Isode

Providing STANAG 5066 services over IP or UDP (S5066-APP4)

20th Dec 2021 Version: 1.2

Status: Experimental

1 Purpose

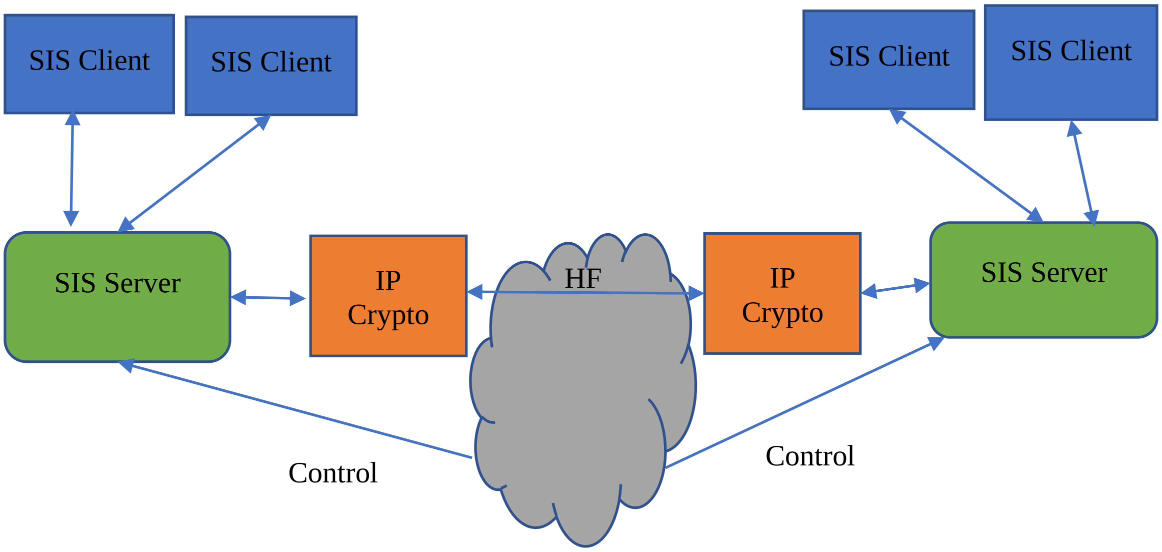
This protocol specifies an approach of providing the STANAG 5066 service over IP, with an alternate option to work over UDP. This is to enable STANAG 5066 to be used over IP and in particular to make of IP Crypto including IPsec and HAIPE. This document specifies and end to end protocol over IP.

Black Side IP over HF is provided using a black side STANAG 5066 system. To provide the full service, this protocol needs to be used with two other capabilities to communicate service elements with the black side STANAG 5066 system:

1. Some STANAG 5066 service elements needs to be communicated out of band to the black side STANAG 5066. Approaches to achieve this are specified in "Providing Control Parameters for STANAG 5066 over UDP through IP Crypto" (S5066-APP9).
2. Confirmation and Rejects need to be provided from black side, as well as flow control. An approach to achieve this is specified in "XML Control Messages for STANAG 5066 over UDP through a Data Diode" (S5066-APP10).

It is anticipated that the black side STANAG 5066 system will provide TRANSEC using AES and the mechanism defined in "STANAG 5066 TRANSEC Crypto Layer using AES and other Protocols" (S5066-EP14).

2 Architecture



This specification specifies behavior of a SIS server, as shown in the diagram above. Notes:

1. SIS Clients communicate with the SIS Server using standard STANAG 5066 SIS protocol. Applications using SIS will operate in a standard manner.

2. SIS servers communicate end to end using the protocol specified in this document using IP.

   A. Operation direct over IP is preferred as it reduces protocol overhead. An option to use UDP is also specified, as some IP cryptos may prevent use of non-standard IP protocols.

3. It is anticipated that this protocol will be sent through IP Crypto to a black side STANAG 5066 system. The PDUs of the protocol specified here along with the IP header will be encrypted and carried as encrypted payload on the black side IP.

4. Some service requirements (ARQ and Priority) need to be communicated out of band to the HF subsystem. This can be achieved by using “Providing Control Parameters for STANAG 5066 over UDP through IP Crypto” (S5066-APP9).

5. Control information from the HF subsystem is needed to provide the SIS service. An approach to this is specified in "XML Control Messages for STANAG 5066 over UDP through a Data Diode" (S5066-APP10).

3 Extended IP Service

The basic approach is to communicate end to end using IP which goes over IP Crypto. Directly mapping applications onto IP over HF leads to poor performance, as described in the Isode white paper "Measuring and Analysing STANAG 5066 F.12 IP Client". To avoid this, the architecture here provides an extended IP service by:

1. Additional control information from red to black side using the mechanisms set out in "Providing Control Parameters for STANAG 5066 over UDP through IP Crypto" (S5066-APP9); and
2. Additional control information from black to red using a data diode as specified in XML Control Messages for STANAG 5066 over UDP through a Data Diode" (S5066-APP10).

Control

This extended IP service is contrasted to standard IP in the foll[illegible].

Capability	Extended IP Service	Standard IP Service
IPv4/IPv6 Source and Destination Addressing	Yes	Yes
Unreliable (non-ARQ) data	Yes	Yes
Reliable (ARQ) data	Yes	No
Handling black side data loss	Yes	No
Priority	Yes	No
Flow Control	Yes	No

4 STANAG 5066 Services Provided

The following STANAG 5066 Services are not provided by this specification:

1. Hard Links. These are not used by any SIS applications.
2. Expedited Data. This is not used by any SIS applications.
3. Management Protocol. STANAG 5066 defines framework protocol, but no use of it.
4. Rank. There is no variation of handling based on Rank.
5. TTL. It is not possible for the application to set TTL, so default will always be used.

For Unidata, the “Non-ARQ with Errors” service is not provided.

Omitting these services is not expected to have any practical impact.

Only destination SAP is used. There does not appear to be operational benefit of allowing source SAP to be different.

5 Providing Services and Protocol

This STANAG 5066 SIS services are provided as follows.

5.1 Bind

Bind services are provided locally by the SIS server.   The server shall enforce a maximum of one connection per SAP.

The MTU will be determined based on constraints of the underlying system. For older systems, it may need to be reduced to ensure no IP fragmentation.   Each PDU will need to be included in a U_PDU of max size likely to be 2048 in the black side STANAG 5066 system. There will be overheads from IP transport and IP crypto.   As a consequence the MTU is expected to be set to a value slightly less that 2048 to allow for these overheads.

5.2 Keep Alive

The SIS server **shall** send Keep Alives at intervals.

5.3 Flow Control

Flow control **shall** be provided to SIS clients based on information from the HF subsystem, provided by a mechanism following S5066-APP10 or equivalent.

5.4 Unidata

Unidata requests and indications and client confirmation are provided by the IP protocol specified below.

Node confirmation and rejects **shall** be provided to SIS clients based on information from the HF subsystem, provided by a mechanism such as the one specified in S5066-APP10.

Unidata priority, “in order”, and ARQ/non-ARQ information is included in the protocol defined below, so that this information can be supplied to the receiving system in S_UNIDATA_INDICATION. This information **shall** also be communicated to the HF subsystem following S5066-APP9 or equivalent procedure.

For Unidata PDUs, the values are taken from the SIS request being processed.   For Confirms, the values are taken from the incoming Unidata PDU that is being confirmed and “in order” is set to false.

Unidata is carried in IP using the following format.

<table>
<tr><td></td><td>MSB</td><td></td><td></td><td></td><td></td><td></td><td></td><td>LSB</td></tr>
<tr><td></td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td colspan="2">Version=0</td><td colspan="3">Not Used</td><td>ARQ</td><td>Client Confirm</td><td>Type=0</td></tr>
<tr><td>1</td><td colspan="4">SAP</td><td colspan="4">Priority</td></tr>
<tr><td>2</td><td colspan="8" rowspan="2">Confirmation ID (optional)</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td><td colspan="8" rowspan="2">U_PDU</td></tr>
<tr><td>n</td></tr>
</table>

The PDU is encoded as follows:

1. Version is set to 0 for this version of the Protocol.
2. The Type field is set to 0 for U_PDU
3. If client confirmation is requested, Client Confirm is set to 1, and the optional Confirmation ID is included in the PDU.
4. If ARQ is requested, the ARQ bit is set to 1.
5. SAP is set to the SAP.
6. Priority is set to the STANAG 5066 requested priority.
7. U_PDU is the U_PDU.

Client Confirm/Reject is provided using the following PDU, when client confirmation is requested and the U_PDU is delivered to the client or when the U_PDU is rejected. Note that rejects are only sent when the sender requests client confirmation.

<table>
<tr><td></td><td>MSB</td><td></td><td></td><td></td><td></td><td></td><td></td><td>LSB</td></tr>
<tr><td></td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td colspan="2">Version=0</td><td>Not Used</td><td colspan="4">Reason</td><td>Type=1</td></tr>
<tr><td>2</td><td colspan="8" rowspan="2">Confirmation ID</td></tr>
<tr><td>3</td></tr>
</table>

Type value is set to 1 for the Client Confirm/Reject. Confirmation ID **shall** be the value taken from the arriving U_PDU. Reason has values according to the following table:

Reason	Code	Description
Confirm	0	Confirmation of passing Data PDU to SIS Client
Not Bound	1	SIS Client not bound on SAP
Version Error	2	Version of protocol in Data PDU not supported
Protocol Error	3	Protocol Error in data PDU

These PDUs **shall** be sent over IP. The IP protocol **shall** be 99: "any private encryption scheme” or another value agreed for the deployment.

If UDP is used, the UDP destination port **shall** be 20515 or another value agreed for the deployment.

IP fragmentation **shall not** be used.

IPv4 or IPv6 may be used. Note that no STANAG 5066 addressing is used in protocol. SIS servers must map provided STANAG 5066 source and destination addresses into equivalent IPv4 or IPv6 addresses.

The provided Rank of Unidata is ignored.

The provided TTL of Unidata is used to set a timer if Node or Client confirmation is requested. In the event of the timer expiring and no reject or confirmation for the Unidata being received, the SIS server **shall** reject the Unidata with reason “TTL expired”.

5.5 Empty PDU

An empty PDU **may** be sent. This will comprise a single zero byte. This **shall** be ignored on reception. This can be a useful optimization when the service detects that IP cryptos are failing to connect due to HF link not being available.