Next Generation, Secure Cloud-based Pan-European Information System for Enhanced Disaster Awareness

Maike Kuhnert
Christian Wietfeld
TU Dortmund University
{maike.kuhnert,
christian.wietfeld}@ tu-dortmund.de

Olivier Paterour
Airbus Defence and Space
olivier.paterour
@cassidian.com

Alexander Georgiev
CloudSigma
alexander.georgiev
@cloudsigma.com

Katrina Petersen
Monika Büscher
Lancaster University
{k.petersen,
m.buscher}@lancaster.ac.uk

Jens Pottebaum
University Paderborn
pottebaum@cik.upb.de

ABSTRACT

Information management in disaster situations is challenging, yet critical for efficient response and recovery. Today information flows are difficult to establish, partial, redundant, overly complex or insecure, besides the interoperability between heterogeneous organisations is limited. This paper presents a novel system architecture that enables combining of several communication technologies in a secure manner. This supports creation of a pan-European 'Common Information Space' by rescue organizations that can enable more efficient and effective information management in disaster response. Moreover, this technology can be used for disaster preparedness (e.g., training, tutorials). The modular architecture is designed to consider future evolutions of technology by defining interfaces for the integration of new technologies and services.

Keywords

information management, pan-European communication, secure cloud-based information sharing, common information space

INTRODUCTION

Today's crisis management processes could be improved through better information gathering, distribution and retrieval before, during and after a disaster. In addition, serious crises are increasingly trans-boundary (Ansell, Boin & Keller, 2010) and therefore the interoperability between diverse rescue organizations becomes more and more important. However, information distribution, let alone sharing, between various organizations does not work well. There are delays, uncertainties about involved persons and their roles, the accuracy, relevance and importance of information and security and privacy requirements. Further, the diversity and complexity of communication technologies hinder efficient use, and languages for information exchange are not consistent. Several solutions exist,

such as EDXL in the US (Oasis, 2013), PRML (Subik, Rohde, Weber & Wietfeld, 2010) and DIN SPEC 91287 (DIN, 2012) in Germany, but currently there is no pan-European solution that covers the large variety of capabilities. Moreover, semantic modeling, e.g., SERSCIS (Surridge et al, 2012) and ontologies (Galton, Worboys, 2011) are indispensable for interoperability and an efficient use of big data in emergency management, especially when integrating information from several sources.

To enhance cross border information exchange and awareness in disaster management the development of a 'Common Information Space (CIS)' is a promising solution. Besides, there exist a high variety of promising information systems, like MIKoBOS (Meissner, Wang, Putz, Grimmer, 2006). In addition to existing approaches, a CIS is a socio-technical concept, based on the idea that, given the right technical support, people can construct a shared information space and create and manage efficient, secure and relevant information channels (Bannon & Bødker, 1997, Turner, Bowker, Gasser & Zacklad, 2006). The CIS concept, combined with cloud computing, is the basis for our vision of next generation, secure cloud-based pan-European information management in disaster preparedness, response and recovery. This concept is similar to the PIE (Precision Information Environment) concept of Kilgore et al (Kilgore, Godwin, Davis & Hogan, 2013). But the novelty of our approach is to use the cloud as a secure and collaborating environment and transmit information securely even when using insecure channels. The presented architecture leads not to replace existing solutions, it will work as a bridge between existing information systems and also technology.

This paper describes a novel information system architecture for enabling the communication within a CIS, developed through a co-design process with users from rescue organisations. However, the overall solution regards various types of stakeholders, like research organizations, media, volunteer and political organizations, to bundle their expertise for crisis management support.

The remainder of the paper is structured as follows: the introduction focusses on a description of CIS technologies and their capabilities, validated by end users during a co-design workshop with representatives of rescue organizations in 2014 (SecInCoRe D2.2). The next section describes the novel system architecture, consisting of cloud based information inventory and secure local communications support, exploring limitations and challenges. The paper ends with a vision of future crisis management and a summary.

Common Information Space

The technological support for the creation of a CIS, as considered in the SecInCoRe project (Figure 1), is not intended to be a catch-all container for information. Rather, it is more like a shared space in which diverse stakeholders and stakeholder groups can interact, but from different perspectives, angles, and layers. Considering CIS as such enables SecInCoRe to treat it as a process that enables practices of exchanging, withholding, translation and sense-making rather than a state of 'blanket' information sharing. CIS technologies are tools that support people in noticing, determining, and improving the relevance, quality, timeliness, appropriateness, and compatibility of information.

In general a CIS enables productive translation between data types and different sense-making practices with the data. A CIS offers a way to have a common object of conversation without expecting the creation of a single way of understanding or engaging that object and a CIS makes it possible to share in one location what is already being gathered by various actors involved in the response.

Using a CIS in crisis response, preparedness and training is the key for efficient cross-border missions and interoperability between different rescue organizations in all phases of crisis management. Benefitting end users are not only rescue organizations, even research, political, volunteer or media organisations. Procurement legislation bodies and information system producers will also enhance their expertise and capabilities in crisis management through the SecInCoRe CIS.

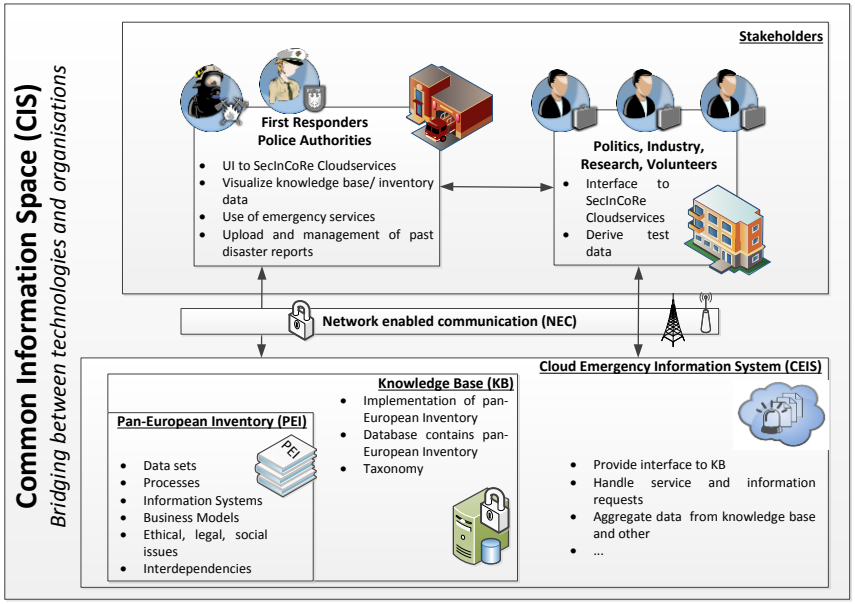


Figure 1: Common Information Space.

Palen et al. conclude that public participation in emergencies can lead to more efficient response (Palen et al, 2010), the CIS contribution and benefit is different for every user. A researcher could rely on real data he otherwise has no access to. For emergency organizations it is more difficult, why should they share the data? First, the organization could use the system for exchange of this data within the organization and benefitting from the cloud-based approach guaranteeing secured availability. Secondly, the organization could benefit from datasets by other organizations and external data sources that are also available in the CIS.

The main challenges of the CIS is the lack of political will to create a common practice required for interoperability. Looking more detailed to the information in the CIS, there is the question of how to define different categories of data and decision making chains or levels of responsibility.

Capabilities

We develop a modular and secure system architecture to enable communication and information management in the CIS for disaster preparedness, response, recovery and training. The architecture takes into consideration the following requirements and capabilities, derived from, and confirmed during a co-design workshop with a broad range of end users from rescue organisations (SecInCoRe D2.2):

- Real world practice-oriented network deployment and management process. The deployment of a network must not hinder first responders' main tasks. The usage of the network should be self-explaining.
- Make supporting technology "as simple as possible" for the use in emergency situations. The challenge here is the definition of "simple". During the co-design workshop "simple" sometimes meant few components or something intuitive that could easily fold into present practices, at other times it meant complex but familiar (e.g., through training or daily use). As such, the requirement is to support the practical achievement of simplicity and familiarity, rather than to 'simply' make simple technologies or to hide complexity.
- Scalability of the developed system: The architecture and CIS should be usable 24/7. They need to be incorporated into everyday practice, not just for the exceptional incident.
- Support for noticing and management of failure situations and recovery behaviour for communication, for example relating to clogged communication lines.
- Flexibly understand and manage the scope of access and data sharing boundaries. Need to access the technology and information may change over time and in an unfolding context. For example, volunteers may have valuable information, but do not have access to the special secure communications equipment of rescue organizations. Support is needed to review and alter topologies of inclusion and exclusion.
- Transparent and reversible: users should be able to understand and

influence design decisions. Informed users support the development of designs, operating parameters and data flows. For example, who decides who gets access to what information, is designed in a user oriented way that makes clear that such decisions are happening and that the user can question them.

- Handle multiple practices and procedures. There will never be 'one' common set of procedures, because every user should keep their existing procedures and inhabit the CIS with the capability to enhance these or make them more efficient and translatable to other processes.

NOVEL SYSTEM ARCHITECTURE FOR A PAN-EUROPEAN CIS

An overview of a novel CIS enabling system architecture design is illustrated in Figure 2. This architecture provides cross border information exchange via cloud based emergency system containing a disaster inventory and emergency information services in a secure manner. Providing information is one part of the common space for inter- and intra-communication of end user organizations. We rely on existing communication technology and combine them for a process-aware use. Currently, TETRA/TETRAPOL cannot handle the amount of data or present the information of the CIS.

- Examples of dedicated wireless networks are *professional mobile radio networks, like TETRA, TETRAPOL.*
- Examples of public wireless networks are 4G/3G/2G networks.
- Fixed networks could be WAN but also LAN both for stationary setups in command posts and preparative use cases.

Access to the CIS is subject to user accreditation and the level of CIS information a user can access depends on its role. These users could be either Public Safety users located in the command control rooms, planning department or the authorities, but also researchers or industry players. To access the CIS, and depending on its location, a user can leverage different kind of networks relying on different existing technology to access securely the CIS (cp. Section Secure Local Communication).

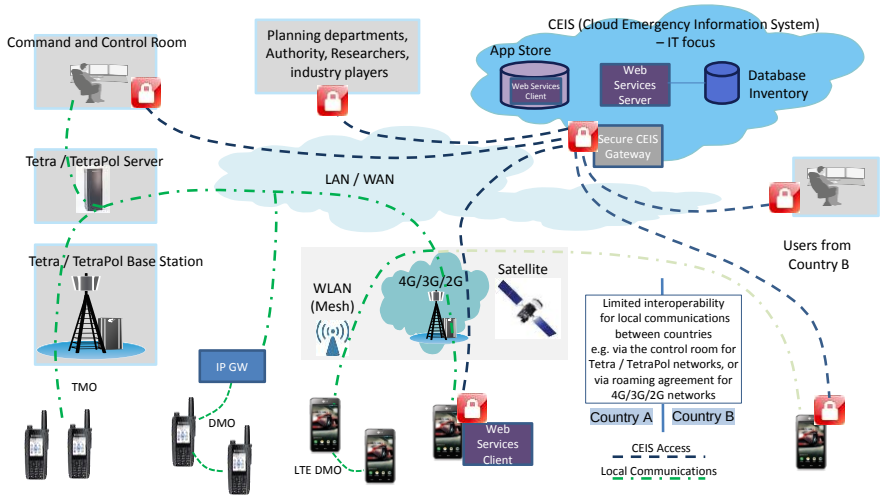


Figure 2: Overview of a CIS enabling system architecture design (TMO= Trunked Mode Operation, (DMO)= Direct Mode Operation).

CIS includes a cloud-based pan-European information system (CEIS) and can be accessed via Internet. Availability and scalability are main advantages of this cloud-based innovative information system. The CEIS consists of an inventory, providing information about past disasters. Web services are defined on this for enabling usage and processing of information for several purposes (e.g., awareness, training, protocol analysis). An application store categorizes and lists these emergency information services.

Moreover, this architecture provides local secure communication services on the field between users attached to different wireless networks. These users are either rescue or even ad-hoc users thanks to a procedure to get credentials to participate to local secure communications.

Cloud Emergency Information System

A detailed overview of the cloud emergency information system (CEIS) is given in Figure 3. Access to the database inventory is role-based, allowing to access and filter data according to the user's role and providing different level-of-detail of datasets. The application subsystem provides a graphical user interface (GUI) for displaying information that is transmitted via a secure gateway. This GUI is realized by using a browser, that means nearly no integration effort and a wide spectrum of usable devices. Provisioning of information is based on web services that allows the user to handle diverse services via an application store.

The web service server collects data from the knowledge base and other external sources and processes them accordingly (e.g., adding mandatory and recommend meta info, check quality, source). Over an integration subsystem the access and role management is linked to these services. Applications build upon the web services offered by the CEIS. The objective in the on-going development process is to create a secure cloud-based solution that combines various data sources and makes them available in the CIS using a browser based presentation.

The service stack can be realised on one or more clouds, subject to data repository and value-added service provider location. Data replication, hosting agreements and data querying capabilities may influence whether it will be best to mirror and host external data sources within the CEIS, or to access it externally on-demand. Provided that a rich querying interface is available conforming to the requirements of the CEIS, this data can remain external. Uptime and redundancy will influence the approach taken, with failover playing a crucial role in the overall architecture.

Secure Local Communication

For accessing the network several technologies are combined. Moreover, an indispensable point is to guarantee network security. The information will be send over public networks and must be secured between trusted points in terms of confidentiality, integrity, and origin authentication.

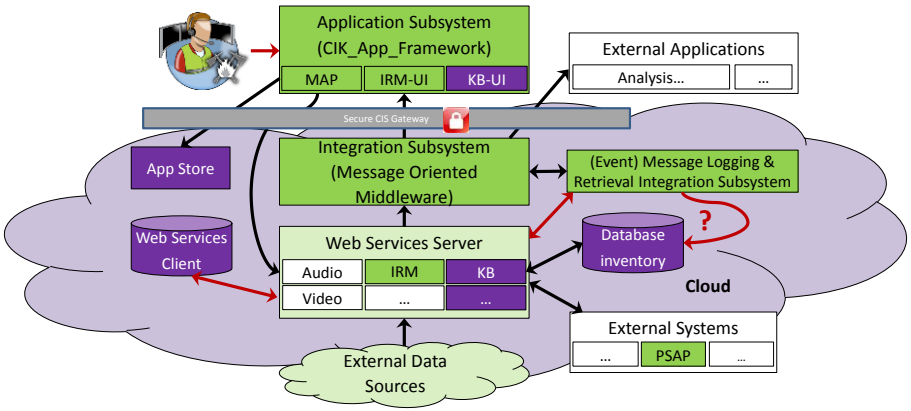


Figure 3: Overview of CEIS architecture design.[1]

The trusted point on the infrastructure side is the *Secure CIS Gateway*. The trusted point on the user side is the *device*. Here, we distinguish between mobile and fixed devices.

[1] Based on the architecture created in the FP7 ICT project PRONTO (www.ict-pronto.org) to support emergency management and activities before and after emergency situations (Pottebaum, Marterer, Koch, 2013)

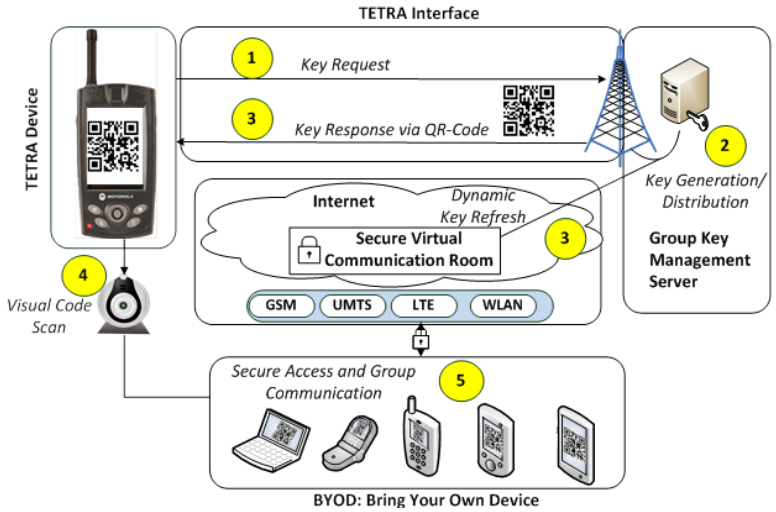
- **Mobile device**: A Secure Element (SE) is used for secure storage of the confidential keys. It is like a secure blackbox that handles cryptographic operations. Stored keys are never revealed outside the SE. Consequently, even if there is a malware running on the device, the attacker can never compromise the keys. Some recent phones include a SE on-board, facilitating the handling of cryptographic operations directly. This however limits device choice and often results in higher manufacturing costs. Even more recent developments in smartphone operating systems have eradicated the need for a physical SE, be it externally via the SD card slot or on-board. For example, Android 4.4 introduces the concept of Host Card Emulation (HCE), which in effect virtualises the SE and hosts it in the cloud. This yields significant benefits and opens up endless possibilities for developing custom SE apps to be consumed in the cloud.
- **Fixed device**: A Hardware Secure Module like a USB secure key could be used, having the same information and secure management as the SE.

The communication between the *Secure CIS Gateway* and the user *device* is secured via the standardized security mechanisms specified in the Basic Security Profile Version 1.1 (McIntosh, 2010).

From a security point of view, we distinguish between two user types, namely rescue personnel and ad-hoc users (e.g., volunteers). Rescue personnel have received the security credentials ahead of the crisis. Ad-hoc users receive the security credentials on the fly using the TETRA-based key distribution method. HCE presents a very interesting new opportunity to develop new solutions for ad-hoc users to authenticate securely with the CEIS.

Group Key Distribution over secure networks is envisaged for ad-hoc users that want to access the system to offer their support in disaster relief. They need the security credentials to establish secure communication with the *Secure CIS gateway*. To do so, we propose to use the secure and efficient scheme that is illustrated in Figure 4. It depicts an example of secure, user-friendly, and efficient group key distribution over TETRA.

TETRA is a professional mobile radio network, which is highly secure and available in rescue operations, it implements a push service to a group of users.



Thus, it is used to push the network credentials to the rescue personnel, and these forward the credentials to the ad-hoc users as follows:

1 Rescue personnel request the credentials from a group key management server in the TETRA control room.

2 The server generates the credentials (access key, group key) in a QR code format. This allows a good usability and multi-level of security.

Figure 4: Group key distribution over secure networks.

3 The QR code is pushed to all the TETRA devices in the corresponding TETRA group. Novel protocols at the network side are used for on-the-fly key refresh at the network access nodes (Sbeiti, Pojda, Wietfeld, 2012). The QR code is independent of the TETRA keys guaranteeing that the security of TETRA is not compromised.

4-5 Ad-hoc users use trusted applications for key-based network access and

group communication. The QR code contains the key for the secure virtual communication room and the local network that is connected via an Interface to TETRA. Using PASER, a secure routing protocol, the connection is secured and the security of TETRA is not compromised.

Vision

Next generation emergency response, recovery and preparedness should learn from current failures and make efficient and supportive usage of evolutionary technology. Our vision from the first alert to the start of a recovery phase looks like this: When an alert has been triggered, first information about the incident scene like type, afflicted area, risk potential, are available for rescue organizations via the CIS, enabling a quick overview about disaster's scale. Required resources are estimated and their location displayed in individuals map in various layers. Besides, the CEIS provides weather data, satellite figures. Several layers of information can be added to the crisis maps. During response interoperability and communication between organisations and even volunteers is guaranteed using secure networks. We assume that there is on-going network provisioning enabling the CIS during the scenario. Network provisioning has its own intelligence allowing self-configuration, self-healing and self-deployment regarding needed capacity and coverage. A first possible intelligent network provisioning solution using self-configuring hose couplings is introduced in SPIDER (Wolff, Sbeiti, Wietfeld, 2012). Even communication between danger zones to command post and the CIS is possible. If risky situations occur, immediate warning of all persons in range will be triggered automatically.

CONCLUSION

This paper describes a vision of next generation pan-European disaster information awareness by the creation of a 'Common Information Space'. A novel secure system architecture is presented for the communication and information exchange in a pan-European disaster environment. The architecture regards the security standards of each technology that is used and combined with other technologies (like, TETRA and IP-based networks). Moreover, it is flexible in its structure to regard the ongoing evolution process of communication technologies (e.g., 5G networks) and the various requirements and regulations from different European countries. During the co-design workshop (SecInCoRe D2.2) end users clearly stated that CIS, inventory and enhanced communication capabilities are essential parts of the future in crisis management. In future end user workshops we will validate our architecture using a prototype.

ACKNOWLEDGMENTS

The authors like to thank Mohamad Sbeiti for his technical assistance. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832 (project SecInCoRe). The text reflects the authors' views. The European Commission is not liable for any use that may be made of the information contained therein. For further information see http://www.secincore.eu/.

REFERENCES

1. Ansell, C., Boin, A. and Keller, A. (2010), "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System", *Journal of Contingencies and Crisis Management*
2. Bannon, L. and Bødker, S. (1997). Constructing Common Information Spaces. *In ECSCW*. Retrieved from http://www.ul.ie/~idc/library/papersreports/LiamBannon/ECSCW.htm
3. DIN SPEC 91287 (2012), Data interchange between information systems in civil hazard prevention. *Technical Rule.*
4. Galton, A., & Worboys, M. (2011). An ontology of information for emergency management. *In Proceedings of 8th International Conference on Information Systems for Crisis Response and Management.*
5. Kilgore, R., Godwin, A., Davis, A., & Hogan, C. (2013). A Precision Information Environment for emergency responders: Providing collaborative manipulation, role-tailored visualization, and integrated access to heterogeneous data. *IEEE International Conference on Technologies for*

Homeland Security.

6. OASIS Emergency Management TC (2013). Emergency Data Exchange Language (EDXL) Distribution Element Version 2.0.
7. McIntosh, M., Gudgin, M., Morrison, K. S., & Barbir, A. (2010). Basic Security Profile Version 1.1., *Web Services-Interoperability Organization (WS-I).*
8. Meissner, A., Wang, Z., Putz, W., & Grimmer, J. (2006). MIKoBOS-a mobile information and communication system for emergency response. *In Proceedings of the 3rd International ISCRAM Conference*.
9. Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010). A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. *In Proceedings of the 2010 ACM-BCS visions of computer science conference*.
10. Pottebaum, J., Marterer, R., Koch, R. (2013). An event driven approach to bridge emergency management, reflective debriefing and experience based learning. *Proceedings des Workshop Interdisciplinaire sur la Sécurité Globale*, Troyes.
11. Sbeiti, M., Pojda, J., & Wietfeld, C. (2012). Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Sydney, Australia.
12. SecInCoRe [SecInCoRe D2.2] (2015). ELSI guidelines for collaborative design and database of representative emergency and disaster events in Europe.
13. Subik, S., Rohde, S., Weber, T., & Wietfeld, C. (2010). SPIDER: Enabling Interoperable Information Sharing between Public Institutions for Efficient Disaster Recovery and Response, *IEEE International Conference on Technologies for Homeland Security*, Waltham, USA.
14. Surridge, M., Chakravarthy, A., Hall-May, M., Chen, X., Nasser, B., & Nossal, R. (2012). SERSCIS: Semantic Modelling of Dynamic, Multi-Stakeholder Systems.
15. Turner, W., Bowker, G., Gasser, L.,& Zacklad, M. (2006). Information Infrastructures for Distributed Collective Practices. *Computer Supported Cooperative Work*
16. Wolff, A., Sbeiti, M., Wietfeld, C. (2012). Performance Evaluation of Process-Oriented Wireless Relay Deployment in Emergency Scenarios. *IEEE Symposium on Computers and Communications*, Cappadocia, Turkey.