TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

SECRICOM SILENTEL – SECURE COMMUNICATION INFRASTRUCTURE FOR CRISIS MANAGEMENT

Vladimir Hudek, Miroslav Konecny, Stefan Vanya

Ardaco a.s., Bratislava, Slovakia

Key words: crisis management, Secure Docking Module (SDM), Secure Agent Infrastructure (SAI), SECRICOM, first responder, push to talk, PTT, seamless communication, end-to-end security.

Abstract

The major incidents such as terrorist attacks in Madrid, London or huge natural disasters (fires, floods etc.) showed that the factor that inhibits the full performance of emergency response is the lack of interoperability between communication systems of different responders over Europe. The SECRICOM project built a solution that seamlessly integrates the communication systems of different organizations located in different EU member states. The term "seamless" means that the communicating parties may use their own communication devices or can use new Secricom Silentel enabled devices over the SECRICOM infrastructure without worrying about what technology or communication system is used by other users. The provided solution offers high level of security in a cost efficient way since it reuses the existing communication infrastructures including public and dedicated ones (eg.: Tetra Radio, GSM, UMTS, Internet).

SECRICOM SILENTEL – BEZPIECZNA PLATFORMA KOMUNIKACJI DO ZARZĄDZANIA KRYZYSOWEGO

Vladimir Hudek, Miroslav Konecny, Stefan Vanya

Ardaco a.s., Bratislava, Slovakia

Słowa kluczowe: zarządzanie kryzysowe, Secure Docking Module (SDM), Bezpieczna Infrastruktura Agentowa (SIA), SECRICOM, responder, PTT opcja naciśnij i mów, „bezszwowa" komunikacja, bezpieczeństwo połączeń.

Abstrakt

Podczas poważniejszych sytuacji kryzysowych, jak ataki terrorystyczne w Madrycie czy Londynie, a także klęski żywiołowe (pożary, powodzie etc.), okazało się, że głównym czynnikiem ograniczającym wydajność reagowania służb ratunkowych jest brak interoperacyjności między różnymi systemami łączności. W ramach projektu SECRICOM zbudowano rozwiązanie, które

umożliwia „bezszwową" integrację środków łączności wykorzystywanych przez różne służby ratunkowe (także działające w różnych krajach). Pod pojęciem „bezszwowa" jest rozumiana możliwość wykorzystywania przez służby ich własnego sprzętu komunikacyjnego (bądź urządzeń wyposażonych w SECRICOM Silentel) na podstawie infrastruktury SECRICOM bez konieczności brania pod uwagę typu sprzętu używanego przez inne podmioty. Zaproponowane w ramach projektu rozwiązanie zapewnia wysoki poziom bezpieczeństwa oraz efektywność kosztową wynikającą z wykorzystania obecnie istniejących rozwiązań telekomunikacyjnych (zarówno publicznych sieci, np. GSM, UMT, Internet, jak i dedykowanych rozwiązań, np. TETRA).

SECRICOM Project Context

The major incidents such as terrorist attacks in Madrid, London or huge natural disasters (forest fires, floods etc.) showed that the factor that inhibits the full performance of emergency response is the lack of interoperability between communication systems of different responders over Europe. The complexity of this problem is increased by the number and structure of responder organizations involved simultaneously at different types of emergency events. These organizations have absolutely different hierarchical governance structures in place, maintain different cultures, pursue different goals and also use different means and tools for communication. After all, the cooperation of these stakeholders is essential for the successful resolution of the most of crisis situations.

The SECRICOM project has built a solution that seamlessly integrates the communication systems of different organizations located in different EU member states. The term "seamless" means that the communicating parties may use their own communication devices or can use new Secricom Silentel enabled devices over the SECRICOM infrastructure without worrying about what technology or communication system is used by other users. Moreover the new capabilities and the secure communication itself can be extended to mass market devices as PCs, mobile phones and tablets to increase cost effectiveness and comfort of users. Of course the preservation of life is the top priority but as the incident evolves the need for the confidentiality and reliability of information is getting more and more important. In SECRICOM, the communication sessions are ciphered, thus end to end security assurance is provided by the SECRICOM enabled devices.

Since most of potential hacker attacks are targeting endpoints in the security infrastructures, the SECRICOM solution introduced comprehensive network monitoring, intrusion detection, a hardware chip called Secure Docking Module and Trusted Docking Station that verifies the integrity of endpoint over the complete chain of trust starting from hardware itself. Thus the SECRICOM solution can provide a high level of security in a cost efficient way since it

reuses the existing communication infrastructures including public and dedicated ones (Tetra Radio, GSM, UMTS, Internet, etc.). The use of different means of communication in parallel increases the availability of communications and makes the SECRICOM solution resilient.

During the analytical phase of the project different scenarios were identified with the involvement of end user group and from different points of view at different levels in the organizational hierarchy. The project results were demonstrated in incremental way as more and more features and capabilities were added during several shows and civil protection exercises. The SECRICOM project has proven the feasibility of cooperation among emergency responders in the face of many of constraints.

Operation Requirements of Communication System

Crisis management deals with unpredictable catastrophic events including terrorism (e.g. Madrid and London, in the future CBRN) and crime, natural disasters (including pandemics, earthquake and hurricane that are exacerbated in poor countries) and major industrial accidents/technological disasters (Toulouse 2001, tanker Prestige, Hertfordshire fire etc.). The increasing heterogeneity of potential crisis situations led to (and will lead to) establishment of rescue organisations accountable for new types of threats. The increasing number of organisations with different command structure and communication systems created the need for a seamlessly integrated and reconfigurable communications infrastructure for use inside and outside the EU. Moreover the future communication systems are required to be secure, smart, open, restorable and ubiquitous. The main challenge of the SECRICOM project was to **exploit the existing publicly available communication network infrastructure with the possibility to add more sophisticated tools**.

Interoperability between various responder agencies may be defined as the capability of two organizations or discrete parts of the same organization to exchange decision-critical information and to use the information that has been exchanged.

The Figure 1 beside depicts the interoperability stack in which compatible high level objectives and physical interoperability (electrical/mechanical interconnections and transmission signalling) reside at the top and bottom, respectively. Lack of interoperability has been recognized as a significant reason for lack of effectiveness of a given crisis.

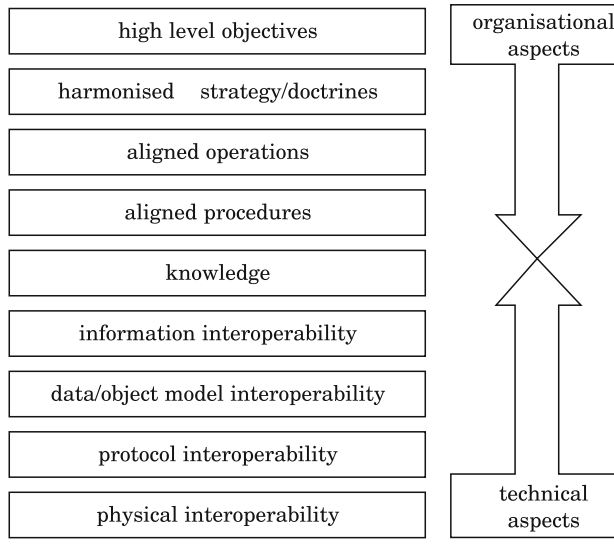

Fig. 1. Interoperability aspects

This is due to the consequential weakening of the process of coordination between emergency response personnel during the crisis management which is brought about by the resulting increased likelihood of poor critical-decision making.

SECRICOM Silentel Architecture

Secricom Silentel is a client-server communication system using Internet Protocol (IP) as illustrated in the Figure 2. It enables the use of mobile devices (i.e. smartphones, tablets or computers) together with technologies currently deployed (i.e. Tetra, SDR, etc.) for daily routines and crisis communication of public safety services. It optimizes and protects the way teams of people communicate without being concerned about misuse of information.

The main parts of the SECRICOM Silentel architecture are as follows:

– The Communication Server is a secure switching center module interconnecting all users of the system – as described by Figure 3.

– The Certification Authority is the trust module for Server and Users certification creation, validation and revocation (user can use his own CA as well).

– The Operator Studio serves as a tool for user account management and their personal contact list definition.

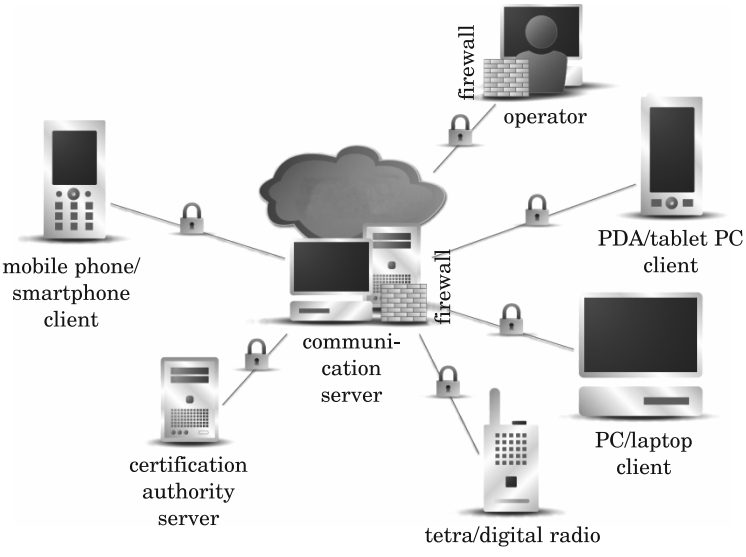

Fig. 2. Secricom Silentel (PTT) high level architecture

The SECRICOM Silentel client application communicates only with the server. This approach was influenced by the fact that there are no static IP addresses and there is no support of IPv6 by current GSM network operators. There are two main communication channels; one is the signalization protocol (SIP) and the other is RTP for audio transmission. SIP uses TCP and RTP uses the UDP protocol.

During the session, the server only uses the SIP protocol to send updates about the presence status of user's contact list; there are also regular "still-alive pings" from client to server.

As soon as the user starts a session, SIP is used to transmit more information, such as Talk Burst requests, text messages, pictures, information about users in the same session (users come and go) and encryption keys. The information structures transmitted by SIP are encoded in ASN.1. Each session is encrypted by different AES256 key. The same AES key is used for encryption of voice. When the user requests the Talk Burst, he can receive it back from the server – the application plays a signalization tone and changes Press-To-Talk button's colour. The audio recording is transformed by AMR compression, then the AES encryption takes place and RTP transmission is started. The server knows what users are in what session and simply serves as router; the server does not process the audio information in any way.

Security provisions of SECRICOM Silentel include besides ciphering functions also user authentication and management tools for the control of user

permissions. Unique user name and password with physical gridcard authentification protects user accounts. Smart card (microSD) and PIN (electronic signature) support the security of access. The Operator studio enables to manage rights, groups and visibility of clients with a possibility to block a suspiciously behaving account in real time.

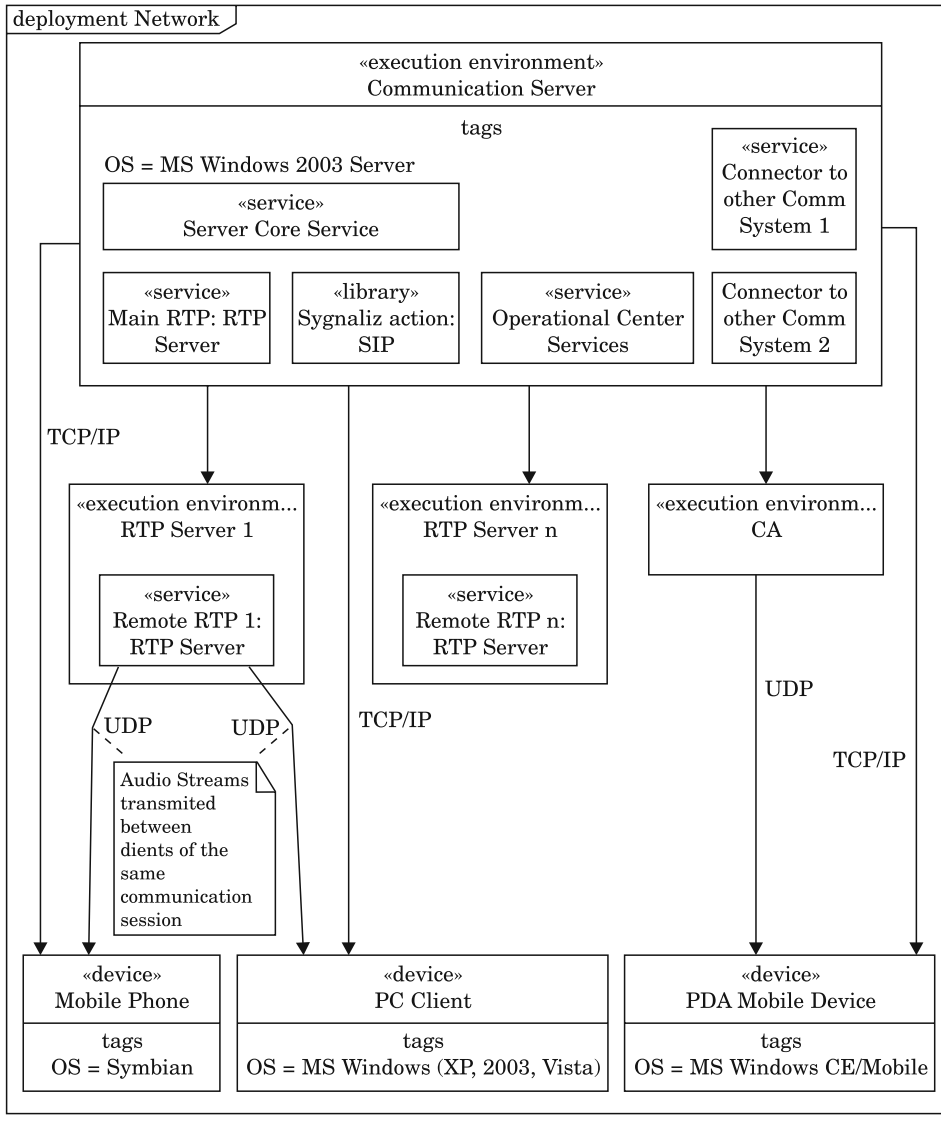

Fig. 3. SECRICOM Silentel Server Components

The client and server have a layered architecture. Each layer, process or module communicates with the rest of the system using asynchronous messages. The concept was proven on various supported operating systems of Secricom Silentel client, i.e. Symbian, Windows Mobile, Android, iOS as well as Windows. Communication gateway was implemented for Tetra and CB radio services, and the implementation allows also integration with further systems. The concept is described on Figure 4.

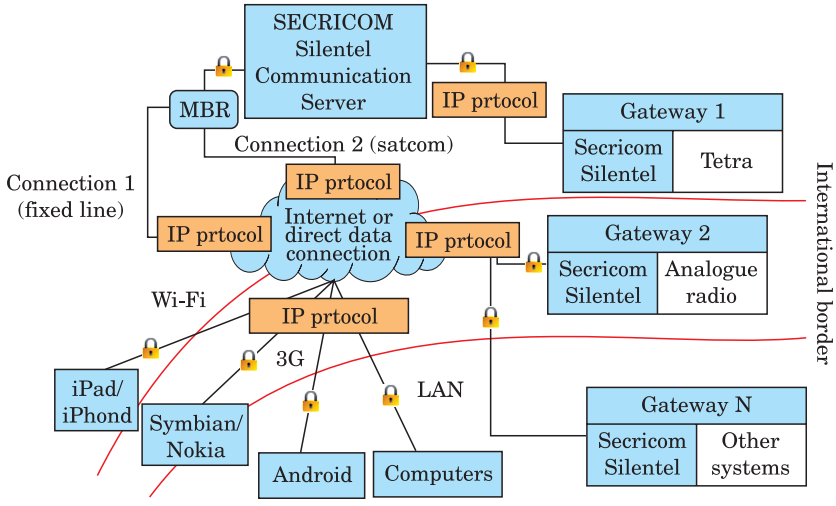

Fig. 4. SECRICOM Silentel Integration with Tetra and Analogue Radio

SECRICOM Silentel Capabilities

SECRICOM Silentel application features were designed to support the operation of public safety agencies and other actors in PTT

daily routines and crisis situations. As defined by the user requirements analysis undertaken by SECRICOM consortium, **voice conversation** still remains the very first requirement. SECRICOM Silentel enables to build a one-to-one call with full duplex voice transfer or one-to-many group call (Fig. 5) with half duplex voice (press-to-talk). The management of any group is flexible with a possibility to add additional members by any of users involved in conversation. This voice service can be used for seamless involvement of actors using different devices and located in different countries.

Another feature offered by SECRICOM Silentel is **textual service** such as instant messaging (one-to-one or one-to-many) or long message up to 1000

Fig. 5. Secricom Silentel Voice Conversation

unicode characters (Fig. 6). These were proven by a demonstration exercise as an useful tool for correct spelling of name (instant messaging) or treatment instructions for hazardous chemical sent by external expert (long message). Both services enable audit trail within protected environment and also delivery and read receipt.

Fig. 6. Secricom Silentel Texting

Emergency response requires all senses in action including visual sense. Visual sense can be supported by **use of images** in daily business and special occasions. SECRICOM Silentel enables to send images in conversation groups, both saved from device memory and taken in real time. This feature was used for sending an image of hazardous barrel label in Portsmouth, UK to an external expert located in Poznan, PL. Similarly, some devices can use hand drawing over defined canvas to share directions – like sketching directions over building floor plan during evacuation (Fig. 7).

Fig. 7. Secricom Silentel Images Transfer

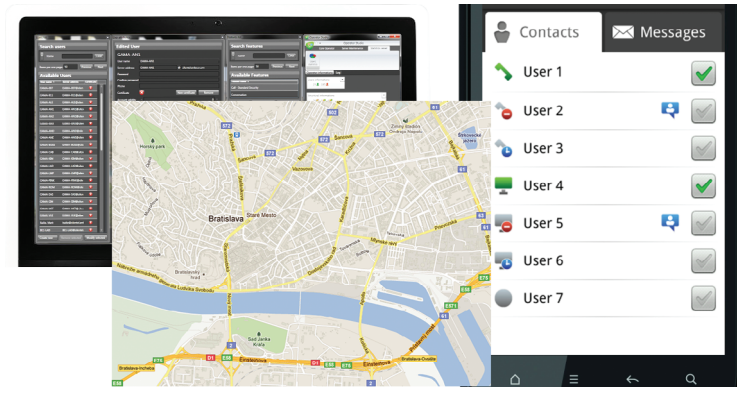

Fig. 8. Secricom Silentel Operator Studio and GPS positioning

When managing a group of actors, their location and availability really matters. SECRICOM Silentel has a **GPS positioning** feature, so a master user (such as an operator) can see the current location of different resources on a map in real time. Every installed application contains a secured contact list with presence status – users can simply select one of pre-defined statuses, such as available/emergency state/non available/etc. This allows identifying **available resources** at a glance (Fig. 8).

Conclusions

SECRICOM Silentel is a scalable ICT solution consisting of a communication server, a certification authority, an operator studio, end user application and interfaces to other systems. It was designed and developed in line with the SECRICOM vision – to provide technologies supporting performance of emergency responders in a comfortable way on standard devices and networks. It introduces new features for standard devices such as smartphones and laptops – they are turned into powerful and secure communication tools suitable for current actors and allowing involvement of new actors with certain responsibilities into emergency actions. These can include officers in emergency agencies, local government officials (county, town) and also infrastructure services (water/gas/electricity/transport).

SECRICOM Silentel is open for further integration with systems currently in use by public safety services. Its ambition is not to replace, but supplement them by adding new devices and actors to emergency teams. Concerns about connectivity of IP based systems can be answered by listing priority users in public/private networks, extendable network means and/or use of Multi-Bearer-Router for seamless connectivity.

SECRICOM Silentel supports heterogeneous actors cooperating during emergency response, both cross-border and inter-agency. Security is taken as an integral part of the service in sense of transfer of data, access and user management. It allows using the infrastructure for security-sensitive operations as well. These features were demonstrated in an integrated demonstration of the project and are to be developed into a product by ARDACO in following months.

Translated by AUTHORS

Accepted for print 30.06.2012

References

EUROPOLTECH 2011. International Fair of Technology and Equipment for the Police and National Security Services. Fair Magazine Article http://www.energia.sk/clanok/veda-a-vyskum/secricom-predstavil-vysledky-dvojrocneho-vyskumu/1885/
http://www.itti.com.pl/en/eu-projects/on-going-projects2.html
http://www.secricom.eu/
http://www.secricom.eu/images/articles/SECRICOM-HN-29-7-2010.pdf
http://www.secricom.eu/images/articles/Secricom-leaflet-4-2010.pdf