RFIDnordic.se
INFORMATION CONCERNING RFID IN SCANDINAVIA Sept 2006

THINKING CLOSETS FOR CLOTHES WILL GIVE MILLION-SAVINGS

With RFID-chip attached to the working-clothes and thinking closets (with installed RFID-antennas), St Olavs Hospital will save millions in logistic- and stockholding-costs.

The top-modern hospital has installed a solution based on closets communicating with the clothes via small RFID-chip in the fabric. A computer is connected to the closets that register and show the contents in the closets continuously.

The closet can separate both the type of clothes and the size. If it for example is running out or trousers in size medium in stock, the system itself will generate an order to the person in charge at the hospital. This person can then send the order to the laundry directly.

The clothes comes clean and folded in piles from the laundry and are being placed in the closets. The staff will use their ID-cards when they pick up new clothes from the closets and by this, the system know to which ward shirts and trousers goes. The clothes will be returned to different depots/dumps after use and will then be registered so the ward can be credited for the returned clothes. And again the clothes will be sent to the laundry. According to Mr Vidar Kvaheim.

BIG SAVINGS IN AREA:

Kvalheim is talking about the savings in area-space as one of the biggest advantages with this solution compared to other machine-solutions. In the other solutions the clothes are being transported and stored on hangers. This is taking a lot of space and it is also very time-consuming for the staff to register every single article of clothing as soon as it comes to the closet.

BIG POTENTIAL:

One of the challenges for Kvalheim and the technology skills in Trondheim was to find a RFID-chip that could stand warm wash and tough/hard treatment and also make the

continue page 2

The staff will use their ID-cards when they pick up new clothes from the closets.

The clothes are stored in piles in the closets. This gives big savings in area

PUBLISHER: *RFID Nordic.* EDITORIAL OFFICE: *Ove Canemyr, Trendsetter AB, Box, 24013, 104 50 Stockholm. Phone +46 8 662 31 95.*
THE BOARD 2006: *Ove Canemyr, Trendsetter AB, Box 24013, 104 50 Stockholm, Tel 08-662 31 95. Björn Söderberg, Kiwok, Gunnar Ivansson, Electrona, Stefan Tjerngren, Electrona, Leif Nordlund, SUN, Johan Malm, Artimas, Olle Hydbom, BioEtt, Angelika Melcior, Föreningssparbanken, Hoss Eizad, Sogeti. Aticles to the editor: ove.canemyr@trendsetter.se*

solution easy to use. Texas Laundry tag was the solution. He also tells
us that the cooperation with dynamic companies and the University hospitals in Trondheim, Tromsø and Oslo has been of vital importance for this solution.

ST. OLAVS HOSPITAL WILL SAVE TENS OF MILLIONS:

St Olavs Hospital has actively participated in this development of the solution and they have so far installed 120 machines divided on 10 store-rooms. When all the installations are done they will have over 300 pcs installed. Helsebygg Midt-Norge believe that the new system will save over 40 million NOK only in area-costs.

Further savings per year will be between 15 -18 millions in working expenses due to less work with all the routines with ordering etc and also timesaving for the staff as it will be much easier to find the right clothes and the right size in right time. So far, all experience with this new system is very positive. The staff is very satisfied and they also find the solution easy to use, according to one of the nurses at St Olavs Hospital.

The RFID-Technique is based on readers from Feig Electronic, 13.56 Mhz and Laundry Tags from Texas Instruments, supplier is Electrona-Sievert AB.

"Helsebygg Midt-Norge believe that this new system will save over 40 million NOK for the hospital only in area-costs".

If you have questions please contact:
Arild Engesbak, Texi , arild.engesbak@texi.biz, tel +47-99535464
or
Vidar Kvalheim, Texi, vidar.kvalheim@texi.biz, tel +47-97147072

RFID

CONTENTS:

September 2006

Page 1	Thinking closets for clothes will give million-savings
Page 2	New tools to simplify
Page 3	ACG brings "mobile" voting to Swedish parliament
Page 4	Public security solution for nurses and service personal!
Page 5	EU e-Passport Project Results
Page8	Using middleware and consultants for a rapid uptake of RFID
Page 9	The slaughter is off
Page 11	SPsion Teklogix Rugged RFID Hand-Held Only One Tough Enough For DoD
Page 12	The Gentle Tag: Putting RFID into a Technology and Society Context
Page 15	Members infomation

NEW TOOLS TO SIMPLIFY RFID INSTALLATIONS

RFID installations often require numerous given functions, for example; triggering via photocells, reading and verification (using light or laser, for example). Sometimes a system is required to open mechanical barriers, trigger messages or distribute data amongst various systems and applications.

A new instrument to simplify all forms of RFID installation has now been developed by RFID Constructors.

"…as so many common actions and functions within RFID systems are repeated from installation to installation, it unnecessary to re-invent the wheel every time a new system is installed. We have created a product, called GrabIT, which manages and seamlessly handles the entire spectrum of common functions and controls; thus greatly simplifying any RFID installation." Says Niklas Hild of RFID Constructors.

Apart from basic functions, GrabIT also manages readers, control units, databases and import/export of data throughout the entire RFID system.

For further information:
Niklas Hild Tel +46 709 98 13 70
Niklas.hild@rfidconstructors

ACG BRINGS "MOBILE" VOTING TO SWEDISH PARLIAMENT

Sweden's parliament, the Riksdag, an institution dating back to the 16th century, has undergone numerous changes over the years in order to keep up with the times. This October, when the new session convenes following nation-wide parliamentary elections, a revolutionary voting system will be awaiting Sweden's new lawmakers.

In fact, over the summer recess, the Riksdag has implemented state-of-the-art voting system based on radio frequency identification (RFID) technology that will enable faster and more secure voting operations.

Up until the last Riksdag session, the 349 members of the Swedish parliament were required to vote from the seat assigned to them at the beginning of the legislature. In order to expedite voting operations, the Swedish parliament has plans to eliminate this constraint by allowing its members to conveniently vote from any seat in the chamber. This objective calls for a secure and efficient identification system for members of parliament.

The system is based on the contactless mifare access control cards already issued to all members of parliament and the newly-installed RFID readers from ACG Identification Technologies, a leading component and technology supplier in the smart card and RFID markets.

The Riksdagsförvaltningen, which is responsible for creating good and functional working conditions for members of parliament, selected the ACG HF Multi ISO reader for this project for its performance and flexibility. The reader's bootloader functionality allows for an easy firmware upgrade if required and therefore protects the investment should new types of contactless ID cards be introduced in the future. The HF Multi ISO reader also provides the highest level of interoperability available on the market, with support for numerous international RFID standards such as ISO14443A/B, ISO 15693, ISO 18000-3, I-CODE as well as NFC (Near Field Communication). In addition, ACG's reader has also demonstrated exceptional performance and reliability even when mounted inside the metallic frames found in the chamber - a level of performance that very few competing readers could match.

The ACG readers have been installed in various places inside the voting chamber. The tender for the implementation of the new voting system was awarded to ACG's partner and leading Swedish system integrator, Syntronic AB.

NEW MOBILE DEVICE FOR PERSONAL SECURITY WITH IMBEDDED RFID PERSONAL SEALS:

PUBLIC SECURITY SOLUTION FOR NURSES AND SERVICE PERSONAL!

A new security device tested and used in the field of security on personal level.

The product also has a seal that prevent the unit form been left or stolen or disappear from the user.

After its final testing of the concept in the phase of electronic product compliance stage, the European company PLEFO AB have produced a new innovation built on the Confidence RFID patent and PLEFOS patented electronic RFID logistic movement. It has passed the qualifying rounds and has confirmed great possibilities.

It is a solution not only for the patrol guard industries but also all other lonely workers that have been waiting for. this type of products The solution are now being recommended to nurses and home assistants alike. Such a recommendation would represent a major European and International market breakthrough for this product. Addressing security, service and identification control solutions, a market worth millions of euros in the long term has been realised

For more information rplease contact
Mr. Lucas Ahlstrom, executive member of PLEFO and the RFIG group.
lucas@plefo.se
www.plefo.se
Phone +46-8-667 4020
Mobile +46-70-182 1500

EU E-PASSPORT PROJECT RESULTS

E-Passport is one of the most focused areas by governments worldwide. It requires an international security infrastructure based on a unit standardization to increase passengers' safety and security globally. Due to the international crime and terrorism changing condition ePassport system has an ongoing boosting process nature.

E-Passport system creates synergies as APIS (Advanced Passenger Information System), NeID (National Electronics ID), International Security Database Infrastructure and more.

"The EU Digital Passport Project" is one the world's efficient program of The EU Commission to harmonize and standardize "A selective electronics based machine readable document system" for the members' countries. The European Union has been funding a three-year project entitled the EU Digital Passport since March 2004. Its purpose is to evaluate the challenges on the implementation of the digital passport in Europe on a technological and security level and to provide input on critical issues to the Commission and national governments. A consortium of large European companies took the challenge to analyze and comment on the preconditions and required modifications with respect to the European landscape.

The project's required a continually connection with other equal international and national programs belong US Homelands Security, China, Japan and more.

Within the 6th framework program (IST_2002_507974) and since March 2004, the European Union has started funding a three-year project entitled the "Digital Passport". The Purpose of this project is to evaluate the challenges on the implementation of the Digital Passport in Europe on technological and security basis and to provide input on critical issues to the Commission and national governments. We, a consortium of large European companies have taken the challenge to analyze and comment the preconditions and required modifications with respect to the European landscape. We are now ready to present our midterm results.

THE ANNUAL EVENT: Smarticware AB as initiator, project manager and informer for The EU Digital Passport Project, arrange the second event, THE ADVANCED INTERNATIONAL E-PASSPORT SYSTEMS & E-ID SYNERGIES, FAIR AND SEMINARS, 1-2 November to disseminate the project's result.

Our events are a part of our activities to be a strategic and trusted partner for governments and other customers in areas related to ePassport, eID solutions and other Trusted Chip Solutions and eServices and thereby contributing to a safer world.

Smarticware managed successfully "The World's First Electronics Passport and Border Control Exhibition", including seminars and a showroom of the Swedish ePassport system, at The World Trade Center in Stockholm, January 26 & 27. More than 500 official representatives from 35 countries and a huge number of related market players attended.
The seminars, as well as updating the pan European state-of-the-art, will include the following points:

- Production of e-Passport booklets.
- Enrolment of e-Passports.
- Personalisation and issuing of e-Passports.
- Distribution logistics for e-Passports.
- e-Border control.
- e-ID processes synergies.

Thanks to the EU project, collected expertise, our industrial know-how and daily contact with the commission, we have recognize a number of complementary and needed products within security systems such ePassport and NeID. Some of them will be presented at our coming fair. Accordingly, Smarticware AB always is looking for new stable partners to fill the market gap of needs. The co-operated partners should have competence in development and sales.

BACKGROUND: After the events of 11 September 2001, the US VISIT programme became a major driver on the standardization and implementation of new personal documents with the aim of providing a better and more secure identification of travelers all around the world. All states are forced to modify their border infrastructure as well as the infrastructure for production and issuing of new passports. The digital photo, the optional inclusion of other biometric data and the personalisation of the chip, requires additional technical infrastructure as well as new legislative preconditions in some states. Also the national processes must be modified to fulfill the new requirements. Compared to the 'old' European passport, additional challenges come from changed legislative and operational preconditions – ranging from the increasing trend to privatisation of governmental organisations and outsourcing of governmental duties, to the foundation of the Schengen area, with common border controls and the possibility of a common infrastructure.

TODAY: Driven by the 11 September events, previously ongoing negotiations about a new and more secure travel document were given extra impetus. Although the digital passport can be only part of a superordinate security concept, the implementation of the digital passport is one of the most challenging operations of the current decade. Improving the qua-

Continue page 6>>

lity of the passport involves the improvement of the document itself, removing potential weaknesses which give offenders the possibility to produce faked or counterfeited documents, but also to improve the background infrastructure.

The trust in the authenticity of a travel document and the reliability of the holder-document relationship is a major part of border security. Also the usability of the document, with respect to border processing, must be considered to maintain the quality of the inspection process.

THE MAJOR ELEMENTS: The following sections describe the major elements of the implementation of the new passport generation and the upcoming requirements, open topics and possible solution scenarios and their requirements in a general overview context.

The International Civil Aviation Organisation (ICAO) – which has provided the technical specifications of the document and some supporting recommendations on an international basis – carries out the technical standardization of travel documents. The current version of the standard includes an improved technical specification of the security printing and the visual contents of the document as well as the specification of the digital data carrier contents (chip) relevant for international data exchange.

Of major concern is the durability of the passport, together with the protection against falsification over the complete lifecycle. Standards are required on this front to allow quality metering in tendering and
production and to avoid fraudulent or accidental modifications of the booklet and its contents.

With the integration of the chip into the new digital passport materials, new technologies and processes are required in the production of the passport booklet. The project covers the scope of the technical production process as well as on the security side. The technical production of the booklet has changed insofar as new materials (holder page, cover page, chip and RFID antenna integration) are to be considered. The basic requirements of detectability of page removal/ exchange as well as the mechanical stability of the holder/cover page and the booklet itself are vital parts of the implementation of the booklet.

Within the processes, new players are added by the chip, which have to provide basic security measures for the chip, its operating system and for the embedding of the chip into the holder/cover page. As these parts will be provided on a product basis to the national governments, regulations and standards are necessary to provide the required security measures to ensure that none of the base products of a national passport can be used to produce faked passports.

THE NATIONAL PROCESS: Based on the ICAO Standards, the national process authorities have to provide the legislative and regulative infrastructure to implement and control the processes for the management, printing, personalization and distribution of passports – in the homeland as well as on demand by diplomatic representations in third party countries.

National processes and their implementation and supervision are a vital part of document security. The quality of the documents security depends to a large extent on the national processes and the infrastructure used to verify the applicant and to issue the passport. Due to the high quality of the new passport document, an increase of the threat potential on the level of processing by attacks to the infrastructure, employees or organisations is highly possible.

In addition, new business models (keywords private public partnership, outsourcing, etc.) provide a fully new landscape for the national implementation of the passport. Other and more general legislative acts and standards have to back the commercial relationships and replace the former trusted relation between the national security printer, issuing organizations (e.g. police) and the national ministries. In some countries and within the European Union, new legislative acts and standards will be necessary to reflect the new requirements of the digital passport.

Within Europe, the Schengen area as a common border for most European states brings up questions concerning a harmonised security level for the travel document. Weak passports which are subject to falsification and decrease the security of the Schengen borders causing a degradation of the high investments to be taken within Europe for the implementation of the new digital passport. Combined efforts of the European states seem to be indicated to harmonise the passport and the associated infrastructure by a legislative and standardization framework to gain full advantage of the new technology and to maintain an equal level of security across all member states of the European Union. At a minimum level, the national implementation of the digital passport must be backed by appropriate security concepts and protection profiles and national authorities are required to request, maintain and verify the implementation of the security processes.

THE BORDER CONTROL: With the introduction of the digital passport, the border control infrastructure and the processing of the passport are to be changed in different areas. A new generation of passport readers with RFID capabilities must be developed and brought into the field. Our project is performing extensive product studies on the possibilities and challenges of the terminal implementation. Speed and reliability of passport scanning and verification of the document are very sensitive areas in border control. The speed of the process is a major concern with respect to growing passenger counts on all borders. Today, the processing speed is limited by the technical specifications of the chip, chip contents and the reader, which leads to extra processing time for the scanning of the passport.

This may lead to a decrease of possible passport verifications on today's staffing levels. Efforts must be taken for the next passport generations to improve and speed up the reading time to allow faster processing of passengers and to increase the amount of verified passports. New infrastructure or processing is to be considered to improve the border
processing time, on the cost side, as well as on the passenger throughput and on passenger convenience.

The integration of biometric data in the

Continue page 7>>

passport requires (based on national or EU law) the protection of the data fields by key material. Also the identification data contents of the passport will be protected by keys. New processes on international level are required to exchange these keys on an international basis and to integrate them into the terminals.

International compatibility is a major issue in the protection of the large investments to be taken over the coming years at an international level and within the European Community. The standards defined by ICAO provide a wide range of opportunities to the implementing countries. Different data contents (bior multilateral data fields), optional national contents and different biometric data formats generate a broad range of variants which must be implemented in all verification systems to gain full advantage of the digital part of the passport. Also, implementation variants lead potentially to incompatibilities and restrictions in the use of the document.
Today, the potentials of possible incompatibilities on a document with such a broad range of variants, with different manufacturers and with different processing requirements, cannot be estimated. Field tests arerequired to analyse the impact of the new technologies, their usability and open issues in a broader range and to prove the maturity of the technology in international use.

Some states have already confirmed that they will carry out field tests, and the ICAO conducts field tests on a periodic basis. The results will offer a glimpse of the problems that will arise in the implementation on an international basis.

SYSTEM COMPATIBILITY: In connection with the digital passport, the future integration with electronic Visa and other add-ons in electronic form (e.g. residence permits) must also be considered. This covers privacy concerns as well as additional technical and security related issues.
The specified optional components of the digital part of the passport and the electronic representation of current and future add-ons, which are possible in the passport, give a high potential of future increase of the value of this document.

The privacy of the citizens is one of the major goals of the European Union and for most states. Therefore, it is necessary to protect all relevant data in the passport against unauthorized access by third parties. This will lead to an increasing number of keys required to authenticate for access to this data including all the required exchange and maintenance procedures in the background. Therefore, for the first phase of any rollout, there seems to be a need to avoid such national (bi-/multilateral) extensions of the passport.

With the integration of the chip into the passport, a new security world starts. No doubt, the digital passport and the implemented biometric identifiers are a major advance in the passport technology and person identification. Nevertheless, we have to bear in mind that the contents of the passport can be only as authentic as the identification data written into the passport. The improved security of the document should also encourage national authorities to rethink the security aspects of the national infrastructure and processes.

New additional security requirements rise from new processes for the collection of data, key management, from outsourcing of governmental tasks to companies out of governmental control and an increased or newly encouraged use of IT-infrastructures for the production of the document.

Each of these new elements brings new potential for attack and has to be covered by a national security policy. The continuous monitoring of the security processes, within governmental organisations (and for subcontractors) is a vital part of the national security infrastructure. Additional measures are necessary to perform an efficient and target oriented security monitoring – especially for subcontractors outside the scope of national or community law.

For tendering procedures, the comparativeness of offers is a major factor for the decision. The application of common standards is required to allow effective comparison. The requirement of security processes is a major concern regarding outsourcing of historically governmental tasks to private companies.

Another part of the national security infrastructure is the Public Key Infrastructure (PKI) required for the personalisation of digitally signed data. Compared with the current lifetime of cryptographic algorithm key lengths, the lifetime of the passport is about two to three times longer. Therefore, high quality key material must be used to withstand attacks for a sufficient period of time and maintain the authenticity of the passport contents over its lifetime of around 15 years.

Within the duties of the process owner (typically the ministry of internal affairs) is also the management of the national key material. This duty covers the delivery of the national certificate to the ICAO Directory as well as the bilateral exchange of key material required for production and third party nation authentication purposes.

National procedures and bilateral agreed procedures are required and must be defined on national level.

EU DIGITAL PASSPORT: The new digital passport can and will be a vital part of the European security infrastructure, allowing a unique and trusted identification of EU citizens on the EU outside borders and by third party countries accepting the passport. The standardisation of the document by the ICAO is almost complete, giving the basis for the production and personalization of the passport booklets.

However, it seems to be indicated that additional efforts are necessary to make the digital passport really work in a convenient and secure way and to gain full advantage of the new technology. This covers technological advances as well as legislative changes and the standardisation of the document internationally by the ICAO.

Additional steps are necessary on a national or community level to provide the necessary security infrastructure on legislative and contractual basis and to harmonise the processes around the passport to a higher extent.

Contct person:
Omid Aval
CEO, Smarticware AB
Mob +46 (0)70 350 23 89
omid.aval@smarticware.com

USING MIDDLEWARE AND CONSULTANTS FOR A RAPID UPTAKE OF RFID

It is often hard to picture how RFID can be applied in different industries. It is therefore becoming increasingly popular to use a new type of consultants, specializing in RFID technology. They will provide innovative ideas and solutions on how to make today°Øs tasks more efficient, and how to be prepared for the future. They will explain to you the advantages of applying RFID to your business, the best way of investing in the technology and where to look for your return on investment.

A consultant will analyze today°Øs routines, and together with the customer decide whether or not to embark on an RFID installation. If RFID is decided upon, the RFID consultants will insure that the correct equipment is chosen, installed and implemented in an effective manner.

As soon as the advantages of RFID are made apparent, the customer learn that they require a new type of back-end software system to fully utilize this technology. The better we manage and present the collected data, the more intelligent will our systems become. The ideal situation for most companies is if innovative principles from an ∞RFID minded consultant can be used directly within their existing logistics and ERP systems. Unfortunately, the chances are small of finding a system that can be integrated with today°Øs back-end enterprise systems, and that will be compatible with future RFID technology. This will change over time, as more system solution companies will develop complete RFID systems for their industries. Until then, collected information from the use of RFID technology must be indirectly integrated with the existing enterprise systems. It is in this process, and in the development of future enterprise systems, that the term RFID middleware has been introduced.

Middleware is known to the world of information technology as a connection between hardware and software, or between different software systems, mostly placed on two or more different computers (client/server systems). By sing a middleware, developers are saving time when they develop a new product, since the data flow will be handled by an existing connection, or middleware if you like. This principle can be applied to enterprise systems and RFID hardware. On the enterprise systems side, the middleware has an open communication protocol. On the hardware side, the middleware already contains libraries for most commercially available RFID readers, as well as the possibility to write custom libraries for other (or future) readers. By separating the logics of the enterprise systems and the RFID hardware it will be possible to use any type of RFID hardware, independent of the choice of back-end enterprise system that will be receiving the information.

WHY DO WE NEED AN RFID MIDDLEWARE?

For easy collection and administration of data from RFID readers.
To use different combinations of hardware and enterprise systems.
To achieve our business goals sooner.
To have more robust system architecture, designed for future technologies.

WHAT ARE THE MINIMUM REQUIREMENTS OF AN RFID MIDDLEWARE?

Integration towards readers that comply with specific standards (from eg EPCGlobal)
Synchronization of data from different readers.
The possibility to add custom libraries
The ability to filter incoming data
Open communication protocol towards enterprise systems

WHAT CAN WE EXPECT FROM AN RFID MIDDLEWARE?

There are three important principles, when we measure the utilitarian value of an RFID middleware; transparency∞integration and independenc. The combination of these principles, and the selection of accompanying tools distinguish a solid RFID middleware.

TRANSPARENCY:

All departments of an organization must at all times be able to view the realtime status of other departments. It does not help to have an advanced logistics system, if it is not made transparent, and is able to offer all departments realtime information about stock contents and other processes. It must be possible to filter the collected information, so that it can be presented in a more efficient and dynamic manner.

INTEGRATION:

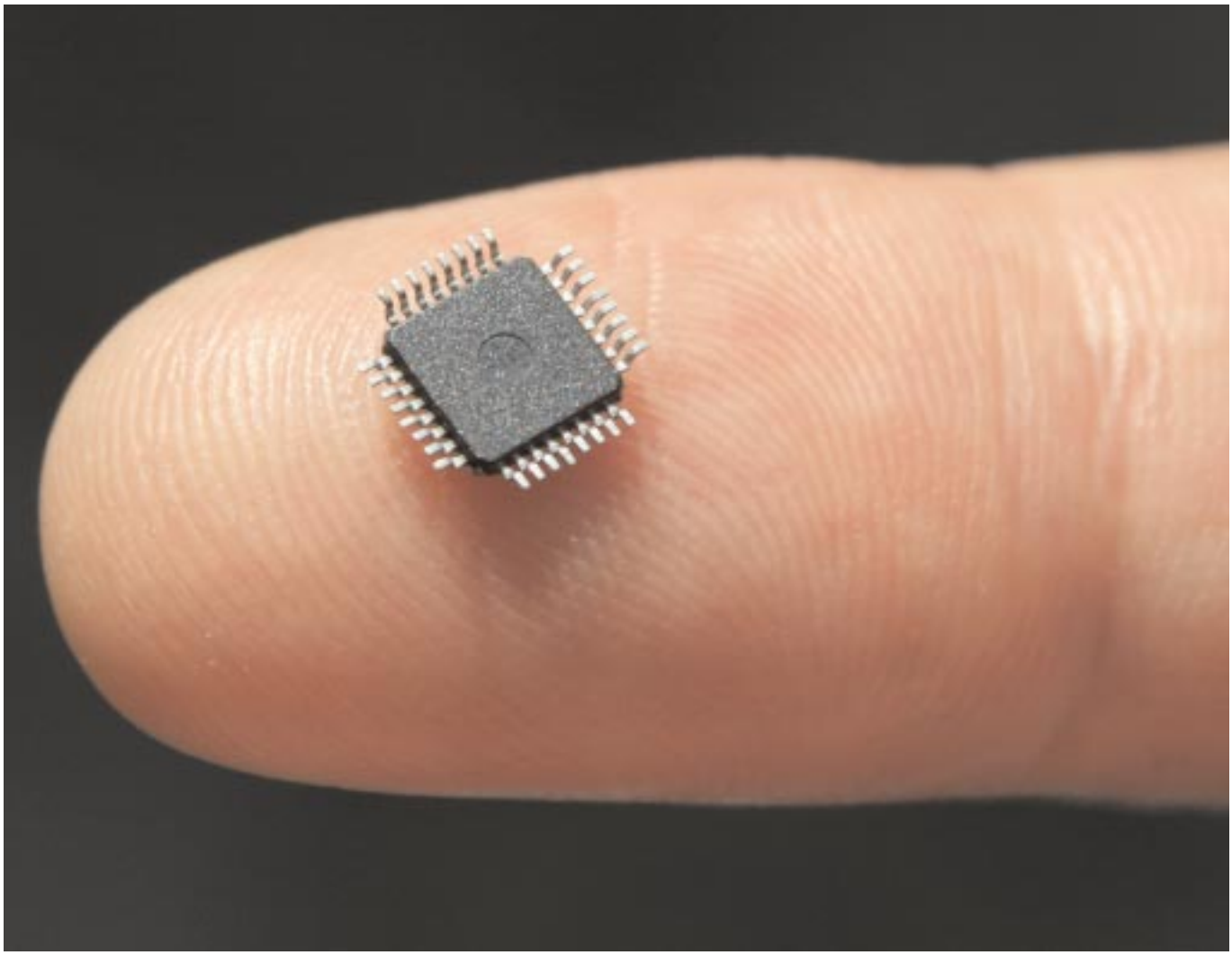
The right information at the right time, is a result of an interconnection of all parts of an organisation. Through an RFID middleware it will be easier to connect different systems and data flows to add increased connectivity. This will allow for an exponential growth in efficiency and presentation of correct information.

INDEPENDENCE:

Independence is more than transparency, in the way that all parts of an organisation no longer only can see each other, but also communicate with and affect each other. Your enterprise systems will no longer be restricted by elements that up until now have obstructed mutual interaction, such as protocols, language, placement and operating systems.

A true intelligent system°± is transparent, integrated and independent. Such a system can be configured to follow rules and to act based on status information from individual or grouped system components. It can be hard to evaluate whether or not todays systems are fully functional, or if RFID can be of help. We recommend that you discuss your current systems with an RFID consultant if you feel that your business is not transparent, integrated and independent. Many businesses will be surprised as to how easy, and to what extent, RFID technology and an RFID middleware can add intelligence to their existing systems.

For further information please contact:
ole@wtek.no



THE SLAUGHTER IS OFF

No more killing of tags at the point of sale, now RFID tags can remain useful throughout product life cycle rather than just being a production line tool. That°Øs the bottom line consequence of the new RFID technology that was brought to market this summer by Danish venture RFIDsec.

When Danish tech-company RFIDsec this summer launched the first working model of their RFID solution, they beat the opponents in the race of bringing the first RFID chip on the market to offer both strong encryption and active access management of chip content. Far from being a sales pitch this marks a new possibility for RFID use in general.

RFIDsec has made available the first series of RFID solutions that completely block unauthorized access to a RFID tag. Using a unique technology implementing cryptography on tag level, the RFIDsec tags are safe for eavesdropping all the way through the product life cycle. This is all well and good, since the security of tag information is a real market obstacle, but being safe is not enough to overcome buyer scepticism towards product°Øs °∞tagged°± with RFID tags. The solution to this is as easy as it has been so far impossible to solve: You need to be able to shut of the tag - and to turn it on again. RFIDsec provides this feature, combining their encrypted tag with an access management system. This means the tag can be ordered into silent mode, maintaining all data for further use in reclaim situations and the like. In short the owner of the product carrying the tag is in complete control of the tag and the way it communicates i.e. °∞Control°± instead of °∞Kill°±.

FIRST MOVER BY COMPANIONSHIP

RFIDsec have been developing their RFID ASIC in concert with market leading companies. Says CEO of RFIDsec Henrik Granau "We are working with the Industry, Large Global Systems Integrators, RFID Tag Manufacturers and RFID ASIC providers and it is definitely confirmed that our technology is addres-

Continue page 10 >>

sing real needs in the Market place across the various Industries. The huge interest we have met tells me that a number of the current RFID Tag Providers will want to integrate our technology on their Tags , as it seams there are no other similar solutions available". Henrik Granau stresses the point that the potentials of the RFIDsec chip and access management system are yet to be explored. °∞As technicians and business people, we have a lot of ways to use the RFIDsec tag in mind, but I think that the market will prove the limits our imagination°±.

SAFETY AT ALL TIMES

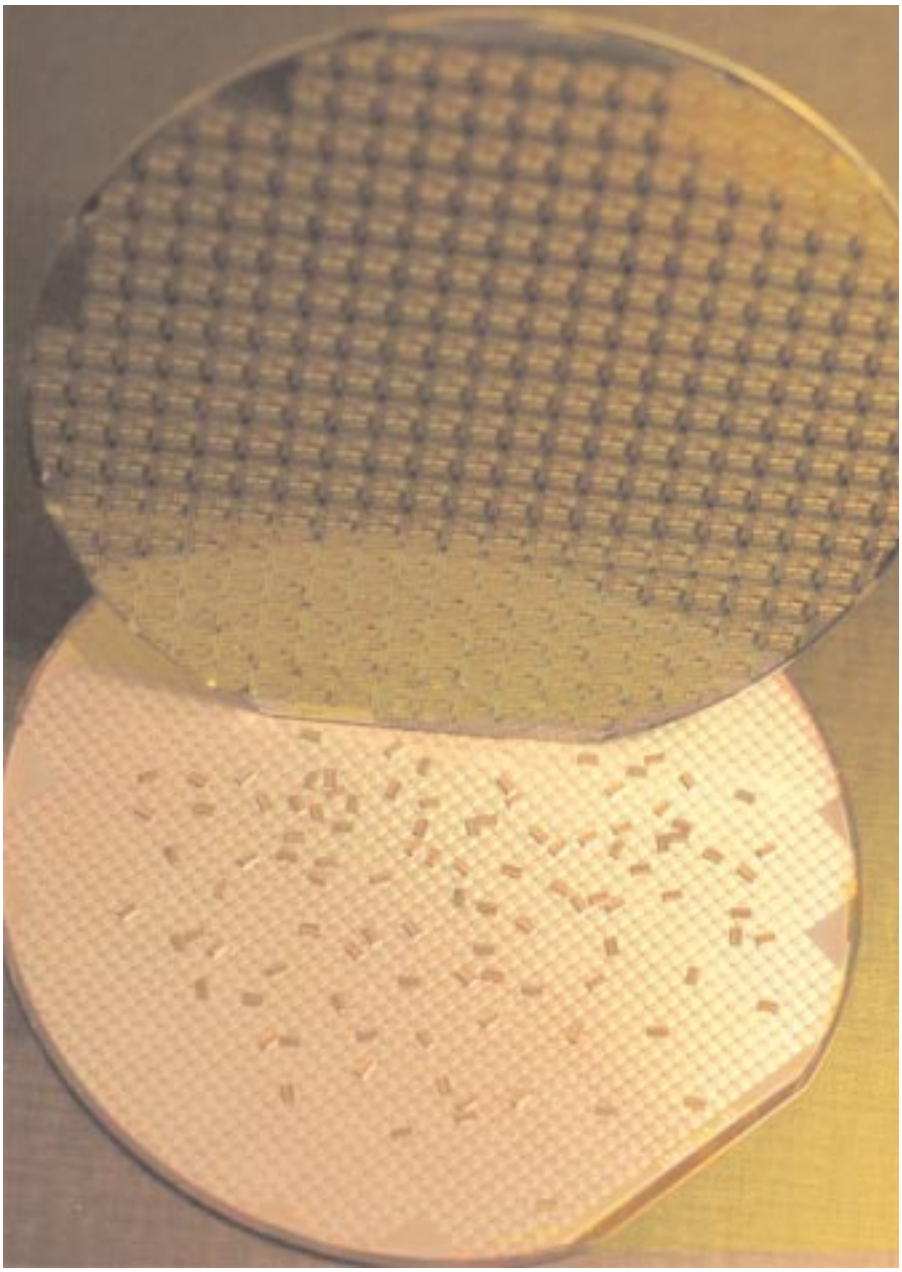
The tag/access management system, is se patent pending, provides in shortlist.

- Differentiated access to the tag, both regarding the right to read and write data on the tag
- ∑Safety and flexibility of use to the users of RFID throughout the product life cycle, due to strong encryption.
- ∑ A set-up with multiple keys, allows to control access and data on the tag in a flexible and dynamic manner.
- ∑Privacy by Design: RFIDsec tags are protected against cloning and copying, providing a platform for product authentication and preventing counterfeit products.

FACTS

Following products are available for delivery;

- For immediate delivery RFIDsec offers a Pilot Project set-up, involving a virtual tag and reader environment, allowing end-user application developments and implementation to start instantly.
- A HF (13,56MHz) ASIC with standard ISO 14443-A functionality supplemented with RFIDsec°Øs own RSP (RFIDsec Secure Protocol). The product is offered as IC (for Tag Manufacturers) and as a Smart Label RFID Tag ready to use. RFID tags can be delivered in volumes during 2007
- A series of basic RFIDsec software products, including the Access management application, a product authentication application and others.



Later in 2007 RFIDsec is planning to deliver a similar UHF EPC Gen2 version of its IC.

ABOUT RFIDSEC

RFIDsec°Øs key business objective is to Research, Develop and Implement methods for Smart and Secure use of RFID technology. Our approach is to produce an RFID tag which provides secure management of information throughout the whole product life cycle from time of production to distribution to point-of-sale and beyond.

Our Corporate Mission is to be recognised as the industry leader implementing state-of-the-art solutions developed specifically to be adopted as global industry standard for security in RFID solutions.

The RFIDsec business model has been structured to form a Networked Business organization based on extensive sourcing from best-of-breed partners in R&D, production, sales, and marketing.

PSION TEKLOGIX RUGGED RFID HAND-HELD ONLY ONE TOUGH ENOUGH FOR DOD

Teklogix partners - CDO Technologies, SYS-TEC and WFI Government Services Awarded Blanket Purchase Agreements to provide Psion Teklogix' 7535 EPC-compliant RD7950 Integrated UHF RFID Reader as the sole hand-held reader for U.S. Department of Defense (DoD) agencies

Mississauga, ON – Sept 13, 2005 – Psion Teklogix (LSE: PON), a global provider of solutions for mobile computing, wireless data collection, imaging and RFID, today announced that its rugged EPC-compliant 7535 Hand-Held Computer with RD7950 Integrated UHF RFID Reader has been the only hand-held reader selected for use by the U.S. Department of Defense (DoD), U.S. Coast Guard and several other federal agencies. Psion Teklogix partners CDO Technologies, SYS-TEC and WFI Government Services have each been awarded a Blanket Purchase Agreement (BPA) from the Army Contracting Agency Information Technology, E-Commerce, and Commercial Contracting Center (ITEC4), for passive Radio Frequency Identification (RFID) Electronic Product Code (EPC) -1 for Multi-protocol (Class 0 and 1) Hand-held Readers.

Under the agreement, winners of the Blanket Purchase Agreement can now be selected by the DLA, or any other agency within the Department of Defense or the U.S. Coast Guard, to integrate passive RFID infrastructure within their supply chain. Under the BPAs, each company can sell the Psion Teklogix 7535 RD7950 Integrated UHF RFID Reader, along with accessories and components such as holsters, batteries, and docking stations. The 7535 RD7950 Integrated UHF RFID Reader can read passive UHF EPC Class 0, 0+ and Class 1 tags and will be upgradeable to Gen2 compliance. Further, it can also be equipped to read 1-D and 2-D bar codes as well as take pictures with its robust imaging and laser bar code scanning capabilities.

"Having all three partners win this agreement is a testament to Psion Teklogix expertise in engineering high performance, rugged and flexible RFID hand-held devices that meet a wide range of data capture needs," said Rob Douglas, president, Psion Teklogix Americas. "We are excited to be working with our partners to deliver comprehensive RFID solutions to the Department of Defense. Psion Teklogix will continue to strengthen its expertise in the RFID market and is committed to developing a range of RFID devices that meets the needs of our customers around the world."

A major factor behind the win is the American National Standards Institute's (ANSI) certification of the RD7950 Integrated UHF RFID Reader as non-incendive electrical equipment. Such equipment has been determined to be incapable, under normal operating circumstances, of igniting a flammable airborne gas or dust due to arcing or thermal means. Flexibility was another major factor in the win as the device possesses robust multimedia data capture capabilities comprising of RFID, imaging and laser bar code scanning.

"Psion Teklogix provided CDO Technologies with the award winning RFID hardware, and its team worked seamlessly with ours to perform throughout the demanding award submission process," said Al Wofford, president and CEO, CDO Technologies.

"We are very pleased to be awarded another BPA, this time for hand-held RFID scanners. The fact that Psion Teklogix' devices could operate in

Continue page 12 >>

explosive environments was instrumental in our success," said Steve Roth, president, WFI Government Services, Inc. "RFID solutions are driving the automation of 'hands-free' supply chain management, however there will always be a need for exception-based scanning using hand-held RFID devices. Providing hand-held devices capable of reading tag type including the next generation, Gen 2, will be key in the success of the DoD as it strives to provide mobility to the soldier."

"The ability to leverage Psion Teklogix' vast RFID expertise in conjunction with our own was key in helping us win the BPA agreement for hand-held readers, "said Cyndi Meszaros, contract administrator, SYS-TEC. "We look forward to expanding our relationship with Psion Teklogix in the future."

Psion Teklogix has more than 400 government installations worldwide, and a Government Solutions Group supporting its Department of Defense and Federal Agency customer base. The Psion Teklogix GSA Schedules code is GS-35F-4620G.

ABOUT SYS-TEC

Founded in 1991, SYS-TEC Corporation has been providing commercial, federal, state, and local government agencies with quality state-of-the-art Automated Information Technology (AIT) products and services. SYS-TEC is a full system and solution provider for automated data collection, warehouse management systems, and wireless networking technology. SYS-TEC's range of products and solutions include off-the-shelf applications, bar code equipment, professional services, Radio Frequency Identification (RFID) systems, Real Time Locating Systems (RTLS), asset locating and tracking systems, labeling and media products, and custom software development. SYS-TEC's custom software is currently in use in the industrial, government, healthcare, and logistics industries around the world. SYS-TEC also offers infrastructure installation to include electrical, Cat-5, fiber, networking and wireless networking. For more information visit www.sys-tec.com.

ABOUT CDO TECHNOLOGIES

CDO Technologies is an information technology integrator and provider of RFID-EPC, bar code, and data collection solutions. CDO Technologies offers supply chain solutions that include systems integration, installation, hardware, software, and nationwide technical support. CDO Technologies also provides RFID compliance solutions for DoD and Wal-Mart suppliers. CDO Technologies is a member of AIM North America, the organization for Automatic Identification and Mobility, and a voting member of the following Standards Committees: Part Marking, Unique Identification (UID) Standards, and Radio Frequency Identification. For more information please visit www.cdotech.com.

ABOUT WFI

Headquartered in San Diego, CA, WFI is an independent provider of systems engineering, network services and technical outsourcing for the world's largest wireless carriers, enterprise customers and for government agencies. The company provides the design, deployment, integration, and the overall management of wired and wireless networks which deliver voice and data communication, and which support advanced security systems. WFI has performed work in over 100 countries since its founding in 1994. News and information are available at www.wfinet.com. (code: WFI-mb)

ABOUT PSION TEKLOGIX

Psion Teklogix is a global provider of solutions for mobile computing and wireless data collection. The company's fully integrated mobile computing solutions include rugged hardware; secure wireless networks, robust software, professional services, and exceptional support programs. Psion Teklogix is committed to helping its customers reap the benefits of new and emerging technologies, including image capture and RFID. With over three decades of industry experience, Psion Teklogix has customers in more than 80 countries around the world, and over 36 sales and support offices in 17 countries. Psion Teklogix is headquartered in Mississauga, Ontario, with additional corporate offices in America, Europe and Asia. Psion Teklogix is the operating business of Psion PLC, which is publicly listed in the London Stock Exchange (PON.L). For more information, visit www.psionteklogix.com.

For more information, please contact:
Charmaine D'Silva Psion Teklogix Inc.
905-812-6382 charmaine.dsilva@teklogix.com Cameron Kenalty High Road
Communications 416-368-8348 ext. 233
ckenalty@highroad.com

THE GENTLE TAG: PUTTING RFID INTO A TECHNOLOGY AND SOCIETY CONTEXT

What technologies are most likely to cause explosive change across society? It is not the highly specialized ones, because they will always be limited to their own applications even when they are inherently powerful. Rockets and nuclear power are impressive, but they do not change society significantly. Instead it is the general-purpose technologies that change everything.

The knife, writing, the steam engine, electricity, the personal vehicle and the computer have utterly transformed our world just because they can be applied in an infinite number of ways. Such technologies may start out as solutions to specific problems like calculating mathematical tables, but soon branch out to new applications. The inventors of the electronic computer never intended video games, the Internet, word processing, digital movie special effects and global credit networks.

When I as a futurist mention the next few such technologies I of course mention IT, biotechnology, nanotechnology and cognotechnology. But recently I have started to add identity technology to the list. Identity technology consists of methods of making objects "know" who, what and whose they are, and allowing automated systems to make use of this information. Identity technology is as transformative as the others. Considering how much of human and machine time is spent on identifying it is going to be profoundly important. It is a general technology that can be applied to nearly anything, combined with other technologies and likely to spawn many new and currently unthinkable applications.

RFID tags are a key component of identity technology. While traditional EAN codes, QR codes, pattern recognition, laser fingerprints, biometrics and other systems are also important, RFID promises many benefits of automation and efficiency they would be hard pressed to match. The sheer commercial interest and technological innovation of RFID is also important. When Edison invented the electric light he did not just invent a light bulb, but also the socket, the distribution system and the electricity meter " all pieces of a greater system that made the technology possible, profitable and extendable. The development of standards and infrastructures that go on today will be very important in defining what kind of identity technology we will get.

"Helping RFID and identity technology become a trusted and trustworthy technology in everyday life".

The debate and assumptions surrounding a new technology can shape it for good and ill. It took a single highly publicized accident to doom Zeppelins to a curiosity, while we still suffer railroad accidents from time to time without anybody considering abandoning rail. The framing of genetic engineering in the 1970's in terms of risk and ethical problems has shaped the field and made agricultural biotech a hard sell in many countries. The current integrity concerns of RFID are a similar risk.

Helping RFID and identity technology become a trusted "and trustworthy!" technology in everyday life and across society requires not just listening to consumer and customer concerns and designing away the worst problems. It requires a proactive stance in acknowledging the problems that exist, suggesting solutions and allowing experimentation.

It is clear that enabling reliable and discreet tracking of things and people poses problems. Tracking people may be the greatest concern but even our possessions contain parts of our extended selves. There are also obvious

continue page 14

security concerns as well as potential problems if tags get broken. But the real problems will not be apparent before they occur, just as spam was not predictable when the first email programs were written. This is something we need to acknowledge and get around.

We can construct trust both by designing trustworthy systems and by engaging stakeholders of all kinds in the development process. Some problems can be solved by engineering, like security, blockable tags or how to handle the data. But much is going to be social interactions: do we trust the different stakeholders, their methods and goals? And stakeholders often do not understand what they want or need; supplying exactly what people ask for seldom works. This is why an exploratory process is going to be necessary where solutions are invented, tested and often discarded.

Getting people to discuss the values and visions they have for their technology is very helpful. This may be the biggest lesson from the GMO issue: as long as proponents of a technology do not argue for why it is good and why they are for it, the opponents can always claim that the technology is immoral even if it is useful. Just explaining why tags are used makes people much more comfortable with them, and admitting the dreams driving much development enables more broad and deep discussions about means and ends.

A focus on end user benefits is often helpful. Consumers have nothing against GMO in Europe if they see a lower price or higher nutrient count. Consumers would love RFID tags if they visibly lowered prices or gave their goods useful capabilities.

It is important to develop visible and transparent technology. Having a sense of control and overview is essential to human wellbeing, regardless of whether it is actually exerted or not. There is nothing more frustrating than devices acting (or suspected to act) outside one°Øs control. Hence technology should not be secretive and its activity should be possible to monitor. Tags should have clear owners and defined loyalties. Maybe markup describing the tag system itself a standard feature, so that people can if they wish check out unfamiliar aspects of an objects identity.

Similarly there is a need to give the user a sense of control over the system. This includes the ability to turn off, remove or shield tags, but also the ability to read tags in the vicinity and to write to owned tags.

The best way of achieving trust and a sense of control is to enable experimentation with technology. At present there is a big risk that industry and critics just think of the big applications like supply chains, producing regulations that are based on these assumptions. But general technologies are innovation friendly. Without people playing around with home computers the Internet revolution would not have taken off or been so accepted. To get the maximum benefit we should have a broad base of bottom up experimentation, ranging from RFID hackers to kids to entrepreneurs, and the understanding that we will see many utterly unexpected uses. Regulations ought to not gel too fast, since they might otherwise trap the technology based on the assumptions of an early stage. Young technologies are vulnerable to overregulation. Computers are not just calculating machines, and tags are not just a convenient stock management tool. But if they are treated like that much of their full potential is lost and it becomes hard to innovate.

These kind of broad considerations based on the history of technology, regulation and public risk perception may appear remote from the everyday business of making real systems that work for real customers. But they cannot be imposed top-down as a plan, but should ideally inform the everyday work. Enable tinkering, transparency and engagement locally, and global effects follow.

Contact RFID nordic organisation

ACG Identification Technologies GmbH
Björn Norinder
Storängsvägen 25
115 42 Stockholm
Tel 08 667 25 00
Fax 08 667 25 40
Mobile 070 657 46 49
Email bjoern.norinder@acg-id.com
http://www.acg-id.com

ACSC International
Pether Axelsson
Box 119, 599 23 Ödeshög
Tel 0144 10 000
Fax 0144 100 82
Mobil 0706 42 42 88
Pether.axelsson@acsc.se

ADAGE Solutions
Juha Rajala
Box 10021, 952 27 Kalix
Tel 0923 668 81
Fax 0923 668 88
Juha.rajala@adage.se

ADC Nordic AB
Björn Hellberg
Box 210 01
200 21 Malmö
Tel 040-680 02 80
Fax 040-680 02 81
bjorn.hellberg@adcnordic.com
www.adcnordic.com

samarbete med:
AIM Denmark
Arne Rask, ordförande
ar@logisys.dk

samt
AIM Europe
milagros@aimglobal.org

ARTIMAS/Datema
Johan Malm,
Drottninggatan 69
411 07 Göteborg
Tel 031 65 11 41
070 289 11 41
johan.malm@ise.se

AVISTA TIME
Ulf Gullstedt
Färögatan 33
164 51 Kista
Tel 08 545 705 16
Mobil 070 663 78 00
ulf.gullstedt@avistatime.com

BAUMER IDENT
Baumer Ident AB, Box 134,
561 22 Huskvarna
Tel 036 139441.
Fax 036 139450
erik.arnalid@baumer.se

BEA Systems
Peter Oldeen
Gustav III:s Boulevard 42
SE 169 27 Solna
Mobil 0708 80 92 03
Office 08 522 260 00
Fax 08 522 260 60
Peter.oldeen@bea.com

BIOETT
Scheelevägen 19 A
SE-223 70 Lund, Sweden
Tel 046 286 39 30
Fax 046 286 39 40
olle.hydbom@bioett.com

CAPGEMINI
David Glans
Gustavslundsvägen 131, Box 825
161 24 Bromma
Mobil 0736 737355
david.glans@capgemini.se

CHECKPOINT SYSTEMS SWEDEN
Jan Ehrensvärd
Kanalvägen 18
194 26 Upplands Väsby
Tel: 08 506 566 00
Mobile: 0709 30 82 76
Fax 08 506 566 97
http://www.checkpointeurope.se/
jan.ehrensvard@eur.checkpt.com

CORDURA A/S
Lau Rasmussen
0045 861 37 777
lau.rasmussen@cordura.dk

CUB Systems i Täby AB
Urban Engström
Ella Gårdsvägen 40 B, 187 45 TÄBY
Tel 08 638 88 50
Fax 09 758 39 70
0705 70 90 80
urban.engstrom@cubsystems.se

DISPLAYONLINE Aductor Group AB
Hans Hindersson
Norrbergsgatan 8, 185 32 Vaxholm
Tel/mobil 08 522 04 660
hh@displayonline.se

Electrona-Sievert AB
Gunnar Ivansson
Vretvägen 13 142 34 SKOGÅS
Tel 08 447 31 10
gunnar.ivansson@electrona.se

First Aid Profile
Eric Ericsson
Munktellstorget 2, 633 43 Eskilstuna
Tel 016 17 80 40
Fax 016 17 80 41
Eric.ericsson@firstaidprofile.se

FREE2MOVE
Per-Arne Wiberg
Pilefeltsgatan 77
302 50 Halmstad
Tel 035 15 22 60
Per-arne.wiberg@free2move.se

Föreningssparbanken
Angelika Melchior
015 34 Stockholm
Tel 08 585 900 00
Angelika.melchior@foreningssparbanken.se

Handelsbanken
Henrik Sirborg
Tegeluddsvägen 31 115 82 Stockholm
Mobil 070 - 53 156 34
hesi02@handelsbanken.se

HP
Per Englund
Gustav lll boulevard 36
169 85 SOLNA
per.englund@hp.com

INFINION TEC SWEDEN
Dan.Wallin@infineon.com
Isafjordsg. 16
16440 KISTA
Tel. 08 757 41 03
Mobil. 070 518 3550
Fax: 08 757 4919

INTERMEC
Thorbjörn Sporre
Vendevägen 85 A
182 91 Danderyd
Tel 08 622 06 63
Mobil 0708 16 03 55
thorbjorn.sporre@intermec.com

ISE DATA AB (Datema koncernen)
SolnaStrandväg 98
Mobil: 0708 89 74 85
Tel 08 517 150 80 (00 vx)
Fax 08 28 77 05
joakim.dahlberg@ise.se

IT universitetet
Peter Öst
Rindögatan 17, 8 tr.
11536 Stockholm
www.it2ospe@ituniv.se

KIWOK
Björn Söderberg
Norrlandsgatan 22
111 43 Stockholm
Tel 08 679 82 00
Fax 08 679 82 10
Mobil 073 805 09 00
Bjorn.soderberg@kiwok.com

LARBERG CONSULT
Rolf Larberg
Rolf.larberg@telia.com

LOGOPAK SYSTEMS AB
Lilla Bommen 1
SE-411 04 Göteborg
tel: (0) 31 - 700 12 30
mobile: (0) 709 - 67 84 70
fax: (0) 31 - 15 12 01
mail: LThuring@Logopak.se
web: www.logopak.se

LXE Scandinavia
Carin Andersson
Sjöflygvägen 35A
S-183 62 Täby
Sweden
Tel 08 544 445 50
Fax 08 544 445 55
c@lxe.com

MECTEC Elektronik AB
Joachim Holgersson
Agnesfridsvägen 189
S-213 75 Malmö
Tel 040 689 25 01 (Direct)
Mobil 070 354 75 01 (Mobile)
Växel 040 689 25 00 (Switchboard)
Fax 040 689 25 25 (Fax)
joachim.holgersson@mectec.se
http://www.mectec.se

MENTOR ONLINE
Lars Nordmark
Tel 042 490 19 17
Fax 042 490 19 99
Mobil 0709 75 99 42
www.mentoronline.se

MODULSYSTEM
Torbjörn Henryson
Tel 08 506 30 115
Torbjorn.henryson@modulsystem.se

MOWISE
Lavendelvägen 5, 192 54 Sollentuna
Tel 08 96 53 87
Mobil 070 662 88 81
Gunnar.widen@mowise.com

NORD-EMBALLAGE
Bo Wallteg
Bankvägen 30
262 70 Stöveltorp
Tel 042/207166
Mobil 0703/207163
Mail: bo.wallteg@n-e.nu

POSTEN Sverige AB
105 00 Stockholm
Tel 08 781 21 15
Fax 08 20 58 80
Tor.Wallin@posten.se

RBS Retail Business System AB
Christer Andersson
Roslagsgatan 6
761 23 Norrtälje
Tel 0176-745 22
Mobil 070 606 33 51
Mail: Christer.andersson@rbs.se

PSION TEXLOGIX
Håkan Nyström
Hammarby Fabriksväg 23
120 33 Stockholm
Tel 08 452 88 80
Hakan.nystrom@teklogix.se

RBS AB
Christer Andersson
Box 274
S-761 23 Norrtälje
Besökadress: Roslagsgatan 6-8
Tel 0176 - 745 00
Direkt: 0176 - 745 22
christer.andersson@rbs.se

I samarbete med:
RFID Society
www.rfidsociety.com

I samarbete med:
RFID Business Association
www.rfidba.org

RFID Constructors
Niklas Hild
Box 14
275 21 Sjöbo
Tel 0416 252 00
Fax 0416 252 80
Mobile 0709 98 13 70
Mail/Skype
niklas.hild@rfidconstructors.com
http://www.rfidconstructors.com

RFIG/PLEFO
Lucas Åhlström
Narvavägen 3
114 60 Stockholm
Tel 08 667 4020
Mobil 070 182 15 00
Mail: lucas@rfig.se

SAP
Magnus Norrman
Box 12297
Gustavslundsvägen 151 D 102 27
Stockholm
Tel 08-587 700 00
Dir 08-587 700 29
Fax 08-587 700 01
Mobil 070-346 19 73
magnus.norrman@sap.com

SCHENKER CONSULTING
Gunnar Schrewelius
Box 8013
163 08 Spånga
08 585 10 832
070 624 83 66
Gunnar.Schrewelius@schenker.com

Continue page 14 >>

SMARTICWARE
Österögatan 1-3, 164 40 KISTA
Omid Aval
Tel 08 750 7660
070 3502389
omid.aval @smarticware.com

SIEMENS AB,
Röntgenvägen 2, SE-171 95 Solna
Tel 08-728 10 00
Direct 08-728 14 30
Mobile073-620 65 30
Maria.lidberg@siemens.com

SOGETI
Hoss Eizaad
Gustavslundsvägen 131
Box 825 161 24 BROMMA
Tel 08 536 820 07
070 922 99 77
hoss.eizad@sogeti.se

SUN Microsystems
Leif Nordlund
Box 51 164 94 KISTA
Tel 08 631 13 00
Leif.nordlund@sun.com

SVENSK HANDEL
Bo Svensson
103 29 Stockholm
Tel 08 762 78 28
bo.svensson@svenskhandel.se

TAGMASTER
Magnus Rehn
Kronborgsgränd 1
164 87 Kista
Tel 8 632 19 50
magnus.rehn@tagmaster.se

TREATY Ltd
Lars-Åke Wernersson
Finlandsgatan 60
SE 164 74 Kista
Tel 08 47 47 301
Fax08 47 47 310
Lars.wernersson@trety.com

TeliaSonera
Alf Johnson
Augustendalsvägen 7
SE 131 86 Nacka Strand
Mobil 070 680 4101
Tel 08 601 8609
alf.johnson@teliasonera.com

TRACTECHNOLOGY
Henrik Österlund
Wenner-Gren Center, 19tr
Sveavägen 166, 113 46 Stockholm
Tel: 08-556 934 03
Fax: 08-556 934 19
Mobil 0707-333 678
henrik.osterlund@tractechnology.se

WTEK AS
Skarpengland
4715 Øvrebø, Norge
Tlf: +38 13 91 53
Fax: +38 13 96 91.
ole@wtek.no

XPONCARD
Eva Maria Matell
Hornsgatan 103 117 28 Stockholm
Tel 08 658 75 10
Mobil 073 684 47 18
Evamaria.matell@xponcard.se

ÅF-PROCESS AB
Greger Du Rietz
Kvarnbergsgatan 2 |
Box 1551, 401 51 GÖTEBORG
Tel 031-743 10 84 | Mobil: 0730 70 10 84
Fax: 031-743 10 10
greger.durietz@afconsult.com

IF YOU WANT TO FOLLOW THE EXITING DEVELOPMENT JUST WATCH WWW.RFIDNORDIC.SE AND GIVE YOUR OWN COMMENTS.

If you want to be a member of the RFID Nordig organisation just give us a call on +46 8 662 31 95
Welcome