BRITISH APCO

Knowledge Exchange for Public Safety Communications ®

Multi Agency Incident Transfer Standard: Protocol

Version: 1.0.0

March 2016

www.bapco.org/uk/mait

Please note: This document is under configuration control. Please inform the author of any new versions.

Summary of document properties

Field	Value
Title	Multi Agency Incident Transfer Standard: Protocol
Sign-off Authority	MAIT Challenge Owner
Delivery Project	MAIT Working Group
Author	MAIT Working Group
Document ID	MAIT/STD/001
Version Number	1.0.0 (Draft 2)
Filename	2016_Multi-Agency-Incident-Transfer_MAIT_v1-0-0_Draft_1

Amendment History

Date	Version	Author	Notes
2006	1b	CAPITA (formerly SunGard Vivista Ltd)	Original – IPR released to Public Domain
2012	1c	BT/ULTRA	UED/BTNRE/FC/748 – Version for DEIT Phase 1a Trial – IPR Release to Public Domain
2013	1d Candidate 1-3	BAPCO MAIT Group	Internal Versions before public release following feedback from Emergency Service User groups and BAPCO members.
24/03/2014	1d Candidate 4	BAPCO MAIT Group (TJG)	Public candidate for Open Standard discussion and participation.
28/03/2014	1d Candidate 5	BAPCO MAIT Group (TJG)	Feedback on forum
31/10/2014	1d Candidate 6	Finalisation Sub-Team (AB/DB/MJ)	Completion of editorial fixes, clarification of terms, addition of standards cross-reference, added message control object, added message versioning, added XSD namespace declaration, details of Extensions, standardised date/time format, inclusion of XML digital signing and renaming HUB to Router.
30/01/2015	1d Candidate 7	Review meeting with James Findlay	Consistent naming of standard (“Incident”, not “Information”), clarified ICM Mode, clarified some wording in 2.1, and clarified the protective marking scheme.
24/03/2015	0.2.2		Version numbering updated to reflect Management Policy
08/04/2016	1.0.0 Draft 1	Paul Chatterton (Capita) Martin Jewell (MPS) Tim Gilberts (S. Wales Fire)	Editorial changes during final review prior to issue.

22/06/2016	1.0.0 Draft 2	Paul Chatterton (Capita) Martin Jewell (MPS) Tim Gilberts (S. Wales Fire)	Final re-read and corrections for quality assurance.
1/08/2016	1.0.0 Draft 3	John Anthony	BSD License details added

Contents

1. Overview

1.1. Introduction

This document defines the Interface and Implementation Guidance used to exchange incident information between any Command and Control (C2/C&C) system for Multi Agency Incident Transfer (MAIT).

The original National System for Police Information Systems (NSPIS) interface, and its associated specification, was developed by SunGard Vivista on behalf of the Highways Agency to provide a standard incident exchange interface that can operate nationally between all C&C systems. This specification is referenced in Appendix A.

Updates to the specification for the use in the Direct Electronic Incident Transfer (DEIT) 1a Router (HUB) Pilot (a standard central exchange pattern to reduce mesh complexity of point-to-point solutions) were carried out by Ultra Electronics and released as DRAFT 1c.

This exchange interface standard has been amended from Draft Issue 1c to Draft Issue 1d Candidate 7, reflecting the lessons learned from the Phase 1a Pilot and workshops hosted by British Association of Public Communication Officers (BAPCO), attended by emergency services and various system suppliers. This is for the purpose of defining the minimum necessary extensions to satisfy the operational requirements of all emergency services, as a foundation for the MAIT project.

The standard has been refined by the BAPCO MAIT Working Group, following a public discussion period, and has been accepted on the gov.uk Open Data Standards Hub as version 1.0.0.

This standard, at the version 1 stage, continues to support backwards compatibility with earlier DRAFT 1x versions (e.g. allowing point-to-point or Router operation).

The XML schemas, as XSDs, are available at www.bapco.org.uk/mait (see the discussion forum) and in the case of a conflict between the schemas and this protocol document or implementation guidance then the schema will take precedence. If any conflicts are found, the BAPCO MAIT Standards Group should be informed so that amendments can be made.

1.2. Structure of Document

Section 1	States the background and intent of the document.
Section 2	Describes the communications and data management issues that need to be considered providing suitable implementation guidance.
Section 3	Describes the interfaces available and defines the XML elements for those interfaces.

2. Operating Protocol

2.1. Communications Management

The exchange of incident information between organisations is based on the following underlying mechanism:

- Messages are formatted using XML.
- Messages are transported between command and control systems using one of two methods;

  1) TCP/IP sockets where ports MUST be a direct message passing socket for the RAW XML

  OR

  2) SOAP (within HTTP) using a system implementing the SOAP Action(s) for all MAIT messages (such as 'IncidentCreation' and 'IncidentUpdate').

  Any system claiming compliance with this standard MUST identify itself as supporting one or both of these options by using a suffix on the MAIT version;–TS if it supports both options, -T if it supports only option 1 and –S if it supports only option 2. E.g. This system complies with MAIT1.0.0-T, MAIT1.0.0-TS or MAIT1.0.0-S. Users of the standard must be careful as directly connected end-systems that are not both using the same protocol option (either –T or –S) on that particular connection will be UNABLE to interoperate.

  MAIT Routers MUST provide the ability to use –T or –S on the end-system connection (as is compatible with the end-system) independently of all other end-system connections.

- Messages are not delimited by start and end characters beyond the XML descriptors.
- Systems MUST ignore any unknown **message types** to allow the standard to expand (this also means systems MUST ignore unknown versions of messages). Unknown **elements** (in valid messages) from Schema 1.0.0 onwards should raise an error as not conforming to the XSD validation and this will result in the message being rejected by the receiving system. See Extensions options for how to add ad-hoc elements without violating these validation rules. It is RECOMMENDED that end systems retain the key information from rejected messages, if it can be retained (such as, OriginOrg, OrigIncidentNum), so that useful error reports can be provided (and sent to the originator, if possible).
- It is RECOMMENDED that End Systems implementations put in place controls for the management of processing invalid messages to assist in the prevention of Denial Of Service (DOS) attacks.

- The MAIT interface from the End System operates to ISO-8859-1 XML encoding standards up to schema Version 1c. Note that to support multi-lingual (including Welsh) character transfer it is necessary that schema 1.0.0 onwards use the UK Open Standard of UTF-8. Therefore systems using UTF-8 MUST include an encoding value attribute in the initial XML header which consists only of ASCII allowing an encoding change if needed i.e. `<?xml version="1.0" encoding="UTF-8"?>` The absence of an encoding attribute will assume ISO-8859-1 (also a single byte standard). It should be made clear that legacy systems MAY immediately translate non ASCII characters and users MUST confirm with the receiving organisation that they will be able to handle information other than the basic ASCII character set – see Control Characters / Non-ASCII Characters.

- An End System may communicate directly with another End System or an End System may communicate with a Router. A Router is identified in the following as a system able to link multiple End Systems using TCP/IP based protocols and to route message between different End Systems.

- The MAIT interface from the End System (or the Router interface) connects to a single IP address for each external organisation with which incidents will be exchanged. The single far end IP address will be visible to the local end in point-to-point (directly connected) interfaces but will not be visible to the local end in the Router connection architecture – only the Router IP address will be visible to the local system in this case. Systems MAY (and any Router solution SHOULD) implement the ability to connect to two alternative address/port combinations if no response is received within a definable timeout, after a configurable number of retries. It is expected that this will allow suitably equipped receiving systems to provide a hot standby server and a cold standby Disaster Recovery Site where IP address management techniques such as HSRP or load balancing are not used.

- The interface connects through a single port number, for both inbound and outbound messages. Port numbers on either organisation side are subject to agreement between the organisations including any Router operator. Each organisation is also responsible for resolving its own IT security issues, including any network (e.g. PSN) accreditation, connection and associated IT health checks if required.

- The communication protocol is connect-send-acknowledge-disconnect (as both RAW and SOAP/HTTP are delivered over TCP/IP). The originating system connects to the receiving system, sends the message, receives the acknowledgement (on the same socket) and disconnects from the recipient system. The resulting effect is that the originating system acts as a client connecting to the receiving system which acts as the server.

- The communication is synchronous using a single two-way socket. As a result, it is only possible to send one message at a time to a given external system. Outgoing messages should therefore be queued as necessary by the sending system to be sent after the acknowledgement for the previous message has been received.

- On failure of a connection, the originating system is responsible for trying to re-establish the connection and taking any consequential action – see also alternative address note above.

- To minimise adverse operational impact, participating organisations SHOULD notify each other when an interface is unavailable (for example due to maintenance). In a Router environment it is RECOMMENDED that a supplier will support some form of out of band management service to exchange basic metadata covering this and other aspects of functionality. The methods for these notifications and out of band communications are not covered in this specification (the Router specification is also not covered in this document).

- Due to the connection protocol being connect-on-demand, heartbeat messages are not required for connection monitoring. If a group of users wish to implement such a system then they MAY agree to use an Incident Update Message (IUM) for a suitable incident, as a form of PING – it is RECOMMENDED that a dummy incident, with the number 0, is used for this purpose and an interval of 10 minutes between pings.

- The sending system must identify itself in every message sent between C&C systems using the *OrigOrganisation* element of the XML messages detailed below. From version 1c the sending system MUST also identify the intended recipient in the *DestOrganisation* element of the XML messages to facilitate interchange via a Router operator.

2.2. Data Management

2.2.1. Data Mapping

Fields that have a constrained list of values in a command and control system may not have the same values in all systems, even between organisations that use the same C&C systems. This is because organisations will always need the flexibility to configure their own system to hold and present local values for specific types of data, for example call origin, grade of response and even incident type. As a result, data mappings will have to be used for data items exchanged between organisations within an incident record.

Historically, these data mappings were performed on the receiving C&C system only, up to version 1c, but this changes from v1.0.0.

The intent is to make use of nationally (or multi-nationally) agreed data values where it is appropriate to do so but these will not be specified in this document (separate specification work is required for this). However, some constrained values and examples of mapping standards are included in this document.

Field content mapping SHOULD be applied to messages by End Systems on Send, to the nationally agreed superset values for the key fields (where they exist). This will allow local

variation but avoid recipients having to create maps for all incoming connections, which would be unworkable on a national level where a Router architecture is in use. The need to map incoming fields from the national superset or specific originators will still be required to allow local coding to be used by the recipient organisation.

If there is a mix of a Router connections and point to point links, suppliers SHOULD additionally provide individual mapping capability on a per-sender basis on inbound data from systems connected as point-to-point (in addition to the mapping applied to the inbound Router connection and the mapping on Send).

Although indicated to be constrained by an asterisk '*' in the schema, some fields such as `<CallOrigin>`, `<Type>` and `<SubType>` do not have a nationally defined constraint list (DTD), which causes problems between agencies. These data elements are discussed in the section XML UK National Element Values with suggested contents that suppliers are strongly RECOMMENDED to implement.

2.2.2. Data Truncation

As many text-based data items have different maximum lengths within the various C&C systems, it is not always possible to specify the lengths of these data items within the XML messages. As a result, when the maximum length of a data item is not specified in the message definitions below, there is a RECOMMENDED **default limit of 512 characters** that can be used to specify the data item (although the XML format has no inherent limit). Additional truncation may be required and will be performedby the receiving system.

There is a need to WARN the sender if additional truncation has happened on receipt. System developers SHOULD ensure that the system provides a suitable error response. This should be achieved using the `<Successful> / <ErrorDescription>` couplet for Incident Creation Acknowledgement Messages (ICAM), or Incident Update Acknowledgment Messages (IUAM) e.g.

```
<Successful>Y</Successful>

<ErrorDescription>#WARNING: Some fields truncated.</ErrorDescription>
```

The sender MAY append a list of field names to the description where truncation has occurred.

It is RECOMMENDED that the receiving system should append the text of any `<ErrorDescription>` to status messages even if the success flag is received.

2.2.3. Control Characters / Non ASCII characters

Some of the data within the XML elements sent across the interface can contain control characters. The receiving system must therefore be able to accommodate these to ensure that the entire field value is used. The control characters that may be received in this way are carriage return (decimal 13) and line feed (decimal 10). The fields which can contain these are:

- VehicleComment
- PersonComment
- Description
- CallerAddress

It should be made clear that accommodating the characters only goes as far as being able to accept a message that contains them. The receiving system is not constrained as to how it deals with them. The fact that the message may contain line feed and carriage return characters does not mean that the fields that hold the data received must be capable of holding multiple lines of data. The receiving system might, for instance, substitute a carriage return with a comma so that it can hold the data in a single line.

The UTF-8 encoding may add significant complexity so systems MAY wish to transform thestream into a text form for onward system compatibility.

See http://tools.ietf.org/html/rfc3490 for the IDNA mechanism as a suitable example.

2.2.4. XML Schema Validation

No mandated validation was executed against an XML schema, XSD or DTD prior to Version 1.0.0. This provided the additional flexibility for an organisation, for its own purposes, to add custom fields to the interface of its own C&C system without disrupting the ability of that system to operate using the national standard defined in this document.

Whilst having no XML Schema or DTD validation allows for variation and extension it brings risks to interoperability so, from version 1.0.0, receiving organisations SHOULD and Routers MUST, ensure validation is applied (a schema extension methodology is provided in this document for built-in flexibility). Suppliers of systems SHOULD follow the guidance paragraphs within this schema to ensure maximum compatibility between systems and commonality of data.

It should be made clear that the XML standard does not specify that the order of the fields will always be that in the schema and suppliers should ensure that systems can cope with out of order XML items.Usage of existing handling libraries will usually ensure this.

To allow compatibility between systems and future growth of the schema, a schema versioning attribute and a name-space modification has been added in 1.0.0 to allow continued use between systems of various schema levels. To retain backwards compatibility, the absence of a SchemaVersion attribute and name-space declaration MUST be interpreted as the message conforming to an older schema, 1c or 1b, which are broadly compatible (as the 1c extensions add functionality for Router and recommended Gaz value operation only).

Where a system receives a different schema level acknowledgement, especially in an ICAM, it SHOULD inform the users of the risk of loss of data. In the case of an IUAM it MUST clearly flag any absence of a Positive Delivery Notification (PDN).

2.2.5. XML Digital Signing

MAIT messages MAY be digitally signed. Where a digital signature is to be included in any MAIT XML message the enveloped method MUST be used (i.e. the digital signature is enveloped in the XML message) and the data object being signed MUST be the XML message (not including the digital signature - <complexType name="SignatureType"> </complexType>).

The digital signature MUST conform to the W3C standard XML Signature 2.0 and employ the following parameters from the options in the standard:-

Digest = SHA256
MAC = HMAC-SHA256
Signature = RSAwithSHA256

2.2.6. XML UK National Element Values

Systems SHOULD provide a configurable way to map, on send, at least the data values for Constrained elements - marked with an * asterisk in element tables. This is in addition to the mapping on receipt for direct point-to-point connections.

This document does not contain full specifications for any of the UK National Elements and a separate document (or set of documents) is required for this. The reason is, partly, that some of the necessary standards do not yet exist so this document provides some examples of appropriate data values which user organisations must agree on for common usage.

2.2.6.1. <DestinOrganisation> and <OrigOrganisation>

There is a vital need to maintain a central list of values for this field. Currently to avoid additional work for any central body it is intended (in the UK) to use the code list maintained by the Cabinet Office for transmission through any UK Government Router as

this contains most organisations that could join the Router and includes namespace to accommodate additional agencies if needed.

System developers SHOULD ensure that the <OrigOrganisation> can be different for calls destined for a Router than that used for point to point links to preserve compatibility with any centrally mandated organisation code.

Systems SHOULD provide a way of managing lookups for user friendly names for organisations as an alternative to the codes used in the Destin/OrigOrganisation fields. Router suppliers SHOULD provide a standard for this. This could be similar to DNS.

The use of a dotted notation is also suggested, for example, in the form uk.GROUP.ORG999 where GROUP is optional and extensible (for multiple levels and for new branches). This would allow multiple agencies with unique identifiers in the form “ORG999” to provide shared Control systems or indeed single agencies to internally distribute to multiple control systems.

The suggestion for dot notation allows for a flexible method of addressing. The Fully Qualified Name (FQN) commences with “uk” (in the UK), then any number of GROUP levels (e.g. in the form group0, group1, group2, etc.) and, lastly, the granular name of the destination – all separated by a dot. This means that a message can be addressed at any level, top down, in the hierarchy from an external system (i.e. one not in the same domain as the destination) or, for a system on the same domain, messages can be addressed bottom up to span any level in the hierarchy. This approach allows a complex organisation (such as shared services) to expose a single FQN externally but then have “private” sub-levels internally as well as exposing direct access to the “private” addresses as needed.

The simple use of this structure for UK domain systems could be just ‘ORG999’, where the value is from the Cabinet Office code list, using the principle of ‘bottom up’ addressing within the same domain. The use of groups can be introduced as more end systems join the MAIT router network.

2.2.6.2. <Gaz> Type fields

Code	Description
0	This means that the Gaz refers to a local ‘non-standard’ gazetteer on the originating system and the reference will only mean something to the receiving system if it also has an understanding of the originating gazetteer.

Code	Description
1	Address Point (deprecated).
2	NLPG / AddressBase Premium (ABP) – the UPRN is the selected key. End Systems SHOULD use this as the preferred method for addressable items. Note that there may be multiple records with the same UPRN as different LPI entries (typically, active entries have a LOGICAL_STATUS = 1).
3	One Scotland Gazetteer (http://www.onescotlandgazetteer.org.uk/).
4	AddressBase / Addressbase+ (not recommended in the UK).
5	UK Emergency Services Gazetteer (Colloquial and Historic) – proposed extensions to ABP.
6	LPI Key (AddressBase Premium) – this is a more specific indicator than the UPRN and may be more suitable in some applications. NOTE: There should be a discussion about the use of LPIs and UPRNs, including mappings between them, as part of the National Standards topic.

2.2.6.3. <MarkingScheme> and <SecurityLevel>

There has been a change in the UK Government policy for protective markings and a new scheme has been created (referred to in this document as GSC). However, a number of organisations affected by this change have yet to adopt the new markings so this standard maintains the previous marking scheme (referred to as GPMS in this document) so as to afford backward compatibility with those organisations.

The marking scheme is denoted by a couplet of <`Marking Scheme`> and <`Security Level`>.

The absence of this couplet (as in older schemas) should be taken to mean Business IL2 or Confidentiality marking of PROTECT / OFFICIAL.

Options for MarkingScheme (SecurityLevel):

BIL(IL0,IL1,IL2,IL3).

GPMS(NPM,PROTECT,RESTRICTED).

GSC(OFFICIAL,OFFICIAL:SENSITIVE).

2.2.6.4. <NotificationReason>

The reason given by the originator for notifying the recipient should be clearly determined. This should support future compatibility with a National Incident Type and Notification scheme. In advance of an agreed national scheme, the general structure should be followed:-

- Advisory – providing non-urgent, non-critical information with no action required
- Alerting – providing urgent or critical information but not requiring action
- Participation – action is expected by the recipient but at least some control is retained by the originator
- Handover – passing complete control of an Incident to the recipient

2.2.6.5. <CallOrigin>

This should identify the method of the call reaching the call handler as that can have implications on the use of caller information (such as Location information). This should cover the current known methods plus allow expansion for future methods. Example of the value that might be used here could be:-

- Private Landline Emer
- Private Landline Non-Emer
- Public Call Box Emer
- Public Call Box Non-Emer
- Mobile LTE Emer
- Mobile LTE Non-Emer
- Telematics (E-Call, for example)
- Softphone (e.g. Skype) Emer
- Softphone (e.g. Skype) Non-Emer

- ESN LTE
- Internal (to the Emergency Service)

2.2.6.6. <Type> and <Subtype>

The Type of Incident and the Sub-Type should be used to align with the Major Incident definitions (aligned with METHANE) but also allow refinement and expansion for non-Major categories.

2.2.6.7. <CoordinateSystem> and < C4SCoordinateSystem >

The Coordinate System should be chosen to best suit the application of the local system and receiving End Systems are responsible for transformations to other coordinate systems if needed.

Where OSGB (BNG) is used, the format of the coordinate values must be applied consistently and support the full geographic coverage of the UK (for example, including Scotland). This may mean that the numeric format has redundant digits when covering some parts of the UK but these must not be lost so as to ensure correct interpretation for the whole of the UK.

2.2.7. Schema Extensions

The schema allows for expansion in a controlled fashion under the name-space mait.org.uk/mait/version/extensions with the creation of triples in the structure <Name>, <Type> and <Value>. Within each mait/version branch, each name MUST be unique. The Type items MUST be one of “string”, “number”, “integer” or “boolean” (not case sensitive). Extensions SHOULD only be used where extending the system is unavoidable and MUST be agreed through the MAIT governance process before use. The intention is that all Extensions are derived from or incorporated into the MAIT development roadmap. The Extension items MUST only be included in ICM type messages.

Receiving systems MAY choose to convert any of the Extension attributes to LOG entries or COULD provide full support for the defined attributes. Routers MAY also act on Extension attributes where they are defined to do so.

An illustrative MAIT root element has been used to demonstrate how to integrate the extensions element within the main body of XML (the version “1.0.0” in the example name-space will be set to match the relevant version of the MAIT standard):

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1.0.0">

      <ext:extensions
xmlns:ext="http://www.mait.org/mait/1.0.0/extensions">

            <ext:number name="example-number-1" value="1.1" />

            <ext:string name="example-string-1" value="" />

            <ext:boolean name="example-bool-1" value="y" />

            <ext:integer name="example-integer-1" value="1" />

            <ext:number name="example-number-2" value="2.1" />

            <ext:number name="example-number-3" value="3.1" />

            <ext:string name="example-string-2" value="Example string" />

            <ext:string name="example-string-3" value="Another example" />

            <ext:integer name="example-integer-2" value="2" />

            <ext:boolean name="example-bool-2" value="n" />

      </ext:extensions>

</mait:root>
```

Any combination of triple types may be present in any order, all name attributes must be unique.

This is also valid (no triples in the extensions element):

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1.0.0">

      <ext:extensions xmlns:ext="http://www.mait.org/mait/1.0.0/extensions"
/>

</mait:root>
```

This is also valid (no extensions element):

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1.0.0">

</mait:root>
```

Two schema support this XML, the root schema (illustrative and to be thrown away):

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

      xmlns:mait="http://www.mait.org/mait/1.0.0"

      xmlns:ext="http://www.mait.org/mait/1.0.0/extensions"

      targetNamespace="http://www.mait.org/mait/1.0.0"

      elementFormDefault="qualified">


    <xs:import namespace="http://www.mait.org/mait/1.0.0/extensions"
schemaLocation="extensions.xsd" />



    <xs:element name="root" type="mait:_root" />


    <xs:complexType name="_root">

        <xs:sequence>

            <xs:element ref="ext:extensions" minOccurs="0" />

        </xs:sequence>

    </xs:complexType>

</xs:schema>
```

Notice how the extensions schema is imported and the extensions element inserted into the root element type.

The extensions schema:

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
xmlns:ext="http://www.mait.org/mait/1.0.0/extensions"
           targetNamespace="http://www.mait.org/mait/1.0.0/extensions"
           elementFormDefault="qualified">

    <xs:element name="extensions" type="ext:_extensions">
        <xs:key name="name">
            <xs:selector xpath="*" />
            <xs:field xpath="@name" />
        </xs:key>
   </xs:element>

    <xs:complexType name="_extensions">
        <xs:sequence minOccurs="0" maxOccurs="50">
            <xs:choice>
                <xs:element name="string" type="ext:_string" />
                <xs:element name="number" type="ext:_number" />
                <xs:element name="integer" type="ext:_integer" />
                <xs:element name="boolean" type="ext:_boolean" />
            </xs:choice>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="_entry">
        <xs:attribute name="name" type="xs:string" use="required" />
    </xs:complexType>

    <xs:complexType name="_number">
```

```
        <xs:complexContent>
            <xs:extension base="ext:_entry">
                <xs:attribute name="value" type="xs:decimal" use="required"
/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="_string">
        <xs:complexContent>
            <xs:extension base="ext:_entry">
                <xs:attribute name="value" type="xs:string" use="required"
/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="_integer">
        <xs:complexContent>
            <xs:extension base="ext:_entry">
                <xs:attribute name="value" type="xs:integer" use="required"
/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="_boolean">
        <xs:complexContent>
            <xs:extension base="ext:_entry">
```

```
                <xs:attribute name="value" type="xs:boolean" use="required"
/>

            </xs:extension>

        </xs:complexContent>

    </xs:complexType>

</xs:schema>
```

The xs:key element ensures all names are unique.

The _extensions type declares the presence of up to 50, which is a default practical limit, of any of the triple types in any order.

The _entry type defines a base type for all triples; the name attribute is the same type for all triples.

The _number, _integer, _string and _boolean types define constraints on the value attribute for triples of that type; these are simple mappings to XSD basic types.

2.3. Presentation Guidance

System suppliers SHOULD take note of the Implementation Guidance paragraphs used elsewhere to ensure the Users of the systems experience suitable two way communication. This section provides some further suggestions, free of IPR, that they may wish to implement as the addition of functionality SHOULD not increase the number of steps required for users wherever possible.

This guidance has resulted from MAIT forum discussions on the application of MAIT and where some advanced features could be implemented using the flexibility of MAIT. Except where the MUST clause is used, these examples do not constitute approved methods nor rigid specifications.

To deal with the possibility of variation in the source of position information, the `<IncidentGazType>`, `<IncidentGazRef>` and `<X>/<Y>` fields COULD be associated a priority level, a time-stamp and an accuracy, implemented in Extensions, as geo-locations may have originated from updated Automatic Vehicle Location System (AVLS) position data or been revised by resources on the ground so may be more accurate and/or recent than initial coordinates. The sending systems MAY recognise these parameters and possibly not transmit the X, Y if it is not sufficiently recent or accurate, unless other reasons apply (e.g. they are the coordinates from the GazRef or had previously been updated, etc.).

Receiving systems MUST ignore partial values and accept X, Y only where both are present and valid.

Systems with mapping interfaces should be able to use the metadata about recipient organisations (which should include a common boundary file) to find out what areas they are interested in (i.e. by geography using an overlay); this lets the machine do the work of offering options, which operators can then select or deselect as they require. Router suppliers SHOULD provide such metadata, either through business processes or through the use of industry standard geospatial interfaces, but these are not specified in this document.

This can be extended to offer recipients the ability to indicate possible interest by maintaining a TAG on Incident Types in their metadata in the central directory, e.g. Highways Agency may be offered as an automatic option by systems even if incidents are outside of their geo-spatial area if the Incident Type mapping equates to VEHICLE.

The Priority of an Incident is pertinent to the local system and the business processes and policy that are related to it. Receiving systems may work under a different priority scheme and/or may prioritise the Incident in a different way to the Originating organisation.

The large numbers of organisations offered by a Router and a central directory will begin to cause a problem for display in systems, which SHOULD allow solutions such as favourites, groups and filters on displayed destinations with the ability to dynamically add and remove them, perhaps from a Router's central directory if required. As the central guidance on interoperability advises, all technology should be used day to day for familiarity, with the ability to scale up if needed in a larger emergency.

For a "change" 'mode' ICM message, all data items included in the message, except for the <MessageControl> data items (that provide key references for the incident), MUST be regarded as being a change to previous information and MUST be regarded as the current information, in the context of the End System that originated the change-mode ICM. It may be that the receiving systems maintain a historic audit of the previous information but MUST be regarded as "aged" and use change information to replace it (under the control of the receiving system business processes). A "change" 'mode' ICM MUST contain the key

reference items and SHOULD only further include the data items that are subject to the change.

The purpose for the change-mode processing is to ensure that communications between End Systems uses the most recent information so as to avoid confusion. It is not intended that this overrides the internal processing of information within any given End System.

The elements that are typically expected to be subject to change (although any element can be changed) are:-

- <ResourceETA>
- <HazardFlag>
- <KnownSceneSafetyIssue>
- <AttendanceRequested>
- <C4Site>
- <PersonConscious>
- <PersonBreathing>

The ICM delete mode follows a similar approach to the change mode above but it is important to ensure references are correct for the deletion of particular elements or objects. For example, to delete one person record from the PersonsInvolved object, the correct PersonSeqNo must be referenced.

Where End System are connected to the PSN there is a code-of-connection obligation for those systems to derive their timing information from the PSN so Date and Time information in those End Systems should be derived from the PSN clock.

3. Interfaces

3.1. Incident Creation

3.1.1. Incident Creation Message

The “Incident Creation” message (ICM) is used by a sending organisation to notify another organisation of an incident that has been recorded by the sender that requires direct response by the receiving organisation or who may need to be informed of the incident. Prior to version 1.0.0 the interface itself imposed no constraint on whether the same incident could be sent from one system to another using this Incident Creation message. It was down to the individual systems within the organisations to determine the appropriate

business procedures to decide if an incident should be sent more than once and how an incident would be handled if it is recognised as a duplicate of an incident already received.

For the avoidance of doubt, systems MUST NOT use “create” 'mode' (either implicitly through the absence of the 'mode' attribute value or explicitly by using the “create” value) to transmit different element values in subsequent ICM messages. In order to provide updated information on these values then the ‘mode’ attribute MUST be present with a value of “change”. The absence of the ‘mode’ attribute MUST be considered a default of “create” to retain compatibility with previous schema versions.

The ICM response is an ICAM from the End System receiving the ICM and this must indicate the receipt state. A positive (true) <Successful> indication MUST be provided when the ICM is received and ingested at the receiving End System correctly.

It is RECOMENDED that the ICAM should be used to handle errors in previous incident creation attempts in order to increase communications resilience:

- A repeat attempt to open an incident (the same incident) should still result in an ICAM of <Successful>N</Successful> but, with an <ErrorDescription>#WARNING: Incident already created as XXXXX</ErrorDescription>”

- In the case of an “change” ‘mode’ attribute, where no incident was previously created then supply an ICAM of <Successful>N</Successful> but, with an <ErrorDescription>#WARNING: Updated Incident XXXXX previously unknown</ErrorDescription>”. XXXXX SHOULD be the Human readable form OrigIncidentNum

- The receiving system may decide what to do with Closed incidents either by re-opening them automatically in which case the response SHOULD be <Successful>Y</Successful><ErrorDescription>INCIDENT XXXXX reopened</ErrorDescription> or it SHOULD respond with a suitable message using the <Successful>N</Successful><ErrorDescription>INCIDENT XXXXX already CLOSED</ErrorDescription> couplet. This is required so that sending systems can respond correctly if they send updates to incidents that have been closed by the recipient organisation.

In order to inform sender organisations of the expected time until a resource will attend Systems SHOULD send an ICM “change” ‘mode’ containing a <ResourceETA> field. Similarly <HazardFlag> and <KnownSceneSafetyIssue> would reasonably be expected to use ICM “change” ‘mode’.

Note in these instances where recipients use ICM “change” ‘mode’ care should be taken to include the correct incident URN as this reverses the normal direction of flow as per ICAM messages or any IUM messages.

The ICM “delete” ‘mode’ is used to identify information that should no longer be associated with the incident where all data items included in the message, except for the <MessageControl> data items (that provide key references for the incident), MUST be regarded as being deleted.

The ICM “close” ‘mode’ is used as a formal notification by a sending organisation when it has completed its own processing of the incident. The “close” MUST be sent to all other organisations known to the sending organisation to be engaged in the incident to inform them that the sending organisation is no longer involved in the incident. This will not imply any change in the status of the incident within any of the receiving organisations since one or more of them may still be involved in handling the incident.

The following is the complete structure of the *IncidentCreation* message shown without any data values:

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1dc6">

            <IncidentCreation schema=”1dc6”
mode=”create:change:delete:close”>

                  <MessageControl>

                        <MessageId></MessageId>

                        <Mode></Mode>

                        <MarkingScheme></MarkingScheme>

                        <SecurityLevel></SecurityLevel>

                        <DestinOrganisation></DestinOrganisation>

                        <OrigOrganisation></OrigOrganisation>

                        <OrigIncidentURN></OrigIncidentURN>

                        <OrigIncidentNum></OrigIncidentNum>

                        <OrigIncidentDate></OrigIncidentDate>

                        <OrigIncidentTime></OrigIncidentTime>

                  </MessageControl>

                  <CallerDetails>

                        <CallerTitle></CallerTitle>

                        <CallerForename></CallerForename>

                        <CallerSurname></CallerSurname>

                        <CallerNumber></CallerNumber>

                        <CallerAddress></CallerAddress>

                        <CallerMobile></CallerMobile>

                        <CallerGazType></CallerGazType>

                        <CallerGazRef></CallerGazRef>

                  </CallerDetails>
```

```
<CallOrigin></CallOrigin>
<Priority></Priority>
<Description></Description>
<Location></Location>
<CoordinateSystem></CoordinateSystem>
<X></X>
<Y></Y>
<IncidentGazType></IncidentGazType>
<IncidentGazRef></IncidentGazRef>
<HazardFlag></HazardFlag>
<KnownSceneSafetyIssue></KnownSceneSafetyIssue>
<C4Site>
      <C4SType></C4SType>
      <C4SGazType></C4SGazType>
      <C4SGazRef></C4SGazRef>
      <C4SAddress></C4SAddress>
      <C4SCoordinateSystem></C4SCoordinateSystem>
      <C4SX></C4SX>
      <C4SY></C4SY>
      <C4SSeqNo></C4SSeqNo>
</C4Site>
<Type></Type>
<SubType></SubType>
<AttendanceRequested></AttendanceRequested>
<NotificationReason></NotificationReason>
<ResourceETA></ResourceETA>
<ResourceID></ResourceID>
<VehiclesInvolved>
```

```
            <Vehicle>
                  <VRM></VRM>
                  <VIN></VIN>
                  <VehicleMake></VehicleMake>
                  <VehicleModel></VehicleModel>
                  <VehicleVariant></VehicleVariant>
                  <VehicleColour></VehicleColour>
                  <VehicleInvolvement></VehicleInvolvement>
                  <VehicleComment></VehicleComment>
                  <VehicleSeqNo></VehicleSeqNo>
            </Vehicle>
            <Vessel>
                  <VesselName></VesselName>
                  <VesselMMSI></VesselMMSI>
                  <VesselIMO></VesselIMO>
                  <VesselSeqNo></VesselSeqNo>
            </Vessel>
            <Aircraft></Aircraft>
            <Train></Train>
      </VehiclesInvolved>
      <PersonsInvolved>
            <Person>
                  <PersonForename></PersonForename>
                  <PersonForename2></PersonForename2>
                  <PersonForename3></PersonForename3>
                  <PersonSurname></PersonSurname>
                  <PersonSex></PersonSex>
                  <PersonSexDescription></PersonSexDescription>
```

```
                        <PersonAddress></PersonAddress>
                        <PersonNumber></PersonNumber>
                        <PersonDateOfBirth></PersonDateOfBirth>
                        <PersonAge></PersonAge>
                        <PersonConsent></PersonConsent>
                        <PersonInvolvement></PersonInvolvement>
                        <PersonArrestInd></PersonArrestInd>
                        <PersonCasualtyInd></PersonCasualtyInd>
                        <PersonConscious></PersonConscious>
                        <PersonBreathing></PersonBreathing>
                        <PersonSeriousBleeding></PersonSeriousBleedin
                        g>
                        <PersonSuspectInd></PersonSuspectInd>
                        <PersonVictimInd></PersonVictimInd>
                        <PersonWitnessInd></PersonWitnessInd>
                        <PersonComment></PersonComment>
                        <PersonSeqNo></PersonSeqNo>
                    </Person>
                </PersonsInvolved>
            </IncidentCreation>
</mait:root>
```

Table 2 specifies each of the data items in the Incident Creation message, how they are expected to be used and any constraints on them. Items marked with an asterisk (*) hold constrained values that will need to be translated by the receiving system to its own set of constrained values and SHOULD be mapped on send to nationally agreed values (see the Data Mappings section).

The DEFAULT constraints that apply where specific constraints are not detailed with the specific data item are shown in the table below. Where existing systems may have a design which would, if unaltered, exceed or otherwise violate the constraints then the BAPCO MAIT body should be informed.

Table 1 - Default Data Item Constraint

Element	Default Constraints
String	No limit in string length. It is RECOMMENDED that string length is limited to 512 characters.
Date	Conforms to ISO 8601 (i.e. YYYY-MM-DD).
Time	Conforms to ISO 8601 with UTC reference (i.e. hh:mm:ss±hh[:mm] for non-UTC times or hh:mm:ssZ for UTC times). Midnight is declared as 00:00:00 and refers to the start of the day identified in Date.
Integer	No upper or lower limit but constrained to whole numbers only. It is RECOMENDED that the value range should be ±32768.
Boolean	Value for TRUE = Y, Value for FALSE = N - (neither are case sensitive)

Table 2 – Incident Creation Elements

Element	Description	Format	Mandatory	Notes
MessageControl	Enclosing element for all message control details	Enclosing Tag	Yes	Only one set of message control details are allowed per message.
Mode	The operating mode of the message	Enum	No	Enumerated values: Create, Change, Delete, Close If absent, default to Create
MessageId	Unique ID of the message	String(18)	Yes	

Element	Description	Format	Mandatory	Notes
MarkingScheme*	Identification of the marking scheme used to code the incident	String(6)	No	This field must only be present if SecurityLevel is present.
SecurityLevel*	Security marking of the incident	String(24)	No	This field must only be present if MarkingScheme is present.
DestinOrganisation	Code for the recipient organisation	String	Yes	Destination organisation.
OrigOrganisation	Code for the Originating organisation	String	Yes	Originating organisation.
OrigIncidentURN	Unique Reference Number of the incident in the originating organisation	String(24)	Yes	The unique identifier of the incident in the originating system. This will not normally be displayed to the user but, could be the same as OrigIncidentNum in some systems.
OrigIncidentNum	Number of incident in originating organisation as known by the users within this organisation	String(24)	Yes	The incident number as displayed to the user within the originating C&C system.
OrigIncidentDate	Creation date of incident in originating organisation	Date	No	
OrigIncidentTime	Creation time of incident in originating organisation	Time	No	
CallerDetails	Enclosing element for all caller details	Enclosing Tag	No	Only one set of caller details are allowed per incident record ID.

Element	Description	Format	Mandatory	Notes
CallerTitle	Title of the caller	String	No	
CallerForename	Forename of the caller	String	No	
CallerSurname	Surname of the caller	String	No	
CallerNumber	Phone number of the caller	String	No	
CallerAddress	Complete address of the caller	String	No	This is free text that captures the human description the original call taker gave
CallerMobile	EISEC data provided by the mobile supplier via BT	String	No	
CallerGazType*	Reference Type of the Gazetteer	Integer	No	This field must only be present if CallerGazRef is present.
CallerGazRef	The reference in the Gazetteer	String	No	Content of the agreed primary key field for the selected gazetteer. This field must only be included if CallerGazType is present. See section Data Management
CallOrigin*	Origin of original call	String(16)	Yes	Origin of original call e.g. Kiosk, mobile, private sub, Officer, e-call etc. See section Data Management. Systems SHOULD pass this through to operators and any nuisance detection systems along with address and number data etc. They SHOULD NOT use it as the source of the incident, which should be based on a human readable form of the OrigOrganisation

Element	Description	Format	Mandatory	Notes
Priority	Priority of the incident	String(20)	No	This is also known as the Grade Code. This is the original organisation's local value – use <AttendanceRequested> and <NotificationReason> for National Inter Agency Priority.
Description	Description of the incident	String	No	
Location	Detailed location as stored in the originating C&C system	String	Yes	This is a text description (probably that originally taken by the call receiver) that can be used by receiving organisations where no addressable location can be matched and for confirmation of raw data
CoordinateSystem	How to interpret the supplied X/Y	String(24)	No	E.g. OSGR (for Northing and Easting), OSGB36 or WGS84 for Lat/Long using these or another internationally agreed geo-spatial projection.
X	The X co-ordinate in the defined co-ordinate scheme	String	No	
Y	The Y co-ordinate in the defined co-ordinate scheme	String	No	
IncidentGazType*	Reference Type of the Gazetteer	Integer	No	This field must only be present if IncidentGazRef is present.
IncidentGazRef	The reference in the Gazetteer	String	No	Content of the agreed primary key field for the selected gazetteer. This field must only be present if IncidentGazType is present.

Element	Description	Format	Mandatory	Notes
HazardFlag	Indication that sending agency has risk information associated for the incident's location or vicinity	Boolean	No	To enable agencies to warn each other that they hold risk information. Log update messages can be used to exchange information that the officers feel is acceptable which may be a telephone number to discuss the issue.
KnownSceneSafetyIssue	Warning that incident scene is known to be unsafe	Boolean	No	Warning that incident scene is known to be unsafe; if receiving agency is responding they will follow their own protocols to attend scene or wait for support (e.g. from Police).If present, values may be Y or N. Absence MUST be UNKNOWN not N.
C4Site	Enclosing tag for sites (such as RVPs) relating to the incident	Enclosing Tag	No	This is an enclosing type it is only expected to contain one instance but, in a multiple agency situation this may grow. To cover C4 (Command, Control, Coordination and Communication) sites like Strategic and Tactical Holding or marshalling areas for CBRNe or MTFA type incidents. Limited to a maximum of 10 instances per message.

Element	Description	Format	Mandatory	Notes
C4SType*	This is the type of the site being specified	String(24)	No	This defines the type of C4 sites as found in the common UK/NATO map symbols which should be used as the constraint list for content. These values from the level below the Building Block level (see the document and the lexicon in the following link). https://www.gov.uk/government/publications/emergency-responder-interoperability-common-map-symbols.
C4SGazType*	Reference Type of the Gazetteer	Integer	No	This field must only be present if C4SGazRef is present.
C4SGazRef	The reference in the Gazetteer	String	No	Content of the agreed primary key field for the selected gazetteer. This field must only be present if C4SGazType is present.
C4SAddress	Textual description of C4 Site	String	No	Contains a text description / additional information of location of C4 Site.
C4SCoordinateSystem	How to interpret the supplied X/Y	String(24)	No	E.g. OSGR (for Northing and Easting), OSGB36 or WGS84 for Lat/Long using these or another internationally agreed geo-spatial projection.
C4SX	The X co-ordinate in the defined co-ordinate scheme	String	No	
C4SY	The Y co-ordinate in the defined co-ordinate scheme	String	No	

Element	Description	Format	Mandatory	Notes
C4SSeqNo	A sequential number allocated to each C4Site in an incident	Integer	No	This allows multiple RC4S instances. Note that if many organisations are involved the sequence number will only be unique when associated with the origin of the message in OrigOrganisation.
Type*	Type of incident	String	Yes	Code for the type of the incident – this is the original organisation code and could be used between similar organisations such as fire to exchange richer data if they both conform to the National Fire Incident Type usage.
SubType *	Sub type of incident	String	No	Code for the sub-type of the incident.
AttendanceRequested	To differentiate between those occasions where the originating organisation is informing the destination organisation of their attendance and where a mobilisation of resources is required.	Boolean	No	However this does not mean that the receiving organisation is required to respond just that the sender requests it. Equally an operator may independently choose to attend, based on received information and local intelligence. Value can be “Y” or “N” but may also be absent. In the absent case, the request for attendance is indeterminate and must be decided by the receiving organisation.

Element	Description	Format	Mandatory	Notes
NotificationReason*	To enable the originating organisation to specify why they are requesting resources from the destination organisation.	String	No	Will enable the destination organisation to send the appropriate resources.
ResourceETA	Time to attend incident from receiving organisation	Time	No	Allows originating sending Organisation to confirm a resource has been dispatched and provide an estimated time of arrival of the first resource. Omission of the tag item should be taken as an indication of no ETA rather than the use of a zero figure which would mean already in attendance. Systems should be able to generate this figure to save operator time. In reverse using the ICM "update" mode it will allow receiving organisations to return their first resource likely ETA
ResourceID	Identifying information for the resource	String	No	This is information to be passed on to the attending personnel in order to allow them to identify the originating organisation's resource. It will be in a form that the originating organisation uses. For example, this might be the Airwave callsign.

Element	Description	Format	Mandatory	Notes
VehiclesInvolved	Enclosing tag which contains information about all the vehicles or vessels involved	Enclosing Tag	No	
Vehicle	Enclosing tag which contains information about one vehicle involved	Enclosing Tag	No	Limited to a maximum of 10 instances per message.
VRM	Vehicle Registration Mark	String(11)	No	The field size is based on known UK and other nations' VRM sizes.
VIN	Vehicle Identification Number	String	No	
VehicleMake	Make of the vehicle	String	No	
VehicleModel	Model of the vehicle	String	No	
VehicleVariant	To record, in investigative and intelligence systems, incomplete information obtained from any source about a motor vehicle model.	String	No	
VehicleColour	Colour of the vehicle	String	No	
VehicleInvolvement	Involvement of the vehicle	String	No	
VehicleComment	Additional comments about the vehicle involved	String	No	

Element	Description	Format	Mandatory	Notes
VehicleSeqNo	A sequential number allocated to each vehicle in an incident	Integer	No	Note that if many organisations are involved the sequence number will only be unique when associated with the origin of the message in OrigOrganisation
Vessel	Enclosing Tag that contains the details about the vessels involved	Enclosing Tag	No	Limited to a maximum of 10 instances per message.
VesselName	The human readable name	String	No	
VesselMMSI	Mobile Maritime Service Identity	String	No	This is a unique 9 digit number given to vessels but, can change if a vessel owner flags the vessel to a different country. This can apply to both commercial and leisure vessels as it is normally associated with communications equipment.
VesselMO	International Maritime Organisation Hull number	String	No	For commercial vessels this is a unique number given on construction and remains the same for the duration that the vessel exists regardless of ownership etc.
VesselSeqNo	A sequential number allocated to each vessel in an incident	Integer	No	Not used by all C&C systems, so it is left as a free text field. Note that if many organisations are involved the sequence number will only be unique when associated with the origin of the message in OrigOrganisation

Element	Description	Format	Mandatory	Notes
Aircraft	General description of any aircraft involved	String	No	
Train	General description of any trains involved	String	No	
PersonsInvolved	Enclosing tag which contains information about persons involved	Enclosing Tag	No	
Person	Enclosing tag which contains information about a person involved	Enclosing Tag	No	Limited to a maximum of 10 instances per message.
PersonForename	Forename of the person involved	String	No	This is the default data item used for Forename where only one forename is used.
PersonForename2	Second Forename of the person involved	String	No	
PersonForename3	Third Forename of the person involved	String	No	
PersonSurname	Surname of the person involved	String	No	
PersonSex	Gender (code) of the person involved	String(1)	No	M, Male; F, Female; N, Not Specified; D, Described
PersonSexDescription	Gender (description) of the person involved	String	No	Not used by all C&C systems, so it is left as a free text field.
PersonAddress	Address of the person involved	String	No	If postal address in entered then each line SHOULD end with a comma (except the last line) and commas SHOULD NOT be used within a line.

Element	Description	Format	Mandatory	Notes
PersonNumber	Phone number of the person involved	String	No	
PersonDateOfBirth	Date of birth (DoB) of the person involved	Date	No	
PersonAge	Age of person if no DoB provided	Integer	No	It may not be possible to obtain a DoB at the time. Value is Years.
PersonConsent	Provides an indication of the consent given by the person to use personal information	String(8)	No	To meet information sharing protocols – values are: IMPLIED, EXPLICIT, DENIED to reflect emergencies, subsequent gathering and the real case where they request NO sharing.
PersonInvolvement	Involvement of the person	String	No	Not used by all C&C systems, so it is left as a free text field. Data mappings could be agreed in this field.
PersonArrestInd	To indicate that the person has been/is being arrested	Boolean	No	The absence of this field implies UNKNOWN. Otherwise Y/N
PersonCasualtyInd	To indicate that the person is a casualty in connection with the incident	Boolean	No	The absence of this field implies UNKNOWN. Otherwise Y/N
PersonConscious	To indicate that the person related to the incident is conscious	Boolean	No	Not mandatory except for when the receiving organisation is ambulance C&C as this is key to their incident triage. The absence of this field implies UNKNOWN. Otherwise Y/N

Element	Description	Format	Mandatory	Notes
PersonBreathing	To indicate that the person related to the incident is breathing	Boolean	No	Not mandatory except for when the receiving organisation is ambulance C&C as this is key to their incident triage. The absence of this field implies UNKNOWN. Otherwise Y/N
PersonSeriousBleeding	To indicate that the person related to the incident is bleeding	Boolean	No	Not mandatory except for when the receiving organisation is ambulance C&C as this is key to their incident triage. The absence of this field implies UNKNOWN. Otherwise Y/N
PersonSuspectInd	To indicate that the person is a suspect in connection with the incident	Boolean	No	The absence of this field implies UNKNOWN. Otherwise Y/N
PersonVictimInd	To indicate that the person is a victim in connection with the incident	Boolean	No	The absence of this field implies UNKNOWN. Otherwise Y/N
PersonWitnessInd	To indicate that the person is a witness in connection with the incident	Boolean	No	The absence of this field implies UNKNOWN. Otherwise Y/N
PersonComment	Additional comments about the person involved	String	No	

Element	Description	Format	Mandatory	Notes
PersonSeqNo	A sequential number allocated to each person in an incident	Integer	No	Note that if many organisations are involved the sequence number will only be unique when associated with the origin of the message in OrigOrganisation

1.1.1 Incident Creation Acknowledgement Message

The “Incident Creation Acknowledgement” message (ICAM) is used to report back to the originating system the success or failure of the receipt of an *IncidentCreation* message.

The following is the complete structure of the *IncidentCreationAcknowledgement* message shown without any data values:

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1dc6">

            <IncidentCreationAcknowledgement schema=”1dC6”>

      <MessageId></MessageId>

      <OrigOrganisation></OrigOrganisation>

      <OrigIncidentURN></OrigIncidentURN>

      <OrigIncidentNum></OrigIncidentNum>

      <OrigIncidentDate></OrigIncidentDate>

      <DestinOrganisation></DestinOrganisation>

      <DestinIncidentURN></DestinIncidentURN>

      <Successful></Successful>

      <ErrorDescription></ErrorDescription>

            </IncidentCreationAcknowledgement>

</mait:root>
```

Table 3 – Incident Creation Acknowledgement Elements

Element	Description	Format	Mandatory	Notes
MessageId	Unique ID of the *IncidentCreation* message being acknowledged	String(18)	Yes	
OrigOrganisation	Code of the organisation sending the acknowledgment	String	Yes	

Element	Description	Format	Mandatory	Notes
OrigIncidentURN	Unique reference number of the Incident created as a result of receiving the *IncidentCreation* message, i.e. in the C&C system which sends the acknowledgement	String(24)	Yes	This is the URN of the incident as used in the C&C system which received the *IncidentCreation* message. If the incident creation fails then a blank field can be sent.
OrigIncidentNum	Number of the Incident created as a result of receiving the *IncidentCreation* message, i.e. in the C&C system which sends the acknowledgement	String(24)	No	This is the incident number as known by operators of the C&C system which received the *IncidentCreation* message. The NSPIS C&C incident numbers are re-incremented from 1 each day.
OrigIncidentDate	Creation date of the incident created as a result of receiving the *IncidentCreation* message, i.e. in the C&C system which sends the acknowledgement	Date	No	This is the incident creation date used in the C&C system which received the *IncidentCreation* message.
DestinOrganisation	Code for the recipient organisation	String	Yes	Destination organisation.
DestinIncidentURN	Unique reference number of the incident in the C&C system which sent the original *IncidentCreation* message	String(24)	Yes	This element is here for audit purposes.

Element	Description	Format	Mandatory	Notes
Successful	Flag to indicate whether or not the incident creation was successful	Boolean	Yes	Possible values are ‘Y’ or ‘N’.
ErrorDescription	Text description of the error in the event of a failure	String	No	Full error text should be used instead of an error code in order to isolate each C&C system from the other. Where it is due to specific data in the previous message, the text SHOULD indicate the specific problem.

3.2. Incident Chronology Update

3.2.1. Incident Log Update Message

The “Incident Log Update” (IUM) message is used by a sending organisation to notify another organisation of new Remarks/Comments to an incident that has either been previously sent to that organisation or previously received from that organisation. The updates to an incident log that may be sent between systems are chronology entries (also known as log lines, remarks and comments). They are not actual field updates if this is required then another Incident Create Message (ICM) with a 'mode’ attribute of “change” MUST be sent. To prevent update messages from being too large and to avoid the receiving C&C system from being cluttered with a large number of log entries from a remote system, an update message should not contain more than one hundred log entries – this is enforced in the XSD.

Although Systems are required to generate an Incident Creation Acknowledgement Message (ICAM) on receipt of an Incident this only indicates successful transmission through a Router and/or into a C&C system.

There is a need to improve the user experience through an acknowledgment sequence that provides positive delivery notification (PDN) which, to avoid extending the interface, should be implemented through this existing Incident Update Message (IUM) mechanism.

I.e. System developers MUST ensure the sending system generates an automatic Incident Update Message (IUM) when a user has interacted with a generated incident utilising a `<CommentDescription>Incident Creation Message has been`

READ</CommentDescription>. This message MUST set the <Manual Acknowledgement> flag to “Y”. The receiving system could usefully include other data if it wishes such as the Incident Number from the original creation message. System developers MAY wish to consider this field as being a state of the main incident header so that all IUM’s after a human interaction will have the flag set.

The following is the complete structure of the *IncidentUpdate* message shown without any data values:

```
<?xml version="1.0" encoding="UTF-8"?>
<mait:root  xmlns:mait="http://www.mait.org/mait/1.0.0">
            <IncidentUpdate schema=”1.0.0”>
      <MessageId></MessageId>
      <OrigOrganisation></OrigOrganisation>
      <OrigIncidentURN></OrigIncidentURN>
      <DestinOrganisation></DestinOrganisation>
      <DestinIncidentURN></DestinIncidentURN>
      <Comments>
            <Comment>
                  <OperationallyUrgent></OperationallyUrgent>
                  <ManualAcknowledgement></ManualAcknowledgement>
                  <CommentDescription></CommentDescription>
                  <CommentDate></CommentDate>
                  <CommentTime></CommentTime>
                  <CommentPriority></CommentPriority>
                  <CommentType></CommentType>
                  <CommentOwner></CommentOwner>
                  <CommentLineNo></CommentLineNo>
            </Comment>
      </Comments>
</IncidentUpdate>
</mait:root>
```

Table 4 - *IncidentUpdate* Elements

Element	Description	Format	Mandatory	Notes
MessageId	Unique ID of the message	String(18)	Yes	
OrigOrganisation	Code of the organisation sending the incident update message	String	Yes	
OrigIncidentURN	Unique reference number of the Incident in the C&C system which sends the incident update	String(24)	No	The unique identifier of the incident from which the updates are being sent.
DestinOrganisation	Code for the recipient organisation	String	Yes	Destination organisation.
DestinIncidentURN	Unique reference number of the incident in the C&C system which receives the incident update	String(24)	Yes	The unique identifier of the incident, on the receiving system, to which the updates are to be applied.
Comments	Enclosing element which contains all the log entries being sent	Enclosing Tag	Yes	
Comment	Enclosing element which contains the details of a log entry being sent	Enclosing Tag	Yes	A maximum of 100 Comments per message.

Element	Description	Format	Mandatory	Notes
OperationallyUrgent	A flag to denote that the contents of this message or log entry require urgent attention/action of the receiving organisation.	Boolean	No	Absence of the element, or a value of “No”, means ‘for information only’.
ManualAcknowledgement	Flag to indicate if this message originated from a human action	Boolean	Yes	To enable the originating organisation to know that the information passed has been acted on by a human – this meets international maritime requirement and general good practice for 'Positive Delivery Notification' (PDN). This should be N for any system generated / auto transmitted messages and Y for human created or actioned transmission.
CommentDescription	Contents of the log entry	String	Yes	
CommentDate	Date the log entry was created on the C&C system from which the update comes	Date	Yes	
CommentTime	Time the log entry was created on the C&C system from which the update comes	Time	Yes	

Element	Description	Format	Mandatory	Notes
CommentPriority	Priority of the log entry in the C&C system from which the update comes	Integer	No	Data mappings could be agreed in this field. Can also be used in conjunction with the OperationallyUrgent flag.
CommentType	Type of log entry in the C&C system from which the update comes	String	No	
CommentOwner	Id of user that created the log entry on the C&C system from which the update comes	String	No	
CommentLineNo	A sequential number allocated to each log entry in an incident	Integer	No	

3.2.2. Incident Update Acknowledgement Message

The “Incident Update Acknowledgement” message is used to report back to the originating system the success or failure of the receipt of an *IncidentUpdate* message.

The following is the complete structure of the *IncidentUpdateAcknowledgement* message shown without any data values:

```
<?xml version="1.0" encoding="UTF-8"?>

<mait:root  xmlns:mait="http://www.mait.org/mait/1dc6">

            <IncidentUpdateAcknowledgement schema=”1dC6”>

      <MessageId></MessageId>

      <OrigOrganisation></OrigOrganisation>

      <OrigIncidentURN></OrigIncidentURN>

      <OrigIncidentNum></OrigIncidentNum>

      <OrigIncidentDate></OrigIncidentDate>

      <DestinOrganisation></DestinOrganisation>

      <DestinIncidentURN></DestinIncidentURN>

      <Successful></Successful>

      <ErrorDescription></ErrorDescription>

      </IncidentUpdateAcknowledgement>

</mait:root>
```

Table 5 - IncidentUpdateAcknowledgement Elements

Element	Description	Format	Mandatory	Notes
MessageId	Unique ID of the message acknowledged	String(16)	Yes	For this message the length of the MessageId element is only 16 characters due to a limitation of one of the C&C systems participating in the exchange of incidents with the Highways Agency.
OrigOrganisation	Code of the organisation sending the acknowledgment	String	Yes	
OrigIncidentURN	Unique reference number of the Incident in the C&C system which sends the acknowledgement	String(24)	No	This is the URN of the incident as used in the C&C system which received the *IncidentUpdate* message. Note that this element is not mandatory as it will not be available if the incident update fails on the receiving C&C system.
OrigIncidentNum	Number of the Incident in the C&C system which sends the acknowledgement	String(24)	No	This is the incident number as known by operators of the C&C system which received the *IncidentUpdate* message. The NSPIS C&C incident numbers are re-incremented from 1 each day.
OrigIncidentDate	Creation date of the incident in the C&C system which sends the acknowledgement	Date	No	This is the incident creation date used in the C&C system which received the *IncidentUpdate* message.
DestinOrganisation	Code for the recipient organisation	String	Yes	Destination organisation.

Element	Description	Format	Mandatory	Notes
DestinIncidentURN	Unique reference number of the incident in the C&C system which receives the acknowledgement	String(24)	Yes	Note that this element is mandatory. This is to cope with the situation when an incident is exported twice to the same destination. Having this field will enable the C&C system that receives the acknowledgement to uniquely identify the incident.
Successful	Flag to indicate whether or not the incident update was successful	Boolean	Yes	Possible values are 'Y' or 'N'.
ErrorDescription	Text description of the error in the event of a failure	String	No	Full error text should be used instead of an error code in order to isolate each C&C system from the other.

ANNEX A: REFERENCES

References/Bibliography	HMG Status
NSPIS C&C Inter-Force Incident Exchange Interface V1b PO0890 NSPIS C&C/1530-XFI-049-042	Ratified
RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt)	Ratified
ISO-8859-1 XML	Ratified
One Scotland Gazetteer (http://www.onescotlandgazetteer.org.uk/)	Ratified
ISO 8601	Unratified
UK Civil Protection map symbology https://www.gov.uk/government/publications/emergency-responder-interoperability-common-map-symbols.	Ratified
W3C standard XML Signature 2.0 http://www.w3.org/TR/2013/NOTE-xmldsig-core2-20130411/	Unratified

ANNEX B: GLOSSARY OF TERMS

Glossary of Terms

Term	Definition
AVLS	Automatic Vehicle Location System
BT	British Telecom
C&C	Command and Control
DTD	Document Type Definition
EISEC	Enhanced Information Service for Emergency Calls
HA	Highways Agency
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPR	Intellectual Property Rights
IT	Information Technology
JESG	Welsh Joint Emergency Services Group
NPIA	National Policing Improvement Agency (most Information Services now returned to the Home Office)
NSPIS	National Strategy for Police Information Systems
PSN	Public Service Network
PDN	Positive Delivery Notification an indication that a human and not a machine has seen the information.
TCP/IP	Transmission Control Protocol/Internet Protocol
User	An individual using an organisational C&C system that has a MAIT interface
URN	Unique Reference Number
VIN	Vehicle Identification Number
VRM	Vehicle Registration Mark
XFI	XML/FML Interface
XML	Extensible Markup Language