THE ROLE OF CECIS – COMMON EMERGENCY COMMUNICATION AND INFORMATION SYSTEM

Regis ELBEZ and Tacis ALEVANTIS
Monitoring and Information Center, DG Environment D.3, European Commission, B-1049 Brussels
Email: regis.elbez@cec.eu.int

Keywords: Emergency Communication and Information System; Emergency response; CECIS.

Abstract: We present in this paper the motivation for the European Common Emergency Communication and Information System CECIS, its objectives and functionalities.

1 INTRODUCTION

1.1 Objectives

The objective of the PROCIV-NET (Civil Protection and Environmental Emergencies European Network) project is to establish the interconnection of National Authorities with responsibility to protect citizens from natural and technological hazards. It constitutes the Common Emergency Communication and Information System (CECIS) provided in the context of the Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced co-operation in civil protection assistance interventions. The mechanism is intended to help ensure better protection, primarily of people but also of the environment and property, including cultural heritage, in the event of major emergencies, i. e. natural, technological, radiological or environmental accidents occurring inside or outside the Community, including accidental marine pollution, as provided for in Decision No 2850/ 2000/ EC of the European Parliament and of the Council of 20 December 2000 setting up a Community framework for co-operation in the field of accidental or deliberate marine pollution[1].

On the basis of the Council Decision creating the new mechanism, the Commission is responsible for the establishment and management of the CECIS according to the following articles:

Article 4 (b): [The Commission shall] establish and manage a reliable common emergency communication and information system to enable communication and sharing of information between the Monitoring and Information Centre and the contact points designated for that purpose by the Member States.

Article 7.2: The Commission shall also in accordance with the procedures laid down in Article 8(3) establish common rules particularly on the following matters: … Paragraph c; the common emergency communication and information system, as laid down in Article 4(b).

To fulfil this obligation the Commission proposed to use the work already accomplished in the context of the PROCIV-NET project conducted in the framework of IDA, because it corresponds more particularly to Stage I of the PROCIV-NET project as described in the Preparatory Report

[1] OJ L 332 of 28.12.2000 p. 1

established in 2000[2]. A Feasibility study for this Stage I was conducted in 2001[3].

1.2 Functionalities

User requirements for the setting up of the network (Stage I) were based on the results of the Preparatory phase mentioned above that concerned the functional User requirements of Civil Protection and Accidental Marine Pollution authorities in view of the establishment of a common emergency communication and information system. On the basis of these requirements the system should be:

- reliable, robust and fully available;
- high performance, high security, easy to use and user friendly system;
- integrated with existing systems and ensure early warning;
- connected with one single point of contact for each organisation and
- make use of existing standards for information exchange.

For the exchange of information, the objective set was to simplify, improve the user-friendliness and expand the scope of existing formats for the exchange of messages like the ones used in the context of the UN/ECE industrial accident notification system and the POLREP reporting system established in the context of several regional agreements for combating accidental marine pollution.

Additionally, the proposed solution took into account the legal obligations arising form the European Parliament and Council decisions concerning IDA - especially the availability of IDA generic services - the existing IT infrastructure in the Member States (an overview of which was established through a survey), as well as the requirements of the Council Decision creating the Community mechanism.

On the basis of the above, three layers were identified for the system, namely Network, Application and Security. These layers are described in detail in Section 1.4 Technical approach below.

1.3 Participants

The following organisations will be the end-users of the Common Emergency Communication and Information System (CECIS):

- The Monitoring and Information Centre (MIC) already established within the Civil Protection and Environmental Accidents Unit of the Directorate General for Environment at the European Commission (ENV/A/5);
- The competent authorities and the contact points that the Member States will designate on the basis of Article 3(e) of the Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced co-operation in civil protection assistance interventions (see above).

Through the CECIS the above organisations will be able to exchange in a secure and reliable way operational and other information as needed for the effective implementation of the new mechanism.

1.4 Technical Approach

1.4.1 Network Layer

The solution adopted is based on permanent accesses of the competent authorities and contact points to TESTA II through the corresponding national network(s).

A TESTA II permanent access will be established as an Off-net connection i.e. direct connection through a 128 kbps leased line between the CP/MP organisation and the nearest Eurogate.

[2] The Preparatory Report was approved by the Permanent Network of National Correspondents in Civil Protection (PNNC) and the Advisory Committee on the control and reduction of pollution caused by oil and other harmful substances discharged at sea (ACPH) on the 15th of September 2000. The Telecommunications Advisory Committee (TAC) also adopted the Preparatory report on the 7th of December 2000. It provided for the implementation of the system in three stages as follows: Stage I: Establishment of the Communication Network; Stage II: Enhancement and consolidation of the Information Content; Stage III: Implementation of additional advanced features in view of improving security and robustness.

[3] The Feasibility Report was circulated to the Members of the User Group of the PROCIV-NET project on the 2nd August 2001 (as well as to the Members of the PNNC and ACPH Committees that had not nominated representatives to the User Group). Several comments were received and incorporated in the Feasibility Report.

1.4.2 Application Layer

On the basis of the initial user requirements, the survey conducted amongst Member States and the provisions of the new mechanism, the solution adopted for the common communication and information system is a central database accessible through a common web browser. The system will ensure the following functions:

Communication: This function includes notification of emergencies (foreseen under Article 2), exchange of early warning and subsequent information messages as well as follow-up of requests for assistance in case of emergencies (foreseen under Article 5). It comprises the introduction of information using a user-friendly interface implementing (through multilingual, multiple-choice screens) existing systems for early warning, information exchange and assistance requests[4]. Information will then be broadcasted to the MIC and the contact points concerned. Follow-up will be ensured through similar (user-friendly, multilingual multiple-choice) screens and users will be notified automatically (push) through their normal e-mail system. Provisions will also be made for alternate notification methods (fax, SMS, etc.). Finally, the system will also offer the possibility to attach various documents to messages/replies as well as additional query and tracking facilities. Through implementation of advanced security features for the profiling of users the system will ensure that only authorised personnel has access to restricted data.

Information content: This function includes the database of messages exchanged in the context of the management of emergencies as described above. It will ensure the optimisation of future disaster procedures and management as well as the production of lessons learnt (foreseen in Article 4.f).

It also includes databases on the following:

- National contact points and competent authorities, assessment, co-ordination and intervention experts and teams as well as other intervention support (foreseen under Article 3).
- Medical resources (foreseen in Article 4.e).

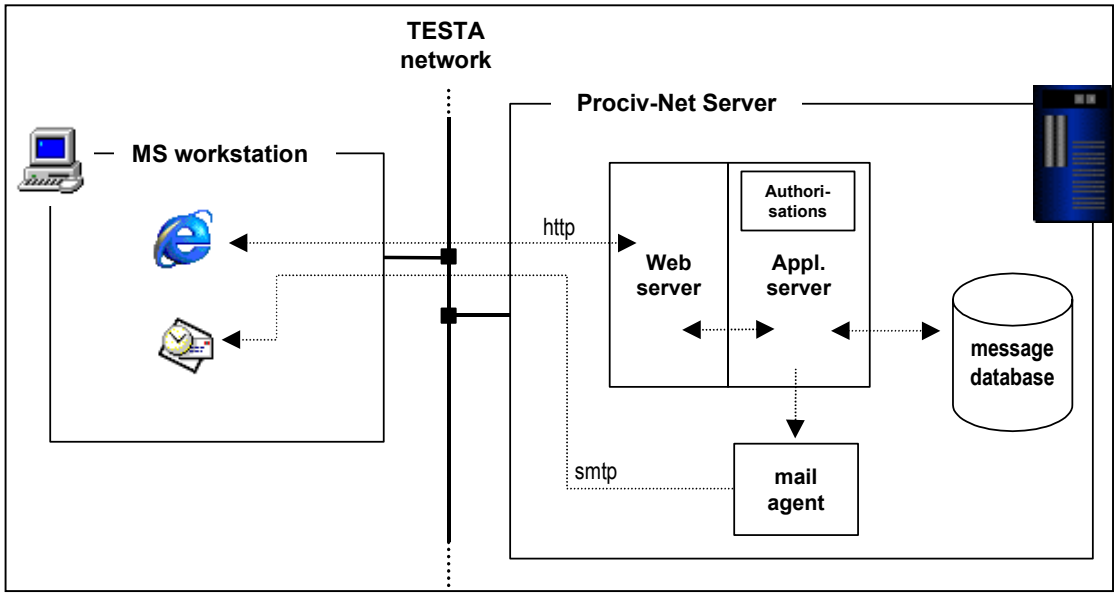

Figure 1 Schematic overview of the CECIS components

[4] Like the system for early warning, information and assistance requests relating to industrial accidents implemented within the UN/ECE Convention on the trans-boundary effects of industrial accidents (approved on the behalf of the Community by Council Decision of 23 March 1998, OJ No L 326, 23.12 1998, in force since November 2000) and the systems in place for the reporting of incidents of Accidental Marine Pollution including requests for assistance (POLREP - Pollution reporting systems implemented within the Helsinki and Barcelona conventions as well as the Bonn agreement, for which the Community is a part).

The schema in Figure 1 illustrates the relation between the different components.

On the basis of the Council Decision on the new mechanism and the existing formats for early warning and assistance requests mentioned above the PROCIV-NET User Group defined a general description of the application layer, including the definition of the fields of the database.

The group also developed a mock-up prototype that was constructed in parallel and helps visualise the work-flows to be implemented in order to ensure the efficient follow-up of an ongoing emergency.

Additionally, in the context of the Feasibility Study of Stage II of the project the further consolidation of the information content of the system will be explored, especially in view of providing additional services and databases (including Decision Support Systems, GIS based risk-maps, models for forecasting the development of emergencies, etc.).

1.4.3 Security Layer

The solution is based on the use of IDA Public Key Infrastructure (PKI) to ensure the E-mail security exchange (S/MIME), as well as the implementation of SSL (Secure Socket Layer) to ensure the session security.

A PKI comprises five types of components namely a Certificate Authority, a Registration Authority, a Certificate Distribution System, a PKI enabled application and a PKI Security Policy.

The schema in Figure 2 describes the procedure for the attribution of certificates.

The session security (based on one-way SSL) solution is used by several applications over the TESTA-II network. This solution is set up and operated by the Commission's Telecom Centre in Luxembourg. The costs of certificates in the IDA PKI will be covered by the Commission.

In the context of the project, a study will determine Registration strategies, and check if the Certificate Practice Statement of the IDA PKI requires modification for the application.

The above mentioned solution will ensure that the CECIS handles documents, databases and information systems classified up to «RESTREINT UE» according to Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC)[5]. For the transmission of documents and information classified «CONFIDENTIEL UE» or higher, special arrangements have to be made between the originator and the recipient(s).

Additionally, in the context of the Feasibility Study of Stage III of the project all available possibilities will be evaluated in view of enhancing

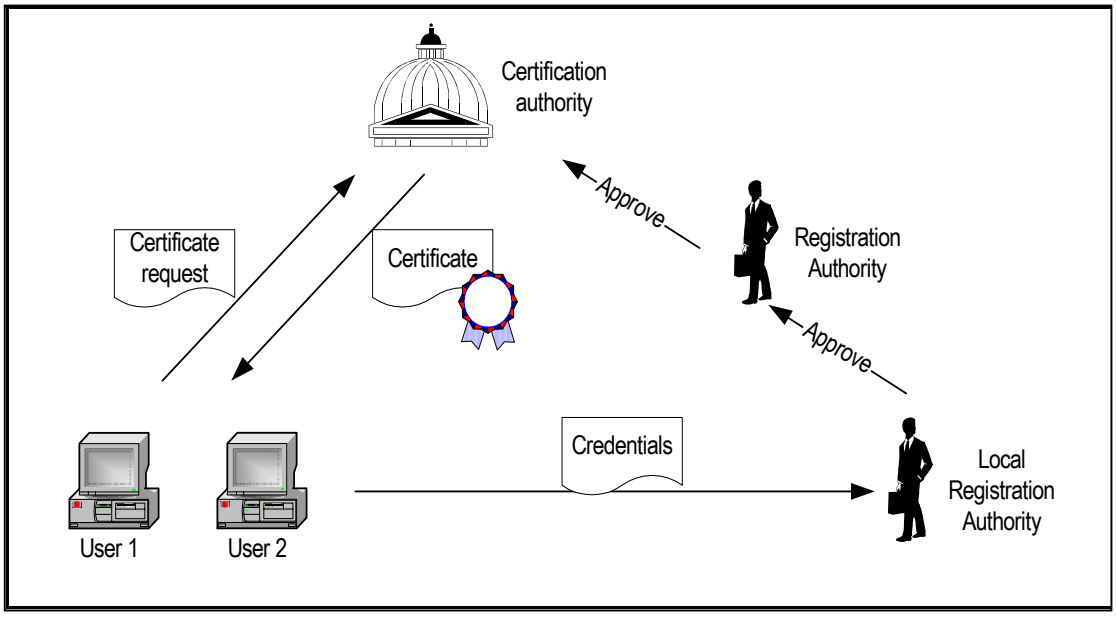

Figure 2 Procedure for the attribution of security certification in CECIS

the end-to-end security features of the system in view of ensuring handling of information classified «CONFIDENTIEL EU» and above.

2. THE EXPECTED BENEFITS AND MEASURING CRITERIA

2.1 Political Efficiency

The PROCIV-NET project provides the basis for the specification of the Common Emergency Communication and Information System, the establishment and management of which constitutes a legal obligation for the Commission. As the Council Decision for the new mechanism was adopted in October 2001 and enters into force on 1st January 2002, launching the development and validation phase almost immediately after, is a sign of efficiency and political commitment for all parties involved.

2.2 Time-saving and improved Efficiency

The time factor is very important in activities related to emergency situations including planning, co-ordination as well as demand, deployment and follow-up of assistance, etc. The deployment of the proposed solution will facilitate the management of these activities by speeding up distribution of the necessary information to the concerned participants during the emergency as well as during the preparation and reconstruction phases.

Moreover, the availability of appropriate information and accessibility to relevant decision makers has a direct impact on the efficiency of the service that the Civil Protection and Accidental Marine Pollution organisations have to provide for the management of the emergency situations. Therefore, the new system will enable the concerned organisations to promptly react, take decisions, plan and co-ordinate necessary activities to effectively manage emergency situations.

Given the fact that today information is exchanged during emergencies by using mainly traditional means (telephones and faxes), the new system will ensure instant information and the additional possibility to re-constitute the full development of the emergency in view of extracting lessons learnt for the future.

2.3 User Friendliness and Flexibility

The system will make use of IDA Generic Services (TESTA II and IDA PKI) already in use by several sectoral projects. On the other hand, the application layer will be based on a full web enabled database solution, using normal e-mail for notification purposes. This proposed solution is the only one that can be upgraded very easily as the overall performance of the system can be increased by adding servers and adapting the configuration. It uses open technology and as such it can support any further business needs including the integration with other systems. Moreover, it requires only that the participating organisations have workstations equipped with web browsers and is thus independent from the computer architecture at the level of the Member States.

2.4 Security

Advanced security is already ensured by the use of the TESTA II network, a private IP network accessible to the Member States' administrations only. Moreover, IDA Public Key Infrastructure (PKI) was selected because it is an IDA Generic Service and a legal requirements of the IDA decision. Furthermore this solution is based on software and organisational aspects and not on hardware and this ensures responsibility at the level of the individual user. TESTA is also considering the implementation of encryption boxes and this will permit the constitution of individual pipelines for even high level security applications.

[5] OJ L 100, 11.4.2001 p. 1