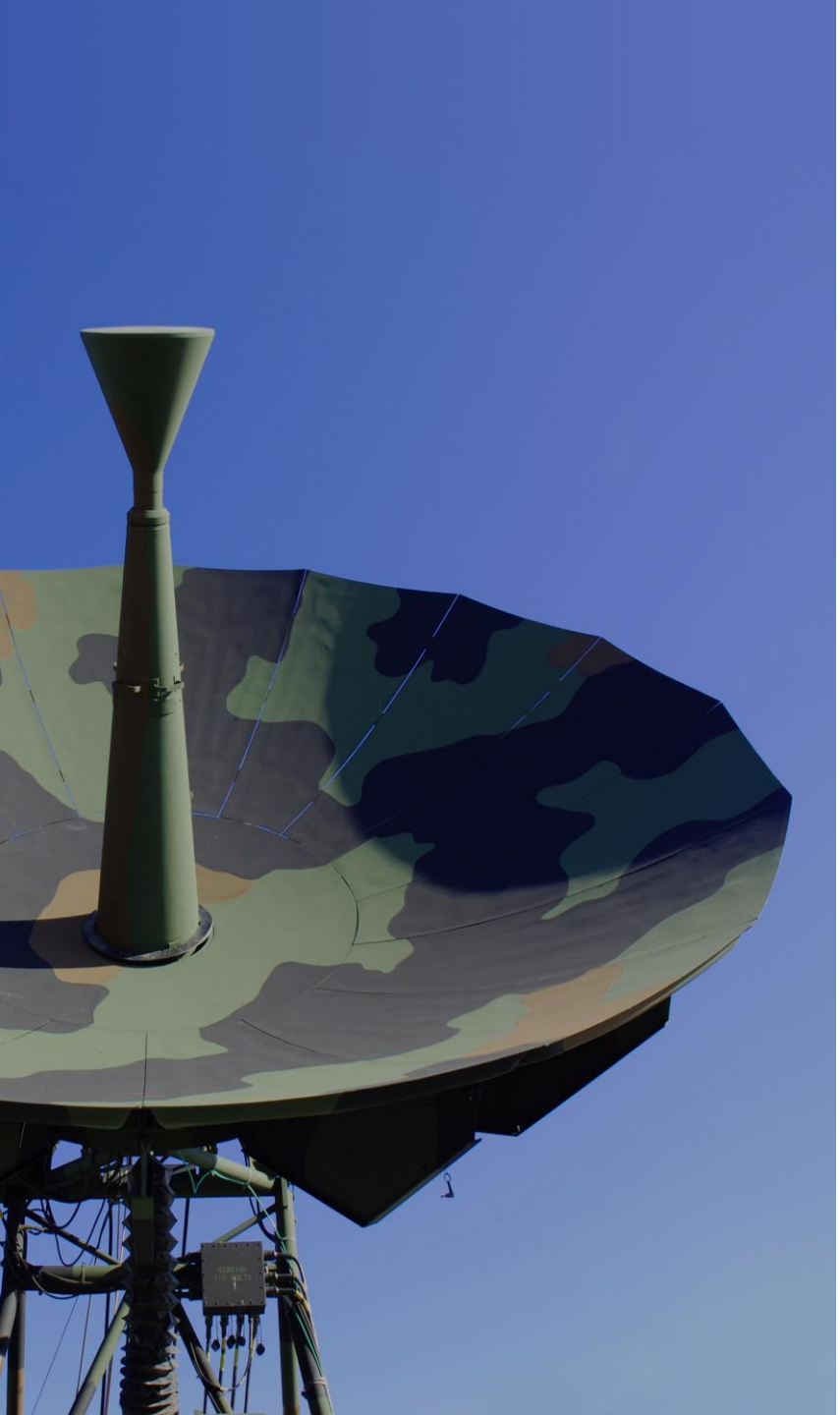
Isode

PRODUCT ANNOUNCEMENT: M-GUARD 1.0 AND ICON-5066 1.2

Steve Kille

CEO Isode Ltd

4th March 2020

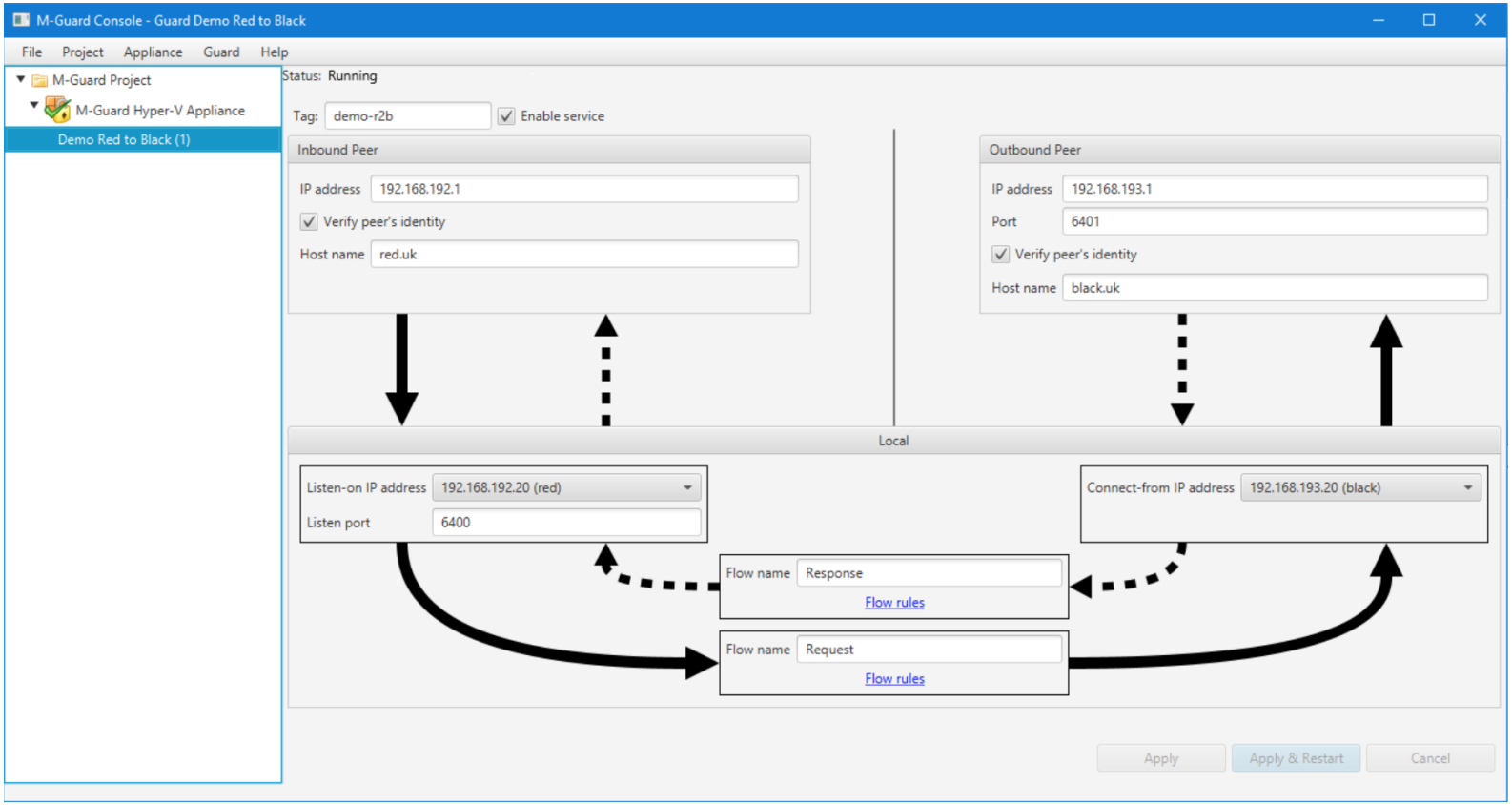


Contents

M-Guard 1.0

- M-Guard 1.0 Launched at WEST (2 days ago)
  - Available immediately
  - Product overview and white paper on Isode web site
- A guard for checking XML content exchanged by applications across network boundaries:
  - Red/Black separation (three Isode applications for HF planned)
  - Cross Domain (XMPP & Messaging Isode applications planned)
- M-Guard can act as an application-level data diode
- Delivered as software appliance package
  - Uses NanoBSD (cut down FreeBSD)
  - Reference Hardware Netgate SG-5100 (shown)
  - Virtual Machines (Hyper-V; VirtualBox)
  - Multiple guard instances can run on single appliance
- Accreditation Planned

M-Guard Management

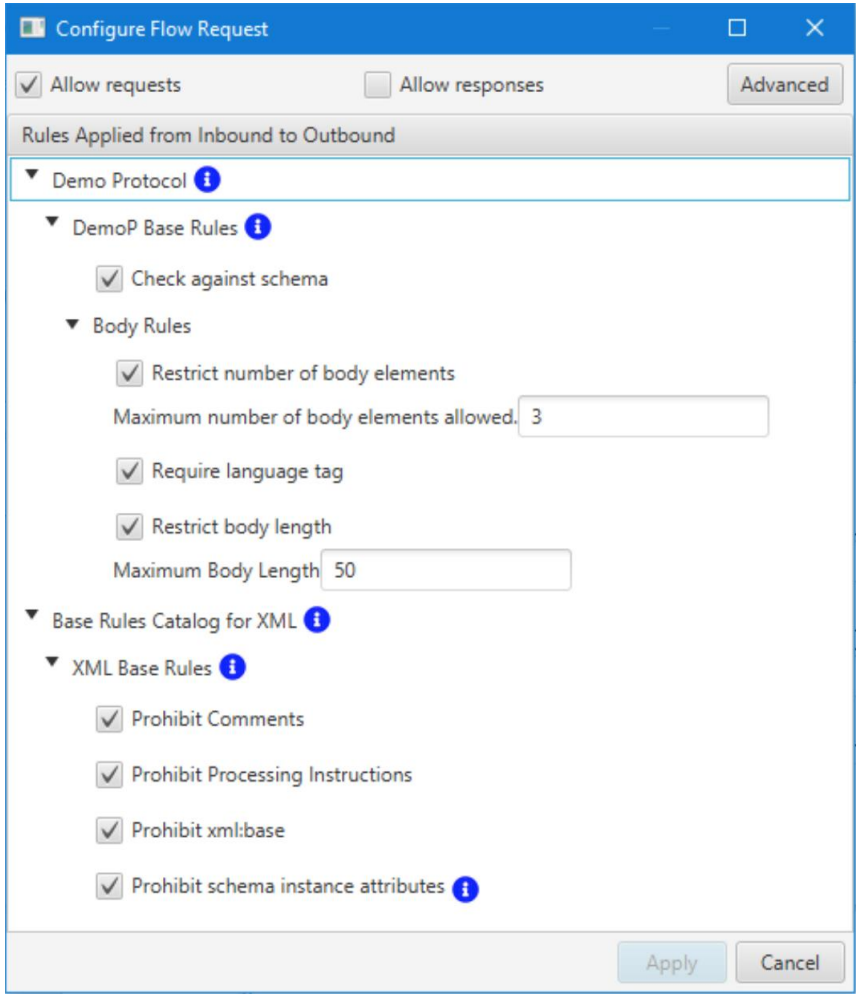


- M-Guard Console (Java GUI) provides appliance and guard configuration

- Connects on separate port
- Minimizes functionality on appliance

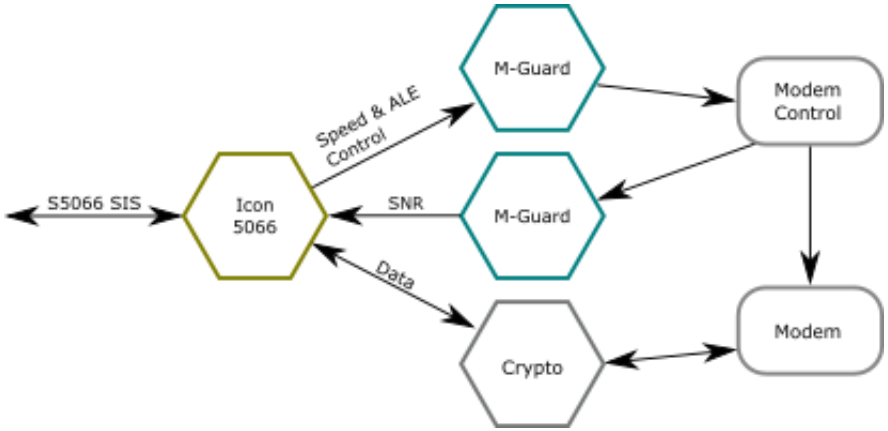
Rule Configuration

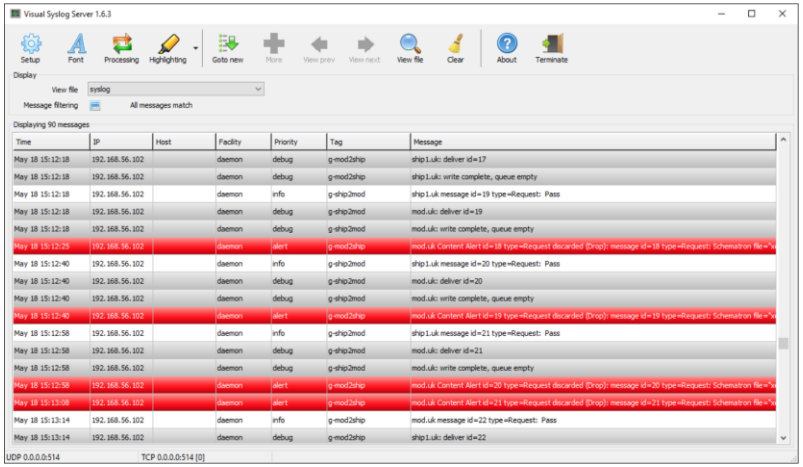
- Rule selection from M-Guard Console
- Flexible XML Rules
  - Key benefit of using XML
  - XML Schema; Xpath; Schematron; RELAX NG
- Application Profiles
  - M-Guard Console can load Application Profiles for applications
  - Application Profiles belong to the application, not M-Guard
    - English description + XML Rules



GCXP and Monitoring

- Syslog monitoring of Guard activity
  - Can feed to system of choice
  - Simple syslog UI shown
  - Separate port
- Applications communicate with M-Guard using Guard Content eXchange Protocol (GCXP)
  - Open protocol
  - TLS with two way strong authentication
  - Open source (C++) reference implementation
  - CBOR (RFC 7049) framing
  - Developed as no suitable open guard interface protocols found





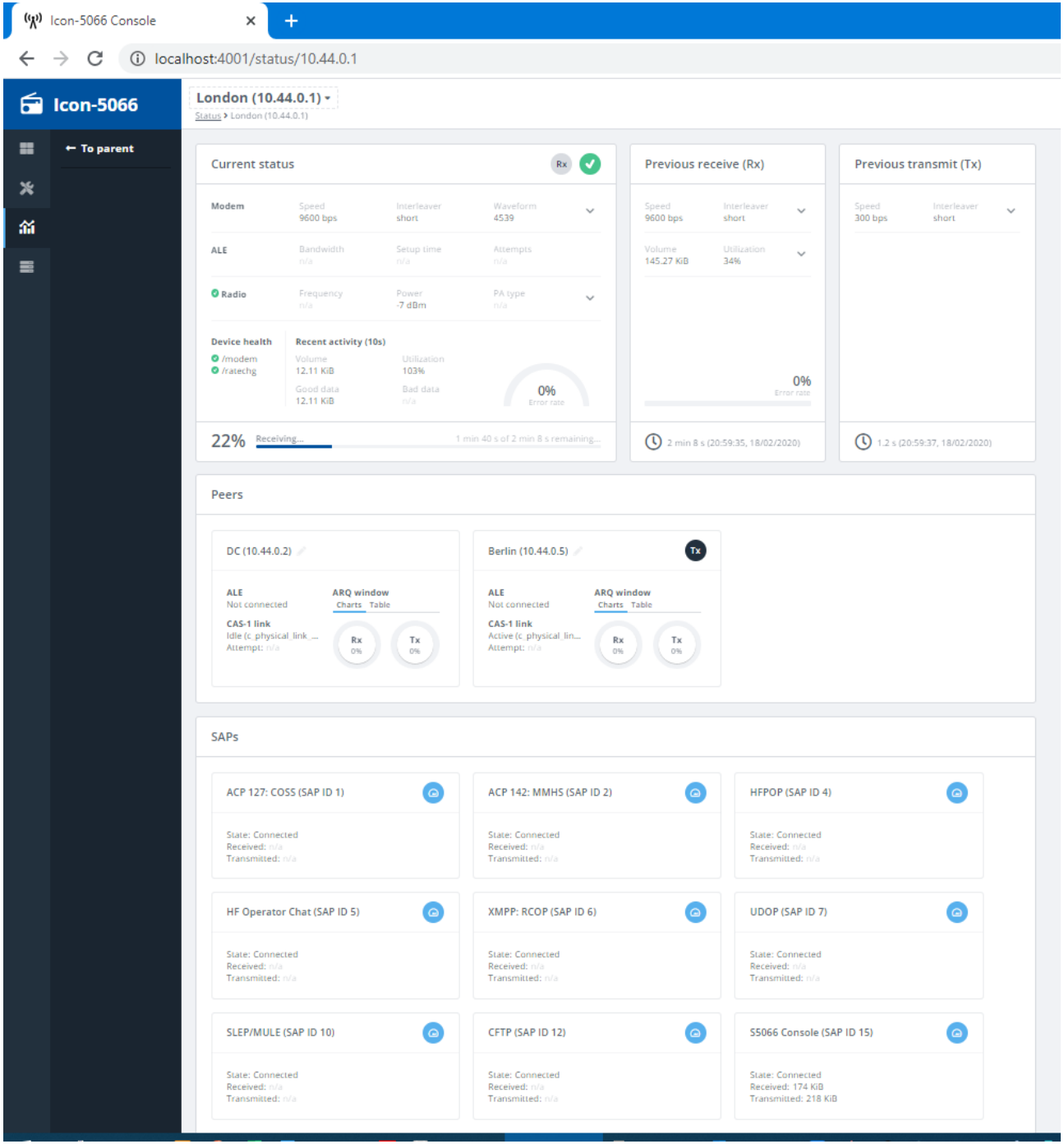
Isode

Any Questions on M-Guard?

(before moving on to Icon-5066)

Icon-5066 1.2

- Complete – shipping March 2020
- Isode's STANAG 5066 Server
  - Modem Independent
  - 1.0 presented to HFIA previously (in Bristol)
- Key changes since 1.0
  - Full support and integration of ALE, including 4G ALE
  - Improved UI (next slide)
  - Monitoring of Power Amplifier (noted as we did not expect to need to do this)
  - Crypto Bypass
    - Can also provide proxy to support remote modem

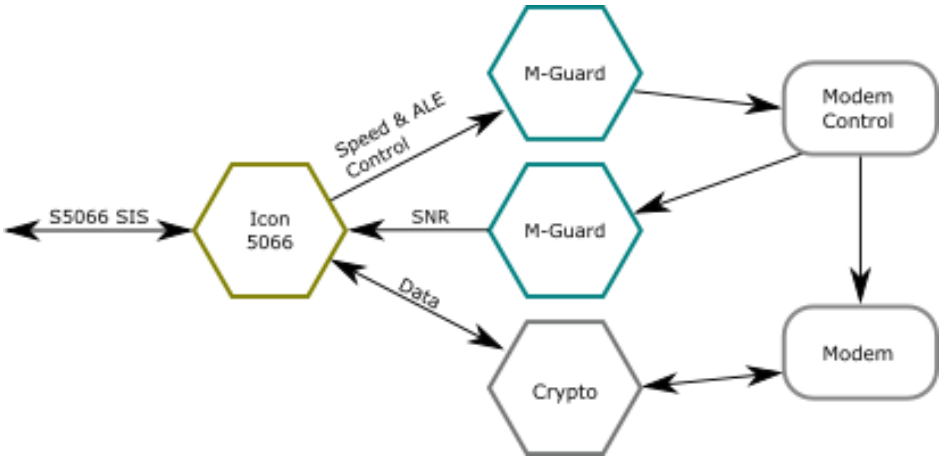

Icon-5066 Console
localhost:4001/status/10.44.0.1
Icon-5066
London (10.44.0.1)
Status › London (10.44.0.1)
To parent
Current status
Rx
Modem
Speed 9600 bps
Interleaver short
Waveform 4539
ALE
Bandwidth n/a
Setup time n/a
Attempts n/a
Radio
Frequency n/a
Power -7 dBm
PA type n/a
Device health
/modem
/ratechg
Recent activity (10s)
Volume 12.11 KiB
Utilization 103%
Good data 12.11 KiB
Bad data n/a
0%
Error rate
22%
Receiving...
1 min 40 s of 2 min 8 s remaining...
Previous receive (Rx)
Speed 9600 bps
Interleaver short
Volume 145.27 KiB
Utilization 34%
0%
Error rate
2 min 8 s (20:59:35, 18/02/2020)
Previous transmit (Tx)
Speed 300 bps
Interleaver short
1.2 s (20:59:37, 18/02/2020)
Peers
DC (10.44.0.2)
ALE
Not connected
ARQ window
Charts Table
CAS-1 link
Idle (c_physical_link_...
Attempt: n/a
Rx 0%
Tx 0%
Berlin (10.44.0.5)
Tx
ALE
Not connected
ARQ window
Charts Table
CAS-1 link
Active (c_physical_lin...
Attempt: n/a
Rx 0%
Tx 0%
SAPs
ACP 127: COSS (SAP ID 1)
State: Connected
Received: n/a
Transmitted: n/a
ACP 142: MMHS (SAP ID 2)
State: Connected
Received: n/a
Transmitted: n/a
HFPOP (SAP ID 4)
State: Connected
Received: n/a
Transmitted: n/a
HF Operator Chat (SAP ID 5)
State: Connected
Received: n/a
Transmitted: n/a
XMPP: RCOP (SAP ID 6)
State: Connected
Received: n/a
Transmitted: n/a
UDOP (SAP ID 7)
State: Connected
Received: n/a
Transmitted: n/a
SLEP/MULE (SAP ID 10)
State: Connected
Received: n/a
Transmitted: n/a
CFTP (SAP ID 12)
State: Connected
Received: n/a
Transmitted: n/a
S5066 Console (SAP ID 15)
State: Connected
Received: 174 KiB
Transmitted: 218 KiB

Isode

Crypto Bypass and STANAG 5066

- Crypto Bypass is a key issue for STANAG 5066
  - Swept under the carpet in the specification
  - Vendor options simplistic or non-existent
- Varying deployment approaches
  - Not used at all in some countries
  - Sometimes system accreditation of quite simple approaches
- Crypto Bypass needs considering
  - Necessary for variable speed, which is important to optimize performance
  - Necessary for ALE
    - 4G ALE is pretty much essential for WBHF

Icon-5066 use of M-Guard for Crypto Bypass



- Icon-5066 has option to use pair of XML Guards
- Modem Control is black side proxy module
  - Part of Icon-5066
- Integration using GCXP
  - Straightforward use of M-Guard; or
  - Enables use of alternate XML Guard
- XML Guard appliance provides red/black separation
- Icon-5066 Crypto Bypass Application Profile
  - Defines XML messages controlled in each direction

Any Questions?