

Using IP Crypto over HF

This whitepaper describes an approach to protect data using IP Crypto over HF communication. The approach described in this document is formally set out in the following open specifications:

1. "Providing STANAG 5066 services over UDP/IP" ([S5066-APP4](#))
2. "Implicit IP Client over STANAG 5066" ([S5066-APP5](#)). Optional.
3. "Providing Control Parameters for STANAG 5066 over UDP/IP through IP Crypto" ([S5066-APP6](#))
4. "XML Control Messages for STANAG 5066 over UDP/IP through a Data Diode" ([S5066-APP7](#))

This paper provides an overview of these specifications and rationale for the approach.

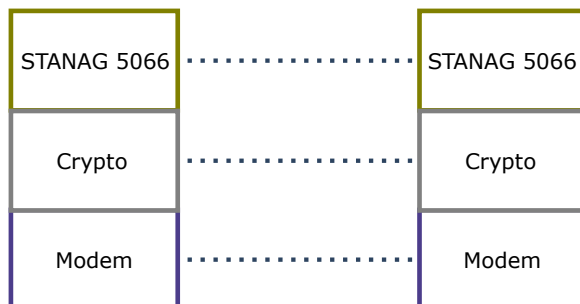


Isode whitepapers are licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#).

1. Background and Requirements

1.1 Provision of HF TRANSEC above Modem

For HF communication, data encryption has typically taken place above the modem using Crypto placed between modem and Crypto, as illustrated below.



Traditionally, this has been performed using synchronous serial devices such as KIV-7. A modern approach is set out in [[STANAG 5066 TRANSEC Crypto Layer using AES and other Protocols - S5066-EP14](#)].

1.2 Providing Type 1 Protection of User Data (COMSEC)

For Military communication over HF, it is usually required to protect all user data with a Type 1 Crypto product which must use Type 1 cryptographic algorithm. Type 1 is defined by NSA for US use. It is used in this specification to refer to a concept which is widely used. Operation directly over the modem is a good architectural choice, as STANAG 5066 protocol includes sensitive information (addressing, protocol) which must be protected.

The synchronous serial devices in current use will need to be replaced medium/long term. Although [[S5066-EP14](#)] provides a framework to achieve this, it is anticipated that some nations will not introduce Type 1 Crypto that can be used in this way, due to the high costs of accrediting such a product.

Provided that Type 1 COMSEC can be achieved for user data, it is generally acceptable to provide protection at the modem level using a product with lower levels of accreditation. S5066-EP14 provides a mechanism to achieve this TRANSEC protection with AES.

A general trend in military communications is to use IP Crypto. NATO have set out a vision of NII (networking and information infrastructure) IP Network Encryption (NINE). This uses High Assurance Internet Protocol Encryptor (HAiPE) which is based on IPsec standards. Countries are developing modern HAiPE/IPsec solutions based on national crypto, with products such as TACLANES. So, Type 1 IP Crypto products are widely available.

This whitepaper shows how COMSEC protection for HF can be provided with IP Crypto.

2 Architecture

IP Crypto sits between red and black sides, providing separation. The use of IP service is explained, and then the architecture is described in three parts:

- Black Side.
- Red Side.
- Red/Black boundary.

2.1. Extended IP Service

The natural and simplest way to deploy IP Crypto is in an environment where all applications run over IP. This is not viable for HF.

Many IP applications, particularly bulk applications and HTTP over TCP will not run efficiently when IP is mapped directly only HF as an IP subnet using STANAG 5066 F.12 IP Client. This is discussed in the Isode whitepaper [[Measuring and Analysing STANAG 5066 F.12 IP Client](#)].

A number of applications built for HF have optimized protocols over STANAG 5066 and it is highly desirable to use these protocols.

As a consequence, IP Crypto needs to be used in a special manner.

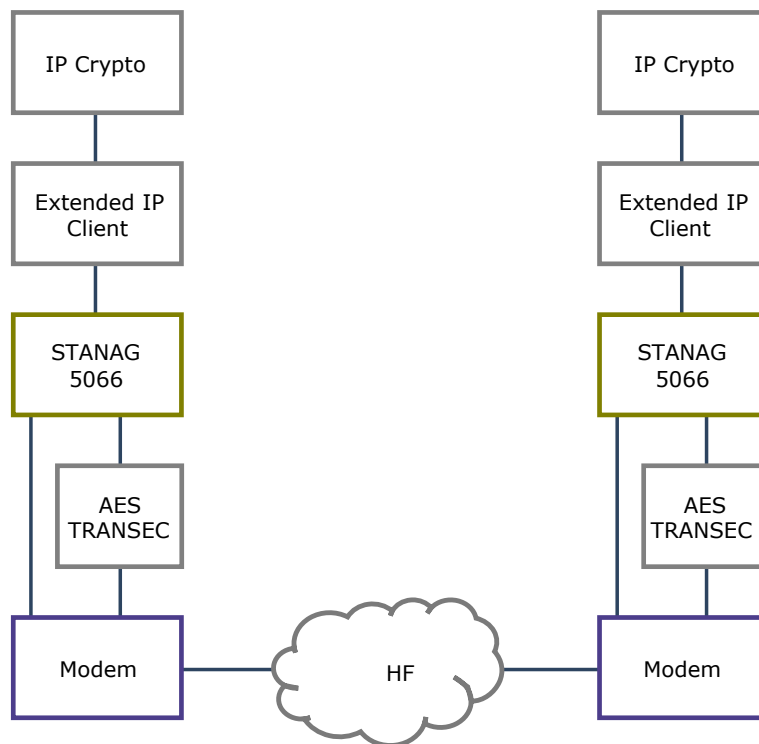
The architecture described here provides an extended IP service by:

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-APP6](#)); 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-APP7](#)).

This extended IP service is contrasted to standard IP in the following table.

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

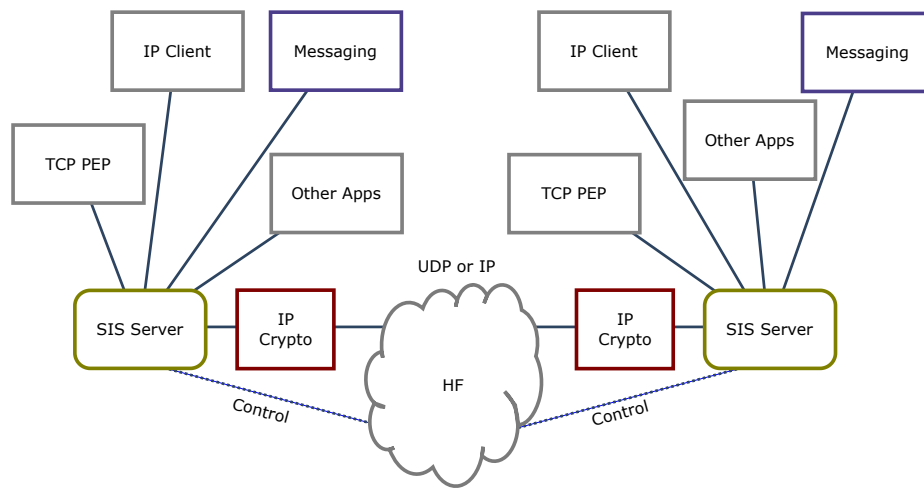
2.2 Black Side Architecture



The black side architecture needs to transfer IP packets being sent through the IP Crypto. This is achieved using standard STANAG 5066 using STANAG 5066 Annex F.12 IP Client to do the IP transfer. Key points on the black side architecture:

1. All Data Transferred through IP Crypto.
2. Standard STANAG 5066 Server is used black side. No changes to STANAG 5066 are needed to support this architecture.
3. IP is the *only* black side service/application. An extended IP Client which can use one of two protocols:
 1. STANAG 5066 F.12 IP Client.
 2. Implicit IP specified in [Implicit IP Client over STANAG 5066 ([S5066-APP5](#))] may be used. This transfers only IP payload, and receiver constructs IP headers from STANAG 5066 addressing. This can be done because there are a constrained number of addresses and mapping is mechanical. This is preferred, as it reduces overhead.
4. Data transfer between STANAG 5066 and modem is protected using AES as specified in [[STANAG 5066 TRANSEC Crypto Layer using AES and other Protocols - S5066-EP14](#)].
5. STANAG 5066 can monitor and control the modem directly, as both modem and STANAG 5066 sit black side in this architecture.
6. QoS, reliability, flow control and error handling are handled across the red/black boundary by the Extended IP Client. These mechanisms are described in the red/black architecture section.

2.3 Red Side Architecture



On the red side, a SIS server provides the STANAG 5066 SIS service to all applications. This looks exactly like standard STANAG 5066 to all of the applications. This makes the service completely transparent to all the HF applications.

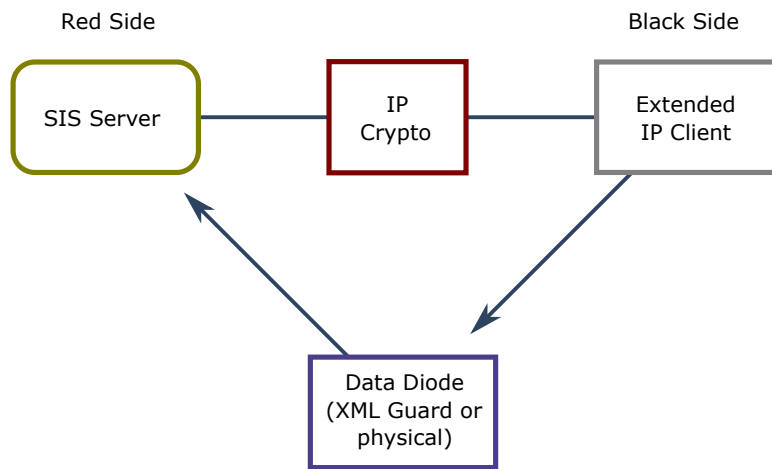
SIS Servers communicate with each other using IP, optionally with UDP over the IP. The IP passes through IP Crypto which provides red/black separation.

Key points on this architecture:

1. All Data through HF goes through IP Crypto.
2. Red side SIS Server provides a subset of the standard STANAG 5066 SIS Service. The following elements of service are not provided (these elements of service are not needed by any applications that Isode is aware of).
 1. Hard Links.
 2. Expedited Data.
 3. Rank.
 4. TTL.
3. All applications, including all IP services, operate over SIS. IP Services can use a red side STANAG 5066 IP Client Service or a PEP service for TCP and other applications.
4. SIS Server communicate with a new end to end protocol operating over either over IP or UDP, that carries SIS U_PDU, priority, ARQ/non-ARQ, SAP. This provides a simple end to end protocol. The protocol provides end to end acknowledgement option, to provide client acknowledgement service. This protocol is specified in [[Providing STANAG 5066 services over UDP/IP - S5066-APP4](#)].
5. Two protocol mapping options are defined (UDP and IP). One of these may be eliminated in future versions of S5066-APP4. Reasons for the choice:
 1. Use of UDP is straightforward in most programming languages and operating systems.
 2. Direct use of IP eliminates the UDP overhead, which is desirable.
6. The S5066-APP4 protocol uses IP addressing, as IP addresses must be included, and it seems wasteful to include a second address. A SIS Server must map the STANAG 5066 addresses used by standard STANAG 5066 applications with IP addresses. It is anticipated that a future extension will be developed to allow applications to use IP addressing and so avoid this mapping.
7. Controls additional to UDP for QoS, reliability and flow control are described in the Red/Black architecture section.

2.4 Red/Black Architecture

The core of the red/black architecture is separation by IP Crypto. In order to address QoS, reliability and flow control, additional information needs to flow in each direction. Red to Black crypto bypass is undesirable for security reasons. It is possible to pass necessary QoS information from red to black without a crypto bypass.



It is necessary to pass monitoring and control information from black to red side. This is achieved by a use of a data diode, which ensures that data only flows black to red. This might be a “physical” data diode that ensures unidirectional data transfer or it may be an XML Guard providing an application data diode service. Further details:

1. IP Crypto provides the COMSEC and primary red/black separation. This can be used with standard IPsec and the architecture does not have any constraints on the IP Crypto used. IP Crypto will encrypt red side IP information (IPsec tunnel mode), as the IP addressing information is sensitive and should be considered as user data. We should also provide an option to use transport mode.
2. IP Crypto key configuration can use two approaches:
 1. IPsec standard session setup (or equivalent) may be used between a pair of nodes not in EMCON (using ARQ transfer).
 2. HAIPE key pre-configuration (or equivalent) is necessary for broadcast, multicast and EMCON operation.
3. Priority and ARQ/non-ARQ need to be communicated from SIS Server (Red Side) to Extended IP Client (black side) to meet QoS objectives. This can be achieved with IP Crypto using one of two mechanisms (the details of which are specified in [[Providing Control Parameters for STANAG 5066 over UDP through IP Crypto](#)]):
 1. DSCP. This is preferred, as it is simple and expected to work in most cases; or
 2. Use of IP address (32 addresses needed for all priority ARQ combinations). This will be necessary for IP Crypto where DSCP is not transferred red to black.
4. Control information needs to flow black to red, and this is achieved with a data diode. There are two options for data diode mechanism:
 1. An XML Guard (Application Data Diode); or
 2. Physical Data Diode that can be interfaced with UDP or a proprietary mechanism
5. The following information needs to be sent over the data diode:
 1. SIS Flow Control. This enables black side flow control to be passed to red side SIS server and on to red side SIS clients. This ensures working flow control. It is why all data must go through SIS.
 2. IP packet matching. Information on each IP packet sent, assigning an “IP ID” to each packet. This will include size, to/from address/, DSCP value, priority, ARQ/non-ARQ. This information will enable the black side to associate an IP ID with each packet sent.
 - NOTE. Sending an IP packet to IP Crypto will generally lead to a matching packet being quickly sent. However, it may lead to the IP Crypto sending IP packets to negotiate link setup. Also need to allow for IP packet loss, which is expected to be very rare.
 3. SIS Confirms and Rejects, using the “IP ID” from b, to enable red side to correlate confirm/reject to initial SIS request. This ensures reliability.

The details are specified in [[XML Control Messages for STANAG 5066 over UDP through a Data Diode](#)].

3 Performance Analysis

This section considers the overheads that are introduced by this approach to use IP Crypto. Application overhead remains the same, as a standard SIS interface is provided by SIS server. Standard STANAG 5066 is used in both cases, and the overheads are going to be very similar. The comparison looks at each of the

overheads introduced.

Layer	Bytes
Black Side IP Client. This has three options, with overhead dependent on the option chosen.	
IPv4	20
IPv6	40
Implicit	1
Red Side IP	
IPv4	20
IPv6	40
UDP (Options)	8
SIS Server Protocol	
Not confirmed	2
Confirmed	40

It is recommended to use Implicit IP on black side. It will generally be sensible to use IPv4 red side, and there will not be any need for red side IP extensions. It is recommended to not use UDP Most STANAG 5066 protocol is not confirmed. So, the minimum overhead of 23 bytes will be common. The maximum overhead is 93 bytes.

At 75bps, a 23 byte overhead is noticeable, but the approach is clearly viable at this bottom HF speed.

For bulk traffic, it will make sense to use maximum size STANAG 5066 MTU of 2048 bytes and to use IP datagrams that lead to this. This leads to a typical (minimum) overhead of 1.1% for bulk transfers.

4 Isode Road Map for IP Crypto over HF

Isode plans to provide COTS products supporting all of the protocols in this specification, with aim to have the full set available by end of 2020. There will be two new products:

1. Icon-IP. The black side Extended IP Client.
2. Icon-SIS. The red side SIS Server.

Icon-5066, Isode's STANAG 5066 server will be extended to provide an AES Crypto option following S5066-EP14.

Icon-IP and Icon-SIS will offer two data diode integration options:

1. UDP. This will enable straightforward integration with a number of commercial "physical" data diode products.
2. Guard Context eXchange Protocol (GCXP). GCXP is an open specification for communication with an XML Guard. This can be used to support any XML Guard, and in particular Isode's M-Guard product (shipping Q1 2020, with accreditation planned). M-Guard operates as an application data diode.

Icon-PEP (Isode product planned for Q2 2020) provides a red side solution for IP services, provided STANAG 5066 F.12 IP Client and a TCP PEP utilizing SLEP (SIS Layer Extension Protocol) streaming services specified in [[SIS Layer Extension Protocol \(SLEP\) - S5066-APP3](#)].


5 Comparison with STANAG 5070

STANAG 5070 is an initiative from Thales and French MoD. It specifies use of IP Crypto with following characteristics:

- AES TRANSEC
- IP Crypto (NINE spec)
- Modified STANAG 5066 red side and black side
- Supports IP directly

- Supports STANAG 5066 Applications
- Data Diode black to red.

This architecture has much in common with the architecture set out in this specification. However, the details are complex do not appear viable. This section gives a tabular comparison of the two specifications.

Capability	This Specification	STANAG 5070
Black Side Server	Standard STANAG 5066	Modified STANAG 5066 (STANAG 5070 Annex D)
Red Side Server	Lightweight SIS Server	Modified STANAG 5066 Server
AES TRANSEC	Specified is S5066-EP14, which addresses some deficiencies in presented STANAG 5070 Annex G	Annex G. Capabilities presented (uses Counter mode, as does S5066-EP14), but specification not shared
DSCP for QoS	Preferred option, but alternate option provided for IP Crypto that does not pass DSCP	Mandatory
Data Diode Protocol	Specified in S5066-APP7 	Left for vendor implementation choice
Operation with EMCON, Broadcast and Multicast	Yes	Not in current STANAG 5070 version. Support planned.
HAIPE pre-configured key approach	Yes	Yes
IPsec Session Setup	Yes	Not in current STANAG 5070 (STANAG 5070 Annex E requires “The security association shall be pre-stored”). Constraint may be relaxed in future version.
IP Crypto Type	Any, including commercial IPsec	IP Crypto compliant to STANAG 5070 Annex E. NINE Crypto recommended. Commercial IPsec generally requires IPsec session setup
Flow Control from Black side applied to applications	Yes	Not defined in current version of STANAG 5070. Left for vendor implementation choice.
Handling Black Side Rejects	Yes	Not defined in current version of STANAG 5070
Handling user IP traffic sent directly to IP Crypto, without red side processing.	No Does not fit architecture	Yes Isode anticipates that performance will be poor.
WBHF (Contiguous)	Yes	Not defined in current version of STANAG 5070. Placeholder for future update
HFXL (Non-Contiguous)	No Recommend to extend STANAG 5066 to support non-contiguous	Yes
Narrowband down to 75bps	Yes	Not in current version of STANAG 5070, as TDD approach is inefficient at very low speeds

6 Conclusions

Use of IP Crypto with HAIPE type devices for operation over HF appears desirable for some nations. This paper describes a set of open specifications that can achieve this in an efficient manner. These specifications are offered to NATO for inclusion in a future edition of STANAG 5066.

Isode plans to provide in 2020 a set of COTS products that implement the protocols described and referenced here.