ND1613:2006/12

Management of NGN Interconnect: Transport Service Layer

Issue:- *Issue 1*

Network Interoperability Consultative Committee
Ofcom
Riverside House,
2a Southwark Bridge Road,
London SE1 9HA
UK
http://www.nicc.org.uk

Normative Information

The Technical Secretary, Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London SE1 9HA.

CONTENTS

1. INTRODUCTION

A significant driver for Next Generation Networks (NGNs) is the realisation of a common network that can simultaneously support multiple services on the same platform infrastructure. NGNs use a number of packet technologies for service transport, of which the most common is Internet Protocol (IP). However, an NGN interconnect also has to support services that are not IP based, therefore the underlying interconnect transport technology needs to accommodate the range of services that require interconnect. In order to use interconnect physical connections efficiently, i.e. fibres, the underlying interconnect transport infrastructure needs to be able to be flexibly configured to allow a range of services to share these connections.

The approach for NGN Multi Service Interconnect (MSI) is to define a common transport infrastructure that is service independent and can offer different transport capabilities to the services requiring interconnect. As new services are added to the scope of the NGN MSI, a new service-specific specification will be produced that will define how the service works and its use of the underlying common transport. This new service specification, or any enhanced service specification, will be included in the scope and associated document references of the NGN MSI Release document.

In order to manage the complex relationship between the services that are defined for using the NGN MSI and other associated UK standards at any one point in time, interconnect release is defined by a top level document for each release.

2. DOCUMENT SCOPE

This document identifies the Purple Release common transport attributes that each CP needs to identify and exchange when interconnecting with another CP.

Each CP will use their own procedures to manage their internal transport functions. For the purposes of interconnect an agreement must be reached on common parameters to enable a common understanding of the transport function management.

3. DEFINITION OF TERMS USED IN THIS DOCUMENT

3.1 Key Words

The key words “**shall**”, “**shall not**”, “**must**”, “**must not**”, “**should**”, “**should not**”, “**may**”, “**need not**”, “**can**” and “**cannot**” in this document are to be interpreted as defined in the ETSI Drafting Rules [1]

3.2 Abbreviations

AES ....Advanced Encryption Standard
ATM.......................................Asynchronous Transfer Mode
CP...Communications Provider
DES ....Data Encryption Standard
ESP...Encapsulated Security Payload
ETSI ....European Telecommunication Standards Institute
GFP ....General Framing Protocol (ITU G.7041)
HMAC-SHA1-96..................Security Hash Algorithm 1
HMAC-MD5-96 ....Message Digest 5 algorithm
IETF ....Internet Engineering Task Force
IKE...Internet Key Exchange
IP ....Internet Protocol
IPsec.......................................IP Security
ISDN ....Integrated Services Digital Network*
LCAS ....Link Capacity Adjustment Scheme (ITU G.7042/Y.1305)
MSI ....Multi-Service Interconnect
ND..NICC Documentation
NGN.......................................Next Generation Network
NICC ....Network Interoperability Consultative Committee
PSTN......................................Public Switched Telephone Network*
SA ....Security Association
TDM.......................................Time Division Multiplex
UK..United Kingdom
VCG ....Virtual Concatenated Group

* PSTN and ISDN when used with the term ‘service’ define the replication of the service set applied to NGNs rather than the legacy networks themselves.

4. HIGH LEVEL REQUIREMENTS

4.1 Purple Release Requirements

All the general requirements in this release are subject to review in subsequent releases.

4.2 Note on the Use of LCAS

LCAS is recognised as a technique for varying the capacity of an Ethernet link carried using GFP-F over an SDH VCG, without the need for an outage on the Ethernet link. LCAS is not a Purple Release Requirement, but may be used across an MSI by bilateral agreement.

5. GENERAL REQUIREMENTS

5.1 Common Transport Function Attributes.

The following are attributes that **should** be known by and exchanged between CPs to facilitate the management of the common transport function. The following addresses the transmission through to the transport capability layers of the Purple Release as represented in the layer diagrams currently in ND1614 [1].

5.2 Common Transport Function attributes that should be exchanged between interconnecting CPs to enable successful management.

5.2.1 Physical Attributes

The physical location of fibre ends.
CPs should note that in a protected configuration there will be more that one fibre and that these may be in more than one location.

5.2.2 SDH Transmission Attributes

The transmission size indicates the size of the SDH transport circuit used over the interconnect; e.g. STM-1, STM-4, STM-16 or STM-64.

The Protection Type indicates whether protection is used. These may be SDH unprotected and SDH MSP 1+1 (Multiplex Switching Protection).

It will be required to identify the transport capability per SDH VC or VCG. Refer to ND1611 [2] for a list of supported transport capabilities.

5.2.3 Ethernet over SDH Attributes

The size of each GFP-F mapped Ethernet link shall be indicated both by its nominal Ethernet capacity and by the size of the virtual circuit Group (VCG) supporting it.

This VCG size shall comprise data on the SDH virtual container type used (VC-12, VC-3 or VC-4) and the number of virtually concatenated VC channels used.
The ability to configure and coordinate the SDH VCG channel count via the LCAS protocol shall be indicated.

5.2.4 Ethernet Transmission Attributes

It will be required to identify the size of the Ethernet transmission link. Refer to ND1611 [2] for the size of Ethernet transmission links.

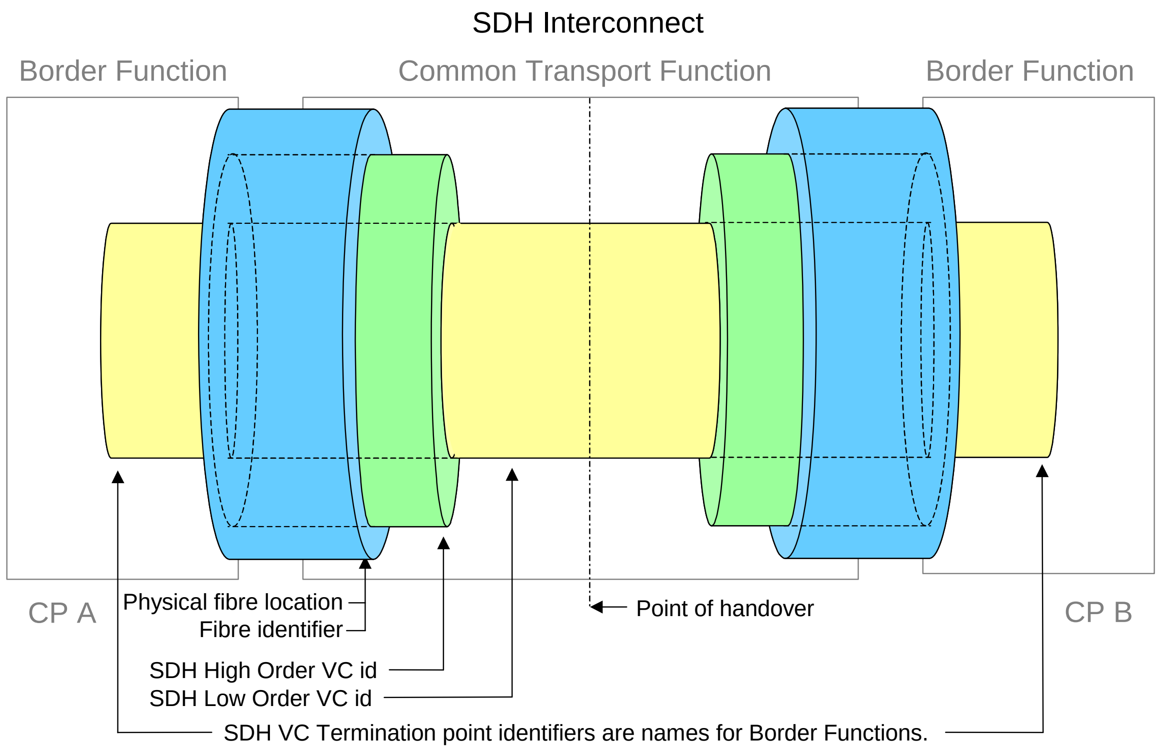
5.2.5 Fibre / Ethernet attributes

Fibre and Ethernet attribute types that need to be checked against the transmission type are included in section 5 of ND1611 [2].

The protection type indicates whether the Ethernet uses protection. The options available are Ethernet unprotected or Eth LAG (Link Aggregation, IEEE 802.3ad).

5.2.6 SDH Transport Capability

The SDH hierarchy needs to be identified for:
a) low order and high order SDH Virtual Containers and
b) Virtual Container end points.
The identifiers required for the SDH transport capability are shown in Figure 1.



This allows CPs to configure their services to understand what is connected to the SDH VC. For example:
CP A – SDH VC Termination point = Bristol 2367. CP B – SDH VC Termination point = CDF12.
It is expected these “names” or “labels” have a meaning to higher layer service systems e.g. an IP address.

Figure 1:- SDH Interconnect Identifiers

5.2.7 Ethernet over SDH Transport Capability

The SDH hierarchy needs to be identified for:

a) low order or high order SDH Virtual Containers Groups and
b) Virtual Container Group end points.

The following Ethernet attributes need to be specified:

a. Whether single or double VLAN tags are used.
b. Maximum transmission rate set by VCG
c. Maximum transmission unit size.
d. Which 802.1 P-bits (Priority) are used.
e. List the Ethernet VLAN IDs.

Per Ethernet VLAN the following needs to be identified:

a. VLAN termination points.
b. Bandwidth.
c. Burst size.

The mixed identifiers required for the Ethernet over SDH transport capability are shown in Figure 2.

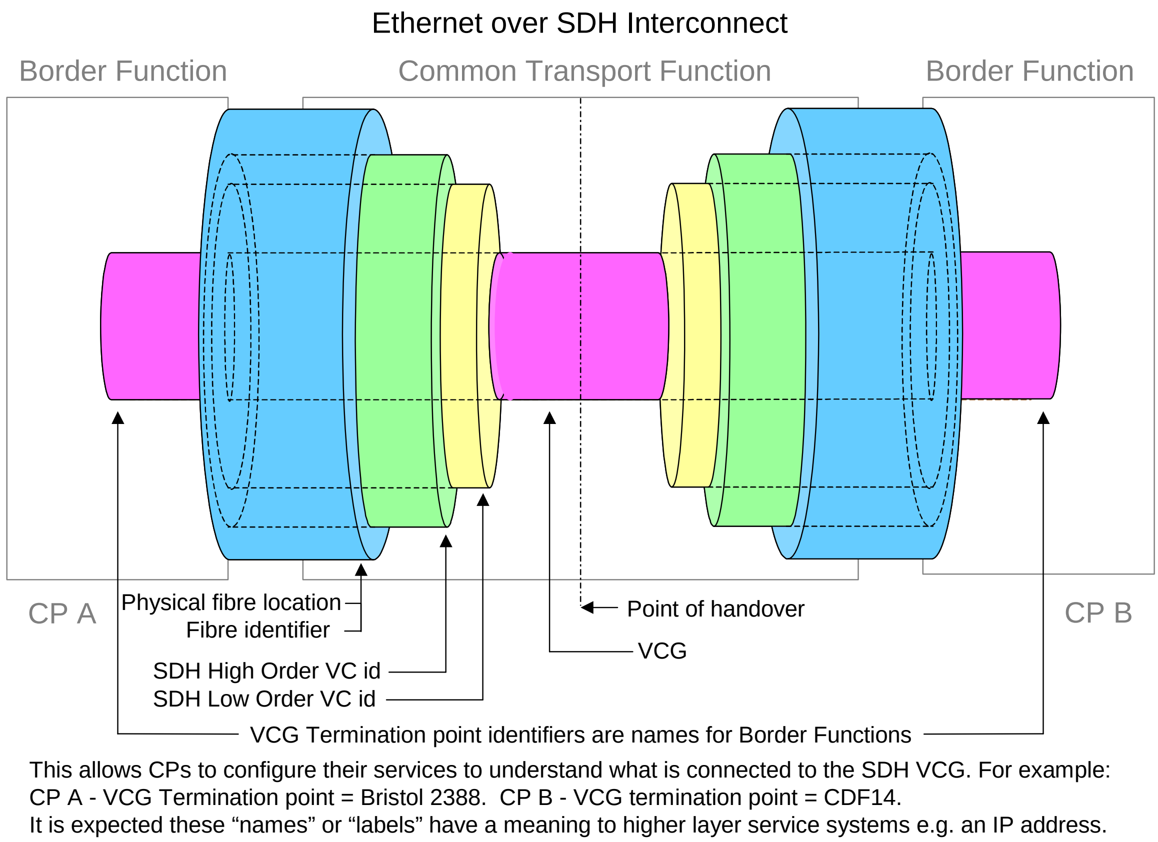
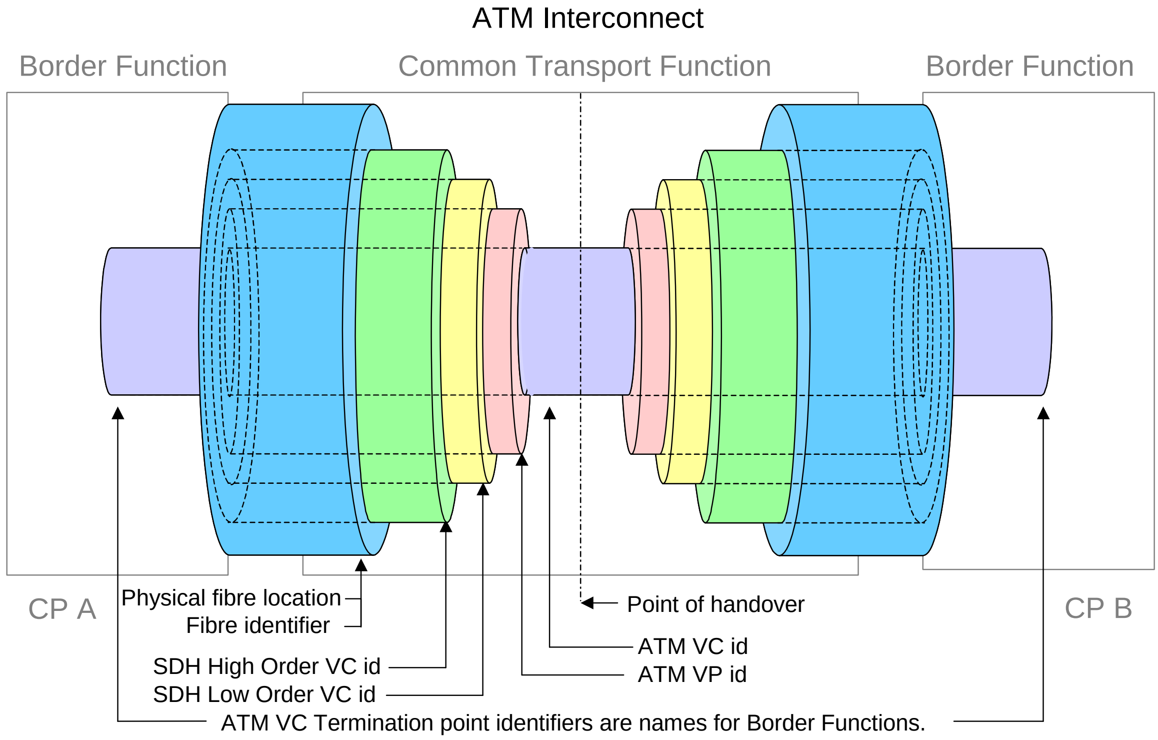


Figure 2:- Ethernet over SDH Interconnect Identifiers

5.2.8 ATM Transport Capability

There is a 1:1 mapping with SDH VCs. The VC end points need to be identified. The identifiers required for the ATM transport capability are shown in Figure 3.



This allows CPs to configure their services to understand what is connected to the ATM VC. For example:
CP A – ATM VC Termination point = Bristol 2367. CP B – ATM VC Termination point = CDF12.
It is expected these “names” or “labels” have a meaning to higher layer service systems e.g. an IP address.

Figure 3: ATM Interconnect Identifiers

5.2.9 Ethernet Transport Capability

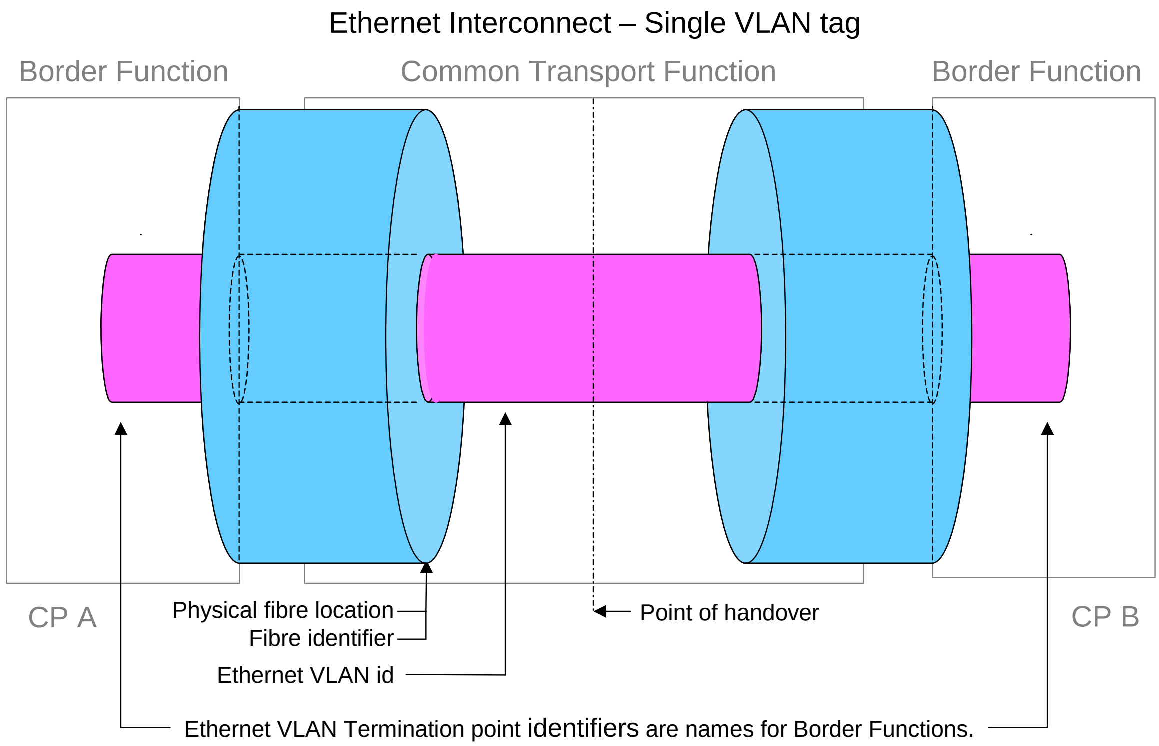
The following Ethernet attributes need to be specified:

a. Whether single or double VLAN tags are used.
b. Maximum transmission unit size.
c. Which 802.1 P-bits (Priority) are used.
d. List the Ethernet VLAN ids.

Per Ethernet VLAN the following needs to be identified:

a. VLAN termination points.
b. Bandwidth.
c. Burst size.

The identifiers required for the Ethernet transport capability are shown in Figures 4 and 5.



This allows CPs to configure their services to understand what is connected to the VLAN. For example:
CP A – VLAN Termination point = Bristol 2367. CP B – VLAN Termination point = CDF12.
It is expected these “names” or “labels” have a meaning to higher layer service systems e.g. an IP address.

Figure 4: Ethernet Interconnect, Single VLAN method, Identifiers.

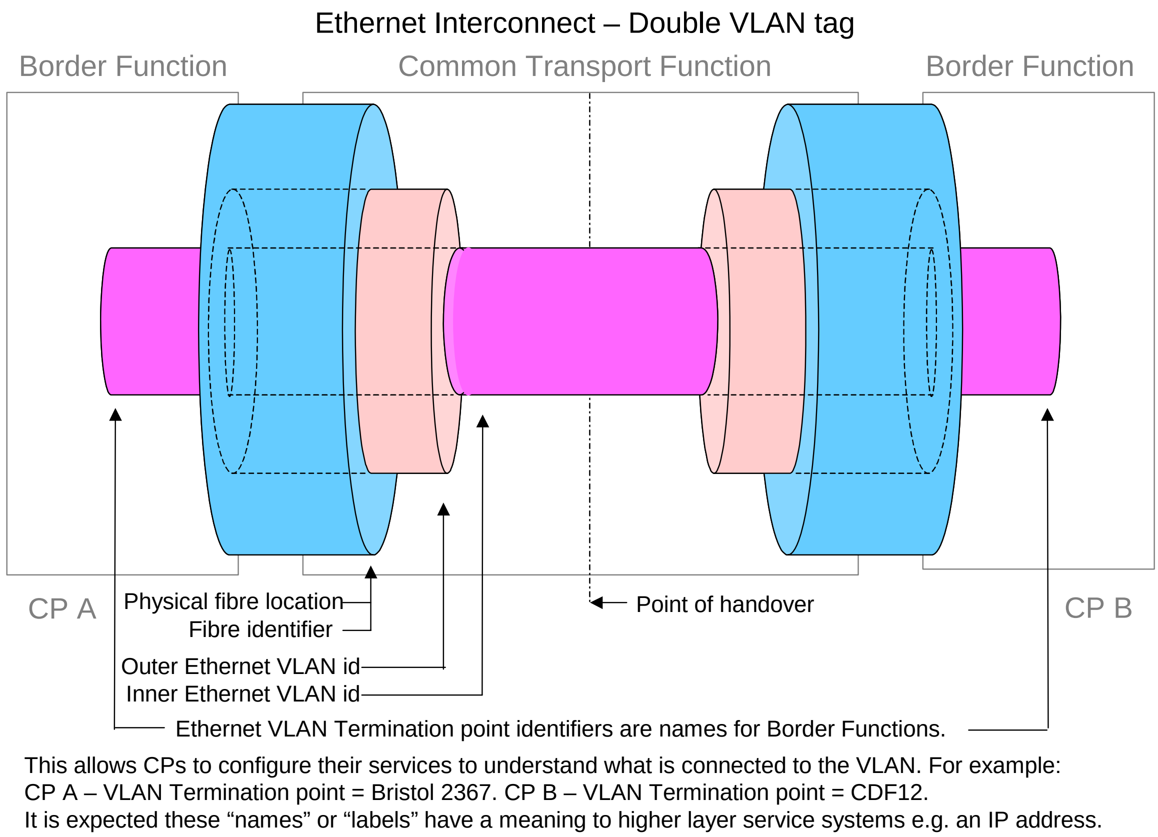


Figure 5: Ethernet Interconnect, Double VLAN method, Identifiers

5.2.10 IP Transport Capability

The following IP attributes need to be specified:

a. Whether single or double VLAN tags are used.
b. Maximum transmission unit size.
c. Which 802.1 P-bits (Priority) are used.
d. List of Ethernet VLAN ids.

Per IP VLAN the following needs to be identified:

a. VLAN termination points.
b. Bandwidth.
c. Burst size.
d. IP encapsulation type.

5.2.11 Security arrangements

The following guidance is offered for IPSec arrangements -

IPsec arrangements **should** use IKEv1 initially, moving to IKE v2 in the longer term. The use of IKE requires a security credential to be allocated to the edge device. Where the number of communicating devices is low, a pre-shared secret distributed over a secure out of band channel **may** be used as the credential. X.509

certificates **should** be used in the longer term.

Note; The use of X.509 certificates is still under investigation and awaits UK industry agreement. However, to use them properly requires a PKI, and the same investigation will also determine how this aspect will be managed.

IKE (Phase 1) renegotiation to renew the IKE Security Association between CPs **should** take place every 12 hours.

IPsec (IKE Phase 2) renegotiation to renew the IPsec SA (note 4) pair **should** take place every 1 hour for critical systems.

AES-128 (note 1) **should** be the default choice for the ESP encryption algorithm.

3DES (note 2) is an alternative ESP encryption algorithm that **may** be used.

DES is too insecure and **should not** be used. NULL encryption **must not** be used.

ESP **shall** be used with a data authentication method. Within IPsec, ESP has the option to use particular authentication options – HMAC-SHA1-96 (note 5) or HMAC-MD5-96 (note 6). CPs **shall** determine bi-laterally which option to use. However, HMAC SHA1 **should** be the default choice.

Notes –

1. AES-128 - Advanced Encryption Standard- an encryption algorithm, with a 128 bit key.
2. 3DES – a stronger form of DES that extends the effective key length of DES encrypted data
3. DES – Data Encryption Standard. Now deprecated its single DES form, which has a 56 bit key length.
4. SA – Security Association. A data structure containing the necessary parameters to set up and run a secure connection. IKE SAs are bidirectional, whereas IPsec SAs are unidirectional – two are required for a link that is encrypted in both directions.
5. HMAC-SHA1-96 – a keyed hash based on the Secure Hash Algorithm 1, using a key for data origin authentication. HMAC-SHA-1-96 produces a 96 bit hash (the high order 96 bits of a standard 160-bit SHA-1 hash)
6. HMAC-MD5-96 – a keyed hash based on the Message Digest 5 algorithm, using a key for data origin authentication. HMAC-MD5-96 produces a 96 bit hash (the high order 96 bits of a standard 128-bit MD5 hash)

6. REFERENCES

Ref no.	Document Reference	Title	Version	Publisher
[1]	ND1614:2006:12	Management of the General Connectivity of PSTN/ISDN Service Interconnect of UK NGNs	Issue 1	NICC
[2]	ND1611:2006:05	Multi-Service Interconnect Common Transport for UK NGNs	Issue 1	NICC

7. DOCUMENT HISTORY

Issue Number	Date	Reason for update
Issue 1	1/12/2006	Initial issue for publication on the Ofcom NICC web site.

- END of DOCUMENT -