



Federal Ministry  
of Education  
and Research

# SoKNOS

Service-Oriented Architectures Supporting  
Networks of Public Security Sector

---



### Vision: Holistic IT Support for Major Incidents and Crisis Management

Catastrophes and other major incidents often lead to chaotic situations and an extreme workload for the responsible personnel and security forces. Decision makers and institutions often lack the infrastructure needed to work together quickly, proactively, and in a coordinated manner. The aim of the SoKNOS project is to develop and test concepts to enable this type of cooperative infrastructure. The project should answer the following questions, among others: How can the existing, distributed infrastructures, data, and processes be jointly used by the different organizations as required? How can the institutions, companies, and federal states in Germany be linked together, ad hoc, depending on the particular situation, without having to invest heavily in new, centralized systems? The intended result of the research is a services platform designed to meet the special requirements of the public security sector. These special requirements focus on the interoperability, security, and robustness of the infrastructure.

### Shortening the Period of Chaos

IT solutions need to be developed to shorten the period of chaos that occurs immediately after a catastrophe. Experience shows that this phase determines the duration and effectiveness of the subsequent phases, such as coordinated damage reduction or clean up efforts. First of all, the involved organizations and their top managers must be able to correctly assess the situation. This can only happen if all relevant information, in particular about available resources, can be gathered quickly. The data must provide a quick and clear overview of the situation. At the same time, it also has to enable an in-depth analysis and a simulation of the alternatives and consequences.

The aim is to base decisions on reliable, secure information, shorten response times, and thus increase the security and success of the action



taken. It must be possible to quickly integrate everyone involved into the decision-making processes. Decisions and actions should be coordinated systematically.

### Research Areas

To set up the services platform described, current technology (hardware, office communication, mobile deployment) is used. In addition, solutions are being sought in the following areas:

**Service-oriented architectures:** To create a foundation, general methods and processes are required to set up, manage, communicate, and design services. It also needs to be possible to check and develop them further.

**Machine-readable semantics:** It is only possible to provide users with the services required in a particular situation if both the individual and the cross-components “understand” each other. The meaning of a service performed by a component is described using machine-readable coding, making it understandable to other components.

**User-friendly workplace:** To be able to make decisions, employees and managers must be quickly and adequately informed. Therefore, the “workplace of the future” in the public security sector needs to enable optimum information transfer and communication facilities. The user interface must adapt to the current user and

scenario and preferably supply information that may be useful in the particular situation. At the same time, it must be possible to request additional information.

**Highly-reliable system behavior:** The public security sector depends heavily on IT systems. Therefore, these systems must be particularly reliable and demonstrate robust runtime behavior resulting from self-configuration and self-healing. A close connection between IT security and public security is essential. The security goals and mechanisms of both areas must be co-aligned and supported by innovative approaches to IT security.

**Integral data processing:** A wide range of new technological developments make internal and external information sources available quickly and in machine-readable form. Sensors report, for example, the parameters of buildings and premises; personnel can call on additional resources using mobile devices. Computer-based information preparation is providing increasing support. For example, it can turn building and installation plans into 3D maps for visualizing possible emergency routes. Thanks to the public and the Internet, immense new sources of information are becoming available, for example photos of accidents taken on people's cell phones or information about construction sites on possible emergency routes. This flood of information from various sources needs to be analyzed in an automated way, further processed, and, depending on its importance, made available to the planned services platform. To this end, an all-encompassing approach is being developed in SoKNOS.

### Application Scenario

In Germany, a number of different organizations are responsible for maintaining public security. These organizations are divided into functional areas (for example, police, fire departments, technical relief agencies), various political and

administrative responsibility levels (for example, local, state, and federal), public and private bodies (for example, regulators and private infrastructure operators), and civil and military units. These different organizations have to interact depending on the scenario. An example scenario will be developed and played out to show how SoKNOS will be able to support cooperation between organizations and an efficient information flow in major incidents. The scenario depicts a long-lasting flooding catastrophe that needs to be managed with national support. An example in the scenario shows how the flooding worsens, threatening a chemical plant. Simulations are used to make forecasts and implement measures. Using SoKNOS, members of the task force can manage this situation from their workplace and show it on the interactive map. As a result, the entire task force can gain a comprehensive idea of what is happening.

---

### Project Data:

Funding program:

ICT 2020 / Research for Innovation

Funding focus: security/reliability

Funding reference: 01ISO7009

Funding amount: €10.8 million

Duration: June 1, 2007 – December 31, 2009

---

## Project Coordinator:

Dr. Thomas Ziegert  
SAP Research CEC Darmstadt  
Bleichstrasse 8  
64283 Darmstadt, Germany  
Tel.: +49 6227 7-68889  
thomas.ziegert@sap.com  
www.sap.com/research

## Project Partners:

**B2M Software AG, Karlsruhe**  
**Berlin Fire Department**  
**Cologne Fire Department**  
**DHI-WASY GmbH, Berlin**  
**ESRI Geoinformatik GmbH, Bonn**  
**Fraunhofer IESE, Kaiserslautern**  
**Fraunhofer IGD, Darmstadt**  
**German Police University, Münster**  
**German Research Center for Artificial Intelligence, Saarbrücken**

**itelligence AG, Bielefeld**  
**ontoprise GmbH, Karlsruhe**  
**Rutgers University (CIMIC), Newark, United States**  
**University of Münster (IfGi)**  
**University of Technology, Darmstadt (KOM, TK)**  
**University of Technology, Dresden (GIS)**  
**SAP AG, Walldorf**

**Further information about SoKNOS at**  
**[www.soknos.de](http://www.soknos.de)**

## More Information:

Project Organizer for the German Federal  
Ministry of Education and Research  
Software Systems and Knowledge Technologies  
in the German Aerospace Center (DLR)  
Rutherfordstrasse 2  
12489 Berlin, Germany

Tel.: (030) 67055 741  
Internet: [www.pt-it.pt-dlr.de](http://www.pt-it.pt-dlr.de)

## Published by:

German Federal Ministry of Education  
and Research (BMBF)  
Public Relations Department  
11055 Berlin, Germany

100011001001100000101001100  
01001111011011011001110001100100011  
110001100110100011101001111  
01110100101101101010110111101001011001011