



BUSINESS SECURITY

SOLUTIONS
FOR
SECURE
COMMUNICATIONS

Encryption for the fu



Sweden's future, network-based defence is getting closer. A new advanced encryption system will be one of the fundamentals for secure information flow.

Today, the Internet is one of the cornerstones in our civilian society. The Internet affects how we communicate, do business and obtain information.

In the future, military operations will also be increasingly based around networks. The decision-making cycles will become shorter and critical assignment information can be rapidly distributed to the right recipient. But in order for this future defence organisation to become a rea-

lity, a series of security questions need to be solved. The challenge lies in creating security that does not restrict the growth and usage of the network. That is where encryption comes into the picture.

On behalf of the Swedish Armed Forces, FMV has been working for several years with developing specifications for a new IP-based encryption system. With the encryption device 920, the new demands for speed, performance and functionality will

be met, regardless of whether it applies to computer, video or voice communication.

Synergy

In May 2002, FMV issued an invitation to submit a tender offer to the industry. Of six tenders, the company, Business Security, met the demands at the lowest price.

"Parallel with the Swedish Armed Force's new encryption system the company is also developing a commercial variant of the system, aimed at larger international companies with very high demands on security, for example, within the pharmaceutical or financial sectors. In this way, the costs for FMV and the Swedish Armed Forces are kept low," says FMV's project manager, Tommy Lydh. But of course, only a part of what is developed for the military can be used commercially.

One of the challenges in the project is to be able to coordinate the high security demands with the demands for a functional, adaptable product. The encryption device 920, is based on the absolute latest IP-technology and meets military demands for ensuring integrity, confidentiality and authenticity. The system is based on real-time solutions designed to securely deliver assignment critical information throughout the entire chain of

command – whenever and wherever. Consequently the system supports satellite communication, which is necessary to quickly establish secure contacts in inaccessible areas. Encryption of videoconferences and IP-telephony is also supported. Other features include an advanced key management system that is specially adapted for IP-encryption.

"In addition, the system is modular. It is important that we can offer the defence forces and other authorities a flexible security solution that works for future communication solutions," says FMV's Kjell Albiin, product manager for IT-security systems.

Test period

After a period of work with functional models, ten prototypes were delivered to FMV in the summer of 2005.

"The prototypes are now being fully tested in the laboratory environments," says Tommy Lydh.

During the spring of 2006 the prototypes will be passed on to users in the Swedish Armed Forces and other authorities, so that final users can try to build a network with them in an actual environment. In the case of the Swedish Armed Forces, it is thought that the encryption attempt will be made down to the unit level.

During the second half of 2006 the first of a total of 350 new



Chief of Staff for the Swedish regiment, P7 Revingehead, Jörgen Forsberg, is participating in testing the new IP-encryption system.



Encryption device 920.

uture

encryption devices will be delivered, and before July the delivery will be completed. Up to now, things have gone according to the established time plans.

"The work has gone extremely well," states Business Security's development manager, Roger Eriksson. "Our work with adhering to time schedules, costs and quality has gotten strong support through FMV's thorough requirement specifications."

Stringent inspections

As a link in the quality-mindedness within defence, the new encryption system will undergo, in addition to traditional encryption analysis, certification in accordance with the international code, Common Criteria. This means that the system will be inspected in regard to configuration, handling, development, functional specifications, design, source codes, user manuals, tests, vulnerability and support systems throughout the product's lifecycle. Every aspect of the formulation of the new encryption device will be documented and illustrated, including those people who participate in the process. In regard to encryption, nothing can be left to chance.

The encryption device, 920 is not only being developed for the Swedish Armed Forces. In FMV's assignment, it is included that the system shall also be adapta-

ble to other authorities with high demands for security protection. This is welcomed by Jens Bohlin, who is an IT security specialist in the Swedish Ministry for Foreign Affairs.

"The ongoing expansion of EU's communication network between member countries places increasingly higher demands on security," he states. The Swedish Armed Forces' investment in new IP-encryption, which can also be used for EU-communication, will strongly support Sweden's possibilities to take a more active part in EU security work.

Battle Group

The encryption device, 920, will get its first baptism of fire in connection with the introduction of EU's joint military group, the Nordic Battle Group. On January 1, 2008 the group will be ready for action and, in addition, Sweden will have supplied the group with a secure management system with encrypted communication.

Over the long-term, there are plans to also integrate encryption connections for individual soldiers. A joint, fit-for-use encryption system is already on the drawing board and is intended for use by, for example, the Markus soldier project (soldier of the future).

COPY: JERRY LINDBERGH
PHOTO: BUSINESS SECURITY

WHAT IS ENCRYPTION?

Traditionally, encryption has been a way to keep information secret – to code messages so that unauthorized personnel cannot read them. The recipient must know what method is used for encryption and possibly the secret key to decipher the message. In today's IT society, however, it is not enough to be able to keep information secret, you must also ensure that no one has altered the information that is sent. This is called integrity control. Even if the message is encrypted so that no one can read it, someone who can access the message can change its content before it is sent further. Consequently, both encryption (read protection) and integrity security (write protection) are important. Origin controls are also important. This is so that you know that the message really does originate from the stated sender.

All encryption is done with the help of a code, which is an algorithm (method) that uses plain language, and a key to generate a coded text. Today's codes use keys that have 128, 196 or 256-bit keys. With a 256-bit key there are approximately 10,000,000 (+ an additional 70 zeros) different keys to test, which is almost as many as the presumed number of electrons in the universe.

Integrity control is solved with the help of a so-called hash sum. This is a method to generate a fixed number of bits that are associated to the message from the message itself. This is then used together with encryption to generate write protection. Origin controls require a little more. Normally it involves the use of a certificate to prove who you are. The certificate must be issued by someone that both parties trust, such as a Certification Authority.

Military, diplomatic and other critical security communications systems demand advanced and very well organized systems for encryption. Here, it is not enough to protect against unauthorized listening and unchecked changes. The information must be able to be kept secret for a long period of time, often several decades. Information that is assessed to have more long-term value is monitored and saved on a routine basis. Even after it has lost its actual news value, it can, in certain cases, be used as an aid in decoding other messages.

Business Security - an introduction

Business Security was founded in 1993. The core business dates back to the 1980s when a group of Swedish crypto experts invented a proprietary hardware-based algorithm.

Today Business Security is one of the world's leading companies within hardware encryption systems for data, voice, fax, video and the Internet. Our teams of experts develops in-house solutions i.e. from thought and innovative ideas to finalized solutions.

Business Security is based in Sweden, known for its technology innovativeness and strong commitment to top quality products. Greenhouse, our HQ in the south of Sweden is a unique environment for development and growth as well as a sanctuary for creativity, innovations and versatility that makes us excel in all aspects of our business.

All our products and solutions are developed in-house by teams of security, crypto experts and R&D engineers. The systems are developed according to Common Criteria highest practical security levels and against specific TEMPEST requirements. All business operations within Business Security work according to ISO9001 to assure the highest quality standard.

Business Security is the host of a Swedish Security Council. A forum where influential security experts, researchers, IT pioneers and crypto scientists in the country gather to discuss security aspects with a unified mission to develop and deliver powerful security solutions that can match the challenges of the future.

Our clients

The one feature common for all our clients is their need for extraordinary security solutions. We establish long-term relations with our clients and often work project-based to cater to our clients need.

Our clients are mainly Defence, Governmental Organizations, Law Enforcement Agencies, Bank & Finance and Multinational Corporations. We offer custom-specific solutions and customized algorithms to meet our clients needs. Business Security has delivered security solutions to over 40 countries worldwide.

We have routines and procedures in place to provide strict confidentiality and integrity for our clients. Upon request, we can present you with strong references that we have received as a courtesy from various prominent clients.

Our products

To give you an idea of what Business Security can offer you as a client, we have listed some of our products below;

SecuriVPN (for high security IP communication)
Hardware based encryption, designed for military and government organizations requiring extraordinary VPN-security. Certified up to Top Secret level in Sweden. EU approval in progress.

SecuriGateway (for secure IP communications)
SecuriGateway is a dedicated and comprehensive VPN system, which provides government and corporate organizations with secure communications over untrusted networks. EU approved on Restricted level.

SecureD® (for secure data storage encryption)
SecureD® offers optimal, high speed protection for stored data on disk. SecureD® is logically and physically separated from the processing unit and the storage device of the computer system. Hardware based security solution with no extra software required.

SecuriFax (for secure fax communication)
SecuriFax effectively eliminates security risks such as wire-tapping and eavesdropping and helps form a robust network that can secure all fax communication.

SecuriVoice (for secure voice communication)
SecuriVoice successfully secure voice communication for both analogue and digital telephones.

SecuriCrypto (for secure data communication)
SecuriCrypto is the perfect way to secure all data transmissions via leased lines and satellite communications. It provides protection against unauthorized interception of on-line data transmitted.

Customised Solutions
Business Security have developed a large number of customised solutions.

If you would like to read more about our products we will be delighted to provide you with specific product information sheets. These include more detailed information to ensure that you make the right decision for your needs.

Security entails
trust and expertise...

...Business Security
at your service



Business Security AB

Box 110 65

S-220 11 Lund, Sweden

Tel: +46 46 38 60 50

Fax: +46 46 38 60 55

E-mail: reqinfo@businesssecurity.com

URL: www.businesssecurity.com