Data Management in Mass Casualty Incidents: The e-Triage Project

Thomas Greiner-Mai

Euro-DMS Ltd.
Anzengruberstraße 10 A
82140 Olching
greiner-mai@euro-dms.de

Anton Donner

DLR
Institute of Communications and Navigation
PO Box 11 16
82230 Weßling-Oberpfaffenhofen
anton.donner@dlr.de

Abstract: The main drawback of paper-based registration systems for organizing mass casualty incidents (MCIs) is that information about affected persons remains among the persons themselves. Data can be duplicated/aggregated by laborious manual copying triage tags only, and the normal medium for exchanging information are voice-based radio systems. Since MCIs normally overwhelm the regularly available rescue resources a particularly effective crisis management has to be applied. Operational command centers and rescue forces need information as fast as possible about type and number of injuries, so that each affected or injured person gets optimal care. This paper gives a general survey of the e-Triage project, in which a coherent overall concept for a MCI data management system is studied.

1 Introduction

Within the e-Triage project [etr10], which is sponsored by the German Federal Ministry of Education and Research, an integrated concept for electronic registration of affected persons is under development. Apart from the technical challenges the degree to which emergency forces accept the e-Triage system will depend primarily on psychological factors. A pre-emptive design of the technology, which accommodates the reduced cognitive abilities of emergency personnel operating under extreme stress, is crucial for a successful deployment. At time of writing, the e-Triage demonstrator system is under implementation; a first trial is planned for January 2011.

The design of the technical concept for the system described within this paper is based on use cases developed from rescue professionals and the derived system requirements,

regarding the user interface, the communication infrastructure, and the database system. Among these requirements it must be assured that the system accomplishes the following general necessities:

(1) Scalability: The system must be able to assist rescue forces in a wide range of mass casualty incidents (MCIs), considering on the one hand their size, and on the other hand, the geographical impact. Moreover, different types of organizations may be active on the disaster area. The system must assure inter-operability among the different forces.
(2) Dynamicity: Rescue teams may join/leave the system at any point in time and space during the rescue operation. The system must support dynamics in order to manage late joins and users leaving the system.
(3) Ease of use: In a general case, the users of the system will be members of rescue forces with (normally) limited technical background. The system must be easy to deploy in the field and must provide a user-friendly interface in order to be operated under heavy stress.
(4) Security: Communication among members of the rescue teams and transmission of data about the victims must be done in a secure way in order to assure integrity and confidentiality of the data being transmitted. Moreover, use of the system (i.e. especially communication bandwidth) by non-authorized persons must be prevented.

The e-Triage approach consists of four main elements: autonomous communication infrastructure, electronic data recording, a distributed database system, and psychological acceptance research. In more details, the technical concept comprises a satellite-based communication system with terrestrial radio cells, matching end devices with dedicated application software for the registration of victims, and a distributed, self-synchronizing database system guaranteeing maximal availability without a single point of failure.

2 Global Architecture

2.1 Communication

During a rescue operation two different areas can be defined: the on-site segment (OSS) with rescue forces in the field and the disaster-safe segment (DSS) with remote coordination facilities. Both segments can be connected using a backhaul communication solution, but an autonomous local coordination of the operation in the field has to be possible, too. It was decided on this basic approach to be able to represent two disjunct areas of security level inside the system (see necessity (4)). At the same time a high level of scalability for the system is secured (see necessity (1)).

Normally, the different elements found in the OSS are mobile actors (see section 2.2) and one or more on-site emergency communications equipment (OSECE). An overview of the general communication architecture is presented in Figure 1 and a detailed description of the satellite-based OSECEs can be found in [VWD10]. Mobile actors' user terminals must have at least intermittent connectivity with one of the OSECEs in order to transmit their data regarding the victims' registration. These terminals are typically laptops or PDAs equipped with WLAN and GSM/GPRS interfaces, GSM/GPRS smart phones,

or TETRA handhelds, supporting voice and data. The authentication and authorization

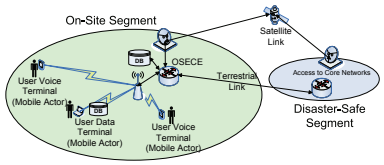


Figure 1: General e-Triage system architecture overview.

on-site is different depending on the access technology: WLAN, GSM/GPRS, TETRA (optional), and DECT (optional). WLAN will use WPA(2)-PSK for access control, and to simplify WLAN access certificates will not be used.

2.2 On-Site Segment (OSS)

In the disaster area there are scores of mobile actors working independently in different roles. A mobile actor can be a physician, doing the classification at the scene, or can be the emergency squad leader who is using the reported data to get an overview of the situation. Earlier works (e.g., [NK09]) have already shown that using electronic devices for MCI data gathering is a worthwhile approach.

The architecture of the end device consists of three main parts: the *user interface*, the *local database instance*, and the *communication unit*. By grouping the functional entities application/database and database/network the user will have a maximum of application performance by writing his data directly into the local database. In the background the database/network entity redistributes the data across the whole system. The flow of events when a mobile actor enters data using an application is used in this section to describe the functional architecture of the mobile actor's end device (Figure 2). In the application/database entity, the steps followed by the mobile actor are:

1. The user starts the e-Triage user interface (e.g., classification, reporting).
2. The user enters data. This can be in the context of the first or advanced classification.
2a. The user enters open data (e.g., classification color, sex), which is written directly into the local database instance.
2b. The user enters secure/advanced data (e.g., name, address). Secure data is locally encoded by an advanced encryption standard (AES) [Ert07] (e.g., Twofish, Serpent).

Necessity (3) "ease of use" has to be the main requirement for the user interface because the acceptance of the overall system will be a matter of the GUI design.

The services related to the database/network entity are:

1. The local database instance makes a local redundant copy of itself on a secondary storage medium (e.g., flash-drive). This is necessary if the primary medium fails or the user terminal cannot be used anymore for some reason, so the mobile actor can use the data with another terminal.

2. The communication unit decides which medium can be used to send the local data to the nearest OSECE (e.g., WLAN, GSM/GPRS) and notifies the local database system.
3. The local database service sends the local data to the nearest OSECE by using the selected network adapter.

In reverse direction, when the application requests data to display (e.g., a report for the squad leader), the local database instance synchronizes itself with the nearest OSECE. The problem of synchronizing distributed databases residing in user terminals and OSECEs via heterogenous networks is another central objective of the e-Triage project and is briefly described in section 2.4. e-Triage local applications implement programmatic authentication,

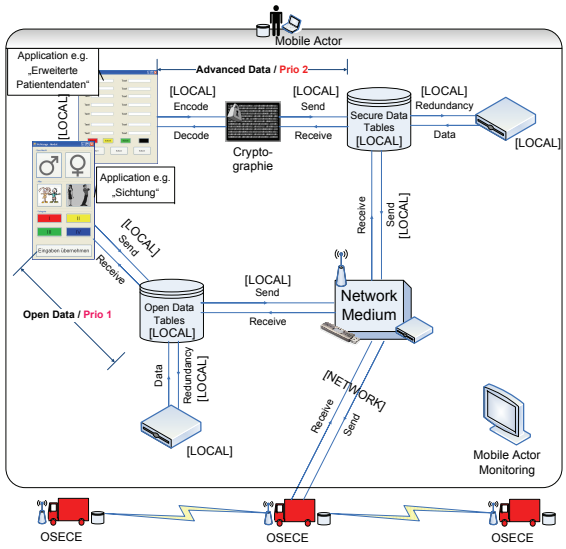


Figure 2: e-Triage mobile actor.

requiring the user to explicitly supply credentials, which are then validated using the local operating system security mechanisms with its underlying database. It is ensured that the secure messages stay private, because they are encrypted/decrypted inside the mobile actor's device. e-Triage uses the approach of authorization through roles. Various roles are created for the envisaged system and respective access rights are assigned to these roles. When each party is authenticated, the credentials applied to the party are mapped to the party's role (through groups in the directory service), which then determines whether or not the party is authorized to access a particular function. In the DSS everyone has to be certified by a security token service, whereas on-site the application signs the messages.

2.3 Disaster-Safe Segment (DSS)

An OSECE establishes the secure interface between OSS and DSS. In the DSS, control centers or hospitals have connection to the e-Triage gateway. To enable this connection,

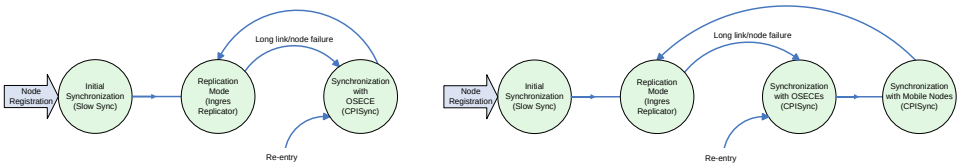
secure tunnels will be built statically because all nodes are known beforehand, including the OSECEs. Each request has to pass through the e-Triage gateway to get authorization for writing or reading from the database server inside a DSS.

e-Triage is based upon a service oriented architecture (SOA) which was chosen to give the system a maximum of adaptiveness to other systems. To make SOA secure, external security is used against outside attacks together with internal security, so that e-Triage supports data confidentiality according to legal requirements. The users in the DSS, namely hospital personnel or control center operators, are authenticated through web-based mechanisms when they connect to the web server. These mechanisms follow a sophisticated mutual certificates authentication schema, based on our specialized applications databases. On software level they communicate via web services [wsa04], where the use of the emergency data exchange language (EDXL) [RWA06] may be considered. There are several broad architectural options for implementing security in the context of web services. For e-Triage it was decided to use an XML gateway. The XML gateway enforces access control rules by processing security tokens contained within incoming messages, and by ensuring that the XML format and content are appropriate for the target. It may use the security assertion markup language (SAML) [CKPM05] to establish the authentication status of an end user or to request attribute information, which is used to make an access control decision. e-Triage strives to re-use the existing security infrastructure, including the pre-configured users, groups, and roles. To do this the XML gateway contains security adapters to existing security technologies such as lightweight directory access protocol directories, traditional firewalls, and public-key-infrastructure. If the incoming traffic bypasses the gateway and reaches the service endpoint, it would also bypass the security provisions implemented by the gateway. Consequently, using this architecture requires additional security provisions. In case of e-Triage the physical nodes, from which the service endpoint can receive service traffic, are restricted. Auditing (internal and external monitoring) is used by each application on the mobile actor's device, the OSECEs and the entities of the DSS.

2.4 Database Management

The current available replication solutions for distributed database systems (DDBSs) do not match the requirements of the e-Triage project, in which there are two main challenges [TDCM10]: (i) Replicated data should be transmitted directly or indirectly in a quasi real-time way towards any nodes existing in the entire system, which have a relatively stable network connection available at the moment. The replication system needs to be robust enough to face temporary (short-term) network interruptions. (ii) In case of intermittent long-term network outages or dynamic changes of the network architecture, the replication system should have an efficient comparison and synchronization solution by using a minimum of communication to retrieve the consistency of data sets when the network connection becomes available again. These requirements define two different modes of operation, which are *quasi real-time replication* and *comparison and re-synchronization*. Both modes must be seamlessly integrated without any user interaction. Nevertheless, it is necessary to make a distinction between the processes performed by an OSECE, and the

operation of the mobile nodes on the field (Figures 3(a) and 3(b)).



(a) Mobile node operation.

(b) OSECE operation.

Figure 3: State diagrams of the mobile node and OSECE operation.

3 Conclusions

The paper has briefly described the global architecture of the e-Triage system. On the one hand data management in MCIs is challenging, and on the other hand a key issue is the development of graphical user interfaces which are intuitive and self-explaining without causing additional stress. The consortium is currently implementing the system, and for 2011 a series of lab tests and field trials are planned. Although earlier and other current works (e.g., [sog09]) have studied single components of electronic MCI management, a unique feature of e-Triage is that for the first time a coherent overall concept consisting of mobile devices, location-independent communication infrastructure, database management, and psychological acceptance research is studied.

References

[CKPM05] Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML). Technical Report v. 2.0, OASIS Security Services TC, March 2005.

[Ert07] Wolfgang Ertel. *Angewandte Kryptographie*. Hanser Verlag, 3rd edition, October 2007.

[etr10] Elektronische Betroffenenerfassung in Katastrophenfällen. [Online]. Available: `http://www.e-triage.de`, 2010. In German.

[NK09] S. Nestler and G. Klinker. Mobile computing in mass casualty incidents (MCIs). In *Mobiles Computing in der Medizin (MoCoMed)*, Lübeck, Germany, September 2009.

[RWA06] Michelle Raymond, Sylvia Webb, and Patti Iles Aymond. Emergency Data Exchange Language (EDXL) Distribution Element. Technical Report v. 1.0, OASIS Emergency Management TC, 2006.

[sog09] SOGRO - Sofortrettung bei Großunfall mit Massenanfall von Verletzten. [Online]. Available: `http://www.c-lab.de/de/forschungsprojekte/sogro/index.html`, 2009. In German.

[TDCM10] Chen Tang, Anton Donner, Javier Mulero Chaves, and Muhammad Muhammad. Performance of Database Synchronization via Satellite. In *Advanced Satellite Multimedia Systems (ASMS) Conference*, Cagliari, Italy, September 2010. Accepted for presentation.

[VWD10] Angels Via, Markus Werner, and Anton Donner. Satellite Communications for Management of Mass Casualty Incidents: The e-Triage Project. In *International Conference on Satellite and Space Communications (ICSSC)*, Anaheim, California, USA, August/September 2010. AIAA. Accepted for presentation.

[wsa04] Web Services Architecture. [Online]. Available: `http://www.w3.org/TR/ws-arch/`, February 2004.