Draft Implementors Note on Harmonizing Certain Identifiers in CAP Implementations

1. Background

Different alerting authorities, intermediaries, and alerting user groups are implementing the Common Alerting Protocol (CAP, Recommendation ITU-T X.1303) in operational applications. Especially as CAP messages become available from many different sources, implementers should harmonize how they identify alerting authorities, alerting policies, particular hazard threats/events, and particular CAP messages.

A single-issue ad hoc workshop was convened at WMO in Geneva, 22-23 June 2009.[1] This workshop, co-sponsored by ITU-T and OASIS as well as WMO, focused on identifiers associated with CAP messages. Participants in this Workshop also met jointly with participants in a MeteoAlarm Workshop on 23 June.

The CAP Implementation Workshop on Identifiers produced this "Draft Implementers Note". This draft is offered for consideration by the CAP maintenance agency, the OASIS Emergency Management Technical Committee, and relevant ITU-T technical groups.

Discussion during the CAP Implementation Workshop on Identifiers included:

- general requirements such as simplicity, usability, flexibility, extensibility, scalability, and deployability;
- considerations about distributed versus centralized management approaches of various identifier schemes;
- considerations about long-term reliability of identifier registrars, and the availability of high-performance tools for discovering information associated with any given identifier.

The Workshop developed suggestions on some specific CAP identifiers, described in section 3 below.

2. Rationale

CAP can be used by anyone for anything, anywhere, at any time. So there is no way to control CAP use. However, common interests may exist among user communities regarding “CAP identifiers” concerning their creation, administration, discovery, verification, and use.

Some of those interests include:

- Enhance the value of the CAP messages by enabling widespread sharing of the related event information and analysis of events over long periods of time

[1] The Document Plan of the CAP Implementation Workshop on Identifiers is available at http://www.wmo.int/pages/prog/www/ISS/Meetings/WIS-CAP_Geneva2009/DocPlan.html

- Enhance the security of CAP messages by enabling information associated with the message to be obtained for verification
- Enhance the flexibility of CAP messages by enabling new or additional information associated with the message to be obtained, e.g., message status

Inclusion of CAP identifiers in a global hierarchical structure would enhance discovery and access of ancillary information, either directly or by recursive queries in the hierarchy. For this reason, the following suggestions focus on the ITU-T and ISO/IEC standard OID tree specifically.

The identifiers discussed below could be assigned within new arcs in the OID tree. The main arc would be named something like "alerting", and the registrar would be an entity within ITU/TSB. (Registration procedures would have to be defined.) That arc is here given as "2.nn"[2] for illustration purposes.

It is important to recognize that some alerting communities may have already created their own identifier schemes and practices. For example, the GLIDE identifier scheme[3] is well-known in the humanitarian response community. Yet, such identifier scheme managers might be amenable to being included in a larger identifier context that would enable worldwide discovery and access with minimal changes to their present practices.

Simply registering the GLIDE identifier scheme in the OID[4] tree would put that scheme in a global identifier context with minimal effort. For illustration purposes, an OID tree arc of "2.nn.1" might be used for event identifiers and the GLIDE number scheme could be registered as "2.nn.1.0". Of course, other schemes of event identifiers could be registered as well.

3. Discussion by Identifier

Within the OID tree arc "2.nn" (alerting), at least one subsequent arc would be requested by WMO, here shown as here shown as "2.nn.0". Within the "alerting/WMO" node, a subsequent arc "2.nn.0.0" could be registered for information about alerting authorities.

a. Authority Identifier

An Expert Team of the WMO Commission on Basic Systems responded positively to a WMO Secretariat proposal to publicize a register of WMO Members warning authorities. The WMO Hong Kong Observatory agreed to set up a register of WMO Member warning authority, replacing the existing list of Members' legal basis for issuing weather warnings presently posted on the WMO Public Weather Services website. This register will contain the following information:

- Country name (and one of the ISO 3166 Country Codes)
- Organizational name of the alerting authority
- Geographic scope for which the organization is authoritative

[2] An actual OID assignment for the arc at "nn" would be in response to an official request. This request will include the contact information of a responsible registrar.
[3] GLIDE is explained at http://www.glidenumber.net
[4] OIDs (Object Identifiers) are explained at http://www.oid-info.com

- Types of messages for which the organization is authoritative
- Internet URL where the alerting authority serves its alert messages

The organization acting as the registrar for an authority identifier within the OID tree may decide to create subsequent arcs. This may be important when the organization operates under multiple legal or policy mandates.

b. CAP Message Identifier

The Workshop suggested that two other subsequent arcs could be registered within the "alerting/WMO" node: "2.nn.0.1" for messages asserted by national authorities, and "2.nn.0.2" for messages asserted by others.

The format of the CAP Message ID could be such that the stem designates an arc of the OID tree inclusive of an ISO 3166 country code. For example, the stem "2.nn.0.1.840" indicates a CAP message issued by the United States. Of course, each actual message should be uniquely identified but it is a matter for the alerting authority to decide how that uniqueness is assured. For example, a unique CAP message identifier could be "2.nn.0.1.840.1.57[2009-06-22T23:56:38-04:00]" (referring to an alert issued for Butler county, Alabama, on 22 June 2009 at 23:56:38).

4. Other Issues

Registrars that assign identifiers should obtain information concerning the registrants or objects to which the identifiers are assigned, with levels of assurance sufficient for the application.

Registrars that assign identifiers should also support common structured query-response availability of the registrant or object information or a pointer to the information location for other users within the same community, as appropriate for the application or usage. This usage can consist of registration in a global system, such as the http://www.oid-info.com repository, coupled with maintenance of a server capable of supporting common structured queries, or potentially in an OID Resolution System.