Consortium members

- **QinetiQ (UK)** - project coordinator
  Internetwork interfaces, interoperable, recoverable and extendable network
- **Ardaco (SK)** - technical coordinator
  Secure wireless fault tolerant communication
- **Bumar (PL)**
  Technical specification and testing, dissemination strategy
- **Infineon Technologies (D)**
  System on chip design
- **Nextel (E)**
  Communication testing, scenarios
- **Hitachi (F)**
  Docking module design, internetwork interfaces
- **Smartrends (SK)**
  Security analyses, intellectual property affairs, chip-level security
- **Br(itish Association of Public Safety Communications Officers (UK)**
  End users view, dissemination
- **ITTI (PL)**
  Administrative tasks, development of system
- **Universite du Luxembourg (LU)**
  IPv6 based secure communication
- **CEA - Leti (F)**
  Dissemination leadership, research
- **IAIK TU Graz (A)**
  Secure docking module
- **Slovak Academy of Sciences (SK)**
  Theoretical background of secure agent infrastructures, analyses

SECRICOM has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013]) under grant agreement n°218123.

SEVENTH FRAMEWORK PROGRAMME

SECRICOM

Seamless Communication for Crisis Management

Recover
quickly

Keep on
talking

Terrorism, major industrial accidents and natural disasters. Unpredictable catastrophic events require new, innovative and affordable solutions for Public Safety Agencies and their first responders. National governments and European institutions are aware of the security threats. A key aspect in helping to recover from these situations is an integrated and secure operating COMMUNICATION system. Currently, there appears to be a certain lack of solutions, which can provide crisis management agencies with secure, trusted communication systems with also wide coverage capability.

The SECRICOM project platform ambition is to provide a solution to this challenging requirement. The abbreviation stands for Seamless Communication for Crisis Management. The project was proposed to the European Commission and selected for funding in 2008 at almost 9 million Euros to a consortium of 13 partners in security topic of FP7 programme. It is proposed as a 44-months RTD project aiming at the development of a reference security platform for EU crisis management operations.

SECRICOM goals:

(A) Solve the problems of contemporary crisis communication infrastructures

a. Extend their interoperability

b. Decrease the vulnerability against tapping and misuse

c. Enhance the possibilities to recover from failures

d. Alternative data carrier introduction

e. Deployment and operational costs reduction

(B) Add new smart functions to existing services

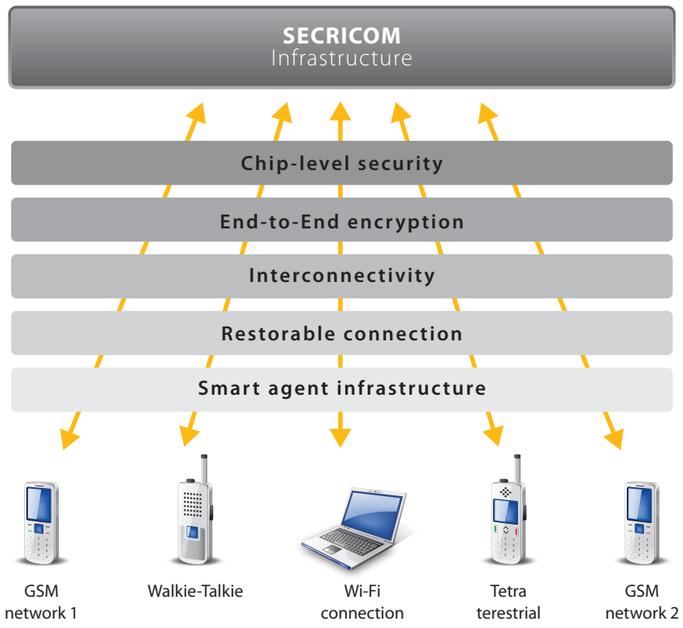
SECRICOM technological pillars:

(1) Secure encrypted mobile group communication

(2) Security based on trusted hardware enhancing the confidentiality and privacy of users

(3) Improved interoperability among various existing communicating systems

(4) Introduction of smart distributed system for independent handling of various first responder's requests



Seamless and secure interoperability

SECRICOM creates interoperability among heterogeneous secure communication systems incorporating the existing hundreds of thousands of radios already deployed. The end to end service will support any SECRICOM user with any connections to any of the selected networks, as well as provide network access to the SECRICOM Control centre that will identify security issues with the provided end to end, multi bearer IP network and user services.

Innovative approach of distributed systems utilization

The rapid location and procurement of resources such as health services, hospital capacities, personal resources, will make the management of crisis situation logistics more efficient and effective. This feature will be based on parallel distributed mobile agent-based transaction systems implemented both in mobile communication devices (an application in mobile phones, walkie-talkies) and central systems in management centres. The access to such services will be protected by customized chip-level security.

Cost effectiveness

SECRICOM fills the gap between deployed technologies providing the intercommunication and extending the security network to mobile phone users, which is affordable in the short term and cost effective over time.

Project achievements and future works

SYSTEM REQUIREMENTS

An in-depth analysis of external and internal system requirements was undertaken under the leadership of the UK's BAPCO association and QinetiQ resulting into system design by Smartrends. Based on that SECRICOM system components are developed.

SECRICOM PTT MODULE

It is a communication system using IP protocol offering secure encrypted voice, multimedia, instant messages and control data transmission in defined closed user groups. Significant advances have been achieved in this area under the leadership of Slovak SME Ardaco. SECRICOM PTT is already available for assorted devices such as mobile phones and laptops and variety of mobile and fixed networks (GPRS/EDGE/UMTS/WiFi/LAN). In addition, universal interface of the SECRICOM to the other communication platforms to create seamless end to end IP service is to be developed (TETRA, TETRAPOL). The idea of this gateway is to allow users from those existing networks to make a conversation with Secricom PTT users and vice versa.

SECURE AGENT INFRASTRUCTURE

Secure Agent Infrastructure is software services design with agent-like features which would execute on secure devices called secure docking stations such as dedicated mobile phones and laptops. Each agent has features used for enactment of certain processes. Based on problem specification in a form of dialog between the software and the user using the trusted device, an agent service will try to identify the most serious problem which is rendered by the crisis situation. The SAI will help to semi-automatically generate in a few incremental steps a concrete plan of crisis situation resolution based on the retrieved disposable resource capacities. Secure agent procurement infrastructure has been designed through collaboration between Slovak, Spanish and Austrian technicians.

SECURE DOCKING MODULE

Secure Docking module is a single-chip security device that protects the information in order to provide security for agents that dock on to a trusted agent network. The protected information is only released to a requesting agent, if the agent can prove that it is in a trusted state. The design of the SDM is based on Trusted Computing principles. A special chip has been already designed in Infineon Technologies with inputs from CEA Leti and Hitachi.

SECRICOM USING IPv6

All the modules developed for SECRICOM should be eligible to cope with an IPv6 environment in the near future. The modules like SECRICOM PTT, Secure Docking Module, Multi-Bearer Router and monitoring and control centres should be capable of handling this communication protocol taking into account defined Quality of Service. The IPv6 environment and its impact for secure communication was studied and described in details by University Luxembourg.

FUTURE WORKS

Polish partners BUMAR-Radwar and ITTI are in charge of testing and further specifications of the SECRICOM components based on the field experiences and real conditions discovered during the crisis situations. Future work covers also network services, the monitoring and control centre definition by Nexter and integration of RTD results with demonstrations.