

# Salutis<sup>®</sup>

High-end-to-end crypto-technology

Background information for  
**Security & IT Management**

This information was assembled with all possible precautions. Nevertheless VZG Communications can not offer any guarantee that this information is precise and/or complete. VZG Communications will not accept any liability for any damage that might have occurred as a result of use of the information in this document.

VZG® and Salutis® are registered trademarks of VZG Communications

Contact: [www.vzg.nl](http://www.vzg.nl) (under construction)

Copyright© 1994 – 2006 VZG communications  
all rights reserved

## Earlier Asked Questions

### Salutis®, the next generation (Super)Crypto Technology

#### A. IDENTIFICATION

Usual activity of the organization:

VZG develops telecommunication applications for a wide range of voice response and call centre facilities for its clientele. These applications are for the customers implemented on the VZG Value Added Network Services (remote service centre) platform.

A special branch of the organisation evaluates for customers ICT systems to determine the security of these systems. This branch also researches cryptographic primitives and their potential for the Salutis SuperCrypto Technology.

#### SUMMARY OF PROJECT *(overview of the projects)*

The next generation cryptographic systems like Salutis are a ***(polymorphic)-polymetric*** encryption system to protect information in a unsurpassed way. Typical for these innovative systems is that they adapt a practical approach in application management and the required infrastructure to exchange the protected information. The aim of the Salutis technology is the sharing of information with the other members

of the group or with members of other groups.

Salutis is a new developed technology and uses this new technology in innovative ways.

#### B. THE PROJECT

1. Please describe the project?

Salutis is a high-end end-to-end (Super)Crypto technology. It is a complete technology to secure the sensitive information itself. Salutis is world wide unique, modular, scalable and adaptable for a wide range of applications implemented in embedded, PC or super computer systems. The status of current knowledge and computational power indicates that breaking the code generated by Salutis is an unfeasible task.

This technology will meet the most stringent demands of commercial and governmental organisations because it offers an application management cycle of 125 years to decrypt messages. Per organisation, 65.000 groups of which each can hold 16 billion group members. Within a group, 250 levels are available to define user rights.

Research shows that 80% of all security related incidents the end user was the cause of all problems. Another issue cryptographers have to deal with is a system to distribute keys and how to generate keys that

## Earlier Asked Questions

meet certain quality demands.

Salutis has a unique innovative automated key schema that is shielded from the users, but also the encryption or decryption process is an automated process. This technology is less susceptible for implementation errors, user errors and is easy to administer.

2. How did the idea of the project materialize?

The dogmatic approach paralyses innovation of cryptographic systems. Critical cryptographers voice their concern and refute the unconditional criteria because it hinders the introduction and acceptance of new ideas. The deliberation should be unconditional because it is essential to accept cryptographic algorithms before practical implementation.

The information society depends on information and therefore has a demand for a means to protect this information. Encryption systems to encode the information become increasingly important. The currently available encryption systems struggle to find an answer for the question: **“How can I transmit the decryption key safely to the receiver?”** *The Salutis technology can ignore this age-old question, because there is no transmission of any key in or with the encrypted information!*

Traditional encryption systems are often not user-friendly and prone to user errors. No wonder, that the code breakers success stories tell us

about user errors eventually enabled them to break the system. The notorious facts are important lessons to be learned. Lessons the designers of the Salutis technology did not ignore.

### C. TIMETABLE

3. What is the **total duration** of the project?

In the year 1994 the work to develop the Salutis technology took off. Development of encryption systems never ends. In the year 2000 a small application to demonstrate the concept of the technology and its potential was presented. The Salutis development team encouraged fellow professional to study this technology and invited them for their comments.

4. Please provide a timetable listing the different stages of the project.

The development project Salutis started in the year 1994 and for reasons we do not want to dwell into it was decided that no project information will be available.

A small application as proof of concept was build and further developed. End users and managers where enthusiastic and surprised by the ease of use. On special request, pilot projects to meet specific demands to demonstrate the feasibility of the technology and the benefit for their

## Earlier Asked Questions

systems.

The technology was nominated “Best invention 2003” and is under review by the Dutch government. Commercial parties and governments of several countries expressed interest in this technology for implementation. The encrypted message produced with Salutis was analysed and shown to have properties similar to those of “white noise”. These results indicate that the information is shielded by this technology in a surpassed way.

5. Where are you now in the implementation of the project?

The Salutis technology is market ready for a diverse range of applications. Beginning 2006 it is anticipated that the Salutis SuperCrypto technology will be commercially applied in applications.

### D. FINANCIAL PLAN

6. Which are the **sources of financing** of the project?

The technological development relies on private funds of the organisation. The European Union has supplied funding to meet the costs of the commercial activities.

### E. ADVANTAGES OF PROJECT

#### ► **Originality of the project**

7. Please specify in which way your project is innovative/original?

The Salutis technology is a groundbreaking approach that led us to design a super crypto system. This technology consists of a virtual network of a specific topology that connects selected autonomous enigma machines, thus creating a polymetric cryptographic system. Each enigma machine is based on cryptographic algorithms available in the public domain. This network could also create pseudo random connections with the different enigma machines thus creating a polymorphic super crypto machine. The aim of this design is to aggravate the work of the code breaker and to create a system that is capable to secure information for up to 125 years.

This (polymorphic-)polymetric encryption system is only realizable if an automated key schema that meets the most demanding criteria could be designed. The discovery of this key schema led to an innovative method to use code books (and one-time pad) to determine the used coding key. Salutis encrypted files only contain an index reference. For a scheme of the Salutis coding system the user is referred to the presentation.

## Earlier Asked Questions

### ► **Impact of project on community**

8. To create, improve or intensify **sustainable links between two groups of individuals**. Please describe how your project contributes to this aim.

Salutis offers an alternative for the CCITT X.509 encryption systems for communications.

Recent reports bring unsettling news about a breach of security that demonstrates painfully that these incidents have serious consequence for their users. The development of secure encryption systems is essential to keep information secluded from rogue parties and to protect the social infrastructure of the information society.

9. What is the **benefit of the project for the community**?

The information society can only exist if communication between parties or data contained within archives is not to be disclosed without agreement or consent of their owners. How to secure data and how to shield this information from rogue parties to transform the data to achieve their immoral purposes is the study domain of the information specialists. The Salutis technology meets the demands of the social order of the of modern information society.

10. Would you describe your project as « simple » and easily accessible to everybody?

The demonstration application shows that the concept is user-friendly and enthusiastically accepted by end-users. This application stores information in digital containers the user can save on his disk or transmit to other group members.

Salutis technology protects the encryption process and keeps it out of view from the user. The user may regard this demonstration program as a tool to compress data or to send information. The user has no knowledge of the internal process.

11. What positive results linked immediately to the implementation of the project do you foresee?

The aim of the Salutis Technology is to contribute to a safer and more fair information society.

12. What is the **economic impact** expected from the project?

The Salutis Technology will offer the information society a safer environment for their information systems on which it relies profoundly. To deal with new age crimes like computer fraud, identity theft, and so on are threads that target society directly.

13. Please specify the framework of the **partnership(s)**.

No external parties have been involved in developing the Salutis technology. VZG has committed itself to research cryptographic

# Earlier Asked Questions

primitives and how their potential can be utilised. The aim is that eventual collaboration bonds between commercial organisations and research institutes will arise.

These alliances are of great importance to develop a wide range of applications that incorporate this new innovative technology. Implementations of this technology requires a small footprint to allow integration with embedded systems, original equipment manufactures or incorporation within systems offered value added resellers to their customers.

## F. PROTECTION OF INTERESTS

14. Which steps to ensure adequate **protection of his interests** are taken?

Detailed information about this technology is guarded as a trade secret; however, all cryptographic algorithms are available in the public domain.

## VZG communications

E-mail contact via [www.vzg.com](http://www.vzg.com) (under construction)