4304-A837-080FA6AD014D"></Participant>
          <Participant Role="operator" Identification="COMIN"></Participant>
          <Participant Role="grc" DateAndTime="2016-05-26T13:18:25" ScenarioGuid="2285DA0F-E980-4F1D-9E7A-E7F2D1FA82B3"></Participant>
        </Participants>
        <XmlMessage SignatureContext="datacontent">
          <Data>
            <CZ906A xmlns="">
              <H>
                <H02>ECR_2016052613181769</H02>
                <H03Q>20160526</H03Q>
                <H04Q>131824</H04Q>
              </H>
              <FE>
                ...
              </FE>
              <Signature Id="signature-213391508" xmlns="http://www.w3.org/2000/09/xmldsig#">
                ...
              </Signature>
            </CZ906A>
          </Data>
        </XmlMessage>
      </EcrEnvelope>
    </Response>
  </s:Body>
</s:Envelope>

```

Note: Because Get operation can download responses to messages which was previously sent in format ECR envelope 2.0, Response message contains both EcrEnvelope and EcrObalka elements (2nd will be used in such cases) - but in all scenarios only one of them will be present.

For every downloaded message client makes Confirm operation with message ADM002 (also enveloped in ECR envelope). Message ADM002 contains hash value calculated by client from message delivered by Get operation. Hash calculation is made this way:

- ECR envelope (extracted from Response message into separate XML document) is transformed using C14N XML canonicalization transform (<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>) - variant „without comments“.
- transformed XML is used as input to one of 3 SHA-2 hashing functions (SHA-256, SHA-384, SHA-512)
- byte array (result of SHA-2 algorithm) is transformed to base64 and included in ADM002 message together with identification of used algorithm

Hub makes formal checks, check of ADM002 XML signature and compares hash value from message AD02 with hash value of stored message (which is to be confirmed). If all checks are OK, COMIN Hub responses with affirmative Response message. After successful check is made, the COMIN Hub marks message as confirmed and stops adding it to message list (Poll operation), so the other messages can be returned in Response (and subsequently downloaded and confirmed).

Example of Confirm operation:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Header>
    <VsDebuggerCausalityData
      xmlns="http://schemas.microsoft.com/vstudio/diagnostics/servicemodelsink">uIDPo1Ue5Zu6KuVDqy4HnEofLksAAAAA/AdpOFQ7KkCP9ZTsWLCsvuxO3uYzMNPyvbd9AJmCQACQAA</VsDebuggerCausalityData>
  </s:Header>
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Confirm xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Confirm1_0">
      <Authorization CommunicationID="14CZ510000EC00066" Password="password123"/>
      <ClientApplication>
        <Identification>Client</Identification>
        <Version>1.0.0.0</Version>
      </ClientApplication>
      <EcrEnvelope xmlns="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
        <Header EnvelopeGuid="82cd81f2-5ed8-4d6e-8ae2-b23607dc6b1b" Domain="NCTS"/>
        <MessageMetadata SecondaryID="ECR_2016052613181769" Type="ADM002"/>
        <Participants>
          <Participant Role="declarant" Identification="14CZ510000EC00066" ScenarioGuid="b1146a3e-b9a9-4ef7-86ba-7ba438825d5f" DateAndTime="2016-05-26T13:18:54.4467736+02:00" ApplicationName="Client" ApplicationVersion="1.0.0.0"/>
        </Participants>
      <XmlMessage SignatureContext="datacontent">
    </Confirm>
  </s:Body>
</s:Envelope>

```

```

<Data>
  <ADM002 xmlns="">
    <Message>
      <GUID>70936fa6-702a-4c2d-92f5-a05db54e910a</GUID>
      <Domain>NCTS</Domain>
      <Type>CZ906A</Type>
      <SecondaryID>ECR_2016052613181769</SecondaryID>
      <HashValue>1FCBC7023DF8F7278C0B83F693E002BD91F2B66F3B5C0C342990948980D67038</HashValue>
      <HashType>SHA-256</HashType>
    </Message>
    ...
    <Signature id="signature-88978768" xmlns="http://www.w3.org/2000/09/xmldsig#">
      ...
    </Signature>
  </ADM002>
</Data>
</XmlMessage>
</EcrEnvelope>
</Confirm>
</s:Body>
</s:Envelope>

```

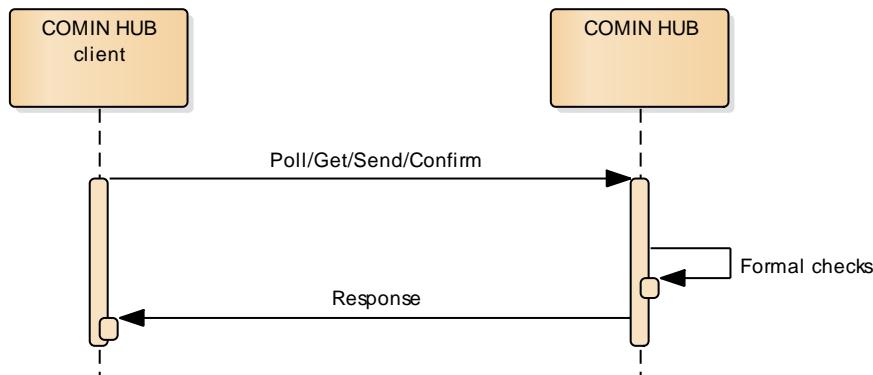
Affirmative Response answer:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response1_0"
      xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0"
      xmlns:extimp1="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
      <OperationSuccessful>1</OperationSuccessful>
    </Response>
  </s:Body>
</s:Envelope>

```

2.3. OPERATIONS WITH FORMAL ERRORS



COMIN Hub makes formal controls for each operation. If any of these controls results in error, message Response with group Error is returned and message processing stops.

Following formal controls are performed:

1. Communication ID and password must correspond with data imported from ASEO system.
2. Client application (including version) must be in list of authorized clients.
3. For each operation (except Poll) the ECR envelope from message is controlled against XSD (actual version is 3.0).
4. For operations Get and Confirm messages ADM001 and ADM002 are controlled against XSD.
5. For Poll operation the period between two Poll operations is controlled (against period from PollInfo sent in last Response message).
6. For Get operation the message must be in correct state (i.e. "To download" or "To confirm")
7. For Confirm operation the message must be in state "To confirm" and hash value sent in Confirm message must be equal to hash value calculated by COMIN Hub.

Example of Response message with formal error (unauthorized client version):

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>

```

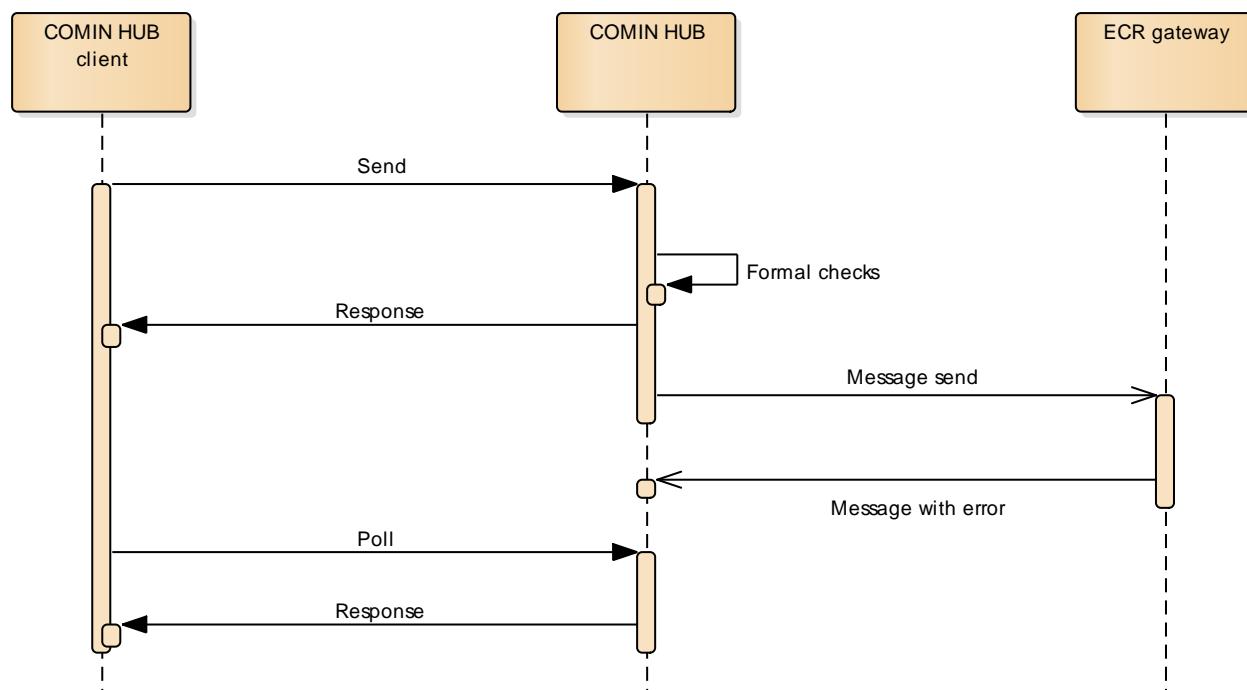
```

<Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response1_0"
xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0"
xmlns:extimpl="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
<Error>
  <Code>21</Code>
  <Description>Unknown client or version</Description>
</Error>
<OperationSuccessful>0</OperationSuccessful>
</Response>
</s:Body>
</s:Envelope>

```

2.4. OPERATION SEND WITH ERROR ON ECR GATE

Special type of error is error which cannot be detected by formal controls in COMIN Hub, but is detected by ECR gate. This type of error can occur when performing Send operation.



If all formal requirements of Send operation are fulfilled, affirmative Response message (without Error group) is sent back to client. Message (ECR envelope from Send) is then sent to ECR gateway. If ECR gateway checks completes with error (for example because transferred ECR envelope is signed by unauthorized certificate), it responds with message containing error details (again in form of ECR envelope) to COMIN Hub. Comin Hub will offer this message in message list for downloading (as any other message). Message processing continues with operations Poll, Get and Confirm (see chapter 2.2).

Example of Response message containing error from ECR gateway:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <Response xmlns="http://www.cs.mfcr.cz/schemas/COMINHub/Response1_0"
    xmlns:extimp="http://www.cs.mfcr.cz/schemas/EcrObalka/V_2.0"
    xmlns:extimpl="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
      <OperationSuccessful>1</OperationSuccessful>
      <EcrEnvelope xmlns="http://www.cs.mfcr.cz/schemas/EcrEnvelope/V_3.0">
        <Header EnvelopeGuid="fd4afbea-8e8e-4fa5-89f2-17def4691719" Domain="NCTS"></Header>
        <MessageMetadata Type="Error" SecondaryID="ECR_2016052613585469"></MessageMetadata>
        <Participants>
          <Participant Role="declarant" Identification="14CZ510000EC00066" DateAndTime="2016-05-26T13:58:54.2385025+02:00" ScenarioGuid="d8c0a673-9bae-454f-b815-fe90bc1eb053" ApplicationName="Klient" ApplicationVersion="1.0"></Participant>
          <Participant Role="operator" Identification="COMIN" DateAndTime="2016-05-26T13:58:55.3507269+02:00" ApplicationName="COMINHubG2IC" ApplicationVersion="2.0.0.0"></Participant>
        </Participants>
      </EcrEnvelope>
    </Response>
  </s:Body>
</s:Envelope>

```

```

<Error Code="18" EnvelopeGuid="3dafc78b-97a0-46ad-a5b4-a73bf8055224" Type="ECRDisassembling"
Description="Incorrect data security found: found encryption: No, sign:Yes; expected encryption Required, sign
Required"></Error>
</EcrEnvelope>
</Response>
</s:Body>
</s:Envelope>

```

2.5. LIST OF OPERATIONS

Operation	Description
Send	Sending of message for ECR gateway in form of ECR envelope.
Poll	Poll for waiting messages.
Get	Request for message downloading. Client must include signed ADM001 message included in ECR envelope.
Confirm	Request for message confirmation. Client must include signed ADM002 message included in ECR envelope.

2.6. DOCUMENTATION OF OPERATIONS AND MESSAGES

Html documentation of operations and messages together with WSDL and XSD definitions is in attached ZIP archive which is part of this documentation.

Html documentation is in directory "HTML" of archive and should be read by opening default.html file in any common Internet browser (IE, Google Chrome, Mozilla Firefox ...).

WSDL and XSD definitions are in directory "WsDL&XSD" of archive. These files should be used to automatically generate client classes (for example by using "Add Service reference" in Microsoft Visual Studio).

2.7. LIST OF ERROR CODES IN RESPONSE MESSAGE

Message Response sends error in Error group (error code and its description). List of possible errors follows:

Code	Description
1	Internal error
10	Invalid request
20	Invalid communication ID or password
21	Unknown client or version
30	Time between last Poll request and current time is smaller than specified poll interval
40	Invalid Get request
50	Invalid Confirm request
51	Invalid hash in Confirm request